

Imagination der Cybersicherheit
IT-Sicherheitskultur – Deutschland und die Niederlande

Inaugural-Dissertation
zur Erlangung der Doktorwürde
der
Philosophischen Fakultät
der
Rheinischen Friedrich-Wilhelms-Universität
zu Bonn

vorgelegt von

Maximilian Berndt

aus

Geilenkirchen

Bonn 2026

Gedruckt mit der Genehmigung der Philosophischen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

Zusammensetzung der Prüfungskommission:

Prof. Dr. Britta Hartmann, Institut für Sprach-, Medien- und Musikwissenschaft
(Vorsitzende)

Prof. Dr. Jens Schröter, Institut für Sprach-, Medien- und Musikwissenschaft
(Betreuer und Gutachter)

PD Dr. Christoph Ernst, Institut für Sprach-, Medien- und Musikwissenschaft
(Gutachter)

Prof. Dr. Adrian Hermann, FIW – Forum Internationale Wissenschaft Bonn
(weiteres prüfungsberechtigtes Mitglied)

Tag der mündlichen Prüfung: 10.12.2025

Inhalt

I. Einführende Worte.....	1
I.I. Grundlegende Herausforderungen der Cybersicherheit.....	4
I.II. Asymmetrische Entgleisung.....	15
II. Forschungsfrage und Ziel.....	19
III. Operationalisierung.....	23
III.I. Risiko des Diskurses – Diskurse über das Risiko.....	27
III.II. Transkulturell vergleichen.....	37
III.II.I. Beobachtungsebene.....	41
III.II.II. Kriterien des Vergleichs.....	47
III.II.III. Added Values des Sicherheitskulturkonzeptes.....	49
1. Quid est Cybersicherheitskultur?.....	59
1.1. Definition der Chimäre Sicherheit.....	62
1.2. Kultur und Institution.....	68
1.3. I'majə, nerē.....	79
1.4. Exegese des Begriffs <i>Sicherheitskultur</i>	88
1.4.1 Der Staat als Garant für Sicherheit?.....	92
1.4.2 Institutionalisierung von Sicherheitskultur.....	96
1.5. Sicherheitskultur trifft auf Informationstechnik: ein Spannungsfeld.....	106
1.5.1 Medium <i>IT-Sicherheitskultur</i> in den Medien.....	114
2 Wie organisieren die Vergleichsländer IT-Sicherheit?.....	127
2.1 Querschnitt: Deutschland zwischen 1945 und 2022.....	127
2.2 Deutschland heute.....	134
2.2.1 Staatsprinzip: Föderale Republik.....	136
2.2.2 Internationale Rolle in Europa und der Welt.....	142
2.3 Wie ordnet sich Cybersicherheit in Deutschland?.....	144
2.3.1 Staatliche Institutionen des Bundes.....	146
2.3.2 Institutionen der Gesellschaft.....	159
2.3.3 IT-Sicherheitsgesetz.....	171
2.3.4 Die Lage der IT-Sicherheit in Deutschland 2019–2021.....	179
2.3.5 Cybersicherheitsstrategie für Deutschland 2021.....	196
2.3.6 IT-Investitionen des Bundes.....	208
2.4 Querschnitt: Niederlande zwischen 1910 und 2022.....	214
2.5 Niederlande heute.....	224
2.5.1 Staatsprinzip: Dezentraler Einheitsstaat.....	229

2.5.2 Internationale Rolle in Europa und der Welt.....	233
2.6 Wie ordnet sich Cybersicherheit in den Niederlanden?.....	238
2.6.1 Staatliche Institutionen.....	239
2.6.2 Institutionen der Gesellschaft.....	250
2.6.3 Wet beveiliging netwerk- en informatiesystemen (Wbni) & Computercriminaliteit III.....	266
2.6.4 Cybersecuritybeeld Nederland 2019–2021.....	279
2.6.5 Nederlandse Cybersecurity Agenda & Nationale Cybersecurity Strategie.....	292
2.6.6 IT-Investitionen.....	304
2.7 Zwischenbilanz – Systeme in den Niederlanden & Deutschland.....	310
3 Cybersicherheitskultur in der Praxis.....	325
3.1 Fallstudie 1: Die Schadsoftware Emotet.....	326
3.2 Fallstudie 2: Einführung des 5G-Mobilfunkstandards.....	337
3.3 Fallstudie 3: BSI und NCSC inszenieren Cybersicherheit.....	350
IV. Conclusio.....	371
IV.I. Evaluation des Forschungsdesigns.....	382
IV.II. Kritische Auseinandersetzung.....	385
IV.III. Ausblick.....	387
Dank.....	389
Hilfsmittel.....	390
Literatur.....	I
Quellen.....	XIII
Onlinequellen.....	XVIII
Videografie.....	XL

I. Einführende Worte

Zum Themenkomplex der Cybersecurity existieren umfassende Abhandlungen auf den Gebieten der Informatik, der Mathematik, der Politik und der Psychologie. Zudem veröffentlichen mit dem Ressort betraute Behörden regelmäßig Berichte, die ebenfalls von zentraler Bedeutung für diese Dissertation sind. Als medienwissenschaftliches oder soziologisches Motiv hingegen ist die Cybersicherheit, geschweige die Untersuchung von Cybersicherheitskultur, bisher seltener zu finden. Kommen Digitaltechnik und Gesellschaft bislang in der Forschung zusammen, steht häufig das Gleichgewicht von Sicherheit und persönlicher Freiheit im Zuge der anhaltenden Überwachungsdiskussionen im Mittelpunkt der Aufmerksamkeit. Cybersicherheitskultur umfasst aber viel mehr: Sie beschreibt eine unübersichtliche Gemengelage, unter anderem aus Handlungsempfehlungen, beschleunigender Technologie oder auch Debatten über den Umgang mit den stets transformierenden Herausforderungen. Vor dem Hintergrund meiner Beschäftigung für das Bundesamt für Sicherheit in der Informationstechnik stehe ich regelmäßig vor der Frage, wie es sein kann, dass auf den ersten Blick eng verwandte Länder und Kulturen den Problemstellungen der Digitalisierung strategisch und strukturell anders begegnen als Deutschland. Daraus speist sich die Motivation, verstehen zu wollen, warum Cybersicherheit diverse Ausprägungen annehmen kann, obwohl die Voraussetzungen nahezu gleich zu sein scheinen. So kann der institutionalisierte Umgang mit den Unwägbarkeiten der Informationssicherheit zweier Gesellschaften, sprich die maßgeblichen Akteure, Administrationen, Vorschriften und Vereine, in zahlreichen Aspekten divergieren. Deshalb versuche ich mich unter anderem daran, „Handlungsziele zu systematisieren und die individuelle wie auch situative Variabilität solcher Zielorientierungen zu untersuchen“ (Otte 2018, 85). Zudem soll der hier angelegte, komparative Ansatz, der bislang nicht oder lediglich in abweichenden Bezugssystemen zur Anwendung gekommen ist, die individuellen Eigenheiten der Vergleichsobjekte offenlegen. Im Bewusstsein, dass Kultur kaum in Gänze zu umreißen ist, stellt diese Arbeit den Versuch dar, einen Anstoß zu geben, damit die regional, biografisch oder ökonomisch unterschiedlichen Anforderungen wie auch Charakteristika künftig vermehrt Einzug in die Betrachtung nationaler IT-Sicherheitsdebatten halten.

Um dies zu erreichen, wird in der nachstehenden Abhandlung der Vergleich mit der Cybersecurity Culture eines europäischen Nachbarn bemüht. Dabei handelt es sich um ein Land, das Laien im Zusammenhang mit Informationstechnik wenig bekannt sein dürfte – die Niederlande. Der westeuropäische Nachbarstaat drängt sich mit diesen spezifischen Eigenschaften als Reflexion der deutschen Security Culture nahezu auf: Einerseits halten die Niederländer an ihrer konstitutionellen Monarchie fest, andererseits gelten Niederländer als besonders liberal, dynamisch und modern (vgl. Kennedy 2017, 373). Der kleine Staat an der Nordsee besitzt bislang keinen nennenswerten sicherheitspolitischen Rang und ist zugleich bedeutender Akteur auf der Bühne der EU, beispielsweise 2020 als die Niederlande mit nur wenigen Unterstützern lange Zeit den postpandemischen Wiederaufbauplan blockierten (vgl. Handelsblatt 2020a). Die Ökonomie der Niederlande ist eindeutig auf Dienstleistung und Innovation ausgerichtet, deren Wachstumsfaktoren unter anderem in neuen Technologien, intelligenten Systemen und Kommunikationsdienstleistungen liegen (vgl. Centraal Bureau voor de Statistiek (CBS) 2020). So kommt es, dass der Dienstleistungssektor etwa 78 % des Bruttoinlandsproduktes erwirtschaftet (vgl. Deutsch-Niederländische Handelskammer (DNHK) 2019). Als flächig und demografisch kleines Land bietet eine derartige Wirtschaftsstruktur Dynamik und Agilität. Entsprechend kann das Interesse der Niederlande an Progression und einer profitablen Teilhabe an der Digitalisierung nur groß sein. Zusätzlich hilft die einheitsstaatliche Organisation, schnell handlungsfähig zu sein. Insgesamt scheinen diese Attribute vermeintlich förderlich für eine angemessene Cybersicherheitsimplementierung zu sein und werfen die Frage auf, ob Cybersicherheit in den Niederlanden eine Gelegenheit zur ökonomischen Entwicklung darstellt und mit der Chancenerwartungen verknüpft ist oder ob sie als notwendiges Übel zum Erhalt des Bestehenden angegangen wird.

Dem gegenüber steht Deutschland als föderalistisch geprägte Bundesrepublik mit moralischem wie finanziellem Führungsanspruch innerhalb der Europäischen Union. Die Bundesrepublik ist zudem das einwohnerstärkste Land des Kontinents. Aus seiner Historie als Technologiestandort zeichnet sich die deutsche Wirtschaft, wenn auch abnehmend, durch die Maschinenbau-, Automobil- und Chemieindustrie aus. Diese Zweige waren zwar über Jahrzehnte Garanten für Wohlstand und Wachstum, zählen aber heute zu den schwerfälligen und wenig anpassungsfähigen Bestandteilen der

nationalen Ökonomie. Hinzu kommt der als enorm geltende deutsche Verwaltungsapparat, der nicht unwesentlich im bundesstaatlichen Zusammenschluss teilsouveräner Länder begründet liegt. Die Bedürfnisse von 16 Bundesländern mit teils großen regionalen Differenzen zusammenzubringen, steht schlagkräftigen Entscheidungsprozessen häufig im Weg. Wenngleich im späteren Verlauf deutlicher wird, wie unterschiedlich und dennoch nah verwandt die Niederlande und Deutschland in vielerlei Hinsicht sind, liegt in genau solchen Widersprüchen das akademische Interesse begründet.

Dieser kurze Auszug deutet an, wie komplex die Untersuchung Deutschlands und der Niederlande unter Berücksichtigung ihrer heterogenen Cybersicherheitskulturen ist. Und wie Endreß und Feißt bereits erkannt haben, „ist die hinter der Sicherheitskultur stehende Praxis die der Kulturreflexion. Abstrakt formuliert versteht sich Kulturreflexion als eine diskursive Praxis, als Befragung verschiedenster Disziplinen, Autoren, Medien, Erfahrungen“ (Endreß/Feißt 2014, 23). Deshalb ist es mein Antrieb, sich den Kulturen der Cybersicherheit durch die Reflexion ebendieser unterschiedlichen Disziplinen, Autoren, Medien und Erfahrungen anzunähern. Im Resultat soll stringent dargelegt sein, dass die Institutionalisierung von und die Kommunikation über Cybersicherheit in beiden Ländern so divergieren, dass sich verschiedenartige IT-Sicherheitskulturen ausbildeten.

I.I. Grundlegende Herausforderungen der Cybersicherheit

Was beide Nationen eint, sind die Herausforderungen, vor denen sie stehen. Denn damit IT-Sicherheit in irgendeiner Form zu einem Gut kultureller Relevanz werden kann, muss es diskutiert und bearbeitet werden, aber vor allem in die Alltagsnormalität der Menschen Einzug halten. Jedoch lassen sich Hemmnisse identifizieren, die dabei helfen, die unterschiedlichen Ausprägungen im Umgang mit Cybersecurity zu rekonstruieren.

Mithin mangelt es schon an Grundlegendem, denn die Vulnerabilität von Informationstechnik ist bei Weitem nicht jedem Anwender¹ bekannt. So ermittelte das in Deutschland mit dem Schutz dieser Infrastruktur betraute Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) in einer repräsentativen Befragung aus den Jahren 2019 und 2020, dass sich 15 % (2020) der Befragten anlassunabhängig über IT-Sicherheit informieren; das Gros der Teilnehmer sucht hingegen nur im Ernstfall nach Hilfestellungen. In diesen Umfragen stellte sich zudem heraus, dass sich zwar 82 % (2019) nach eigenen Angaben Sorgen um ihre Sicherheit im Internet machten, jedoch lediglich 61 % (2019) Antivirenprogramme verwendeten, nur 36 % (2019) installierten Hersteller-Updates. eco, der Verband der Internetwirtschaft e. V., veröffentlichte ebenfalls 2019 eine Untersuchung, nach der nur 41 % der befragten Unternehmen regelmäßige IT-Sicherheitsschulungen für ihre Mitarbeiter anboten. Allein 57 % hatten zu diesem Zeitpunkt einen Notfallplan für einen Cyberangriff auf die Firmenstrukturen ausgearbeitet (vgl. eco – Verband der Internetwirtschaft e. V. 2019).

Die Zahlen deuten zwar im Vergleich mit den Vorjahren ein wachsendes Bewusstsein für Problemstellungen der Informationstechnik an, legen aber auch offen, dass ein Gespür für mögliche Risiken aus dem Internet bei einer signifikanten Menge der deutschen Bevölkerung nach wie vor ausbleibt. Privatanwender haben den Schutz sensibler Daten bisher nicht dem Schutz des eigenen Hauses gleichgestellt, obwohl vergangene Aufklärungsarbeit dieses Bild häufig bemüht hat. Zudem haben professionelle Entscheider bislang nicht in allen Fällen die Sicherheit relevanter Systeme als Unternehmensressource für Stabilität und Vorsprung entdeckt.

¹ Zur besseren Lesbarkeit findet in dieser Dissertation das generische Maskulinum Anwendung. Die Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Das führt unweigerlich zu der Frage, warum noch kein intrinsisches Interesse eines jeden Einzelnen besteht, die individuellen Schutzmaßnahmen auf ein zweckmäßiges Niveau anzuheben? Andy Oram und John Viega erläutern den augenscheinlichen Berg des Sisyphos wie folgt: „Books on hacking into systems sell much better than books about how to protect systems [...]“ (Oram/Viega 2009, Xii). Oram und Viega spannen damit den Bogen zur grundlegenden Annahme von Filmen, Büchern und Videospielen, dass das Dunkle, Verborgene und mitunter Böse eine größere Anziehungskraft entwickelt als das vermeintlich Gute. Der sonntägliche Tatort erzählt von Mord und Vergewaltigung, während in Videospielen wie Days Gone Horden von Untoten nur darauf warten, niedergemetzelt zu werden. Der geschützte Raum, in dem Kriminalität simuliert und Verbotenes schadlos erlebt wird, scheint deutlich attraktiver zu sein als die Erzählung von Wirklichkeiten ohne antizipierbare, gegenständliche Bedrohung. Wer kennt schon jemanden, der sein finanzielles oder soziales Wohl tatsächlich ernsthaft bedroht sah, weil er einem Internetkriminellen zum Opfer gefallen ist? Die Bedrohungslage erscheint vage und fern, ist gleichzeitig aber konkret und präsent. „Der Feind hat kein Gesicht mehr, nicht, weil er ‚gesichtslos‘ geworden ist, sondern weil er eine Gestalt annimmt, die keinen Kopf mehr hat“ (Horn 2007, 479). Eva Horn meint mit dieser Aussage zwar sich gegenüberstehende Nachrichtendienste, skizziert aber damit zugleich auch eine Expression gegenwärtiger Internetkriminalität. Ohne greifbare Vereinigungen oder legitimierende Staaten agieren die sogenannten Black Hats, also Hacker mit illegalen Absichten, auch ohne manifeste Flagge oder Uniform und taugen daher nicht zum separierbaren Feindbild. Gegen wen sollen Anwender sich verteidigen? Welche Motive hat die Gegenseite? Auf diese Fragen können Sicherheitsexperten keine einfachen und deckungsgleichen Antworten geben. Somit überfordert die Komplexität der vorhandenen Problemstellung die nicht in Informatik oder Mathematik ausgebildete Öffentlichkeit derart, dass der katalysierende Schwellwert nie erreicht wird, dessen Überschreitung so lange Ablehnung und Wut befeuert, bis sich das reproduzierbare Porträt eines Antagonisten etabliert.

Ohne Vorstellungen von den möglichen Folgen, die ein IT-Vorfall hervorrufen kann und ohne Skizze eines Feindes kehrt sich die obige Frage nach der intrinsischen Motivation um und man ist stattdessen geneigt zu fragen, warum Anwender dann Zeit und Mühe in die Abwehr dieser abstrakten Gefahr investieren sollten? Dem ist mit einem ganzen Arsenal rational einleuchtender Erklärungen zu begegnen, die jedoch in Ermangelung

ausdrucksstarker, evidenter Exempel zuweilen nicht in nachhaltig revidierte Anschauungen überführt werden konnten. Dabei gibt es genügend gängige Begründungen, die auf diese Frage erwidert werden: der Schutz der Privatsphäre, die Vermeidung von Finanzbetrug oder das Verhindern von Gerätedefekten – allesamt unangenehme Tatsachen, jedoch nicht existenziell bedrohlich. Bereits die grundsätzliche Erzählung von Informationstechnik, ihren mutmaßlichen Auswirkungen und den möglichen Schadensfällen tritt gemäßigt auf und reflektiert nicht das tatsächliche Potenzial für Tragödien, das in der unzureichend gesicherten Vernetzung von Computersystemen steckt. Dieser nachlässigen Einschätzung steht der stetig zunehmende Komfort zur Seite, den Technologie und Konnektivität schaffen. Solch positive Assoziation

verführt dazu, alle elektronischen Geräte in das Internet einzuspeisen. Zusätzlich sorgen die erhöhten Erwartungen und der damit verbundene Druck für eine Sehnsucht nach technologischen Erleichterungen und Hilfestellungen, die in der Anschaffung wieder neuer Technologien münden. Dieser Konsum von internetfähiger Elektronik beflügelt Versuche, in noch größerem Maßstab Daten zu zentralisieren (Berndt 2017, 34).

Zeitgenössische Hochtechnologie verspricht Bequemlichkeit, Geschwindigkeit und Teilhabe. Diese Versprechen lassen sich jedoch nur in Aussicht stellen, indem Daten in großen Mengen akkumuliert und analysiert werden. An genau diesen Knotenpunkten, den Servern und Rechenzentren globaler Tech-Unternehmen, sind Informationsdiebstähle dann besonders lukrativ.

An dieser Stelle schimmert ein Paradoxon durch: Schon die Kleinsten werden mit strengster Eindringlichkeit darauf geschult, die Haustür abzuschließen und auf Wertgegenstände Acht zu geben. Im Digitalraum, zugegeben, einem Raum, der erst seit wenigen Generationen besteht, werden diese Werte hingegen nicht mit der gleichen Selbstverständlichkeit weitergetragen und manifestiert. Im Gegensatz zu den Folgen eines Raubs oder einer Gewalttat sind die Konsequenzen einer Cyberattacke oft viel subtiler und bleiben unsichtbar. Wenn die Heizungssteuerung beispielsweise in ein Botnetz integriert wird, sind gewöhnliche Benutzer nicht in der Lage, diesen stetigen Fernzugriff oder auch nur die Infektion des Netzwerks zu detektieren. Zusätzlich hat ein solches Botnetz nicht unbedingt spürbar negative Auswirkungen für den Betroffenen, seine unzureichend geschützten Geräte unterstützen ab diesem Zeitpunkt aber strafbare Handlungen, die wiederum nützlich sind, um kriminelle Strukturen zu finanzieren. Beispiele dieser Art könnten hier vielzählig aufgeführt werden und demonstrieren, dass

die Verheißung von Informationstechnik einerseits und die angenommene Mittelbarkeit der Bedrohungen andererseits durchaus zu einer gewissen Leichtfertigkeit verführen.

Die Sensibilisierungsarbeit für Themen des IT-Schutzes würde dort enden, wo es gelungen ist, diese Sorglosigkeit in allgemein anerkannte Relevanz zu verkehren. Zurzeit indessen leidet die Prävention digitaler Vorfälle unter vielseitigen Widrigkeiten, die nachfolgend anhand sieben wesentlicher Ursachen zusammengefasst werden:

1) Die genannte Leichtfertigkeit beziehungsweise die Absenz weitreichend bekannter und im kollektiven Gedächtnis verankerter Desaster sind Gründe, weshalb ein Antrieb fehlt – ein Impuls, der zur permanenten Sicherung aller betriebenen IT-Systeme führen würde. Die Zahlen des Digitalbarometers und anderer Studien lassen den Schluss zu, dass Anwender mehrheitlich erst handeln, wenn Einschränkungen der Benutzbarkeit des jeweiligen Geräts ans Licht treten. Bleiben Bankkonto, Instagram-Account und Funktion des Smartphones unberührt, fällt eine Infektion oftmals nicht einmal auf. So sind Kriminelle im Darknet in der Lage, Rechner nichts ahnender Menschen als Server für illegale Angebotsplattformen zu missbrauchen oder Downloads von Raubkopien über Fremdrechner zu leiten (vgl. Schrödel 2014, 100). Diese Schäden betreffen die Anwender oft gar nicht oder nur auf Umwegen. Sie werden vielmehr unwissentlich zu Werkzeugen der Täter. Ferdinand Grapperhaus, niederländischer Minister für Justiz und Sicherheit im dritten Rutte-Kabinett, diagnostizierte diese Unbedarftheit als Grundübel:

Mensen gedragen zich online minder veilig dan ze denken en schatten de kans dat ze schade ondervinden van online risico's laag in. Bij veel succesvolle cyberaanvallen zijn onvoldoende basismaatregelen voor digitale weerbaarheid getroffen² (Officielebekendmakingen 2021).

Die als Folge schlechter Passwörter oder nicht durchgeführter Updates erforderliche Detektion und Beseitigung von Schäden – sei sie nun unmittelbar oder nur indirekt für den Anwender spürbar – verlangt dann obendrein mindestens basale Kenntnisse und ein gewisses Engagement. Ähnlich verhält es sich mit Maßnahmen, die eine Infektion im Vorfeld abwehren sollen: Präventive Sicherungsinstrumente verlangen zusätzliche Arbeit, indem Passwort-Manager eingerichtet, Back-ups erstellt, Geräte aktualisiert und die dazu besten Hilfsprogramme ausgewählt werden müssen. Nach wie vor gestaltet sich die Konservierung und Verwaltung von Zahlen, Größen, Werten und Buchstaben

² Deutsch: Menschen verhalten sich im Internet unsicherer als sie denken und schätzen das Risiko, dass sie durch Online-Bedrohungen Schaden nehmen, als gering ein. Bei vielen erfolgreichen Cyberangriffen wurden nur unzureichende Basismaßnahmen zur digitalen Abwehr ergriffen.

auf Digitalsystemen aufwendig und erfordert ein Wissen, das in einigen Fällen bis zur Expertise reichen muss. Das bedeutet, dass gewöhnliche Endanwender Hochleistungscomputer und -smartphones erwerben und a priori mit den verbundenen Herausforderungen weitestgehend allein zurechtkommen müssen.

2) Dennoch verfolgen Hersteller von Soft- und Hardware fortwährend nicht das Prinzip des Security-by-Design. In diesem Konstruktionsprinzip implementiert der Produzent schon bei der Planung des Geräts oder Programms die entsprechenden Sicherheitsspezifikationen. So wären zumindest die vertreibenden Unternehmen in der Lage, Sicherheit so zu integrieren, dass diese die Endanwender nicht belasten. Die Verantwortung verlagert sich demnach bei diesem Ansatz, wenn auch nur zum Teil, vom Anwender auf den Produzenten. Derartig ausgearbeitete Geräte erweisen sich als sicherer, da in ihnen bereits verwurzelt ist, dass sie beispielsweise nur per VPN-Verbindung kommunizieren, gewisse Aktionen blockieren oder rekursive Back-ups erstellen. Solche Technologie zeigt sich zudem tolerant gegenüber Fehlern, funktioniert also weiterhin robust, wenn nicht nur „menschliche Misserfolge, sondern auch technische Ausfälle“ auftreten (Kaufhold/Reuter 2018, 33). Gegenwärtig stülpt man Sicherheitstechnologien hingegen nachträglich über Entwicklungen und adaptiert sie. Dies führt dazu, dass im Laufe der Zeit an den Schnittstellen zwischen Security Tool und System kontinuierlich überwindbare Schwachstellen aufbrechen, deren Entstehung nahezu unvermeidlich ist. Erschwerend kommt hinzu, dass Nutzer bei solch nachträglich installierten Mechanismen eine *shadow security* entwickeln. Das bedeutet, sie erarbeiten Arbeitsabläufe, die die Sicherheitsmechanismen umgehen, weil die vorgesehenen Prozesse zu umständlich oder unhandlich sind (vgl. European Union Agency for Network and Information Security (ENISA) 2018, 24).

Bereits in den 40er-Jahren des vergangenen Jahrhunderts erkannten Max Horkheimer und Theodor W. Adorno zudem, dass die schiere Größe der Kulturindustrie es verlangt, dass „gleiche Bedürfnisse mit Standardgütern beliefert werden“ (Adorno/Horkheimer 2019, 129). Dies wiederum trägt bereits die Konklusion in sich, dass sich Konstruktionsfehler oder Versäumnisse aus Fahrlässigkeit, wenn nicht ökonomischem Kalkül, über millionenfache Chargen hinweg ebenso reproduzieren. In der technologisierten Gegenwart führen solche Fehler oftmals nicht mehr zu Materialermüdungen, sondern sie werden sichtbar, wenn einfallsreiche Spezialisten die Konstruktionsmängel internetfähiger Geräte entdecken und die daraus ableitenden

Optionen für sich nutzen. Dies kann heißen, dass sie die Schwachstelle melden und so dazu beitragen, sie zu schließen und damit den restlichen Anwendern zu helfen. Häufig bedeutet es jedoch, dass weniger integre Personen Nutzen aus global kopierten Fehlern ziehen und die Straftat bei so vielen Geräten wie möglich imitieren wollen – solange bis der Hersteller reliable Instrumente zur Abwehr bereitstellt.

Die ursächliche Intention der Produzenten von Informationstechnik liegt, wie bei jedem ökonomisch agierenden Organ, in der Maximierung des Umsatzes bei gleichzeitiger Minimierung der Kosten. Cybersicherheit, das kann kaum bestritten werden, gehört heute noch zu den Entwicklungsbelastungen eines Produktes statt zu den angesagten Features. Demzufolge steht die Absicherung von technischen Erzeugnissen augenscheinlich oft im Widerspruch mit anderen Unternehmenszielen konservativer Unternehmensstrategien, wie der Produktivität (vgl. European Union Agency for Network and Information Security (ENISA) 2018, 10). Unternehmerische Ressourcen, die IT-Sicherheit herstellen, gelten als Kräfte, die an anderer Stelle fehlen (vgl. Strohschneider 2010, 166f). Dabei liegt es nahe, Cybersecurity gelegentlich anders zu betrachten und als nur selten besetzte Nische zu begreifen. Ein bekanntes Beispiel für ein Unternehmen, das ebendiesen Ansatz verfolgt, ist der kalifornische Technikkonzern Apple. Ohne eine Bewertung ihrer tatsächlichen Implementierung von Sicherheitsvorkehrungen anzulegen, ist festzustellen, dass die offensiven Kampagnen und die über Jahre verfolgte Strategie der Markenbildung damit spielen, dass Apple-Produkte sicherer seien als Produkte der Konkurrenz. Mit Werbeslogans wie „Wir nehmen den Schutz deiner Daten ernst“ oder „We believe privacy is a fundamental human right. This is one of our core principles at Apple. It’s why we design iPhone from the ground up to keep your personal information private and secure. And it’s one of the things that sets iPhone apart“ spricht das Unternehmen den Schutz von Daten und Privatsphäre an (Apple 2020a/2020b). Damit erzeugt Apple einen mindestens kommunikativen Vorsprung auf einem Gebiet, auf dem der öffentliche Wettlauf bislang nicht mal angefangen hat. Sicherheit bei Auslieferung ist immer noch erkennbar ein Spezifikum, eine Extravaganz, auf die in Abgrenzung zu übrigen Akteuren aufmerksam gemacht werden kann. Dies legt offen, dass ein Umbruch zu von Grund auf abgesicherter Technologie bis jetzt nicht vollzogen ist. Denn sobald Eigenschaften den Zustand der Inhärenz und der Selbstverständlichkeit erreicht haben, werden sie in der Regel trivial und nicht bewerbenswert. Während Fernsehgeräte beispielsweise zu

Beginn der 2010er-Jahre offensiv beworben wurden, weil sie seitdem eine Internetkonnektivität aufwiesen, gelten Geräte ohne eine Anbindung mittlerweile als unverkäuflich. Das Smart-Sein geriet immer mehr zu einer nicht weiter erwähnenswerten Grundannahme beim Kauf eines Fernsehers. Ein ähnlicher Wandel, nun zum Sicher-Sein, scheint jetzt nötig, um zu einer internalisierten Betrachtung von IT-Produkten als selbstverständlich sichere und zuverlässige Erzeugnisse zu gelangen.

Wie Friedrich Kittler in seiner Charakterisierung des *Protected Mode*³ darlegt, sind Computertechnologien als Systeme der Macht aufzufassen. Die Geräte sind eigenständig in der Lage, Programmen und Anwendern Zugriffsrechte zu verweigern, Privilegien zu erteilen oder zu entziehen, und die Rechenkapazität umzuverteilen (vgl. Kittler 1993, 213f). Kittler sieht hier einen Umbruch, seitdem der Computer den Bedienenden unter dem Mantel des Systemschutzes bevormundet. Die Algorithmen, die über diese Ver- und Gebote im Einzelfall entscheiden, beruhen auf Entschlüsseln, Absichten und Dogmen der Programmierer. Der Computer ist für die Produzierenden somit zum Instrument zur Übertragung von subjektiven Auffassungen, aber insbesondere zur Etablierung von Hierarchien geworden (vgl. Kittler 1993, 221). Im Umkehrschluss misst diese Machtstruktur den Produzenten, also den Machthabern, eine verdichtete Verantwortung zu, da die Bedienenden viele Berechnungen und Prozesse nicht mehr dirigieren können. Darin liegt die Gefahr, dass die bereits verfestigten Oligopole von Unternehmen wie Google, Amazon oder Alibaba, die Wettbewerb nur eingeschränkt ermöglichen und nicht zu erdenken waren, als sich Kittler den Protected Mode vornahm, weiter Macht akkumulieren und ohne entsprechende Konkurrenz keiner Veranlassung zum Umdenken gegenüberstehen (vgl. Ramge 2018, 89). Gleichzeitig liegt in dieser Machtkonstellation die Chance, Informationssicherheit künftig als eine Grundlage der Produktivität und nicht als einen Stolperstein zu begreifen.

3) Wie in einem kapitalisierten System aus Angebot und Nachfrage üblich, müssen auch die Endverbraucher bereit für das soeben erwähnte Umdenken sein, sodass sich das evolvierte Angebot schließlich auch finanziell lohnenswert für die Produzenten niederschlägt. Verteidigen Kunden, Anwender oder Betroffene dann jedoch in großer Zahl die Ansicht, dass sie nichts zu verbergen hätten, bagatellisieren sie den Wert der privaten Daten mit dieser Einschätzung und sensible Informationen verkümmern somit

³ Ein bis heute angewandtes Prinzip von Hardware-Herstellern zum Schutz ihrer Produkte, das ursprünglich von Intel entwickelt wurde.

zu nicht schützenswerten Gütern. Auch an dieser Stelle greift der Vergleich mit Situationen aus anderen Lebenswelten. Die Frage eines absolut Fremden nach der Kreditkarte und dem Personalausweis würden die meisten Menschen selbstredend verneinen. Im Internet sind diese Daten mit vergleichsweise geringen Kenntnissen auffindbar, weil die Eigentümer sie selbst unwissentlich oder fahrlässig an eine Vielzahl unbekannter Online-Händler und Dienstleister verteilen.

Doch wo liegt der signifikante Unterschied zwischen dem Internet und anderen Infrastrukturen des Alltags? Das Suppositum liegt nahe, dass die Differenz so plausibel wie gravierend ist – das Internet und die dahinter verborgene Welt ist nicht sichtbar, nicht fühlbar und erst recht nicht durch Laien formbar. David Lyon nimmt an, auch wenn er seine Aussage auf Big Data-Analysen richtet, dass dieser in Relation noch sehr junge Bereich menschlicher Interaktion „trivial, fragmented, inconsequential“ ist und aufgrund dieser mangelnden Plastizität nur wenig Evidenz bietet (Lyon 2015, 95f).

Zugleich mag den Bedienern der Eindruck entstehen, wehrlos zu sein und vor einem Berg an Schutzmaßnahmen und Handlungsspielräumen zu stehen, der kaum zu überblicken ist. Diese Freiheit, also die Freiheit sich zu schützen, die Freiheit es zu unterlassen sowie die kumulativen Optionen des Digitalraums stellen Unsicherheit her, die wiederum zu einer Angst vor Fehlentscheidungen oder Opferwerdung und schließlich zu Resignation führen kann. Im Umkehrschluss heißt dies, dass die Angst ein Resultat oder ein Symptom ebenjener überfordernden Perspektiven darstellt. Angst ist damit Ausdruck der Bewältigung einer unerwarteten oder unüberschaubaren Vielfältigkeitskonfrontation. Der Bediener kann in dieser Situation folglich einen Zustand der Ablehnung und der Entmutigung erfahren, der sich zu jeglicher Ausbildung von Resilienz zweckwidrig verhält.

4) Neben unzureichend geschützten Anwendern und teils wenig an Sicherheit interessierten Herstellern ist die fortgeschrittene Professionalisierung der Gegenseite ebenso Bestandteil der Wahrheit. Während das Gros der Bediener die technischen Prinzipien moderner Rechenmaschinen nur rudimentär durchblickt, befinden sich im Lager der Angreifer mehr und mehr bestens geschulte Informatiker und Dienstleister, die ihre Fähigkeiten an Laien verkaufen. Auch der Lagebericht 2019 des BSI stellt im Berichtszeitraum zwischen Juni 2018 und Mai 2019 fest, „dass es eine wachsende Zahl von Dienstleistern gibt, die Schadsoftware und Exploits anbieten, oder sogar selbst Cyber-Angriffe operativ durchführen“ (Bundesamt für Sicherheit in der

Informationstechnik 2019a). Das meint, dass die Angreifer ein Angebot geschaffen haben, für das eine rege Nachfrage besteht. Damit wächst die Verlockung, es anderen Kriminellen gleichzutun und ebenfalls derartige, gut bezahlte Tätigkeiten anzubieten. „Es war nie einfacher als heute, zum Verbrecher zu werden. Früher musste man sich dafür noch in körperliche Gefahr begeben. [...] Für die meisten Cyber-Kriminellen sind die Risiken heutzutage zu vernachlässigen“ (Aiken 2018, 463). Hacker, Informatiker, aber auch technisch wenig versierte Menschen werden in die Lage versetzt, die gegebenen Handlungsoptionen und Fähigkeiten so nutzen zu können, dass sie sich entweder monetär in besonderem Maße auszahlen oder einer Gegenpartei den ersehnten Schaden zuführt. Das bedeutet, dass den Strafverfolgungsbehörden, den Sicherheitsforschern, den Unternehmen und weiteren Organisationen, die IT-Sicherheit erarbeiten, eine große Vielfalt von Angreifern mit noch vielfältigeren Angeboten und Motivationen gegenübertritt. Auftragshacker mit monetärem Interesse; politische Aktivisten, die Daten ihrer Opposition stehlen; gekränkte Ex-Partner mit Zugängen zu gewissen Accounts; konkurrierende Unternehmen, die folgenschwere Fake News über Botnetze verbreiten oder Terroristen, die einfach nur möglichst großen Schaden anrichten möchten – es ist erkennbar, wohin dieses Argument führt.

Zwar ist es möglich, sich gegen besagte Angriffe wirkungsvoll zu schützen, jedoch verlangt dies ein hohes Maß an Gefahrenbewusstsein, nötiger Kenntnisse und gewisser Anstrengung. So schwingt die Prämisse mit: Cyberkriminalität wird nur selten bestraft und ist deshalb lukrativ. So wird allzu oft angenommen, dass man mit Straftaten wie Urheberrechtsverletzungen nur Großunternehmen schadet, die davon gar nichts spüren. Teils greifen sogar Umverteilungsnarrative, die sich aus Erzählungen wie Robin Hood oder dem Grimm'schen Meisterdieb speisen. Der Hacker gilt dann als Idealist, als Anprangerer von Missständen oder als Freibeuter, der die Kassen von globalen Großkonzernen erleichtert. Die massenmediale Narration, wie in *Password: Swordfish*, *Mr. Robot* oder *Watch Dogs*, glorifiziert den Hacker als Figur mit nahezu übernatürlichen Fähigkeiten und zeichnet so das Porträt eines kühnen Heroen. „Wie den Piraten umranken auch den Hacker viele folkloristische Legenden, darunter ein David-gegen-Goliath-Narrativ [...]. Hacker wirken magisch, ja, geradezu übermenschlich“ (Aiken 2018, 442). Aus dem Blick gerät in dieser Beschreibung schnell, dass Internetkriminelle häufig nicht nur edle Motive verfolgen, sondern auch im Auftrag von

Regierungen handeln, Spionage betreiben, Krankenhäuser sabotieren oder Pädophilie Vorschub leisten (vgl. Süddeutsche Zeitung 2019).

5) Die schon mehrfach erwähnte Komplexität der Informatik, innovativer Technologien und damit auch von Sicherheitsmechanismen findet sich zusätzlich abträglich im assoziierten Sprachgebrauch wieder. Schon die Angebotsseite für ein gewöhnliches Tablet liest sich für Laien wie ein Text einer Fremdsprache: Das Display löst in WUXGA auf, der Arbeitsspeicher ist vom Typ LPDDR4 und die WLAN-Verbindung entsteht mittels 802.11 a/b/g/n/ac. Hier sei nebenbei vermerkt, dass die Seite keine Information über implementierte Sicherheitsmerkmale enthält. Es ist deutlich sichtbar, dass die, zugegeben selektierten, Angaben äußerst kryptisch anmuten und dem Verbraucher keinen Hinweis darauf geben, ob er diese Funktion oder jene technische Ausstattung auch benötigt. Werden laienhafte Anwender Opfer von Internetkriminalität, setzt sich die Fremdwörteraufzählung fort: Malware, KI, Back-ups, Phishing, DDoS, Ransomware, 5G oder Smarthome. Für Interessierte und Experten stehen all diese Begriffe für augenscheinlich selbsterklärende Konzepte; für alle anderen stellen sie nachvollziehbare Hürden zum rudimentären Verständnis von Informationstechnik dar.

„We should stop trying to ‚fix the human‘ and fix the security instead. Insecure behaviour is largely driven by security being too complex and/or effortful“ (European Union Agency for Network and Information Security (ENISA) 2018, 18). Es fehlt offenbar an einem niedrigschwelligen Zugang zu Cybersicherheit. Weiterhin existieren keine universell bewährten Konzepte, solche Wege zu ebnen. Zusätzlich zur ohnehin schon abschreckenden Komplexität der Informationssicherheit unterliegen sowohl die Angriffsvektoren als auch die Verteidigungsmechanismen immerwährender, rapider Veränderungen (vgl. Oram/Viega 2009, 185). Glaubt man, Zusammenhänge begriffen zu haben, können sie sich bereits im folgenden Augenblick zersetzen.

Diese kontextspezifische Sprache ist ein ambivalentes Konstrukt. Sie ist gleichzeitig in der Lage, die Annäherung an eine Materie zu verhindern, indem sie durch enorme Komplexität exklusiv wirkt, kann jedoch auch simplifizieren und somit Teilhabe begünstigen. Im Fall der Informationstechnik ist der Sprachgebrauch hoch spezialisiert und entmutigt Laien. Für eine akademische Disziplin wie die Informatik ist die Entwicklung von Fachbegriffen zwar üblich, jedoch fixieren sich zugehörige Termini der Disziplin zwangsläufig immer mehr in der alltagsnahen Diktion, da die Anwender der Technologie vermehrt keine Spezialisten mehr sind, sich die Technik aber zunutze

machen. Dabei ist die Sprache das entscheidende Werkzeug, um Wissen zu internalisieren und Wirklichkeit zu externalisieren (vgl. Schwarz 2014, 85f). Aus diesem Druck enormer Komplexität heraus hat sich die Strategie des Anthropomorphisierens, also der Übertragung körpereigener Fähigkeiten auf Gegenständliches, etabliert (vgl. von Foerster 1989, 33): Die Festplatte eines Computers gilt im informellen Sprachgebrauch als elektronisches *Gedächtnis*; Schadprogramme sind *Viren* und können Digitalgeräte *infizieren*; das iPhone antwortet schließlich auf die Frage ‚Siri, welches Smartphone ist das Beste?‘ mit ‚Moment; das heißt, es gibt noch andere Telefone?‘. Es ist deutlich, dass Analogien zum Menschlichen, ergo die Humanisierung von Technologie, vielfach Anwendung finden. Sie bestimmen *Sprache über, Design von* wie auch *Erfahrungen mit* Technik. Mittels dieser Relationen werden die im Grunde komplexen Vorgänge eingängig und ansprechend; sind dann zugleich aber auch auf eine wesentliche Funktionalität reduziert. Für eine zugängliche Heranführung an Informationstechnik ist die Plausibilität und Reproduzierbarkeit von Sprache essenziell, da es laut Martin Schwarz „von der imaginierten wie auch von den sozialen Wirklichkeiten abhängt, wie implizierte Regelwerke, Rollenmuster, Normen und Erwartungshaltungen durch den Sprechakt bestimmt werden“ (Schwarz 2014, 87).

6) Abschließend bleibt noch, auf die Grundproblematik jeglicher Präventivmaßnahmen hinzuweisen. Im Zuge der SARS-CoV-2-Pandemie formulierte der Virologe Christian Drosten im Podcast Coronavirus-Update einen Ausspruch, der das Dilemma vorbeugender Strategien auf den Punkt bringt. Mit „There is no glory in prevention“ geht Drosten auf das Phänomen ein, dass nach einer überwundenen Krise – aufgrund von erfolgreich umgesetzten Präventivmaßnahmen – die Behauptung im Raum steht, die Krise sei nur wenig bedrohlich gewesen (Coronavirus-Update 2020). Er benennt damit ein allgemein zu beobachtendes, interdisziplinäres Attribut der Prävention.

Projiziert auf Cybersicherheit, bieten sich einige Beispiele an. Auf technischer Ebene zeigt eine funktionierende Firewall, wovon Drosten spricht. Solange die Software die digitalen Bedrohungen abwehrt, ist sie nicht wahrnehmbar. Erst im Moment ihrer Fehlfunktion oder ihrer Überwindung wird sie dem Bedienenden erneut sichtbar und fällt negativ auf. Richtet man den Blick auf den Bediener, muss voranstehen, dass Präventionsmaßnahmen, egal ob von außen induziert oder aus einem inneren Antrieb, zunächst Handlung erfordern und damit derzeit meist entweder Einbußen im Bedienkomfort oder mindestens einen erhöhten Aufwand bedeuten. Schon die wohl

gängigste Empfehlung, also die Einrichtung individueller, langer und Zufalls-generierter Passwörter für jeden einzelnen Account, setzt voraus, dass die Passwörter jeweils erstellt und zudem sicher sowie praktikabel auffindbar abgelegt werden. Schnell zeigt sich, dass jegliche Art digitaler Vorbeugung einer gewissen kontinuierlichen Arbeit bedarf und obendrein bei Erfolg keine spürbare Wirkung zeigt. Der Niederschlag präventiver Mechanismen liegt in der Vereitelung schadhafter Folgen, ergo dem Erhalt eines bedarfsgerechten Zustands. Dies hat zur Folge, dass die investierte Arbeit keinen Wertzuwachs generiert, sondern häufig nur als Loch für Ressourcen wahrgenommen wird.

Sei es nun die mangelnde Attraktivität von Cybersicherheit, die Ahnungslosigkeit der potenziell Betroffenen oder lediglich das fatalistische Motiv digitaler Obliquität: Umstände dieser Art ersticken eine Vielzahl bedeutsamer IT-Sicherheitsbestrebungen.

I.II. Asymmetrische Entgleisung

„In den Zeiten der flüchtigen Moderne wird das Spiel der Eroberung nicht mehr zwischen den »Kleineren« und den »Größeren« gespielt, sondern zwischen den Schnelleren und den Langsameren. Wer schneller beschleunigt als seine Verfolger, hat gewonnen“ (Bauman 2000, 220). Diese Annahme trifft im doppelten Sinn auf die großen digital-kapitalistischen Erfolgsgeschichten des einundzwanzigsten Jahrhunderts zu. Die global wertvollsten Unternehmen, darunter Apple, Google oder Amazon, haben Innovationen vor ihrer Konkurrenz auf dem Markt platziert und sich so auch mittelfristig durchgesetzt. Zudem sind ihre Produkte Werkzeuge zur Beschleunigung beziehungsweise zur Erzeugung von Unmittelbarkeit. In Addition führt dies zu einer Akkumulation von Geschwindigkeit und schließlich zu einem gegen unendlich wachsenden Wettbewerbsvorteil. Die Ausgangsgröße ist in diesem Szenario nahezu irrelevant. Vergleichbares gilt für das Verhältnis von Cyberkriminalität und Sicherheitsorganen. Es gewinnt die Partei, die es schafft, Schlüssellösungen schneller hervorzubringen als ihre Widersacher – ohne der Gegenseite eine Chance zur Abwehr zu lassen. In vielen Fällen heißt dies, dass meist die Angreifer ein neues Einfallstor entdecken und förmlich losgelöst von ihrer Personenzahl sabotieren, stehlen und spionieren.

Cyber-Sicherheit stellt sich asymmetrisch dar: Um eine Kritische Infrastruktur erheblich beeinträchtigen zu können, muss ein Angreifer lediglich eine einzige Schwachstelle erfolgreich ausnutzen. Betreiber Kritischer Infrastrukturen

müssen hingegen einen ganzheitlichen Schutz gewährleisten, um sich umfassend abzusichern (Bundesamt für Sicherheit in der Informationstechnik 2019a, 46).

Die Opfer können bei solch asymmetrischen Angriffsvektoren in der Regel nur noch versuchen, den Schaden zu begrenzen und ihre reaktive Rolle zu erfüllen. Offensichtlich ist die Geschwindigkeit bei diesem fortwährenden Wettlauf ein entscheidender Faktor für Erfolg.

Die Widrigkeiten bei der Verteidigung von IT-Strukturen des vorigen Kapitels lassen den Digitalraum für Angreifer gleichzeitig noch lohnenswerter erscheinen. Straftaten wie Raub, Betrug, oder Erpressung verüben im physischen Lebensraum vornehmlich einige wenige Täter an einigen wenigen Opfern. In dem Bewusstsein, dass es seit jeher zudem organisierte Kriminalität und Verbrechen von Vielen an Wenigen gibt, kann man vorbringen, dass es sich auch in solchen Fällen zumeist um überschaubare Geschädigtenzahlen gehandelt hat. Täter, Werkzeug und Opfer müssen in diesen Szenarien räumlich wie zeitlich zusammenkommen und miteinander interagieren. Befindet sich der potenzielle Betroffene und sein Hab und Gut an einem vom vermeintlichen Täter entfernten Ort, können Gewalttaten oder Diebstahl verlässlich abgewendet werden. Zudem besteht für den Kriminellen die Gefahr, aufgrund hinterlassener Spuren entdeckt und dingfest gemacht zu werden. Will man einer anderen Person etwa Geld stehlen, ist es notwendig, sich selbst oder Mittäter zu exponieren und dem Risiko der Sanktionierung auszusetzen. Man geht bewaffnet in eine Bank oder bricht nachts in ein Haus ein, stiehlt so viel Bargeld, wie man findet, und versucht unbemerkt und ohne verfolgbare Spuren zu entweichen.

Die Gattung des Verbrechens hat sich mit dem Anbruch des Informationszeitalters nicht geändert – ihre Ausführung jedoch erheblich. Zwar gibt es nach wie vor klassische Überfälle oder Gewaltdelikte, jedoch haben sich innerhalb weniger Jahre neuerliche Möglichkeiten ergeben, subtil vorzugehen, Spuren nachhaltig zu vermeiden und obendrein einen ungleich höheren Ertrag zu erzielen beziehungsweise einen ungleich größeren Schaden anzurichten. Zusätzlich sinken die notwendigen finanziellen und personellen Ressourcen für die Täter. Was klingt wie ein Schlaraffenland für Verbrecher, ist eine offenliegende Realität im digitalen Raum der Gegenwart. Mit ausreichender Technik und dem nötigen Wissen ausgestattet genügt eine Person, um Unternehmensserver zu sabotieren, Ampelsteuerungen zu manipulieren oder Regierungsnetze außer Kraft zu setzen. Ein Täter hat leicht zugängliche Ressourcen, die

ihn in die Lage versetzen, signifikante Wirkungen herbeizuführen. Auch das „BSI beobachtet eine konstant steigende Professionalisierung von Angreifern bei sinkenden Aufwänden für die Durchführung der Angriffe“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 39). Gleichzeitig gibt es für die Opfer – seien es nun Individuen oder ganze Staaten – häufig wenige Möglichkeiten, die Angriffe zurückzuverfolgen, das Motiv des Täters zu identifizieren oder die Attacke gar im Vorfeld abzuwehren. Ein Vorfall wird häufig erst durch die Entdeckung des Schadens bemerkt. Zu einem solchen Zeitpunkt haben Täter bereits alle verfolgbaren Indizien verborgen. Danach beginnt eine Maschinerie, die Zeit zeitintensiv und wenig zielführend ist: Die Polizei wird eingeschaltet, weitere Kompetenzen werden hinzugezogen, Geräte sowie Netzwerke werden untersucht und am Ende steht die Feststellung, dass der Täter aus dem Ausland agiert hat und daher nicht belangt werden kann. Diese sinnbildlichen Guerillakämpfer schlagen aus dem Nichts zu und verschwinden ebenso schnell wieder im Dunkeln. Den Attackierten bleibt nichts weiter übrig, als die Wunden zu lecken und zukünftig noch konsequenter vorbereitet zu sein – ohne dabei zu wissen, aus welcher Richtung der nächste Angriff kommen wird.

Der Niederländer Oerlemans illustriert in seinen juristischen Erläuterungen, worin die Stärke der Cyberkriminellen beziehungsweise die Schwäche staatlicher Verteidigungs- und Ermittlungseinrichtungen liegt. Das sogenannte Territorialitätsprinzip besagt, dass derjenige Staat für die Verfolgung oder Abwehr eines Verbrechens zuständig ist, dessen Staatsgebiet oder dessen Souveränität von der Tat betroffen ist.

Het internationaal strafrecht is duidelijk: de uitvoerende jurisdictie van een staat is beperkt tot de territoriale grenzen van een staat. Dit beginsel staat op gespannen voet met de aard van internet dat niet tot de territoria van staten is beperkt⁴ (Oerlemans 2019, 219).

Das bedeutet, dass die Zuständigkeit eines jeden Staates an dessen Grenzen endet und die Verfolgung von Tätern entgegensteht, die von einem fremden Staat aus agieren, ihre Datenströme über wieder andere Staaten leiten, um dann schließlich ihrem Ziel zu schaden. Diese Regelung stammt aus den Zeiten staatlicher Territorialherrschaft und sieht eine digitale, supranationale Kriminalitätsbekämpfung nicht vor. Da Internetbedrohungen derart schwer greifbar sind und ihr Ursprung häufig zunächst

⁴ Deutsch: Das internationale Strafrecht ist eindeutig: Die Exekutive eines Staates beschränkt sich auf die territorialen Grenzen eines Staates. Dieses Prinzip steht im Widerspruch zum Wesen des Internets, das nicht auf das Territorium von Staaten beschränkt ist.

unklar ist, sieht internationales Recht vor, die nationale Jurisdiktion festzustellen, indem man sich auf die Wirkungsdoktrin beruft. Demnach ist der Staat zuständig, bei dem ein wesentlicher Zusammenhang zwischen der Tat und dem Staatsterritorium besteht respektive der am massivsten von den Folgen der Handlung betroffen ist (vgl. Oerlemans 2019, 212). Diese Vereinbarung lässt aber entscheidende Freiräume offen, die Henrik Kaspersen ausmacht:

Dat klemt des te meer indien de ene nationale wet bepaalde gedragingen verbiedt terwijl een andere – buitenlandse – wet die gedraging juist vrijlaat. Dat laatste bevordert het ontstaan van zogenaamde data havens, elektronische plaatsen van waaruit men onder bescherming van de eigen rechtsorde strafbare feiten kan plegen die effect hebben op het territorium van andere staten⁵ (Kaspersen 2004, 4).

Denn indem keine internationale Einigkeit sowie entsprechende Gesetzgebung existiert, können betroffene Staaten nicht in die Souveränität des Tatterritorioms strafverfolgend eingreifen. Es entstehen Rückzugsorte für Kriminelle; Oerlemans führt den Begriff *mare liberum* an und allegorisiert so den Internet-Piraten (vgl. Oerlemans 2019, 209). Um internationalen Schlupflöchern vorzubeugen, beschlossen 38 Staaten im Jahr 2001 die Cybercrime-Konvention, die die Gerichtsbarkeit im Wesentlichen dann eindeutig definiert, wenn festgestellt werden kann, von welchem Hoheitsgebiet eine Tat ausgeht oder welchem Staat die Täter angehören (vgl. Europarat 2001). Diese Übereinkunft schließt zum einen jedoch nicht alle Staaten der Welt ein und trifft zum anderen keine Festlegungen über den Standort von Netzwerken und Computerinfrastrukturen. Hierzu wird erst das Tallinn Manual von 2017 präziser, das jedoch bislang keine juristisch bindendes Gesetzesblatt, sondern eine ausschließlich akademische Leistung darstellt. Folglich bleibt die internationale Zusammenarbeit zur Verfolgung von Internetkriminalität eine auf Kooperation und Wohlwollen ruhende sporadische Angelegenheit, die nur selten von bindenden Abkommen flankiert wird. Diese Diskrepanz zwischen den territorialen Machtmechanismen des 20. Jahrhunderts und den beweglichen, dezentralisierten wie grenztranszendierenden Eigenheiten des Internets öffnet ein Gewaltvakuum, das sich als Nährboden für virtuelle Entgleisungen geradezu aufdrängt.

⁵ Deutsch: Dies ist umso dringlicher, wenn ein nationales Gesetz ein bestimmtes Verhalten verbietet, während ein anderes – ausländisches – Recht dieses Verhalten zulässt. Letzteres fördert die Schaffung sogenannter Datenhäfen, elektronischer Orte, von denen aus man unter dem Schutz der eigenen Rechtsordnung Straftaten begehen kann, die das Territorium anderer Staaten betreffen.

II. Forschungsfrage und Ziel

Ziel der Dissertation ist es, national unterschiedliche Strukturen zur Etablierung und Anwendung von IT-Sicherheit aufzuzeigen. Der Fokus der Gegenüberstellung liegt auf der Untersuchung öffentlicher Cybersicherheitsinstitutionen, gesellschaftlicher Anstrengungen und der Vermarktung von Cybersicherheit in medial wirksamen Awareness- und Sensibilisierungsanstrengungen. Daraus kann ein unübersichtliches Volumen an Informationen entstehen, die auf keinen Erkenntnisgewinn hinauslaufen. Dies gilt es selbstredend zu vermeiden, was wiederum zu der Frage führt, wie man sich wirksam an das Forschungssujet herantastet und vermeidet, unzureichende Ergebnisse zu veröffentlichen. Um diese Frage hinlänglich zu beantworten und ein zielgerichtetes Untersuchungsdesign aufzustellen, folgen ausführliche Erläuterungen zur Herangehensweise und den konstatierten Hypothesen. Auf dem Weg zur Herstellung einer Leitfrage begegnet man in der Literatur verschiedenen Ansätzen. So wird vorgeschlagen, eine Frage zu wählen, die bislang nicht mit Studien untermauert wurde; eine vermutlich zu falsifizierende Hypothese zu suchen; eine wissenschaftliche Debatte anzufeuern oder aufzulösen; eine Frage zu ermitteln, die bislang beiseitegeschoben wurde oder aber Ideen anderer Wissenschaften auf das eigene Forschungsgebiet zu übertragen und so neues Wissen zu generieren (vgl. Jahn 2013, 187).

Es zeigt sich, dass in der Literatur bislang zwar über Sicherheitskulturen diskutiert, dabei aber das spezifische Feld der Cybersecurity Culture außen vor gelassen oder rudimentär abgehandelt wird. So beziehen weder Daase, Lange noch Endreß den Digitalraum als verhältnismäßige Größe in ihre Abwägungen ein. Wird diese Verknüpfung dann einmal hergestellt, handelt es sich zumeist um Cybersecurity Culture auf rein organisationaler Ebene. Lediglich Aufsätze wie der von Rita Haverkamp bilden eine nennenswerte Ausnahme, wobei sie sich überwiegend auf Überwachungsinstrumente, Kontrolltechniken wie auf Human Security konzentriert (vgl. Haverkamp 2014, 185). Zudem legen die Autoren in vielen Fällen deutlich mehr Vergleichsobjekte nebeneinander, konzentrieren sich dann aber auf nur wenige Vergleichsgrößen; beispielsweise Bulanova-Hristova und Andere 2016 in ihrer polizeilichen Betrachtung von Cybersicherheitsstrukturen in zahlreichen Mitgliedsstaaten der EU. In derartigen Analysen fassen die Beobachter dann einen Akteur oder eine Partei ins Auge, die sie hervorheben. Die vielschichtigen Akteure, Institutionen, Gesetze oder aber auch extrinsischen Kräfte, die Einfluss auf die Adaption

von IT-Sicherheit in einer Gesellschaft haben, bleiben dann außen vor. Unter Beachtung dieser Defizite ließe sich zwar bereits ein Einblick in die jeweilige Cybersicherheitskultur erhaschen, allerdings bliebe so die Frage nach den Ursachen dieser Kulturkalibrierungen gänzlich unbeantwortet. Daher kann es diese Dissertation nur angemessen vervollständigen, wenn abschließend eine historische Kontextualisierung steht; wenn sich also entpuppt, warum die Niederländer eben ihre Strategien und verfestigten Handlungsmuster, Paradigmen sowie Leitvorstellungen pflegen und die Deutschen ihre eventuell ganz eigenen.

Die Arbeit zielt auf mehrere Leistungen ab. Es entsteht eine belastbare Konkretisierung von Cybersicherheitskultur, die so bislang nicht besteht und anschließend universell anwendbar ist. Ferner entwickelt sich im Verlauf dieser Dissertation eine Methode, die auf weitere Vergleiche dieser Art anwendbar sein, zu reliablen Resultaten führen und Eigenschaften sichtbar machen wird, welche ohne dieses Werkzeug nur Annahmen blieben. Dazu entspinnt sich notwendigerweise zunächst eine ausführliche Bestandsaufnahme der jeweiligen Organisationen, Gesetze und Strukturen. Dies bildet die Grundlage für den formalisierten Vergleich, der schließlich in der Gegenprüfung anhand von realen Zwischenfällen der jüngeren Vergangenheit mündet. Um den Kurs für dieses Vorgehen zu setzen, gliedert sich die Forschungsfrage demgemäß in mehrere Teilfragen auf. Die motivgebende Prämisse der Arbeit, die zu evaluieren ist, lässt sich folgendermaßen formulieren: *Deutschland und die Niederlande verfolgen unterschiedliche Modi zur Synthese von Cybersicherheit.*

Daraus gehen nachstehende Fragen hervor, die es erlauben, einer Verifizierung der Hypothese von verschiedenen Seiten näherzukommen.

- 1) Was ist eine Cybersecurity Culture?
- 2) Wie organisieren die beiden Länder IT-Sicherheit?
- 3) Wie formatieren die Institutionen die Logik der Informationssicherheit?

Im Mittelpunkt steht also die Annahme, dass trotz der gemeinsamen westeuropäischen Prägung und der geografischen wie kulturellen Nähe beider Länder Kontraste im Umgang mit Informationssicherheit bestehen. So wird der Versuch unternommen, sich dieser Unterschiede wissenschaftlich anzunähern und gegebenenfalls schon Hinweise auf die Ursachen für Differenzen darzulegen. Beginnend mit einer Art Bestandsaufnahme der Länder, schlägt die Untersuchung in der zweiten Hälfte die

Brücke zu den Imaginationen, zu den Narrativen und den vorherrschenden Bildern, die in beiden Gesellschaften jeweils über Informationssicherheit bestehen.

Doch um die vor uns liegenden Fragen überhaupt besprechen zu können, ist es ebenso notwendig, einen Rahmen zu setzen. Klar ist nun, dass die Ansätze der Niederlande und Deutschlands untersucht werden. Was jedoch fehlt, ist ein zeitlicher Ankerpunkt, eine temporale Einfassung, die präzise einzufassen ist: Der sicherheitspolitische Ausgangspunkt der Betrachtung wird auf 1990/91 festgelegt. In diesen Zeitraum fällt die Gründung des BSI – unmittelbar nach der Wiedervereinigung der Bundesrepublik sowie in einer sehr frühen Phase des privat und kommerziell utilisierten Internets (vgl. Abbate 2010, 16f). Dabei reicht die Historie von Schadsoftware wie Creeper oder Brain zurück bis in die 1970er-Jahre. Das NCSC der Niederlande besteht dagegen seit 2012; nur einige Monate nach der aufsehenerregenden Entdeckung des Sabotagesoftware *Stuxnet*. Für die Bundesrepublik Deutschland und die Niederlande sind zudem ein Rückblick bis circa 1945 notwendig, um die Wendepunkte und Zäsuren der vergangenen Jahrzehnte zu erkennen und als relevante Faktoren für die gegenwärtigen (Re-)Aktionen der Cybersecurity Culture zu identifizieren. Die Untersuchung endet schließlich Anfang 2022 mit dem Beginn des russischen Angriffskrieges auf die Ukraine. Dieser Krieg annulliert bisherige Glaubensgrundsätze, indem er unumstößlich geltende Annahmen über europäische Partner, Sicherheitsgarantien, Energiepolitik wie auch über grundlegendes Völkerrecht sowie staatliche Souveränität plötzlich verwirft. Zudem vermischt dieser Konflikt den sichtbaren, physisch-substanziellen Krieg und den Cyberkrieg durch Hacks, Propaganda und Desinformation; die Untersuchung dieser äußerst komplexen Verstrickungen und der verschobenen Sicherheitstektonik obliegt dann zukünftigen Arbeiten. Unter Berücksichtigung der obigen Teilfragen formt sich ein Eindruck davon, wie die jeweiligen Gesellschaften, die zweifellos nicht trennscharf zu betrachten sind, mit der Komplexität der Digitalisierung umgehen. Als eine entscheidende Vergleichsgröße werden die Ziele der Länder identifiziert und als kultur- oder mediensoziologische Ausprägung kulturellen Handelns verstanden. So zeichnet sich ein temporärer Sachstand und illustriert die zugehörige Historie. In dieser Dissertation wird beiläufig der bisherige Weg zum reizvollen Ziel einer resilienten und robusten Security Culture innerhalb der beiden genannten Länder aufgezeigt, diese miteinander verglichen und ein Ausblick gegeben. Anders formuliert steht die Frage im Raum, wie intensiv die beiden

Staaten im Rahmen ihrer Möglichkeiten auf eine Implementierung von sicherer Informationstechnik in die jeweilige Gesellschaft hinarbeiten. Auf diese Weise ist zwar keine globale Aussage möglich, jedoch steht am Schluss eine Bilanz, die beispielsweise erkennen lässt, welches der zwei Länder mit größerem Einsatz ebendieses Ziel ansteuert. Die auf diesem Weg immer wiederkehrenden Vergleiche offenbaren Unterschiede, aber auch Gemeinsamkeiten innerhalb der Praktiken.

Diese Forschung schließt nicht an solche Projekte an, die einen holotischen Anspruch verfolgten (vgl. European Security Research and Innovation Forum (ESRIF) 2009, 243). Der Versuch, ein allumfassendes Abbild eines chronologisch determinierten Zustandes zu erschaffen, ist aufgrund der unüberschaubaren Menge akademischer Disziplinen, die potenziell berührt werden, unmöglich. Der vordringliche Zweck dieser Dissertation ist es, die Cybersicherheitskulturen mithilfe des jeweils anderen Landes als Reflexionsfläche zu identifizieren und erkennbar darzulegen. Nicht die ganzheitliche singuläre Betrachtung, sondern die unumwundene Gegenüberstellung hebt Eigenheiten wie auch Homogenitäten der Forschungsobjekte hervor (vgl. Hepp 2011, 131). Dabei soll eine Methode entstehen, die ein funktionales Instrument zum weiteren Vergleich von Cybersicherheitskulturen sein kann, um zukünftige akademische Betrachtungen zu erleichtern.

III. Operationalisierung

Die soeben formulierte Leitthese mitsamt ihren zugehörigen Kernfragen lassen sich zur Präzisierung feiner granulieren. Die folgenden Submotive dienen insbesondere der Herstellung eines systematisierten argumentativen Unterbaus. Zu Beginn ist es notwendig, den Begriff der Security Culture zu klären, um darauf aufbauend Luzidität herstellen und ihn mit Informationstechnik verbinden zu können. Anschließend wird Literatur aus deutschen und niederländischen Quellen der Felder Politik, Informatik, Soziologie und Medienwissenschaft herangezogen (vgl. Jasanoff 2015a, 29). Die Quellen sind in diesem Fall äußerst vielfältig und reichen von Berichten und Sachbüchern über popkulturelle Medieninhalte bis hin zu Vorträgen wissenschaftlicher Konferenzen. Durch diesen Querschnitt kann die jeweils vorherrschende Sicherheitskultur zusammengefasst und wiedergegeben werden.

Neben der umfangreichen Arbeit an und in der Literatur sind die Untersuchungsgegenstände die Behörden, Institutionen und Regelwerke der Länder selbst. Welche Parallelen gibt es im Hinblick auf IT-Sicherheit beispielsweise zwischen dem BSI und dem NCSC (Nationaal Cyber Security Centrum⁶)? Oder operiert das BSI beispielsweise in Handlungsfeldern, die in den Niederlanden vielmehr dem AIVD (Algemene Inlichtingen- en Veiligheidsdienst) obliegen? Die Recherche der Organisationsstrukturen sowie eine Einordnung in den nationalen wie europäischen Kontext sind deshalb notwendig, um aussagekräftige Schlüsse auf die jeweilige Priorisierung von IT-Sicherheit zu ziehen. Es gilt herauszufinden, welche Institutionen innerhalb der Staaten im Wesentlichen mit der Cybersicherheit betraut sind und wie lokale Vernetzungen oder weitergehendes Engagement hervortreten. Die nachstehenden Kapitel legen deshalb dar, dass Kultur und damit auch IT-Sicherheitskultur per definitionem einem Zustand unter anderem zeitlicher, geografischer, intranationaler und topologischer Unvollkommenheit unterliegen. Die inhärente Flüchtigkeit des anvisierten Untersuchungsgegenstands macht es herausfordernd, adäquate Erhebungswerkzeuge zu identifizieren, die den Gegebenheiten gerecht werden. Hinzu tritt ein ausschlaggebendes Charakteristikum der wissenschaftlichen Leistung: Der Untersuchende nimmt eine emische wie etische Position zu seinem Forschungsobjekt ein. Schon aus der erwähnten Beschäftigung beim Bundesamt für Sicherheit in der Informationstechnik resultiert der interne Blick eines Teilnehmers, partiell emisch als

⁶ Deutsch: Nationales Cybersicherheitszentrum

Akteur der deutschen Cybersecurity-Infrastruktur, partiell aber auch etisch als Betrachter der niederländischen Bemühungen. Diese Rolle als Beteiligter an den im Folgenden betrachteten Strukturen bringt unweigerlich ein gewisses Maß der Befangenheit mit sich, das Einzug in die Evaluierung halten muss.

Nun könnte hier angesetzt und die Forschungsbeschaffenheit bemängelt werden, da im Gegensatz zum etischen Blick die subjektive Färbung durch den Autor punktuell zu erahnen sein wird. Dem ist zu entgegnen, dass gerade diese ungewöhnliche Konstellation Einsichten und Interpretationen erlaubt, die Außenstehenden verschlossen bleiben. An dieser Stelle sei jedoch gesagt, dass der involvierte Hintergrund des Forschenden keinesfalls zu weniger wissenschaftlichen Ergebnissen führt – vielmehr wird die objektivistische Idee noch erweitert.

Daß in ihrer Erkenntnis [der Geisteswissenschaften] das eigene Sein des Erkennenden mit ins Spiel kommt, bezeichnet zwar wirklich die Grenze der ›Methode‹, aber nicht die der Wissenschaft. Was das Werkzeug der Methode nicht leistet, muß vielmehr und kann auch wirklich durch eine Disziplin des Fragens und des Forschens geleistet werden, die Wahrheit verbürgt (Gadamer 1986, 494).

Hier stellt sich zu Beginn die Frage nach der grundlegenden Herangehensweise, die im Folgenden begründet wird. Also: Können die Forschungsfragen eher quantitativ, eher qualitativ oder mit Funktionen aus beidem ergiebiger beantwortet werden? Um den übergeordneten Beobachtungsgegenstand der IT-Sicherheitskultur beider Länder komparativ mittels definierter Kulturräume gegenüberzustellen, kann nur die Forschung mit qualitativen Hilfsmitteln in befriedigender Weise zielführend sein. Quantitative Prozedere setzen voraus, dass „die soziale Realität als objektiv und mit kontrollierten Methoden erfassbar“ gilt (Röbken/Wetzel 2016, 13). Man versucht, Forschungsobjekte unter Verwendung großer Mengen von „Daten möglichst genau zu beschreiben und vorhersagbar zu machen. Das Verhalten wird in messbare Einheiten zerlegt (elementaristische Vorgehensweise) und als Beobachtungseinheit definiert“ (Röbken/Wetzel 2016, 13). Genau hier liegen die große Stärke wie auch das signifikante Problem zahlenbasierter Instrumente: Sie erfassen skalierbare, zählbare, sichtbare, oder mindestens hylische Tatsachen und erlauben bei sachgerechter Umsetzung eine Kontrollmessung oder vergleichende Untersuchungen, die relative Abweichungen im zeitlichen Verlauf nachzeichnen können. Dabei werden wenig flexible Wege bestritten, die aufgrund ihrer Porosität kaum Möglichkeiten bieten, so flüchtige Gefüge wie Gesellschaft, Kultur oder zwischenmenschliches Verhalten mensurabel zu erschließen.

Eben an diesem Punkt setzt die qualitative Forschung an. Natürlich ist auch dieses Konzept nicht frei von Unzulänglichkeiten. So scheitern qualitative Untersuchungen in der Regel dort, wo quantitative ans Ziel führen: Sie sind nur bedingt evidenzbasiert, sie argumentieren meist nicht mittels standardisierter Daten und sie lassen gelegentlich kühle Objektivität vermissen. Stattdessen sind qualitative Wissenschaften „explorativ und hypothesengenerierend angelegt“ (Röbken/Wetzel 2016, 14). Sie ertasten eine Erscheinungsform und können immer dann erfolgreich angelegt werden, wenn Sachverhalte von innen heraus zu beleuchten sind. Zu ihnen gehören nicht repräsentative Stichproben, gewöhnlich bestehend aus einer überschaubaren Anzahl von Interviews, Gruppengesprächen oder Beobachtungen. Sind Einstellungen, Motive oder Erwartungen im Fokus der Betrachtungen, liefern qualitative Methoden somit Instrumente, diesen diffusen, temporären Zuständen überhaupt konzentriert und akademisch beizukommen.

Hans Lietzmann veranschaulicht exemplarisch, wozu eine anhaltende gänzliche Ausklammerung explorativer, dynamischer und theoriegeleiteter Forschungsinstrumente führen kann.

Dieser Verzicht auf eine gesellschaftliche Perspektive unterschlägt aber einen entscheidenden Aspekt der politischen Dynamik. Die sich immer mehr herausbildende »politische Gesellschaft« nimmt wesentlichen Einfluss auf politische Strukturen und Entscheidungen. Diese bleiben aber mit der alleinigen Konzentration auf die »positiven«, rechtlich fixierten oder formal errichteten Institutionen außer Betracht. Deren praktische, gesellschaftliche Existenz – ihr Vollzug in der politischen Gesellschaft – bleibt neben ihrer formalen Existenz unterkomplex (Bergem et al. 2019, 16).

Da sich diese Arbeit der Verhandlung von IT-Sicherheit in Deutschland und den Niederlanden widmet, ist es gerade die von Lietzmann vorgebrachte gesellschaftliche Perspektive, die von Interesse ist. Demzufolge versuche ist diese Dissertation der Versuch, die ebenfalls bislang weitestgehend entsoziologisierte Cybersecurity, die zumeist auf unwiderlegbare Zahlen und technozentrierte Kriterien blickt, mit qualitativ erfassbaren kultur- und medienwissenschaftlichen Attributen zu beschreiben. So werden auf den folgenden Seiten zwar auch statistische Vergleiche hinzugezogen; die Instrumente zur Validierung der Kernhypothese werden aber weniger nach dem Kriterium der Reliabilität ausgewählt, sondern nach ihrem Vermögen, ein qualitatives Bild als Basis für spezifizierende, teils auch quantitative Untersuchungen zu zeichnen.

Mit Blick auf diese Art geisteswissenschaftlicher Forschung liegen die Untersuchungsmodalitäten gewissermaßen offen. Nach der Beleuchtung der zugrundeliegenden wissenschaftlichen Theorien gilt es, die jeweiligen nationalen Verflechtungen aus Institutionen, Unternehmen und Behörden zu entwirren, die sich mit IT-Sicherheit beschäftigen. Dies zielt auf möglichst deutlich erkennbare Abbilder der strukturellen Gegebenheiten ab, die dann einen Vergleich erlauben. In dieser Position lassen sich die Ausgangsthesen ein erstes Mal überprüfen. Eine Gegenprobe steuert anschließend die Verifizierung beziehungsweise Falsifizierung bei, indem anhand mehrerer Einzelfallbetrachtungen Rückschlüsse gezogen werden. Die Ansicht beispielhafter, teils regionaler, teils nationaler Projekte und Initiativen demonstriert schließlich, inwiefern die auf staatlicher Ebene auferlegten Maßnahmenkonstruktionen adaptiert oder negiert werden. Gleichzeitig wird erkennbar, ob die vorhandenen Einrichtungen und Reglementierungen so geraten sind, dass sie den durchaus unterschiedlichen Bedürfnissen im alltäglichen Umgang mit Cybergefahren zweckmäßig und konstruktiv begegnen. Eine Konfrontation dieser Art vermittelt einen fundierten Eindruck. So ermöglicht die resultierende Ableitung, die eingangs determinierten Forschungsfragen zu beantworten.

Bei jeder Auswahl einer qualifizierten Methode ist es substanziell für den weiteren Forschungsverlauf, den Maslow'schen Hammer zu meiden und ausgehend vom Problem zu selektieren. „I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail“ (Maslow 1966, 15). Das bedeutet, es gilt, den Bearbeitungsgegenstand zu identifizieren und zu ermitteln, ob es sich tatsächlich um einen Nagel handelt. Erst danach steht die Suche nach dem Instrument, das die Schwierigkeit überwinden kann. Maslow unterstellte mit seinem Aphorismus, dass die Auswahl der Forschungsmethode den Blick auf das Untersuchungsobjekt so verstellt, dass es verzerrt oder eingeschränkt wird. Mit dem Ziel, den Hammer zu benutzen, wird so unter anderem der Faden oder die Schraube als Nagel deklariert. Das Ergebnis ist in einem solchen Fall jedoch mangelhaft, mindestens aber eindimensional.

III.I. Risiko des Diskurses – Diskurse über das Risiko

Die Betrachtung von Diskursen wendet sich dem gesprochenen und geschriebenen Wort, einzelnen Aussagen, aber insbesondere dem Austausch ganzer Semantiken zu. Es werden Aussagesysteme abgesteckt, die potenziell jede mögliche Äußerung einer umrissenen Gruppe innerhalb eines Beobachtungszeitraums zu einem Thema umfassen – das können etwa Aussprüche relevanter Personen, symbolisierte Gesten oder ganze Medienformen sein, die eine Botschaft in die diskursive Praxis eintragen (vgl. Auerbach et al. 2019, 707). Nach Reiner Keller gestattet die Diskursanalyse den Blick in zwei Richtungen, nämlich auf die Ursachen und auf die Effekte von Diskursen. Die detaillierte Auseinandersetzung mit einer relevanten Kontroverse erlaubt „Annahmen über Gründe und Zusammenhänge für die rekonstruierten Diskursentwicklungen“ und zugleich approximative Aussagen über die Auswirkungen des Diskurses bei stabilen, diskursinternen wie -externen Parametern (Keller 2005, 267). Michel Foucault mustert den Diskurs als historisch bedingte Sozialkonstruktion, die sich vorwiegend in Sprache niederschlägt. Sie determiniert „das zu sagen Mögliche“ und charakterisiert das „Denksystem“ (Busse 1987, 223). Wenngleich er auch nonverbale Diskurskomponenten erkennt, kreist Foucaults Argumentation um die performative Kraft von Sprache. Der Diskurs prägt somit die interpersonellen Netzwerkmöglichkeiten. Bei Jürgen Habermas hingegen sind es die zwischenmenschlich geltenden Normative, „denen alle möglicherweise Betroffenen als Teilnehmer an rationalen Diskursen zustimmen könnten“ (Habermas 1992, 138). Erst die intersubjektive Zustimmung definiert, welche Aspekte eines Diskurses abschließend als gültig erfasst sind und allgemeine Berücksichtigung einer Gemeinschaft erfahren. Während der Habermas'sche Diskurs also durch die Umwelt limitiert scheint, ist der Diskurs bei Foucault als Macht konstruierendes Werkzeug freier angelegt. Für Foucault schafft erst der Diskurs, „der Wille zur Wahrheit“, Ordnung und sortiert für die Debattenteilnehmer die Wahrheit von der Fabelei (Foucault 1970, 16). Die öffentliche Konversation verhandelt dem folgend, was die Welt ist und welche Prämissen ihr zugrunde liegen.

Auch für Peter Berger und Thomas Luckmann ist der Diskurs wesentlicher Bestandteil für die titelgebende *gesellschaftliche Konstruktion der Wirklichkeit*, jedoch unter der Prämisse, dass jedem Individuum der eigene Ort innerhalb gesellschaftlicher Kategorien bekannt ist (vgl. Berger/Luckmann 2018, 43). Mit ihren Ausführungen stellen sie

heraus, dass die Relativität von Diskursen genau im Zerrfeld der Pole von Foucault und Habermas steht und sie ebenso historisch-soziologisch bedingt, wie sie konstituierend wirkmächtig sind. Der Diskurs steht nicht vor der Wirklichkeit, obwohl er sie festschreibt. Zugleich besteht keine Wahrheit ohne eine vorausgegangene Besprechung. Ekkehard Felder spricht davon, dass „Fakten gemacht und diskursiv hergestellt werden“ (Felder 2013, 16). Er sieht die Ursache darin, „dass sie [die Fakten] von verschiedenen Diskursakteuren unterschiedlich und nicht je identisch konstituiert werden und dass bei jeder Sinnherstellung für jemanden (HÖRMANN (1978)) spezifische Nuancierungen ins Sprachspiel hineinkommen“ (Felder 2013, 16). Dem folgend sind Wissen oder Wirklichkeit keine ausschließlich objektivierten Größen, sondern individuell erweiterte, aber kollektiv produzierte Diskursresultate. Achim Landwehr setzt diesen Gedanken fort und formuliert gar, dass es nie „[d]as unbezweifelbare Wissen von *der* objektiven Wirklichkeit gibt“ oder je gab; stattdessen staffieren Gesellschaften ihre Realität „mit bestimmten Bedeutungsmustern aus, erkennen bestimmte Sichtweisen auf diese Umwelt als Wissen an (während andere als Aberglaube oder Unsinn abqualifiziert werden)“ (Landwehr 2008, 18f). Das führe dazu, so Landwehr weiter, dass eine vermeintliche Wirklichkeit als naturgegebene Tatsache akzeptiert wird und nicht als jene individualisierte, kulturzentristische Lesart der Welt, die sie eigentlich ist (vgl. Landwehr 2008, 19). Auch Niklas Luhmann hielt fest, dass das Kommunizieren über etwas diesem Etwas Relevanz verleiht. Dabei führt der Systemtheoretiker aus, dass solche Sinnzusammenhänge innerhalb ihres jeweiligen Systems – beispielsweise der Massenmedien – Gültigkeit besitzen, ohne dass sie zunächst Dependenz zur Wissenschaft oder anderen Umweltfaktoren aufweisen (vgl. Luhmann 2017, 53). Das bedeutet für Landwehr, dass Diskurse Mechanismen zur „Formung eines historischen Bewusstseins“ sind. Das vermeintliche Wissen über Tradiertes, über vorausgegangene Generation oder nur über zwei Monate zurückliegende Ereignisse ist bestimmt durch die Kommunikation über diese Vergangenheit, schlägt sich aber fortlaufend auf die Selbstwahrnehmung einer Gesellschaft nieder (Landwehr 2008, 148). Gleichzeitig schließt diese Erkenntnis ein, dass gesellschaftliche Konstruktionen durchaus falsch sein können – und mithin die Identität, die aus ihnen hervorgeht (vgl. Landwehr 2008, 153). Deshalb geht die historische Diskursanalyse nach Landwehr vorrangig der Frage nach, wieso sich Realitäten regional und temporal unterschiedlich ausprägen und welche Umstände dazu führten, dass sich gewisse Sichtweisen,

Argumente, Wahrnehmungen, politische Systeme oder auch Produkte etablieren konnten und andere Entwürfe wiederum zerfielen (vgl. Landwehr 2008, 19).

Wenn daher im weiteren Verlauf dieser Analyse von Kultur und Security Culture im Speziellen die Rede ist, wird sich diese Rekursivität zwischen Wahrheit und Diskurs erneut zeigen. Reiner Keller unterscheidet aus diesem Grund zwischen dem Ereignis, das den Diskurs initiiert und dem allgemeinen Narrativ über dieses Geschehen, das vom Ereignis abweichen kann. Er konstatiert, dass der „Kollektivvorrat an Mythen, allgemein bekannten Geschichten und verfügbaren Deutungsmustern“ vorausgehen muss, einen Vorfall oder einen Sachverhalt erlebbar zu machen und die Einstiegshürde für die Teilnahme herabzusetzen (Keller 2005, 302). Demnach ist nicht die Frage entscheidend, ob die Wahrheit den Diskurs bedingt oder der Diskurs die Wahrheit erst ausbildet. Denn Keller schafft hiermit eine Art klare Unklarheit, wenn er das inhärente Durcheinander interpersoneller Kommunikation hinnimmt, ohne gleichzeitig eine Rangfolge zu reklamieren.

Mit dieser Gleichwertigkeit von Diskurs und Wahrheit im Hinterkopf gelangt man bald zu der Einsicht, dass das wohl bedeutendste Werkzeug zur Betrachtung eines Diskurses die Frage ist. Mittels folgender exemplarischer Fragen unternimmt Reiner Keller den Versuch, den Diskurs zu formalisieren (Keller 2005, 257f):

- „Wie, wo, mit welchen Praktiken und Ressourcen wird ein Diskurs (re-)produziert?“
- „Welches Wissen (Deutungen und Problemlösungen) wird also erzeugt und verbreitet?“
- „Wer ist Träger, Adressat, Publikum des Diskurses?“
- „In welchem Verhältnis steht der Diskurs zu anderen zeitgenössischen oder historischen Diskursen?“
- „Wie verhalten sich soziohistorischer Kontext, diskursive Felder, Diskurse, Praktiken und Dispositive zueinander?“

Diese Fragestellungen artikulieren den Kern der Diskursanalyse. Es ist ein Vorhang-lüftendes Instrument, um das Verstehen von Debatten, Streitpositionen sowie kulturellen Strömungen auszuarbeiten sowie Diskurse erfassbar und konkludent zu machen. Mittels der Diskursanalyse lässt sich illustrieren, wie sich in einem Wechselspiel aus Hall und

Widerhall, aus These und Antithese, aus Aktion und Reaktion, Resonanz produziert und welche Diskrepanzen sich zwischen ausgewählten Vergleichsobjekten auftun. Es geht nicht nur darum, den Inhalt einer Nachricht zu deuten, sondern ihn zu dechiffrieren, „wie und von wem [etwas] geäußert wird, wann und unter welchen Umständen und zu welchem Preis“ (Auerbach et al. 2019, 707). Das schließt sogar ein, „was nicht geäußert wird oder nicht geäußert werden kann“ (Auerbach et al. 2019, 707).

Die Diskursanalyse beruft sich unter anderem auf spezifische Diskurstypen. Mit dem Risikodiskurs etwa führt Reiner Keller aus, dass Diskurse über Risiken oder Katastrophen nur funktionieren, wenn rund um diese Ereignisse Geschichten erzählt werden, sodass diese für „ein nicht unmittelbar anwesendes Publikum erfahr- und verstehbar“ werden und ein variables Maß der Empathie hervorrufen (Keller 2005, 303). Dabei spielen, so Keller, insbesondere Massenmedien eine bedeutende Rolle, da sie – begründet in ihren verschiedenen Agenden – teils sehr divergierende Erzählungen und Bewertungen vornehmen (vgl. Keller 2005, 303). Das ist insofern eine verantwortungsvolle Funktion von Medien, als „die gesellschaftliche Resonanz der Diskurse über ein katastrophisches Ereignis [...] die von ihm ausgehenden Wandlungsimpulse“ maßgeblich dirigiert (Keller 2005, 304). Sicherheit wurde in den vergangenen Jahrzehnten immer dann zu einer relevanten Größe, wenn äußere, zumeist unkontrollierbare Anomalien in weiten Teilen moderner, transnationaler Gesellschaften Angst oder mindestens Beunruhigung hervorriefen. Dabei ist nicht die Art der Bedrohung selbst ausschlaggebend, sondern vielmehr das damit verbundene Unbehagen, egal ob objektiv angebracht oder völlig irrational. Die Terroranschläge vom 11. September 2001, die Reaktorkatastrophe in Fukushima oder das Corona-Virus: Die Bedrohungslage war in allen Fällen völlig verschiedenartig. Der darauffolgende Ruf nach mehr Sicherheit aber eint diese Szenarien (vgl. Müller 2012, 223f). Die Sehnsucht nach Sicherheit schlägt sich dann nieder, indem einerseits die Bevölkerung ihren Bedarf an den Staat richtet und von diesem verlangt, die akute Gefahr zu beseitigen oder eine Wiederholung zu vereiteln. Andererseits kann eine Sicherheitsdebatte, beispielsweise infolge eines gewaltsamen Attentats, ein politisches Instrument zur Aggregation von Wählerstimmen und zur Stärkung von Polizei und Militär sein. Polizeibehörden oder Geheimdienste nehmen in derartigen Zeiten exponierte Stellungen in der medialen Öffentlichkeit ein und die Legitimierung staatlicher Exekutiven wird zu einem Leitmotiv strategischer Kultur. Es ist die Entdeckung neuer Gefahren, die das

Verständnis von Risiken begründet und neue „Perspektiven, Mechanismen und Institutionen zur Überwindung der Unsicherheitskonstellation“ ermöglicht (Miller 2015, 284).

Man stellt also fest, dass die Zeitdimension ein wichtiges Kriterium zur Herstellung des Vergleichs von graduell inkonstanten Systemen darstellt. So war das Sicherheitsempfinden westlicher Gesellschaften am 10. September 2001 ein völlig anderes als ab dem Folgetag oder als heute. Politikwissenschaftler wie Paul Pierson oder Elizabeth Cohen messen der Zeit eine zentrale Bedeutung bei der Betrachtung von Phänomenen, sozialen Gruppen oder Diskursen bei.

We cannot see or feel a date on a calendar, or a deadline on a schedule, in the same way that we might be able to see armed guards standing in a row or feel razor wire installed in the ground. But the date and the deadline can divide people and political power at least as effectively as the armed guard or the fence (Cohen 2018, 30).

Die Zeit scheint offenkundig ein entscheidendes Substanzkriterium gesellschaftlicher und schließlich kultureller Debatten zu sein. So ereignete sich die Nuklearkatastrophe von Fukushima am 11. März 2011. Die unmittelbare Berichterstattung im deutschsprachigen Raum hielt, trotz der Schwere des Unglücks, nur etwa bis zum Sommer des gleichen Jahres an. Zu diesem Zeitpunkt führte die deutsche Öffentlichkeit eine Debatte über den Atomausstieg und beschloss Veränderungen. Weiterhin bestehende Probleme mit alten Kernkraftwerken, der Entsorgung von radioaktivem Material oder dem erst 2022 abzuschließenden Ausstieg behandelte die Presse im Nachgang unregelmäßig. Damit soll an dieser Stelle nicht bestritten werden, dass bis dato gelegentlich Berichte oder Reportagen über Fukushima publiziert werden. Quantität und breite Wahrnehmung haben jedoch unzweifelhaft abgenommen. Das führt vor Augen, dass Sicherheitsdiskurse dann schnell und wirksam vorangetrieben werden, wenn die Gefahr unmittelbar im Gedächtnis verankert ist (Abbildung 1: Moment B) oder in seltenen Fällen in unvermeidlicher Sichtweite liegt (Abbildung 1: Moment A).

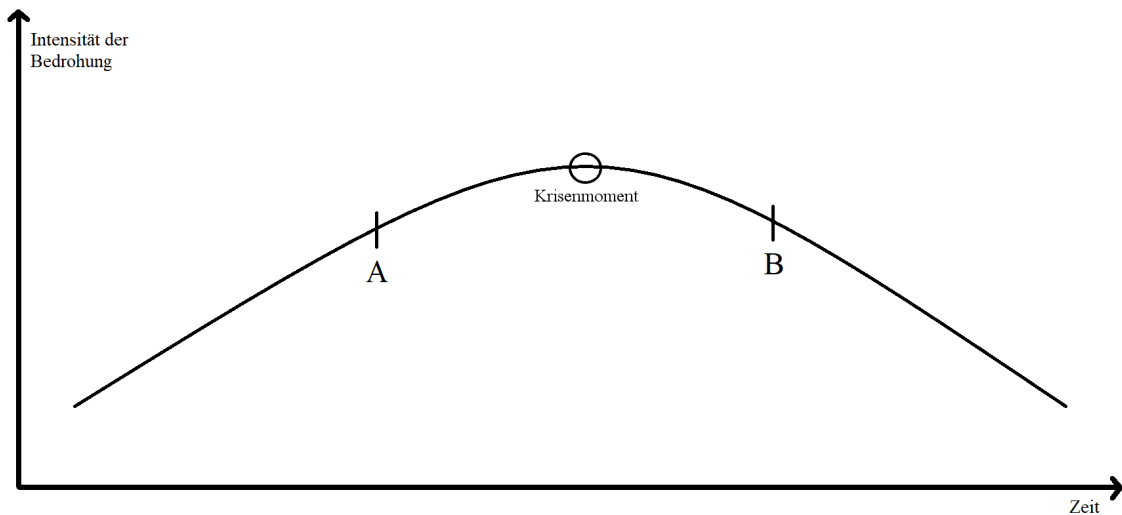


Abbildung 1: Debattenmomente, eigene Darstellung

In diesen drastischen Momenten entstehen neue Regelungen, politische wie strategische Kultur begegnen sich und Überzeugungen verändern sich. In ihrer Untersuchung der Medienberichterstattung in Deutschland während der ersten drei Monate nach dem 11. September stellt Michaela Maier ähnliches fest: Während die Berichterstattung unmittelbar nach dem Ereignis anschwillt, nimmt sie bereits nach einigen Tagen wieder eklatant ab und wird nur durch konsekutive Ereignisse, wie der Operation Enduring Freedom vom 7. Oktober, gelegentlich erneut angefacht (vgl. Maier 2003, 16f).

Die Zeit ist folglich ein entscheidendes Kriterium für das gemeine Empfinden von Gefährdung wie auch für das Begehren nach Sicherheit. Epochale Ereignisse nehmen eine strukturelle Position ein und sind somit nicht nur Glieder in einer kausalen, sondern ebenso in einer chronologischen Kette (vgl. Zerubavel 2012, 12).

[...] [T]ime and space are involved in the formation, or reformation, of conceptual, material and social orders, thereby helping to explicate such pervasive shifts in consciousness as the Reformation, the Enlightenment, decolonization, globalization, racial and sexual emancipation, and modernity itself (Jasanoff 2015a, 14).

Der Zeit kommt soziopolitisch zugleich eine ordnende wie auch eine distinguierende Bedeutung zu (vgl. Cohen 2012, 33). Sie vermittelt Stabilität, beispielsweise indem Strukturen und Institutionen auf mehrere Jahre oder gleich Dekaden angelegt werden. Indes lässt Zeit Trends und Ären zumeist vergehen, sodass retrospektiv Demarkationslinien sichtbar werden. Dieser Annahme folgend unterliegen Krisenerlebnisse und die einhergehende Sicherheitskommunikation einer klaren temporalen Reglementierung und sortieren sich zielsicher um ein konkretes Ereignis,

indem sie „den gesamten Verlauf von der Prävention über proaktive Maßnahmen bis hin zur Reaktion“ durchlaufen (Giebel 2014, 367). Überdies haben die aus den Diskursen erwachsenden Sicherheitsüberlegungen eine unveränderliche Wirkrichtung: Wie schon in den einführenden Worten zur Sicherheit erläutert, kann Sicherheit nur für eine noch herzustellende Zukunft produziert werden. Das Wissen um eine mögliche Wiederholung der Gefahr, die Unzulänglichkeit der Präventivmittel und die infolge der Bedrohung veränderten Umstände machen eine progressive Adaptierung von Sicherheit dann zwingend erforderlich.

Mit der Zeitabhängigkeit eines Sicherheitserlebens ist die Schwere des erwartbaren oder zu beseitigenden Schadens untrennbar verwoben. Alle oben vorgebrachten Beispiele waren zweifellos radikale Katastrophen, jedoch mit unterschiedlichen Wiederholungswahrscheinlichkeiten. Während eine globale Epidemie nur in enormen zeitlichen Abständen auftritt und auch Reaktorkatastrophen dieser Größenordnung bisher selten geschahen, sind Terroranschläge ein vergleichsweise häufiges, wenn auch regionales Phänomen. Trotz dieser auseinandergehenden Bedrohungsniveaus zielt ein beträchtlicher Teil der Sicherheitskultur auf die Frage: Wie verhindern wir das erneute Unglück? Die Beantwortung dieser Frage wird laut W. Penn Handwerker lediglich nach einer Abwägung von Kosten und Nutzen zur Vorbeugung eines mutmaßlichen Schadens vorgenommen (vgl. Handwerker 2009, 92). Stochastische Annahmen werden jedoch in drängenden Sicherheitsdiskursen hintangestellt. Das bedeutet, die Furcht vor dem Risiko wiegt schwerer als das Wissen um die Unwahrscheinlichkeit der Wiederholung. Nach den Terroranschlägen von New York, um bei den erwähnten Beispielen zu bleiben, bestand in den Vereinigten Staaten große Einigkeit: Die USA verschärften Gesetze, ermächtigten Sicherheitsbehörden und zogen in den folgenden Jahren in verschiedene militärische Auseinandersetzungen – ausgelöst durch die vermeintlich unbeherrschbare Bedrohung von außen (vgl. Landeszentrale für politische Bildung Baden-Württemberg 2005). Die emotionale, öffentliche Debatte in den USA tendierte zu Uniformität: „Intense selection pressure makes for cultural uniformity. Little or no selection pressure makes for cultural diversity“ (Handwerker 2009, 94). In diesem Fall offenbarte sich der Druck sogar als besonders groß, sodass die UNO eine Anti-Terror-Resolution beschloss und auch Deutschland tiefgreifende sicherheitspolitische Veränderungen erließ. Darunter befanden sich die Abschaffung des sogenannten Religionsprivilegs im Vereinsrecht, die Einführung intensiver Kontrollen vor Flugreisen

oder die signifikante Expansion der Befugnisse von Verfassungsschutz und Bundesnachrichtendienst (vgl. Welt 2011). Die Anschläge aus dem Jahr 2001 führten offenbar zu einer Provokation des gesamten NATO-Raums. Diese wiederum äußerte sich, wie auch bei den anderen genannten Fällen, in schnell erarbeiteten Maßnahmenpaketen, die vermeintliche Sicherheit vor einer nicht gänzlich abzusehenden Gefahr gegen Freiheiten oder mindestens Komfort eintauschten, ohne entscheidende publike Gegenwehr (vgl. Schaar 2017, 197). Michael C. Frank beschreibt, den Blick auf Derrida gerichtet, ein Trauma, dessen Veranlassung nicht in dem vergangenen Ereignis in Manhattan bestand, sondern in der induzierten Angst vor einer Wiederholung oder Eskalation des Erlebten in der individuellen, baldigen Erfahrungswelt (vgl. Frank 2019, 137). So ist anzunehmen, dass neben dem Faktor Zeit und der Qualität der Bedrohung ebenso die geografische wie auch die emotionale Nähe zu Geschehnissen, Tätern oder Opfern eine bedeutende Rolle für die Wahrnehmung von (Un-)Sicherheit spielen (vgl. Giebel 2014, 367).

Ähnliches stellt die Publizistik mit der Nachrichtenwerttheorie fest, die wesentlich Lippmann, Schulz oder Ruge vorantrieben und ihre Wurzeln im frühen 20. Jahrhundert hat. Zwar bezieht sich diese Theorierichtung nicht per se auf Bedrohungen; jedoch bildet Berichterstattung und die Auswahl des Relevanten ein zentrales diskursives Element für die Perzeption von Gefahr. Die Nachrichtenwerttheorie beschreibt sogenannte Nachrichtenfaktoren, zu denen unter anderem ‚Zeit‘, ‚Nähe‘ oder ‚Prominenz‘ zählen. Dabei verstärken sich die Nachrichtenfaktoren additiv. So reicht es nicht, dass ein Ereignis heute oder in räumlicher Nähe geschehen ist. Treffen diese zwei Faktoren jedoch zusammen, erhöht sich das publizistische Interesse eventuell bereits. Kepplinger erweitert den Nachrichtenwert um Selektionskriterien, da Nachrichtenfaktoren allein ihm zufolge nur „die Merkmale der zu selektierenden Objekte“ wiedergeben, nicht aber „die Kriterien der Selektion“ (Kepplinger 2011, 62). Berechtigterweise führt Kepplinger nämlich an, dass sich Selektionskriterien mit der Zeit wandeln „und mit ihnen vergrößern oder verringern sich die Publizitätschancen von Meldungen, die die entsprechenden Nachrichtenfaktoren aufweisen“ (Kepplinger 2011, 64).

Nach Reiner Keller können solche Unsicherheitsrezeptionen mittels zweier Kategorien von Risikodiskursen stimuliert werden. Rundum unter anderem terroristische Anschläge oder epochale Naturkatastrophen sind Gefahrendiskurse

vorherrschend: Die Akteure dieser öffentlichen Konversation neigen dazu, die Gefahr wiederholt zu erzählen und sie über Repetition, aber auch durch rhetorische Ausschmückung, zu überzeichnen. Der Gefahrendiskurs stilisiert ein „Ereignis zum Symbol“ und greift auf Narrative zurück, die mithilfe von „ästhetischer Inszenierung“ zielorientierte Botschaften zulassen (Keller 2005, 305). Demnach kreisen diese Debatten häufig um Schuldzuweisungen und Feindbilder. Infolge der Terroranschläge 2001 bildete die US-Regierung klare Täter- und Opferrollen aus. Mit Al-Qaida identifizierte man Schuldige, die die bis dahin angenommene Kontrollsituation ins Wanken gebracht hatten (vgl. Landeszentrale für politische Bildung Baden-Württemberg 2005). Der Terrorismus wurde unter anderem durch US-Präsident Bush, das transatlantische Empathievermögen und die mediale Fokussierung zu einer der größten Bedrohungen der frühen 2000er-Jahre stilisiert. Bush formierte insbesondere innerhalb der NATO ein antiislamisches, antiafghanisches und zugleich proamerikanisches Milieu, das eine Intervention in Afghanistan zur Bekämpfung der Taliban schließlich legitimierte. In der Phrase „War on Terrorism“ kumulierte das Weiße Haus in den folgenden Jahren das Motiv jeglichen politischen Handelns und entmenslichte die anhängigen Schicksale mit dem substanzlosen Konzept. Nicht nur, dass die US-Regierung damit Terrorismus zu einer Form der asymmetrischen Kriegsführung erklärte. Die Vereinigten Staaten konnten mithilfe dieser simplen *Sie gegen uns*-Erzählung einen rechtmäßigen Krieg führen, der zugleich der Prävention als auch der Vergeltung dienen sollte (vgl. Schneckener 2003, 4f). Nur zwei Jahre später zeigte sich, dass Gefahrendiskurse ebenso bereits vor dem konkreten Eintreten einer Bedrohung reale Effekte haben können: So führte die US-Administration mit dieser Form der skandalisierenden Kommunikation einen Präventivkrieg gegen den Irak, weil sie das „Bedrohungspotenzial irakischer Vernichtungswaffen“ fingierte (Spiegel.de 2016). Damit ist der Gefahren zentralisierende Diskurs ein wirkungsvolles Werkzeug, um die subjektive von der objektiven Bedrohungssituation zu entkoppeln und so ideologische oder politische Agenden zu forcieren.

Demgegenüber steht gemäß Keller der Kontroll- oder Normalisierungsdiskurs. Diese diskursive Praxis dient im Gegensatz zum Gefahrendiskurs der „Entverantwortlichung von beteiligten Entscheidungsinstanzen“, indem Unsicherheiten als seltene Unglücke respektive außerordentliche Fehlritte bewertet oder indem sie zur neuen Ordinarität deklariert werden (Keller 2005, 304). In solchen Debatten ist dann die vermeintliche

Unvorhersehbarkeit schuld – man war also gar nicht in der Lage, das Unheil zu verhüten. Ein solcher Kontrolldiskurs ließ sich beispielsweise 2015 nach dem Absturz des Germanwings-Flugs 9525 in den französischen Alpen beobachten. Politiker und Lufthansa-Verantwortliche drückten ihr Mitgefühl aus, der Vorfall selbst wurde jedoch als bedauerlicher Einzelfall stigmatisiert. Germanwings gab zwar zu, von der psychischen Erkrankung des Co-Piloten gewusst zu haben, die Debatte verschob sich jedoch auf die allgemeine Notwendigkeit psychologischer Tests für Piloten und auf den verbauten Sicherheitsmechanismus der Cockpit-Tür (vgl. WDR 2020b). Abschließend stand die wesentliche Forderung im Raum, Piloten künftig regelmäßig zu untersuchen. Mit dieser Fußnote lag die Diskussion nicht mehr bei der Person des Co-Piloten und genauso wenig bei der Lufthansa oder den Flugaufsichtsbehörden. Vielmehr entstand der Eindruck, das Unglück sei nicht abwendbar gewesen. Die Forderungen nach neuen technischen Sicherungen und engmaschigen medizinischen Überprüfungen hatte die Funktion, die zuvor als gegeben betrachtete Kontrollsituation wiederherzustellen, sodass die „angeschlagene institutionelle und symbolische Infrastruktur restabilisiert“ werden konnte (Keller 2005, 304f).

Schließlich lässt sich festhalten, dass Sicherheit und die umgebenden Diskurse dann am intensivsten geformt werden und das öffentliche Leben bewegen, wenn das bedrohliche Ereignis sowohl zeitlich wie räumlich in der Nähe liegt, ein erhebliches, fundamentales Unheil darstellt und eine nachvollziehbare Dramaturgie liefert. Liegt die Gefahr einige Monate in der Vergangenheit oder war sie nur begrenzt bedrohlich, fällt die anschließende gesellschaftliche Reibung deutlich geringer aus. Dabei entscheidet die Schwere eines Ereignisses erkennbar darüber, ob das Motiv wenige Wochen oder mehrere Jahre vorrangig diskutiert wird oder sich gar in Institutionen materialisiert. Die zuletzt angestellte Differenzierung nach Keller zwischen Gefahren- und Kontrolldiskurs dient als Beitrag zur Analyse der diskursiven Charakteristika, ganz besonders in der Dualität. Beide Diskurstypen treten nicht in akkurater Exzision auf, sondern können abhängig von der individuellen Subjektwirklichkeit oder politischen Lagerzugehörigkeit für Einzelne variieren. Auf diese Weise bäumen sich hybride oder gar konfligierende Sicherheitsdiskurse auf (vgl. Keller 2003, 409). Gemein haben beide Formen des Sicherheitsdiskurses, dass sie als Narrationen funktionieren. Jene, die die Hoheit über die Erzählung haben, bestimmen Protagonisten und Antagonisten, identifizieren ein zu bekämpfendes Problem und stellen einen positiven Ausgang in Aussicht – eine

klassische Heldenreise nach griechischem Vorbild, mit Skandalisierungspotenzial, Emotionalität und aussichtsreichen Verkaufschancen (vgl. El Ouassil/Karig 2021, 55). Somit lassen die Gefahren- und Kontrolldiskurse nach Keller trotz – man könnte auch sagen wegen – ihrer hybridisierenden Disposition Aussagen zum Beispiel über die soziale Stabilität, politische und gesellschaftliche Prioritätensetzung oder über substanzielle Kollektivängste und Mythen einer Gemeinschaft zu.

III.II. Transkulturell vergleichen

Wenngleich der anschließende komparative Prozess staatlich geprägt ist und sich damit in gewisser Weise innerhalb erkennbarer territorialer Räume bewegt, so stellt die staatliche Distinktion nur eine Ebene der Vertiefung dar. Denn zugleich muss der Vergleich moderner, globalisierter Medienkulturen immer ein transkultureller und damit grenzüberschreitender sein. Andreas Hepp erklärt diese Parallelität so, dass sich zeitgenössische kulturelle Ausprägungen nicht mehr an geografische Gegebenheiten binden, sich stattdessen frei von diesen verbreiten, ohne regionale Erscheinungsformen zwangsläufig zu unterminieren (vgl. Hepp 2011, 132). Damit versucht er, „die Binarität eines internationalen und interkulturellen Ansatzes [zu überwinden], ohne den Staat und die Nation als mögliche Bezugspunkte des Vergleichs auszuschließen“ (Hepp 2011, 132). Hepp weist damit auf die eigentlich offenliegende Tatsache hin, dass Kulturen selbstverständlich nicht an Landesgrenzen enden und jenseits des Limes ein neuer Kulturraum beginnt. Ganz im Gegenteil kann man von Deterritorialisierung sprechen. Das bedeutet, „dass viele der gegenwärtigen kulturellen Formen sich nicht mehr konstitutiv auf bestimmte Territorien beziehen lassen“ (Hepp 2011, 132). Glücklicherweise bieten sich neben staatlicher Grenzen noch weitere Differenzierungsmarker an: „Cultuur [...] is altijd een collectief verschijnsel, in meerdere of mindere mate gedeeld door mensen die leven of leefden in dezelfde sociale omgeving: de plaats waar deze cultuur werd verworven“⁷ (Hofstede/Minkov 2016, 17). Wenn also im Folgenden vom Deutschen oder Niederländischen die Rede ist, schwingt zwar auch der jeweilige Staat mit, jedoch markiert dies vielmehr Kulturräume. Eine niederländische Kultur endet nicht nach Enschede und in Gronau fängt eine erkennbar deutsche Kultur an, sondern die Umgangsformen, Traditionen und Mentalitäten

⁷ Deutsch: Kultur ist mehr oder weniger immer ein kollektives Phänomen, in mehr oder weniger ausgeprägtem Maße von Menschen geteilt, die in derselben sozialen Umgebung leben oder lebten: dem Ort, an dem diese Kultur erworben wurde.

assimilieren einander, sodass fließende Räume entstehen. Vielmehr noch sind diese Räume oft nicht mehr zu lokalisieren, da Globalisierung und Leitmedien die „nationalen Container“ aufbrechen (Hepp 2011, 132).

Dieser Doppelperspektive schreibt er dann zu, dass sie eine umfassendere Untersuchung ermöglicht und Ergebnisse jenseits nationaler Kategorien hervortreten (vgl. Hepp 2011, 133). Diese Annahme liegt auch bei der folgenden Untersuchung zugrunde. Die nationalen Maßstäbe sind Grenzziehungen, hinter denen mindestens abweichende Gesetze gelten und soziohistorische Prägungen vorliegen (vgl. Jasanoff 2015a, 26). Sie sind das Mittel zur bedingten Pauschalisierung, die unbedingt notwendig ist, um Aussagen über ein Kollektiv zu treffen.

Für den Vergleich von Kulturen oder von kulturellen Eigenschaften sind grundsätzlich Gemeinsamkeiten erforderlich, mit deren Hilfe die Eigenschaften in Beziehung gesetzt werden können. Der Vergleichsgegenstand wird methodisch als ein bestimmtes hypothetisches Konstrukt gefasst, welcher einer bestimmten Denkstruktur, Gewohnheit oder Fähigkeit, kurz unseren Kollektivmerkmalen entspricht (Scheffer 2009, 27).

Gleichzeitig aber riegeln nationalstaatliche Gebilde nicht hermetisch ab, sondern lassen insbesondere in Europa Austausch und Kommunikation zu. Somit werden Deutschland und die Niederlande zwar als zwei Staaten betrachtet, jedoch stets unter der Prämisse, dass sich fortlaufende und wechselseitige kulturelle Interaktion vollzieht. „Fallen hingegen die vorgegebenen Grenzen zur räumlichen und terminologischen Kategorisierung von Kultur weg, verlieren kollektive Vergleiche ihre entschiedene Bezugsbasis“ (Scheffer 2009, 30). Nick Couldry bestärkt Scheffers Annahme, dass Rahmungen notwendig sind, um einen Vergleich durchführen zu können. Diese sind ihm zufolge nicht zwangsläufig abschließend, sondern nützen der intersubjektiven Verständigung auf vergleichbare Parameter (vgl. Couldry 2012, 157). Das bedeutet, dass sich die hier ergebenden Resultate auf regional wie kulturell definierte Räume beziehen. Während die Analyse die Permeabilität dieser Räume nicht ignoriert, stellt sie die gesellschaftlichen, grenzüberschreitenden Interferenzen nicht in den Mittelpunkt.

Zur Durchführung eines solchen wissenschaftlichen Vergleichs bieten sich diverse Forschungsdesigns an, die alle darauf abzielen, zwei oder mehr Objekte einander gegenüberzustellen. Die spezifischen Designs beschreiben dann die Auswahl der Vergleichsfälle, die Menge der Variablen oder den Einfluss externer Varianz. So widmet sich der schon zitierte Detlef Jahn in seiner *Einführung in die vergleichende*

Politikwissenschaft im Besonderen der Betrachtung von Staaten und legt dabei die möglichen Herangehensweisen zur vergleichsbezogenen Auswahl der Studiengegenstände dar. Jahn führt in seinen Erklärungen drei für diese Arbeit infrage kommende Ideen ein, von denen aber nur eine als tatsächlich zielführend identifiziert wird: die negative und positive Fallauswahl, die Konkordanz- und Differenzmethode sowie das *most similar* und *most different systems design* (vgl. Jahn 2013, 226).

Die negative beziehungsweise positive Fallauswahl ist die simpelste der drei Möglichkeiten. Bei der positiven Auswahl blickt man auf Einschlussaspekte, also zum Beispiel auf die geografische Lage oder die Population. In den allermeisten so ausgewählten Fällen kämen jedoch auch andere Fälle in Betracht, die dieses positive Kriterium ebenfalls erfüllen. Wie der Name nahelegt, funktioniert die negative Auswahl umgekehrt, ergo über den Ausschluss. Beide Ansätze führen entweder zu einer großen Grundgesamtheit oder im Fall weniger ausgewählter Vergleichsobjekte zum Anschein von Beliebigkeit. Dies wird selbst dadurch nur gemildert und nicht ausgeräumt, dass eine weitere positive oder negative Voraussetzung definiert wird (vgl. Jahn 2013, 234). Da die Forschungsfrage aber verlangt, mehr Kriterien anzulegen, scheidet die negative oder positive Fallauswahl aus. Die Konkordanz- und Differenzmethode setzen stattdessen voraus, dass der Forschende sowohl bereits die Resultate der unabhängigen als auch der abhängigen Variablen kennt. Er wählt dem folgend Fälle aus, die sich ähneln und dennoch abweichende Ergebnisse produzieren (Differenzmethode) oder er wählt Fälle, die sich grundlegend voneinander abheben und dennoch auf das gleiche Ziel hinauslaufen (Konkordanzmethode) (vgl. Jahn 2013, 240f). Diese Vorgehensweise bietet den Vorteil, ausgehend vom Ergebnis die Unterschiede oder Ähnlichkeiten der Fälle ermitteln zu können. Zugleich ist sie kaum generalisierbar und hat den entscheidenden Nachteil, dass sowohl der Fall als auch das Ergebnis in gewisser Weise bekannt sein müssen. So steht die Ursache für Abweichung oder Ähnlichkeit im Vordergrund.

Das *most similar systems design* setzt voraus, dass nur Systeme, im vorliegenden Forschungsdesign Länder, herangezogen werden, die sich ähneln. Aufgrund des ähnlichen Ausgangspunkts der Fälle ist davon auszugehen, dass diverse Kriterien ausgeblendet werden können, weil diese sich ohnehin decken (vgl. Jahn 2013, 237). Dementsprechend spielt es auf den kommenden Seiten zum Beispiel eine zu vernachlässigende Rolle, dass Deutschland Mitglied der NATO ist, da die Niederlande

dies ebenso sind. Gleichzeitig minimiert sich auf diese Weise die externe Varianz. Beides ist für den Vergleich der Cybersicherheitskultur hilfreich, da dies den Brennpunkt scharf stellt und unnötige Blickwinkel ausblendet. Daraus folgt, dass die Variablen konzentriert werden; das Ergebnis beruht also auf einer fokussierten Beobachtung. Die größte Gefahr dieser Arbeitsweise besteht wohl darin, dass die Ähnlichkeit der Fälle eine zu geringe Varianz der Ergebnisse nach sich ziehen kann (vgl. Jahn 2013, 237). Das bedeutet, dass es vorkommen kann, dass eine Untersuchung westeuropäischer Demokratien als Resultat hat, dass alle die Gleichheit von Mann und Frau, eine liberale Religionsausübung und die Meinungsfreiheit als grundlegende Werte festgeschrieben haben. Somit wären die unabhängigen Variablen, also die westeuropäische, geografische Lage und die Staatsform der Demokratie, nicht ausreichend, um Unterschiede zu entdecken. Wenn die Suche nach Differenzen im Vordergrund steht, wäre dieser Ansatz demzufolge sehr risikobehaftet.

Trotz dieser augenscheinlichen Schwäche und der geringen Fallzahl von zwei ist das *most similar systems design* dennoch der günstigste Entwurf zur Auflösung der Forschungsfrage. Die Reduzierung der externen Varianz und die überschaubaren unabhängigen Variablen stellen die abhängigen Variablen in den Mittelpunkt. Vereinfacht gesagt ist die Suche nach unterschiedlichen oder ähnlichen Handhabungen der identischen Problemstellungen von zentraler Bedeutung und weniger die sich gleichenden Voraussetzungen. Unterschiedliche unabhängige Bedingungen, wie die differierende Bevölkerungsgröße oder abweichende politische Gestaltungsprinzipien, rücken dann in den Vordergrund, wenn die übereinstimmenden Attribute ignoriert werden. Daher kann an dieser Stelle auch dem Postulat Jahns teilweise widersprochen werden, wenn er sagt, dass die abhängigen Variablen immer „möglichst stark variieren“ sollten (Jahn 2013, 237). Die minimierte Varianz der unabhängigen Variablen bei derart ähnlichen Systemen oder Staaten wie den Niederlanden und Deutschland ermöglicht vielmehr die Offenheit gegenüber dem Grad der Ergebnisvarianz. Hier greift die Weiterentwicklung des *most similar systems designs*, nämlich die *most similar systems with different outcomes*.

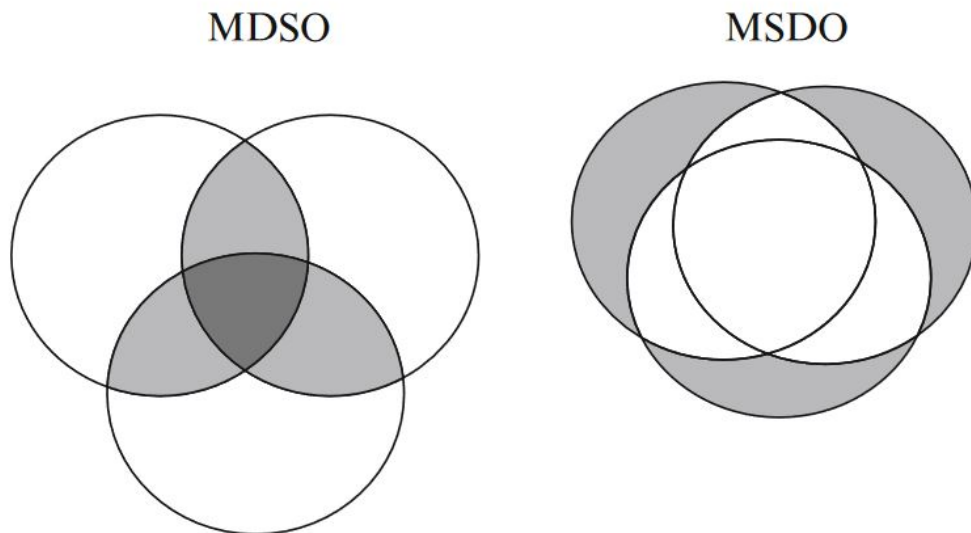


Abbildung 2: MDSO- und MSDO-Designs (Berg-Schlosser 2016, 9)

Bei *most similar systems with different outcomes* bleiben die Schnittmengen außer Acht und die Annäherung findet über die unterschiedlichen Ergebnisse statt (vgl. Berg-Schlosser 2016, 9). Wo liegen bei aller Ähnlichkeit die Unterschiede und warum produzieren derart ähnliche Strukturen differierende Resultate?

Da zum Beginn dieser Untersuchung nicht vollends abzusehen ist, inwieweit sich die deutsche und niederländische Umsetzung von IT-Sicherheit ähneln, wird diese Unbekannte erst zum Anlass des Vergleichs. Diesem qualitativen Ansatz kann zwar gegebenenfalls seine Generalisierbarkeit abgesprochen werden, jedoch nicht seine Wirksamkeit bei der Offenlegung von Zusammenhängen und Kontrasten (vgl. George/Bennett 2005, 33).

III.II.I. Beobachtungsebene

Zu genau diesem Zweck werden an dieser Stelle notwendige Festlegungen der verlustärmsten Beobachtungsebene und der anzulegenden Vergleichskriterien getroffen. Doch dazu muss deutlich sein, was unter der Beobachtungsebene zu verstehen ist. Eine treffende Determinierung ergibt sich aus der wissenschaftlichen Intention: „[...] [T]here is no way of exhaustively mapping the media cultures of the world: the point instead is to get a clear sense of the significant differences that shape their endless variety“ (Couldry 2012, 160). Dem folgend ergibt sich die Ebene der Betrachtung aus den Schnittstellen und Differenzen der fokussierten Objekte. Wenn diese Unterschiede das Ziel sind, so muss die Beobachtungsebene so bemessen sein, dass die maßgebliche Spannweite zu sehen ist. Detlef Jahn fordert in einem Beispiel ganz konkret, dass man

Parteiprogramme untersuchen sollte, um Positionen politischer Parteien zu identifizieren und dazu nicht die Wähler zu befragen seien (vgl. Jahn 2013, 186). Eine Befragung des Volkes würde zu einem abweichenden Ergebnis führen und nicht die tatsächliche Position der Partei widerspiegeln, sondern die Erwartungen oder Wünsche der Wählerschaft. Er appelliert folgerichtig, dass Beobachtungsebenen vorab festzulegen und stringent während der gesamten Forschungsarbeit einzuhalten sind. In diesem Fall, in dem die Cybersicherheitskulturen in Deutschland und den Niederlanden nebeneinander stehen, ist zur korrekten Bemessung der Beobachtungsebene eine funktionale Auflösung zu wählen. Mit anderen Worten ist es zu diesem Zweck wenig förderlich, die Satzungen einzelner IT-Sicherheitsinitiativen zu sichten oder zu schauen, wie es um die Ausstattung der Schulen in Rheinland-Pfalz mit manipulationssicherer Informationstechnik bestellt ist. Die Beobachtungsebene muss stattdessen einerseits zielführend sein, also die passend dazu identifizierten Kriterien müssen sich der Forschungshypothese unterordnen. Andererseits muss die Skalierung auf beide Staaten anwendbar sein und für beide gleichartige Ergebnisse ermöglichen.

Nun lassen sich die Forschungsfragen eins und drei⁸ auf der Suche nach der korrekten Beobachtungsebene zunächst hintanstellen, entweder weil sie grundlegend theoretischer Natur sind oder weil sie teils auf den Resultaten der zweiten Frage fußen. Aus *Wie organisieren die beiden Länder IT-Sicherheit?* leitet sich dagegen bereits ab, dass die Betrachtung von Organisationsstrukturen im Kontext der IT-Sicherheit eine Beobachtungsebene anbietet. Nebenbei löst dieser Ansatz die Herausforderung auf, objektiv vergleichbare Größen zu finden. Jedoch ist damit noch nicht klar, welche Organisationsform, in welcher Zeitspanne oder unter welchen Rahmenbedingungen zu einer validen Aussage verhilft. Wenngleich der Institutionen- und Organisationsbegriff selbst im Folgenden noch präzisiert wird, ist schon hier festzuhalten, dass die akademische Auseinandersetzung anhand nichtkommerzieller, überregionaler, staatlicher Organisationen und Institutionen vorgenommen wird, die Cybersicherheit in den beiden Ländern in hohem Maße mitgestalten. Darunter sind etwa Ministerien, Ämter, Vorschriften, Notfallpläne, politische Positionen oder auch praktische

⁸ Zur Erinnerung: *Deutschland und die Niederlande verfolgen unterschiedliche Modi zur Synthese von Cybersicherheit.*

Daraus gehen nachstehende Fragen:

- 1) Was ist eine Cybersecurity Culture?
- 2) Wie organisieren die beiden Länder IT-Sicherheit?
- 3) Wie formatieren die Institutionen die Logik der Informationssicherheit?

Krisenreaktionen zu fassen. Denn der Staat mit all seinen Behörden, Gesetzen und Texten tritt im demokratischen Verständnis immer auch als Abbild diverser Kulturausprägungen hervor. So ist das Gesetz

eine Institution mit einer Bedeutung, ein Symbol, ein Mythos und eine normative Aussage mit einem Sinn, der eine Unzahl menschlicher Handlungen organisiert, eine Vorschrift, die mitten im Bereich des Möglichen eine Mauer zwischen Erlaubtem und Verbotenem zieht, einen Wen schafft und das gesamte Bedeutungssystem neu anordnet (Castoriadis 1990, 239).

Diese Annahme bedeutet, dass Konstellationen staatlicher Organisation Rückschlüsse auf die zugrundeliegenden Normen, Werte und Intentionen beispielsweise der Sicherheitskultur zulassen (vgl. Moravcsik 1997, 517). Betrachtet man daher, in welchen Scharnieren der Gesellschaft der Staat wirkt, beispielsweise durch Regulative, lassen sich Aussagen treffen, die einen internationalen Vergleich erlauben. Auf dieser Ebene ist es möglich, die jeweilige staatlich betriebene Cybersicherheitsstruktur herauszuarbeiten, sodass Schwerpunkte oder Auffälligkeiten hervortreten. An dieser Stelle sei erwähnt, dass Eigenheiten der deutschen Bundesländer, also unter anderem Gesetze oder parlamentarische Beschlüsse, weitestgehend außen vor gelassen werden und sich stattdessen der Blick auf die bundesweite Dimension richtet, um eine passgenaue Vergleichbarkeit herzustellen. Bemerkenswerte Kennzeichen können dann mit kulturellen Beobachtungen verknüpft werden, um eine Seite der IT-Sicherheitskultur herauszustellen. Denn in politischen Agenden werden Vorstellungen erschaffen, die ein wünschenswertes oder aber ein abschreckendes Bild der Zukunft schaffen, anhand dessen in der Gegenwart Maßnahmen rechtfertigt werden können. „Policy documents, no less than judicial opinions, can be mined for insights into the framing of desirable futures“ (Jasanoff 2015a, 27). Unabhängig davon, ob der Staat Urheber einer Idee war oder sie lediglich in ein politisches Aktionsprogramm gießt, setzt er somit die Agenda und zeigt eine Richtung auf, die die breite Medienöffentlichkeit dann wieder diskursiv verarbeitet.

Hans Simons stellt in seiner Arbeit über niederländische Identitätspolitik fest, dass Politik danach strebt, legitimiert und durchsetzbar zu sein. Daraus folgt er, dass Politik und Identität miteinander verbunden sein müssen, sodass schließlich Positionspapiere und politische Strategiedokumente Identität aufarbeiten und vollziehen.

What matters more is that in such official documents we may find an understanding of how governments envision national identity, and how it came

to be that it is this particular representation that is articulated and not another (Simons 2014, 59f).

Eine Untersuchung von Sicherheitskultur, die auf diesem Verständnis aufbaut, liest Staat, Regierung oder Politik als repräsentative Figurationen von Gesellschaft und Öffentlichkeit. Dabei können amtliche Bekanntmachungen oder Entscheide dieser Erwartung nicht vollends gerecht werden, sondern sie bilden auf parlamentarischer Ebene immer nur eine Teilmeinung des sozialen Spektrums ab und werden aus performativer Sicht von Menschen gemacht, die in ein oft bürgerliches, wohlständiges Milieu eingefasst sind. Entsprechend gilt es, diese Ausschnittshaftigkeit im Folgenden zu beachten, oppositäre Positionen zu berücksichtigen und die Ergebnisse als das zu werten, was sie tatsächlich sind; nämlich das Abbild einer gesellschaftlichen Teilmenge. Der 20. Deutsche Bundestag beispielsweise ist nach wie vor überwiegend akademisch, männlich und ohne Migrationshintergrund (vgl. Tagesspiegel 2021). Solche Gewichtungen disqualifizieren keinesfalls die Beobachtungsebene, müssen aber gleichwohl Beachtung finden. Dabei sei erwähnt, dass der Staat seit jeher ein artifizielles Konstrukt bildet, das als Werkzeug für die Fertigung von unter anderem Identität, Macht und Sicherheit fungiert.

So wird in der Regel von allen Beteiligten anerkannt, dass der Staat die Pflicht und das Privileg hat,

die Rahmenbedingungen der öffentlichen Sicherheit aufrechtzuerhalten, das staatliche Gewaltmonopol – verstanden als grundsätzliches Rechtsprinzip – einzufordern, Strafverfolgung und Rechtsprechung zu garantieren sowie den militärischen Schutz der Gesellschaft zu erhalten (Lange 2010, 337).

Diese Regeln zementieren Identität und Institutionen, indem sie allen Staatsbürgern auferlegt und zugleich von diesen gebilligt werden. Ebendarum bieten sich Organisationen, Gesetze und Strategien als Skalierungsmaßstäbe für die Beobachtungsebene an. Jedoch können diese politischen Utensilien, wie im Folgenden noch ausgeführt wird, nicht die einzigen Kennzeichen einer IT-Sicherheitskultur sein.

Diesbezüglich macht Hans Simons den wertvollen Vorschlag, der Methodik von Lene Hansen zu folgen, die ihre Beobachtungsebene sowohl über Intertextualität als auch über Genealogie absteckt. Diese beiden Dimensionen lassen sich mithilfe von vier Fragen so zuschneiden, dass schließlich eine nachvollziehbare und adäquate Beobachtungsebene gefunden ist. In Ihrem Review trägt Floyd diese wesentlichen Fragen zusammen: „What temporal perspective is being studied? How many events are

being studied? In which intertextual model/models is the discourse located? And, what is the number of selves (one or multiple) to be studied“ (Floyd 2007, 215)?

Beginnend also mit der Frage nach der historischen Perspektive, steht man zunächst vor der Wahl, ob ein Zeitpunkt oder eine Zeitspanne zu betrachten ist. Während der Zeitpunkt auch losgelöst von historischem Kontext oder Zukunftsfantasien betrachtet werden kann, birgt die Betrachtung eines Untersuchungsobjekts über einen definierten Zeitraum die Gelegenheit, Progression und Transformation zu beobachten und Verkettungen der zugrundeliegenden Ursachen zu deuten. Da auch Kultur nur im historischen Kontext sinnvoll zu betrachten und auch Sicherheit ein relatives, sich anhaltend mutierendes Konstrukt ist, kann die Wahl hier nur auf einen chronologischen Korridor fallen. Wie bereits vor einigen Seiten erläutert, reicht der Untersuchungszeitraum vom Januar 1991 bis zum Februar 2022; von der Gründung des BSI bis zum Angriff Russlands auf die Ukraine.

Die zweite Frage von Floyd zielt auf Hansens Suche nach den zu ergründenden Events respektive Ereignissen ab. In Fällen, in denen mehrere Ereignisse betrachtet werden – so wie hier – sind diese entweder über den identischen Zeitabschnitt verbunden oder sie sind durch die Fallkonstellation miteinander verwandt (vgl. Hansen 2006, 80). Bei der Wahl des adäquaten intertextuellen Modells bemerkt Simons, dass die drei Modelle nach Hansen ihren Erhebungsumfang stufenweise öffnen (vgl. Simons 2014, 58). Denn während Modell eins alleinig offiziell-amtliche Diskurse in den Blick nimmt, darunter öffentliche Verlautbarungen oder Erlasse, und Modell zwei dies um die breitere politische Debatte mitsamt der politischen Opposition und der Medienberichterstattung verlängert, inkludiert das dritte Modell auch popkulturelle Darstellungen und randpolitische Diskurse (vgl. Hansen 2006, 64). Für die vorliegende Studie findet Modell zwei Anwendung, weil hier vorwiegend politische Agenden, öffentliche Institutionen und mediale Resonanz in den Blick genommen werden. So zeichnet sich die Genese einer nationalen Cybersecurity Culture ab, ohne dass die Skala aufgrund unwesentlicher Aspekte zu groß gefasst ist. Weitere politische oder massenkulturelle Analyseobjekte, die für die Fragestellung nicht zielführend sind, werden somit wirkungsvoll ausgeblendet. Das heißt keinesfalls, dass solche Parameter keinen wissenschaftlichen Mehrwert bieten. Jedoch hat diese Arbeit den Anspruch, als mögliches Muster für ähnliche Vergleiche zu dienen, sodass das Forschungsdesign weniger auf Ganzheitlichkeit, sondern auf Signifikanz abzielt.

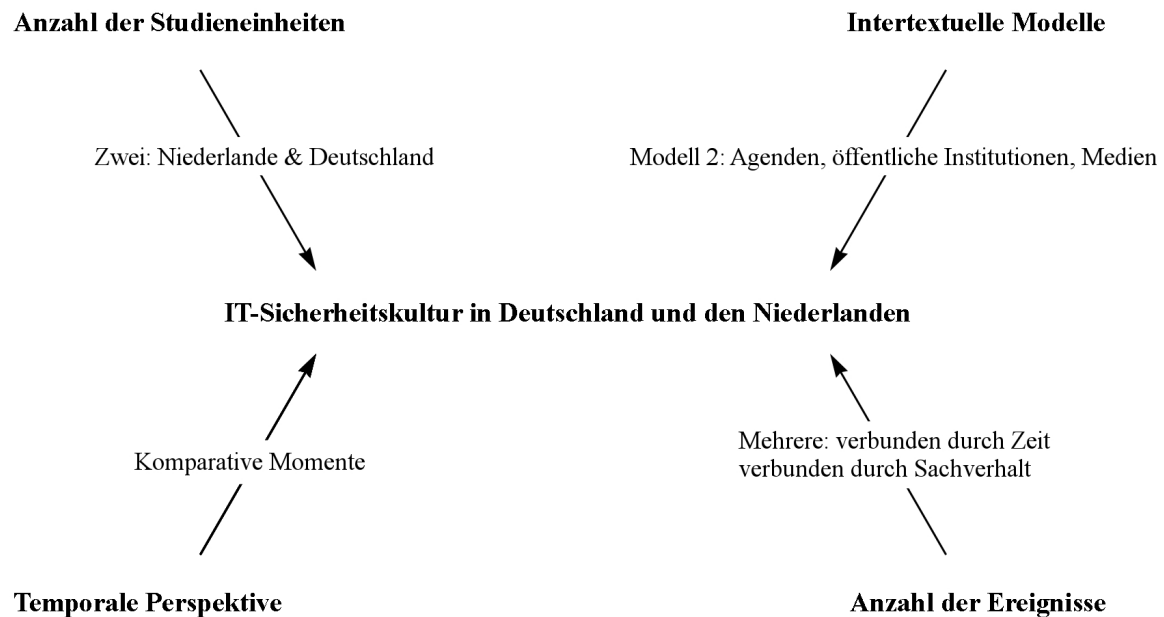


Abbildung 3: eigene Darstellung nach Hansens „Research designs“ (Hansen 2006, 81)

Die abschließende Suche nach der Auswahl der Studieneinheiten kann schon aufgrund des namengebenden Vergleichs kurz beantwortet werden. Es handelt sich um den wohl simpelsten Entwurf, da weder multiple Objekte ins Verhältnis gesetzt werden noch eine Entität in Abgrenzung zu allem Anderen analysiert wird (vgl. Hansen 2006, 76). Dagegen liegen mit den Niederlanden und Deutschland zwei geografisch, politisch, ökonomisch und historisch differenzierbare Referenzen vor. Bei beiden handelt es sich um souveräne Staaten, die damit formell auf dem gleichen Machtniveau agieren. Zudem begegnen sowohl Deutschland als auch die Niederlande mit der Unsicherheitsdeterminante des Digitalen den identischen technisch-sozialen Problemen und stellen damit zwei ebenbürtige Referenzpunkte dar (vgl. Hansen 2006, 77).

Diese vier Dimensionen definieren sowohl die Möglichkeiten als auch die Limitierungen der angelegten Analyse. Auf diese Weise verdichtet sich eine Beobachtungsebene, die es erlaubt, auf die Leithypothese⁹ adäquat einzugehen und ihr mit den passenden Instrumenten näherzukommen. Die geschilderte Disposition legt den Grundstock für die Reproduzierbarkeit und Intersubjektivität des Vergleichs, sodass die

⁹ Zur Erinnerung: *Deutschland und die Niederlande verfolgen unterschiedliche Modi zur Synthese von Cybersicherheit.*

folgenden Kriterien und Mechanismen der Untersuchung kritischer Überprüfung standhalten.

III.II.II. Kriterien des Vergleichs

Die Festlegung der Beobachtungsebene gibt den Grad der Skalierung, den Maßstab, an, sagt jedoch nur wenig darüber aus, welche Eigenschaften in den Blick rücken. Beschließt man beispielsweise, dass sich die Beobachtungsebene eines Vergleichs auf die Eigenschaften zweier Häuser erstreckt, ist dem Rezipienten noch nicht klar, welche Kriterien beziehungsweise welche Merkmale herangezogen wurden, um Unterschiede auszumachen. Wurde die Anzahl der Räume als Richtmaß genommen oder war es die Farbe der Fensterrahmen? Vielleicht hat man die verbaute Heizung betrachtet? Und wird zur Untersuchung ein Lineal, eine Waage oder gar ein Kompass benutzt? Um solche Unklarheiten vorneweg auszuschließen, müssen die Kriterien, die dem Vergleich zugrunde liegen, determiniert und zweckvoll kombiniert werden. Nur so kann ein Ergebnis entstehen, das nach wissenschaftlichen Prinzipien kausale Zusammenhänge offenbart und zugleich objektiv, verifizierbar und transparent ist.

Da auf den anschließenden Seiten der Versuch unternommen wird, zwei Staaten hinsichtlich ihrer Cybersicherheitskultur zu vergleichen und die Beobachtungsebene durch obige Dualitäten abgesteckt wurde, bleibt die Näherung an die Vergleichsattribute. So kommt auf den ersten Blick eine schier unendliche Zahl an Aspekten in Betracht, die als Kriterium dienen könnten: Beschäftigungs- oder Produktionssektoren, Population, Bildungsgrad, Wohlstand, Bevölkerungswachstum, Urbanisierung, Regierungsformen, Verfassungen oder Nationale Machtverteilung. Bei näherer Betrachtung zeigt sich dann, dass es sich bei diesen Kennzeichen um unpräzise Merkmale von Staaten handelt, die es ermöglichen, den politischen wie wirtschaftlichen Zustand eines Landes zu ergründen, aber nur bedingt zur spezifischen Fragestellung beitragen können.

Aufgrund der Vergleichsgestaltung nach dem *most similar systems design* können stattdessen diverse Kriterien beiseitegeschoben werden, da sie in beiden Ländern identisch sind. Allgemeine, übereinstimmende Eigenschaften werden im Verlauf der weiteren Untersuchung weitgehend außer Acht gelassen, da sie das Resultat des Vergleichs nicht prägen.

Zur besseren Nachvollziehbarkeit empfiehlt es sich, die relevanten Kriterien in zwei Ordnungen zu teilen. So kennzeichnen einige Attribute das Klima, in dem sich Cybersicherheitskultur verdichtet. Diese dienen der Draufsicht und erlauben grundlegende Schlussfolgerungen. Zu dieser Art der komparativen Betrachtung gehören vor allem Attribute staatlicher Organisation. Hier ist insbesondere der Unterschied zwischen dem niederländischen Einheitsstaat und dem deutschen Föderalismus auffallend. Gleiches gilt für die Größe der Länder, sowohl geografisch als auch demografisch, das Haushaltsvolumen oder den Umfang der verantwortlichen Behördenstrukturen. Um den Einfluss vergangener Ereignisse auf die gegenwärtige Strategie auszuloten, richtet sich der Blick außerdem auf zentrale sicherheitspolitische Erfahrungen der letzten Jahrzehnte. Aus diesen Parametern lassen sich wichtige Erkenntnisse über die zugrundeliegenden Rahmenbedingungen gewinnen, unter denen IT-Sicherheit jeweils produziert wird.

Dem schließt sich dann die zweite, handlungsorientierte Klassifizierung der Kriterien an. Hier stehen einander unter anderem die Cybersicherheitsstrategien Deutschlands und der Niederlande gegenüber. Dazu werden Gesetzestexte, Strategiepapiere und Lageberichte zurate gezogen. Auf diese Weise liegt offen, welche Bedrohungslage die jeweiligen öffentlichen Einrichtungen kommunizieren oder welche Akteure und Netzwerke, auch aus Wirtschaft und Zivilgesellschaft, von Bedeutung sind. Schließlich stehen diese strategischen Semantiken ihrer massenmedialen Resonanz gegenüber, sodass ein direkter Abgleich von politischer Aktio und ziviler Reaktio an die Diskursoberfläche tritt. Die Beobachtungsebene macht daneben weitere Kriterien erforderlich. So geben geförderte IT-Projekte und Großinvestitionen Aufschluss über den Aufbau der Sicherheitsarchitektur wie auch über bedeutende Akteure etwa aus der Privatwirtschaft. Exemplarische Diskursbetrachtungen verraten, ob das Themenfeld akademisch-exklusiv beziehungsweise partizipativ-fassbar behandelt wird. Nicht zuletzt geht aus den Texten und Medien hervor, ob das Hauptaugenmerk jeweils auf dem Schutz inländischer Strukturen und der Bevölkerung liegt oder ob die Staaten und ihre Akteure stärker darauf abzielen, international als Thought Leader aufzutreten und das außenpolitische wie ökonomische Gewicht zu stärken.

All diese Merkmale münden schließlich in einer „multiperspektivischen Kritik“, die den Blick für die Komplexität des Netzwerks öffnet, aus dem Cybersicherheitskultur jeweils hervorgeht (Hepp 2011, 137). Hepp spricht davon, dass die „Monosemierung dieser

Komplexität“ zu verhindern sei, denn das Ziel besteht im Gegenteil darin, die Multidimensionalität von IT-Sicherheitskultur in der Gegenüberstellung zu dechiffrieren (Hepp 2011, 137). Denn wie bereits eingangs erwähnt sind es Konstellationen äußerer wie innerer Faktoren – darunter stabile Variablen wie Wohlstand, Population, geografische Besonderheiten, aber genauso dynamische Variablen wie die Bedrohungslage oder Regierungskonstellationen – die den Stimulus für Sicherheitsempfinden, Agenda Setting oder Strategiewechsel setzen. Somit ist die zuvor gewählte Beobachtungsebene auch nach der Eingrenzung der gebotenen Kriterien passgenau, da sich Sicherheitspolitik, Institutionen, Regeln und Normen der Cybersecurity Culture auf diese Weise einfangen lassen. Dieses methodische Vorgehen markiert kulturelle wie politische Eckpfeiler Deutschlands und der Niederlande, die sich dann hinsichtlich ihrer Unterschiedlichkeit beziehungsweise ihrer Similaritäten studieren lassen.

III.II.III. Added Values des Sicherheitskulturkonzeptes

Die Erklärung der Vergleichskriterien hat offengelegt, dass die Hypothesen und Forschungsfragen immer wieder an den Punkt gelangen, an dem sich Dualitäten, teils Antinomien, auf tun: Versuchen Deutschland und die Niederlande den Status quo zu konservieren oder gehen sie mit progressiven Impulsen voran? Ist ihr Sicherheitsbestreben innen- oder außenpolitischer Natur? Übernimmt der Staat durch Regulation und Förderung die Verantwortung für die allgemeine Cybersicherheit oder bestimmt jeder Einzelne über die persönliche digitale Sicherheit?

Zusätzlich ist kaum zu bestreiten, dass IT-Sicherheit als Objekt kulturbildender Besprechung die Subkategorie eines holotischen Sicherheitsbegriffs darstellt. IT-Sicherheitskultur ist zugleich Bindeglied und Spannungsfeld zwischen Jung und Alt, Staat und Wirtschaft oder Autokratien und Demokratien. Jedoch kann eine Annäherung an den Kulturbegriff und damit auch an den Begriff der Sicherheitskultur nur so erfolgen, dass sowohl die Einfassung der Untersuchungsgegenstände in ihre Umwelt als auch die angelegte akademische Beobachtungsweise des Forschenden berücksichtigt werden. Dieser Blick unterliegt einer Chronik, ist bedingt durch Standpunkt und Fähigkeit des Betrachtenden und ist damit unausweichlich partiell subjektiv (vgl. Winter 2011, 425). Mittels der hier vorgestellten Kategorien kann die Sicherheitskultur daher mit einem objektivierenden Unterbau versehen und dementsprechend transparent sowie differenziert exploriert werden.

In ihren *Konjunkturen des Kulturbegriffs* erweitern Daase, Junk und Rauer die relationale Idee der Sicherheitskultur um binäre Aspekte, zwischen denen sich ihr Konzept bewegt. Dazu nennen sie die Pole *innen* und *außen*, *zivil* und *militärisch*, *Mikro* und *Makro* sowie *subjektiv* und *objektiv* (vgl. Daase et al. 2014, 47ff). Diese Binärpaare dienen jeweils der Veranschaulichung der Schnittstellenfunktion von Sicherheitskultur – nicht nur zwischen politischer und strategischer Kultur, sondern zugleich auch zwischen den genannten Oppositionen. Die Autoren stellen damit infrage, dass die oben skizzierte Vorstellung von politischer Kultur als Abbild der Bevölkerung und von strategischer Kultur als Repräsentation gesellschaftlicher Eliten ausreicht, um „die zukünftigen dringender werdenden Fragen nach einer demokratischen Sicherheitskultur zu beantworten“ (Daase et al. 2014, 52). Sie verfolgen mit ihrer Idee der Added Values die Absicht, bisherige Sicherheitskulturkonzepte zu verbinden, sodass sie realitätsgetreuer und präziser anliegen.

Vorherige Arbeiten von beispielsweise Geert Hofstede, Jacques Demorgon oder Edward Hall brachten zwar Modelle mit effektiven Kulturdimensionen hervor, jedoch entstanden diese Denkwerkzeuge aus einem spezifischen Organisationskontext heraus oder sie pauschalisieren verschiedenste Ebenen der Kultur und verzerren damit in beiden Fällen das Untersuchungsergebnis (vgl. Layes 2005, 71). Die Leistung der Arbeit von Daase, Junk und Rauer besteht vor allem darin, dass sie zuvor getrennte Dichotomien, wie die zwischen innerer und äußerer Sicherheitspolitik, gemeinsam betrachtet und die Vermittlungsleistung von Sicherheitskultur hervorhebt. Denn wie die deutsche Debatte um Nord Stream 2 belegt, können solch innere energiepolitische Themen entscheidende Konsequenzen für nationale Außen- und Sicherheitspolitik haben.

Die besagten Dualismen sind von den Autoren ausdrücklich als nicht abschließende Empfehlungen gekennzeichnet, die dazu einladen, adaptiert und modifiziert zu werden. Daher können die vorgeschlagenen Pole, die sowohl Hofstede, Demorgon und Edward Hall als auch Daase, Junk und Rauer formulieren, als Inspiration dienen, um eigene, dem Forschungsgegenstand angepasste Dimensionen zu entwerfen, zwischen denen Sicherheitskultur vermitteln und sich positionieren kann. Denn zwei Vorteile dieser Herangehensweise können nicht bestritten werden: Erstens helfen duale Modelle bei der nachvollziehbaren Vereinfachung und Eingrenzung des Objektes und zweitens dienen ihre Pole als Inspiration für die Entwicklung von reliablen Kriterien.

Gabriel Layes empfiehlt, obendrein drei Filter zu verwenden, die Jacques Demorgon geschaffen hat, um Mängel bei der Arbeit mit Kulturdimensionen zu vermeiden. Demnach ist es entscheidend, die Ebene der Beobachtung wie auch der Kultur zu identifizieren, über die eine Aussage getroffen wird. Sind gewisse Muster innerhalb aller gesellschaftlichen Räume zu finden oder gelten sie nur in wenigen Kategorien der Kultur? Während die Skizze der Beobachtungsebene bereits besteht, ist das, was Demorgon und Layes *Lebensbereich* nennen, noch undefiniert. Der Lebensbereich, hier aufgrund der nationalen Dimension eher als Kontext zu verstehen, ordnet ein, unter welchen Rahmenbedingungen sich das kulturelle Verhalten ausprägt. Auf Sicherheit übertragen bedeutet dieser Filter, dass sich eine Gruppe, die sich in völliger Sicherheit wähnt, anders gegenüber sicherheitspolitischen Fragen verhält als eine Gruppe, die ständig existenziellen Bedrohungen ausgesetzt ist. Abschließend ist die *Geschichte* ein hilfreicher Filter, um auszuschließen, dass das beobachtete Verhalten lediglich einen vorübergehenden Ist-Zustand abbildet. Erst der Blick in die Vergangenheit erlaubt demnach die Beurteilung, ob es sich um einen kulturell tradierten oder um einen unüblichen Habitus handelt (vgl. Layes 2005, 70f).

Mit dem dedizierten Augenmerk auf Cybersicherheit ergeben sich so neue Vermittlungsfelder, wohingegen andere für die kommenden Beobachtungen zu vernachlässigen sind. Die Klassifizierungen sind weniger als akkurate empirische Werkzeuge denn als Leitgedanken zu verstehen, entlang derer nachstehende Betrachtungen einzuordnen sind. Die Pole sind zu betrachten wie schwarz und weiß, in deren Zwischenraum sich vielfältige Schattierungen wiederfinden lassen.

Nevertheless, it is important to keep in mind that these are ‚ideal types‘. We hope they will prove useful as conceptual devices for organizing a discussion of media and political systems in comparative perspective [...] (Hallin/Mancini 2004, 69).

Sie sind deskriptiver Natur, das heißt, sie verdichten die aus den Vergleichskriterien destillierten Ergebnisse zu einem Muster und unterstützen dabei, sowohl funktionale Kriterien zu bilden als auch die Untersuchungsergebnisse schließlich zu veranschaulichen. Unter Bezugnahme auf die komparativen Untersuchungsgegenstände liegen insbesondere sechs binäre Paarungen an.

Mikro / Makro

Die Zweiteilung der Beobachtung in eine Mikro- und eine Makroebene erscheint naheliegend. Denn während Cybersicherheit auf der Mikroebene von jedem einzelnen

Bediener umzusetzen ist, entwickelt die Makroebene Strategien, Gesetze und Technologien, die dann der Mikroebene an die Hand gegeben werden. Diese Skalierung lässt sich plastisch verdeutlichen. Auf der Makroebene hat die Europäische Union die Zahlungsdiensterichtlinie PSD2 beschlossen, die am 14. September 2019 schlussendlich wirksam wurde (vgl. Amtsblatt der Europäischen Union 2018). Diese Richtlinie sieht erhöhte Sicherheitsstandards für die Online-Verwaltung von Bankkonten vor, darunter fällt die verpflichtende Einführung einer sogenannten Zwei-Faktor-Authentisierung. Auf Mikroebene war zu diesem Zeitpunkt allgemein bekannt, wie ein sicheres Passwort herzustellen ist. Gängige Zugangsdaten waren trotzdem häufig schwach; ein zweiter Faktor als zusätzliche Barriere in der Regel unbekannt. Die darauffolgenden technischen Konfigurationen der Online-Zugänge durch die Finanzinstitute, die einhergehenden Umstellungen für die Kunden sowie die begleitende mediale Berichterstattung schufen Debatten innerhalb der Makro- und der Mikroebenen, aber vor allem auch zwischen den Ebenen. Es entstanden erklärende Texte und Videos; die Politik nannte repetitiv die Vorteile der Richtlinie, während Privatanwender sowohl den Komfortverlust bemängelten als auch den Sicherheitsgewinn begrüßten (vgl. heise online 2019a). Reibung, Uneinigkeit, Streit und schließlich Akzeptanz und Adaption sind die wesentlichen Schritte des beschriebenen Prozesses, bei dem sich über Kommunikation und die Herstellung einer Öffentlichkeit motivorientierte Kultur entfaltet (vgl. Giebel 2014, 363). Indem die Sicherheitskultur Perspektiven verändert und neue Tatsachen – die regulierte Log-in-Methode – schafft, verändert die innerhalb des Diskurses gewonnene Erfahrung zugleich die Behandlung zukünftiger Kontroversen; ein weiterer Beleg dafür, dass Kultur stets voranschreitet und nur im zeitgenössischen Bezugsrahmen probate Klassifizierung erfahren kann. „We build on our past and shape the future with it. This implies that what exists now could not exist without what went before and what exists now sets limits to what can come next“ (Handwerker 2009, 79). Die Relation der Mikro- mit der Makroebene eignet sich, um herauszustellen, welche Verantwortungen in staatlichen und welche in privaten Händen liegen und wie diese ineinandergreifen. Bei einem Vergleich zweier ärarischer Systeme ist es von großem Interesse, aus welchen Lagern die überwiegenden Akteure dieser Sicherheitskultur stammen. Ist IT-Sicherheit eine vom jeweiligen Staat erkannte Herausforderung oder sind es vorwiegend private Handlungstreiber und Nichtregierungsorganisationen, die das Thema forcieren? Initiativen, einzelne Akteure und tief verankerte Meinungen der gesellschaftlichen Basis fließen ebenso in die

Beobachtungen ein wie Behördenstrukturen, Gesetze, politische Resolutionen oder internationale Abkommen. Obwohl häufig angenommen wird, dass der Staat das Sicherheitsmonopol innehat, also das, was Foucault als rechtlichen respektive juristischen Mechanismus und als „Disziplinarkorpus“ umschreibt, können ebenso gut Interessenverbände, Unternehmen, Arbeiter oder auch Schüler Agenden setzen, die schließlich nationale Relevanz erlangen (Foucault 2004, 22). So konnte etwa die Bewegung Fridays for Future weltweite Aufmerksamkeit erlangen, indem sie starke Gruppenkohäsion generierte und das Thema Umweltschutz emotional besetzte (vgl. Brünker et al. 2019, 308f). Diese Initiative ist jedoch längst aus dem Stadium einer reinen Umwelt-Protestaktion herausgewachsen und mahnt mit sicherheitspolitischen Werkzeugen, indem sie vor sozialer Destabilisierung, Klimaflucht und schwindenden Lebensräumen warnt. Mithilfe dieser Polarität kann aufgedeckt werden, aus welchen politischen, sozialen oder gesellschaftlichen Gefügen Topoi der Cybersicherheit aufsteigen.

Subjektiv / Objektiv

Wie schon umrissen, können objektive Bedrohungslage und subjektives Bedrohungsempfinden auseinander liegen. Das wiederum kann wirkungslose oder gar schädliche Praktiken nach sich ziehen. Werden Probleme langfristig unterschätzt, und dies gilt explizit für die IT-Sicherheit, werden sie zwangsläufig nicht aus der Welt geschafft und akkumulieren stattdessen. Zielen die Strategien dagegen darauf ab, nachvollziehbare Bedrohungsparameter zu minimieren, kann davon ausgegangen werden, dass den objektiv bestehenden Gefahren Rechnung getragen wird. Das Gegenteil ist der Fall, wenn Anstrengungen beispielsweise auf Basis einmaliger Vorfälle oder öffentlicher Aufregung unternommen werden. Diese Einordnung zwischen subjektiv und objektiv ist nicht abschließend, sondern dient als Werkzeug, um zu ermitteln, was jeweils als potenzielle Bedrohung wahrgenommen wird. Inwieweit hat sich eine Sicherheits- beziehungsweise Angstkultur herauskristallisiert, in der Sicherheitsdiskurse durch irrationale Befürchtungen geleitet werden und nicht durch den nachvollziehbaren Wunsch, vorbereitet zu sein? Aus welcher gesellschaftlichen Richtung stammt der Auslöseimpuls für vorherrschende IT-Sicherheitsthemen? Im Grunde zeichnet dieses Spektrum zwischen subjektiv und objektiv den Ursprung des dominanten Narrativs nach, das ursächlich ist für das jeweilige politische Handeln. Der menschengemachte Klimawandel zum Beispiel steht exemplarisch für eine reale,

existenzielle Bedrohung, die erst durch jahrzehntelange Anstrengungen der Zivilbevölkerung auf die Agenda zum Beispiel Deutschlands und der Niederlande kam. In diesem Fall musste erst aus der hohen objektiven Bedrohungslage eine ebenso hohe subjektive werden, damit die mit intensivem, individuellem Engagement in die politische Dimension induziert werden konnte.

Restaurativ / Progressiv

Wenn auch engstens miteinander verwoben und freundschaftlich verbunden, sind Deutschland und die Niederlande durch teils sehr unterschiedliche historische Ereignisse geprägt. Hier ist das 20. Jahrhundert hervorzuheben, in dem beide Länder wechselweise partnerschaftlich interagierten oder zutiefst verfeindet waren. Aus den in der Vergangenheit liegenden Geschehnissen wurden unterschiedliche Erzählungen und Tradierungen über den jeweils Anderen fortgeschrieben, die das Selbstbild und zugleich das Bild vom, somit auch die Beziehung zum, Nachbarland nachhaltig eingefärbt haben. Zugleich beeinflussen die Erfahrungen der Vergangenheit, wie Sicherheitskultur ausgestaltet wird. „[I]t is only by following ideas through time that one gains a feel for what is fixed and what is changeable in social self-understandings as well as the reasons why“ (Jasanoff 2015a, 28). Gemäß Jasanoff zeigt erst die Geschichte einer gesellschaftlichen Gruppe, welche ihrer Überzeugungen verhandelbar sind und wo sich ihre unverrückbaren Linien und elementaren Prinzipien befinden.

Das bedeutet auch, dass in der Sicherheitskultur die Erfahrungen der Vergangenheit auf die Gefahrenantizipation der nahen Zukunft treffen und auf diese Weise mitbestimmen, wie Sicherheit Form annimmt. Zu diesem Zweck werden je die einschneidenden nationalen Erlebnisse des vergangenen Jahrhunderts ermittelt und kontextualisiert. In der Folge lassen sich diese historischen Perspektiven den nationalen Anstrengungen für homogene IT-Sicherheitsstandards gegenüberstellen. Dies erlaubt Aussagen darüber, ob und gegebenenfalls welche handlungsleitenden Motive der Vergangenheit stets Einfluss auf die gegenwärtige Cybersicherheitsstrategie haben. Vor allem aber offenbart dieser Blick, wie sehr die Handlungsweisen aus der Vergangenheit abgeleitet werden oder wie konsequent es gelingt, Historisches hinter sich zu lassen, um die agilen, asymmetrischen Sicherheitsprobleme der Digitalisierung zu bewältigen. Denn um Cybersicherheit realisieren zu können, ist es zwingend, die Anforderungen an Technik und Technikumwelt regelmäßig anzupassen – in einem dramatisch höheren Tempo als in der prädigitalen Zeit (vgl. Kurz/Rieger 2018, 264). Mithilfe dieser Polarität wird sichtbar,

ob die Vergleichsobjekte an ihrer Geschichte festhalten und konservierend, vielleicht gar restaurativ agieren oder ob sie renovierend, innovativ und erneuernd handeln und sich von altbewährtem Problemlösungsverhalten freimachen.

Technikfokus / Bedienerfokus

Diese Paarung steht im Zeichen einer der grundlegenden Problematiken von IT-Sicherheit. Der naheliegendste Ansatz zur Herstellung sicherer IT-Strukturen ist die Förderung von sicherer Technologie, sodass optimalerweise alle Bediener und Dienstleister sicher sind. In dieser Einschätzung steckt jedoch eine gewisse Ignoranz, denn sie lässt den Faktor Mensch außer Acht, der fehlerhaft bedient, der bestechlich ist oder der mutwillig Schaden zufügt. Diese Komplikation kann als mögliche Schwachstelle jeglicher Hochtechnologie und Sicherheitsbarriere dienen, sodass die Mensch-Maschine-Interaktion einen mindestens ebenso wichtigen Baustein von Cybersicherheit darstellt wie die Sicherheit der Technik selbst. Ein häufig zu beobachtendes Beispiel: Ein Anwender erstellt für sein E-Mail-Postfach ein langes, sicheres Passwort und verwaltet dieses vertraulich und integer. Wenig später lässt sich dieser User von einer gefälschten E-Mail täuschen und gibt sein Passwort nun preis, weil er überzeugt wurde, dass ihm sonst zukünftig etwa der Log-in nicht mehr möglich sei. Auf diese Weise gelangt ein Passwort, dessen Berechnung mit technisch-mathematischen Mitteln viele Jahre gedauert hätte, innerhalb weniger Momente in die falschen Hände – nur durch menschliche Fehleinschätzung. Angesichts dessen liegt ein Augenmerk darauf, ob sich Maßnahmen darauf konzentrieren, technische Sicherheitsbarrieren zu schaffen und zu stärken oder ob der Bediener als Einfallstor wenigstens mitbedacht ist. Das bedeutet, es wird untersucht, ob Sicherungsmaßnahmen und Strategien ausschließlich auf programmierbare, berechenbare Hard- und Software-Mechaniken setzen oder inwieweit unter anderem Weiterbildungen, Antikorruptionsprogramme und Aufklärungsarbeit in die Abwägungen einbezogen werden. Mit dieser Anwendersensibilisierung, bestenfalls im Einklang mit technischen Sicherheitsoptimierungen, soll dann das Risikobewusstsein steigen und zu einer nachhaltigen Handlungsänderung führen.

Innen / Außen

Das Weißbuch der Bundesregierung hielt 2016 fest, dass die Gefahrenabwehr von inneren und äußeren Bedrohungen nur gesamtheitlich zu betrachten ist. „Störungen und Gefährdungen bewegen sich vielfach an deren Schnittstelle“

(Bundesregierung 2016, 48). Das bedeutet, dass nicht nur Angriffe, seien sie physisch oder virtuell, von aggressiven Drittstaaten außerhalb der EU drohen, sondern zugleich Kriminelle und demokratiefeindliche Gesinnungsträger innerhalb Deutschlands und Europas auftreten. Mehr noch: Externe und interne Gefahrenquellen greifen ineinander. So nahm der sogenannte Islamische Staat Einfluss auf die europäische Sicherheitslage, indem er etwa die islamistische Radikalisierung in den EU-Mitgliedsstaaten befeuerte (vgl. Bundesministerium des Innern, für Bau und Heimat 2019, 175ff). Zudem eignen sich ausländische Massenmedien, um mittels gezielter Falschnachrichten beispielsweise das rechtsextreme Gewaltpotenzial zu stimulieren, und so Destabilisierung und politische Unruhe herbeizuführen (vgl. Tagesschau 2020). Derartige Methoden werden allgemein als hybride Bedrohungen zusammengefasst. Sie verbinden unterschiedlichste Vorgehensweisen, um möglichst anonym und zugleich wirkungsvoll im eigenen Sinne auf die Stabilität eines anderen Staates einzuwirken (vgl. Bundesministerium des Innern, für Bau und Heimat 2019, 317f). Die Niederlande haben im Grunde denselben Herausforderungen zu begegnen. Im Inneren bedrohen Desinformation, extremistische Populisten und tiefgreifende gesellschaftliche Unruhen die demokratische Grundordnung, wie etwa die *Coronarellen* – ein niederländischer Begriff für die extremen Tumulte, denen sich das Land 2021 stellen musste. Insbesondere nach dem Absturz des Flugs MH17 fühlen sich die Niederlande von außen durch Russland bedroht und sahen, wie ein Papier aus 2019 zeigt, durch Russland herbeigeführte Energieabhängigkeiten und einhergehende Engpässe voraus (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019b, 23).

Cyberangriffe, Desinformationskampagnen, ausländische Direktinvestitionen, Influencing, oder die Finanzierung radikaler Vereinigungen sind nur ausgewählte Techniken, die sich beliebig kombinieren lassen und die Grenzziehung zwischen inneren und äußeren Aggressoren für die Niederlande wie auch für Deutschland erschweren.

Klassische Herausforderungen wie die militärische Bedrohung unseres Territoriums durch Streitkräfte anderer Staaten sind gegenüber diffusen und nur schwer zuzuordnenden hybriden Gefährdungen in den Hintergrund getreten. Angreifer nutzen in wachsendem Maße die Möglichkeiten, die sich aus Globalisierung, Technologisierung und Digitalisierung ergeben, um unsere offenen Gesellschaften zu attackieren (Weißbuch 2016, 49).

Inmitten dieses abstrakten Unsicherheitskontextes zählen Cyberangriffe zu den wirkungsvollen Instrumenten, weil sie aus Täterperspektive multiple begünstigende

Eigenschaften besitzen. Der Schaden, den digitale Attacken anrichten können, ist nahezu unlimitiert, die Attribution der Tätergruppen gestaltet sich mühsam und die Aktion selbst kann aus dem Ausland erfolgen respektive sogar multinational verschleiert werden. Aufgrund der Vielfalt innerer, äußerer und hybrider Angriffsvektoren ermöglicht der Blick auf den Umgang der Niederlande und Deutschlands mit digitalen Gefährdungspotenzialen aus dem In- oder Ausland, strategische Unterschiede beider zu identifizieren. Aus der Beobachterperspektive erschließt sich, ob die etablierten Strukturen angemessen sind, um den multidimensionalen Angriffsmöglichkeiten gerecht zu werden und in welchem Ausmaß mögliche Konsequenzen antizipiert werden. Die Ergebnisse zeigen, ob sich die Länder auf die Bekämpfung innerer Gefahren konzentrieren oder ob sie sich international, mindestens europäisch ausrichten, um gemeinsam Bedrohungen von außerhalb zu begegnen.

Chance / Risiko

Die Kommunikation der Niederlande sowie Deutschlands über BSI, NCSC, Ministerien, Politiker, Presse oder Verbände gibt Aufschluss darüber, wie die Länder Informationstechnik und Cybersicherheit begreifen. Klingen Hoffnungen und Möglichkeiten an und diskutiert man Chancen, entsteht ein völlig anderes Bild von Cybersecurity als in einem Land, das Risiken hervorhebt, Skepsis und Unbehagen thematisiert und in dem Wünsche nach Restauration überwiegen. Dabei haben diese Pole sicherlich Verwandtschaft mit der Paarung subjektiv/objektiv, denn wenn das Gefahrenempfinden der Bevölkerung groß ist, unerheblich ob objektiv nachvollziehbar oder nicht, ist anzunehmen, dass Debatten über Risiken und Risikovermeidung dominieren, während Chancen unbemerkt bleiben.

Heißt die deutsche Sicherheitspolitik die vielfältigen Gelegenheiten der rasanten Digitalisierung willkommen und schauen die Niederländer mit einer tendenziell pessimistischen Grundhaltung auf dieses Wagnis oder haben vielleicht beide Länder eine nahezu identische Haltung? Die vielen Texte und Medien, von denen diese Arbeit ausgeht, weisen in Summe eine Tonalität auf, die eine, wenn auch pauschalisierte, Zuordnung zu einem der beiden Nullpunkte zulässt und die jeweilige Cybersicherheitskultur ein weiteres Stück charakterisiert.

1. Quid est Cybersicherheitskultur?

Sucht man bei Google nach ‚Security Culture‘, erhält man Stand 13. Februar 2022 2.810.000.000 Ergebnisse. Acht der neun Treffer auf der ersten Seite behandeln explizit die Sicherheitskulturen in beruflichen Organisationsstrukturen. Nur eine der angezeigten Seiten hebt die IT-Sicherheit besonders hervor. Es fällt auf: Die Suchmaschine Google zeigt IT-Sicherheitskultur nicht global, sondern vielmehr in kleinsten Entitäten, die überschaubar bleiben. Unternehmen, Behörden oder Verbände sind exklusive Lebenswelten, die nach strengen sozialen Normativen funktionieren. Innerhalb dieser Räume existieren definierte Regeln, deren Missachtung eindeutige Sanktionen nach sich zieht. Für außen liegende Bereiche, wie das Zuhause oder den öffentlichen Raum, besitzen derart limitierte Vorgaben keine Legitimierung. Auf die Informationstechnik übertragen bedeutet das, dass die restriktivsten Maßnahmen nur einen geringen Effekt außerhalb des reglementierten Geltungsbereichs *Büro* zeigen, wenn die zugrundeliegende Dringlichkeit, der Kern der Botschaft, nicht zum Empfänger durchdringt. Diese Segmentierung von Rollen und Aktionsterritorien unterminiert erforderliche Transferleistungen. Wenn beispielsweise im Beruf sicher durchgeführte Prozesse in privat vergleichbaren Situationen nur mit einem schwachen Passwort umgesetzt werden, kann das eine eigentlich sichere Technologie durch menschliche Unterlassung angreifbar machen.

In einem Papier aus dem November 2017 stellt ENISA fest, dass Cybersicherheitskultur aus eben zwei ganz grundlegenden Elementen besteht, auf die dann individuelle, skalierte Maßnahmen aufbauen können:

The majority of data breaches within organisations are the result of human actors, and while cybersecurity policies are commonplace among organisations, employees may view them as guidelines rather than rules. Similarly, technologies cannot protect organisations if incorrectly integrated and utilised. Against this backdrop, the development of a CSC achieves a change in mindset, fosters security awareness and risk perception and maintains a close organisational culture, rather than attempting to coerce secure behaviour. (European Union Agency for Network and Information Security (ENISA) 2017, 7).

Auf der einen, offensichtlichen Seite identifiziert die Agentur technische Defizite, die von der Gegenseite ausgenutzt werden können. Diese Sichtweise befreit den Nutzer eines Computersystems gewissermaßen von seiner Verantwortung, da die entscheidende Unzulänglichkeit nicht auf seine Handhabung zurückzuführen ist. Deshalb ergänzt

ENISA diesen Ansatz und bezieht die Bedienenden in die Idee einer sicheren Cybersicherheitskultur ein. Was dort für Arbeitnehmer festgehalten wurde, gilt ebenso für die private Nutzung von Informationstechnik – Risikobewusstsein, Resilienz sowie die Fähigkeit, Technik möglichst sicher zu betreiben, sind in diesem Kontext essenziell bedeutsam. Diese Notwendigkeit führt ENISA vornehmlich auf drei Ursachen zurück, die als Katalysator für Cyberkriminalität dienen: „[...] phishing emails, human errors, and deliberate misuse“ (European Union Agency for Network and Information Security (ENISA) 2017, 29). Zwei dieser drei Auslöser liegen erkennbar in fehlendem Wissen, Unachtsamkeit oder Ignoranz, ergo in menschlichem Fehlverhalten begründet. ENISA umreißt damit immerhin relevante, wiederkehrende und vor allem menschengemachte Stimulanzien für mangelhafte Informationssicherheit und fordert vor diesem Hintergrund eine intensiviertere, organisationsbedingte Cybersicherheitskultur (vgl. European Union Agency for Network and Information Security (ENISA) 2018, 24ff).

Indessen spezifiziert die Europäische Agentur bei ihrem Ansatz nicht, was Kultur, im Speziellen Cybersicherheitskultur, ist und welche sozialen Rohstoffe sie manifestiert. Den ENISA-Papieren folgend entsteht der Eindruck, dass Security Culture in limitierten Ökosystemen mit klaren Rahmungen und nur wenigen, deutlich identifizierten Netzwerkpunkten außerhalb der Systeme besteht. Für diese theoretischen Räume können dann präzise zugeschnittene Sicherheitskonzepte entwickelt werden, welche dann bestenfalls menschliche Akteure mit inhärentem Sicherheitsbewusstsein versehen. Einleuchtende Beispiele sind Firmeninfrastrukturen, Vereine oder Ministerien. Dann werden Regeln und Leitfäden entworfen, Angestellte geschult und Handlungen sanktioniert beziehungsweise honoriert, bis die gewünschten Aktionen in robuste Automatismen überführt wurden. Zum einen führen solche Diktate nicht selbstverständlich zu einem Austausch zwischen den Mitarbeitern und insbesondere zwischen den Hierarchieebenen der Organisation. So entstehen weder Inklusion noch eine memorable Kultur. Allerdings sehen solch organisationsbasierte Sicherheitskulturkonzepte, wie ENISA sie wünscht, zwar verschiedene Szenarien, Nutzerverhalten und Angriffsvektoren vor, jedoch decken sie nie das gesamte Spektrum möglicher Unsicherheitsfaktoren ab. Damit soll diesen Konzepten nicht pauschal ihre Wirksamkeit abgesprochen werden. Sie bleiben allerdings unvollständig, ja sogar fragmentarisch, solange die fundamentalen Mechanismen nicht nur als hinderliche

Pedanterie empfunden, sondern in Routinen überführt wurden. Ihr wohl größter Nachteil liegt darin, nur die IT-Sicherheitskultur der jeweiligen Organisation anzufassen. Unter anderem der niederländische Psychologe René Diekstra zeigt auf, dass die gegenwärtige Situation andere Herausforderungen an den Umgang mit Informationssicherheit stellt: „De publieke ruimte, de ruimte die principieel van ons allemaal is, wordt in toenemende mate – het woord ‘reusachtig’ is werkelijk op zijn plaats – bezet of eigenlijk ingepikt, geannexeerd door techniek“¹⁰ (Diekstra 2009, 212). Er diagnostiziert demnach eine völlige Durchdringung, sogar eine Okkupation des Öffentlichen und Privaten durch Digitaltechnologie. Ähnliches stellt Peter Schaar fest, wenngleich er nicht so weit geht, von Annexion zu sprechen. Er erkennt ebenfalls den Einfluss, den die Digitalisierung auf gegenwärtige Gesellschaften hat, rät aber von „einer eindimensional quantitativen, rein funktionalen Sichtweise“ ab (Schaar 2015, 204). Damit plädieren Schaar und viele seiner Kollegen auch, darunter Matthew Smith oder Constanze Kurz, für einen multiperspektivischen Blick auf die Herausforderungen von Digitalisierung und Online-Bedrohungen, der die Aufgabenstellung zwar nicht übersichtlicher gestaltet oder vereinfacht, aber dafür realistischer begreift als ein technozentriertes Dogma. Die folgenden Seiten sind daher der Versuch, IT-Sicherheitskultur umfassender darzustellen als es oben genannte Konzepte tun und zwei Beispiele für gesamtgesellschaftliche Sicherheitskulturausprägungen abzubilden.

Der titelgebende Ausdruck der IT-Sicherheitskultur ist ergo keine Innovation dieser Schrift. Das erste Aufkommen der Vokabel Sicherheitskultur lässt sich sehr präzise auf das Jahr 1986 datieren. Infolge der Reaktorkatastrophe von Tschernobyl wurde erstmals die strukturalisierte, menschliche Beteiligung an organisationsbedingtem Versagen einer Sicherheitsstruktur in den Fokus gerückt (vgl. Haverkamp 2014, 180f). Im Gegenzug zu bis dato angelegten Begriffen, wie politischer Kultur, technischer Sicherheit oder Sicherheitspolitik, versuchte man mit Sicherheitskultur, den Phänotypen eines umfassenden, dynamischen, auf tangierende Bereiche ausfransenden oder diese gar einnehmenden Sicherheitsorganismus abzustecken. Auf die terminologische Zugehörigkeit zur Kultur und vor allem der dieser zugrundeliegenden Idee andauernder gesellschaftlicher Wechselwirkungen ist es zurückzuführen, dass die Sicherheitskultur

¹⁰ Deutsch: Der öffentliche Raum, der Raum, der hauptsächlich uns allen gehört, wird in zunehmendem Maße – das Wort ‚riesenhaft‘ trifft es wirklich genau – besetzt oder eigentlich angeeignet, annektiert durch Technik.

stetem Wandel unterworfen ist. Das stellt diese Dissertation vor eine Herausforderung, da Sicherheit wie auch Kultur – so folglich auch Sicherheitskultur – nie feststehend sein können. Das betrifft selbstverständlich sogar den kulturwissenschaftlich vergleichsweise kurzen Bearbeitungszeitraum dieser Abhandlung. Gesellschaft und die in ihr verhandelte Kultur sind menschengemacht und wirken auf den Menschen als Produkt seiner Gesellschaft zurück (vgl. Berger/Luckmann 2018, 65). Schon aufgrund dieser Rekursivität kann keine Stagnation stattfinden. Deshalb projizieren wissenschaftliche Abbildungen kulturellen Handelns immer nur einen Ist-Zustand aus der Vergangenheit des Lesenden und geben keineswegs die aktuellen Konditionen zum Zeitpunkt der Rezeption wieder.

Damit anschließend Klarheit herrscht, schreiben die kommenden Zeilen das zugrundeliegende Verständnis mehrerer Bezeichnungen fest, die dann im Kontext dieser Arbeit gelten. Diese Vorgehensweise hat zum Ziel, ein zeitgemäßes und hinlänglich umfassendes Begriffsfundament zu schaffen, auf dem in der Folge die weiteren Ausführungen fußen können. Danach liegt die Destillation beider Wortbestandteile von Sicherheitskultur nahe. Die Begriffsemulsion verbindet die im allgemeinen Sprachgebrauch einander kaum nahestehenden Termini der Sicherheit und der Kultur. Zur Verschränkung beider und folglich zur Fabrikation eines neuen Gehalts kam es bisher zudem nur selten im Zusammenhang mit Informationstechnik.

1.1. Definition der Chimäre Sicherheit

Der Definitionsversuch von Sicherheit ist per se dazu verurteilt, in Unzufriedenheit zu enden. Denn das rein theoretisch existierende Konzept totaler Sicherheit krankt an zwei inhärenten Dilemmata: Erstens kann absolute Sicherheit nur hergestellt sein, indem jeder Winkel, jeder Umweltfaktor und jede Handlung kontrolliert und von jeglicher Unsicherheit befreit wird; ein nicht zu erreichender Zustand (vgl. Endreß/Feißt 2014, 22). Dabei kam schon Wilhelm von Humboldt nicht umher, anzuerkennen, dass Sicherheit eine Implikation von Freiheit ist. Schließlich ist der Mensch ohne Sicherheit nicht in der Lage, „weder seine Kräfte auszubilden noch die Früchte derselben zu genießen; denn ohne Sicherheit ist keine Freiheit“ (von Humboldt 1851, 45). Daraus schließen Endreß und Feißt zunächst:

Es kann immer nur eine relative Sicherheit geben, die durch ihre notwendige Differenz zu einer nie erreichbaren absoluten Sicherheit charakterisiert ist. Wir bewegen uns immer in einem Spannungsfeld zwischen erreichen wollen und

nicht erreichen können, zwischen Freiheit und eingeschränkten Handlungsspielräumen, zwischen Kontrolliertem und Unkontrollierbarem (Endreß/Feißt 2014, 22).

Sicherheit ist demzufolge Utopie und Dystopie zugleich. Das Versprechen auf die Absenz von Unsicherheit hört sich verlockend an. Es offeriert körperliche Unversehrtheit, den Erhalt von Wohlstand und die Auflösung vieler Ängste. Zugleich führt vollkommene Sicherheit unausweichlich zu totalitären Gesellschaftsordnungen, Unfreiheit und Monotonie. Ebendarum zielen die meisten Versuche der Sicherheitskonstruktion auf das Arrangement relativer Sicherheit ab. Damit verbunden ist die Akzeptanz gewisser Unsicherheiten und Gefahren, die bestenfalls weitestgehend kalkulierbar sind.

Zweitens stehen Sicherheitsbemühungen immer vor der Krux, Sicherheit nur für eine spekulative Zukunft produzieren zu können. „Insoweit als das Unbekannte dem Bekannten ontologisch vorausgeht, nimmt Sicherheit eine charakteristische zeitliche Struktur an“ und kann „nicht durch eine unmögliche Rückkehr zu einer unschuldigeren, sichereren Vergangenheit, die tatsächlich nie existiert hat“ (vgl. Frohman 2017, 299). Durch das Erfahren des Unsicherheitsmoments wird der Rückweg in eine verflossene Konstitution unwiederbringlich verbaut. Das bedeutet, dass Sicherheit lediglich durch Reaktion, also indem ein akuter Gefahrenmoment beseitigt wird, oder durch Prävention, also indem Unsicherheit vorweg vermieden wird, für einen kommenden Augenblick verfasst werden kann.

Der unerreichbare Status absoluter Sicherheit sowie die zukunftsgerichtete Wirkung von Sicherheitsmaßnahmen prägen die anhängigen Diskurse rund um Fürchte, persönliche Freiheiten, kollektive Werte und Normen oder politische Programmatiken. Das interdisziplinäre Forschungsprojekt ‚Barometer Sicherheit in Deutschland (BaSiD)‘ hat sich daher der Modellierung des Begriffs *Sicherheit* angenommen und stellt voran, dass Sicherheit objektiv und subjektiv völlig unterschiedliche Zustände einnehmen kann. Zur Verdeutlichung wurde 2012 durch das Max-Planck-Institut für ausländisches und internationales Strafrecht im Rahmen dieses Projektes, an dem unter anderem das Bundeskriminalamt und das Bundesministerium für Bildung und Forschung beteiligt waren, eine Visualisierung dieses Phänomens veröffentlicht.

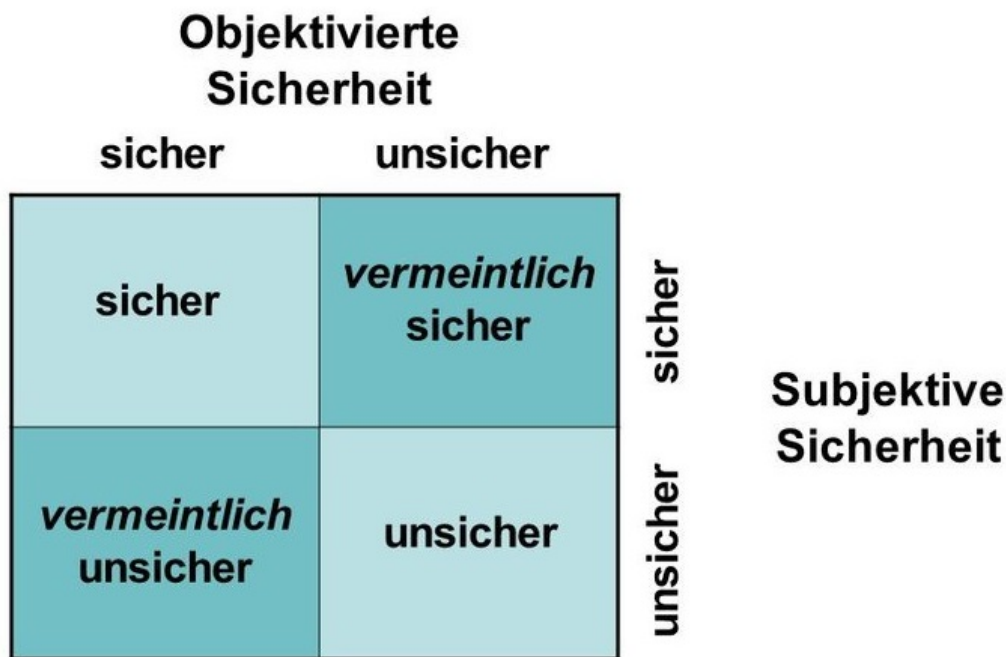


Abbildung 4: Sicherheitsquadra(n)t (Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht 2012)

Das Quadrat dokumentiert die mögliche Differenz zwischen objektiv tatsächlich existierender Sicherheitslage und der von Gruppen oder Individuen empfundenen Sicherheits- beziehungsweise Bedrohungslage. Dabei lässt dieses einfache Schema die Art der Gefahr und die ökonomischen, sozialen oder historischen Umstände bewusst außer Acht und ermöglicht so ein abstrahiertes Verständnis der behandelten Divergenz. Dieser folgend ist es möglich, dass sich eine Person anhand objektiver Daten in völliger Sicherheit befindet, sich aber dennoch akut bedroht sieht. So stigmatisierten besonders Boulevard-Medien in den Jahren 2015 bis 2018 Geflüchtete mit Artikeln, wie „Wenn er abgeschoben worden wäre, würde sie noch leben“ (Bild 2018) oder „Wohin mit kriminellen Flüchtlingen“ (n-tv 2016), sodass die verschärfte Rhetorik zugewanderte Personen als Menschen mit erhöhtem Kriminalitätspotenzial erscheinen ließ. Dem entgegen stehen aus dem gleichen Zeitraum die Berichte des Bundeskriminalamts. Im Bundeslagebild *Kriminalität im Kontext von Zuwanderung 2016* gibt das BKA an, dass zwar „die absolute Zahl der Straftaten mit mindestens einem tatverdächtigen Zuwanderer“ um 42 % beziehungsweise etwa 87.000 Delikte angestiegen sei, gleichzeitig sei zwischen Beginn 2015 und Ende 2016 „die Gruppe der nach Deutschland gekommenen Zuwanderer stark angestiegen“ – um 490 % (Bundeskriminalamt 2017, 42). Stellt man demnach die große Zahl der Zuwanderer mit der Zahl der gestiegenen Kriminalität in Relation, wird offenbar, dass hier die

Skalierung der Messung einen falschen Eindruck vermittelt und nur ein geringer Teil der Zuwanderer tatsächlich straffällig wurde. Die objektiv kaum erhöhte Gefahr, Opfer von Kriminalität eines Geflüchteten zu werden, stand spürbaren subjektiven Vorbehalten und großen Ängsten gegenüber. Derartige Framing-Mechanismen dienen dazu, Realität zu schaffen, indem gewisse Aspekte intendiert ausgewählt und mit Bedeutung aufgeladen werden (vgl. Hoffmann 2014, 93f).

Ebenso kommt es vor, dass Menschen eine Gefahr unterschätzen und sich trotz bestehender Bedrohung sicher fühlen. Während bis Mitte Februar 2020 das Corona-Virus in der Öffentlichkeit nur eine ferne Randnotiz aus Asien war, berichtete kurz nach den Karnevalstagen sogar die New York Times über den kleinen Ort Gangel-Langbroich, in dem die Krankheit ab diesem Zeitpunkt zu der weltumspannenden Pandemie anwuchs, die heute jeder Mensch kennt (vgl. New York Times 2020). COVID-19 war rückblickend bereits zu diesem Zeitpunkt eine existenziell bedrohliche Erkrankung, die in weiten Teilen des Okzidents jedoch zu Jahresbeginn noch als ein Erreger unter vielen angesehen wurde.

Selbstverständlich kann der subjektive Eindruck ebenso gut mit der objektiven Lage einhergehen. Auch hierfür eignet sich die Corona-Pandemie als eindrückliches Beispiel. Nur wenige Wochen nach dem Ausbruch der Krankheit in Westeuropa sowie Nordamerika galt in den meisten Staaten der Welt eine Ausgangs- oder Kontaktsperrung. Bei circa einer Million Infizierten, knapp fünfzigtausend Toten weltweit sowie weiterhin stark zunehmenden Erkrankungsständen erwuchs schon Anfang April 2020 eine objektiv wie subjektiv apperzipierte, fundamentale Unsicherheit (vgl. Johns Hopkins University 2020). Diese Überschneidung von Unsicherheitsempfinden und Bedrohungslage gestattete erst radikale Gegenmaßnahmen mit vorübergehenden Grundrechtsbeschränkungen.

Das Sicherheitsquadrat stellt daher im Wesentlichen eine Annahme dar: Die subjektive Einschätzung einer Bedrohungslage kann, muss aber nicht, von der objektiv tatsächlich vorherrschenden Situation divergieren. Anders gesagt, spiegelt das Sicherheitsempfinden von Einzelnen oder von sozialen Gruppen nicht zwangsläufig den Ist-Zustand ab. Sicherheitskrisen tragen demzufolge das Potenzial in sich, Gefahren subjektiv größer erscheinen zu lassen als sie objektiv sind, „weil ihnen über ihre unmittelbare barbarische Wirkung hinaus eine symbolische Bedeutung zukommt“ (Müller 2012, 230). Diese Diskrepanz wird für die Auflösung der hier behandelten

Fragestellungen immer wieder relevant sein: Denn die Aufschlüsselung konstitutiver Institutionen und Beteiligter kann nur ein erster Blick auf die deutschen wie niederländischen Cybersicherheitslandschaften sein. Das bedeutet, anschließend Berichte zugrunde zu legen, die verlässliche Aussagen über die wirkliche, akute Bedrohungslage treffen – jene Bedrohungslage, der die Institutionen als Repräsentanten der Bevölkerung begegnen sollen. Solche Untersuchungen ermitteln unter anderem Schadenzenzahlen oder gängige Angriffsvektoren und geben aufgrund ihrer wiederholten Durchführung Auskunft über die Entwicklung der Sicherheitslage. Sie lassen sowohl Schlüsse über den Zustand der aktuellen Sicherheitsinfrastruktur als auch über die Bemühungen der Angreifer zu. Damit entsteht ein Bild der Nahtstelle, die unter anderem diese Dissertation offenlegt: Angenommen, es decken sich Informationen über eine widerstandsfähige Infrastruktur sowie eine realistische Gefahrenperzeption, kann von einer ausgeprägten Cybersecurity Culture die Rede sein, da anzunehmen ist, dass die Problemstellung auf gesamtgesellschaftliche Aufmerksamkeit stößt. Sofern sich aber ein Glied der Sicherheitsarchitektur nicht auf dem Niveau der jeweils anderen befindet, lässt sich ein Ungleichgewicht ausmachen und Missverhältnisse ausdeuten.

Christopher Daase unternimmt den Versuch, Sicherheit greifbarer zu machen, indem er den politischen Sicherheitsbegriff mittels vier verzweigter Dimensionen erweitert. Damit zielt er darauf ab, das seit dem Zweiten Weltkrieg bis heute veränderte Sicherheitsbedürfnis wirklichkeitsgetreu wiederzugeben und das dynamische Konstrukt Sicherheit möglichst objektiv aufzuzeichnen. Daase legt deshalb Dimensionen an, die er anhand zugehöriger Fragen ermittelt: So ergibt sich die Sachdimension, indem er fragt, in welchem Sachgebiet eine Gefahr oder ein Risiko besteht (vgl. Daase 2010, 4). Durch die Frage nach den möglichen Betroffenen einer Bedrohung erschließt sich für Daase die Referenzdimension (vgl. Daase 2010, 9). Diese Größe ist ein wichtiger Indikator für die Skalierung eines Sicherheitsphänomens. Ähnlich verhält es sich mit der Raumdimension, die sich aus der Frage deduziert, welche geografische Ausdehnung eine Gefährdung betrifft (vgl. Daase 2010, 12). Damit geben Raum- und Referenzdimension den möglichen Maßstab der Sicherheitsherausforderung an, indem sie Auskunft über die potenzielle räumliche Ausdehnung und das Ausmaß der Benachteiligten gibt. Die Gefahrendimension schließlich „bestimmt, wie die Unsicherheit definiert wird, die sicherheitspolitisch überwunden werden soll“ (Daase 2010, 15). Daase unterscheidet hier zwischen der konkreten Bedrohung, bei der

ein Antagonist benannt und eine gegnerische Handlung erahnt wird; der Verwundbarkeit, bei der eindimensionale Interdependenzen ohne ausdrückliches Feindbild zu Abhängigkeiten von anderen Akteuren führt; und dem Risiko, das diffus sowie geografisch ungebunden daher kommt und daher präventiver, antizipierender Methoden bedarf (vgl. Daase 2010, 15ff).

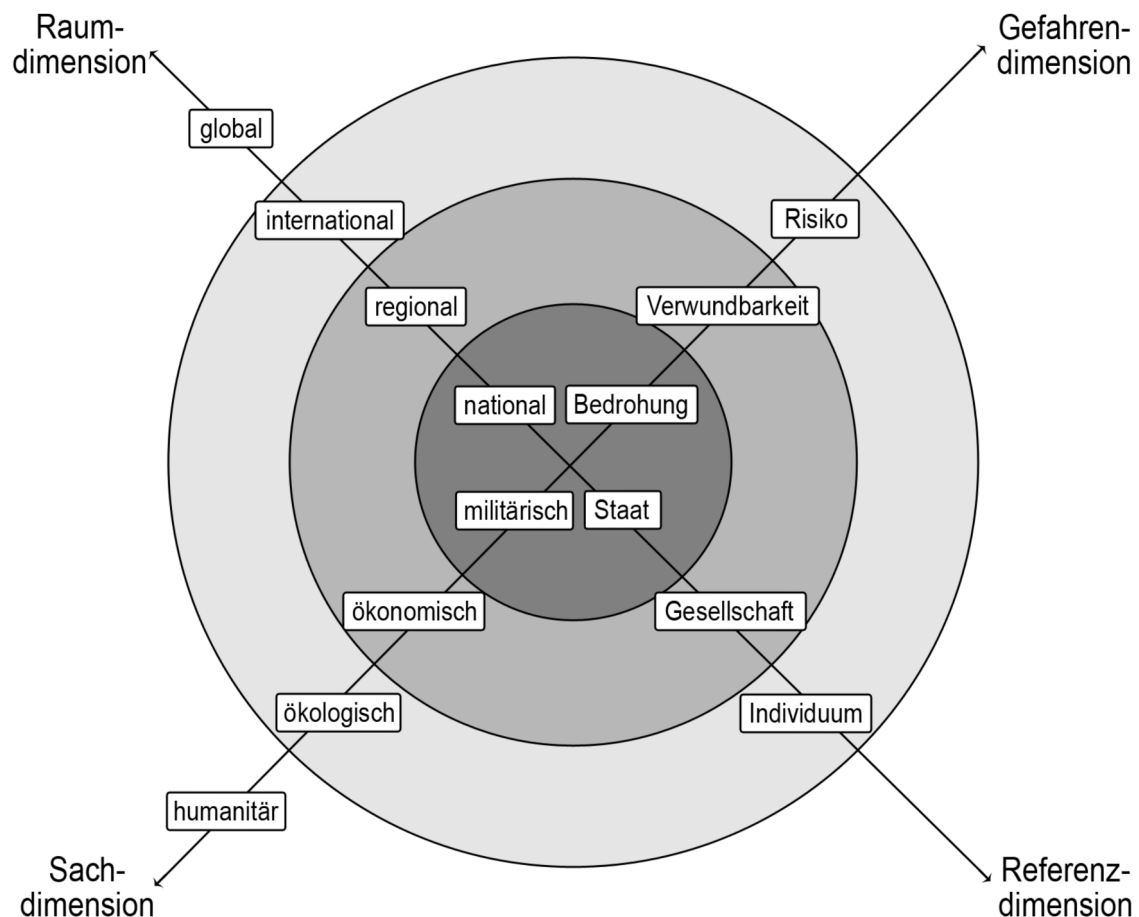


Abbildung 5: Der erweiterte Sicherheitsbegriff (Daase 2010)

Diese vier Dimensionen, die überdies unterschiedliche Ausprägungen annehmen können, geben bei korrekter Einschätzung der jeweiligen Lage eine sichtbare Impression der gegenwärtigen Gefahr ab. Der erweiterte Sicherheitsbegriff trägt folglich der anschwellenden Multidimensionalität aktueller Sicherheitskomplikationen Rechnung. Daase hält fest, dass internationale Verflechtungen zu mehr Unwägbarkeiten und damit zu weniger absehbaren Konsequenzen führen. Gegenüber dieser Prämisse greift ein einfacher, militärisch geprägter Sicherheitsbegriff sicherlich zu kurz (vgl. Daase 2010, 18). Der erweiterte Sicherheitsbegriff allerdings führt Wertigkeiten ein, die nur aus gewissen Perspektiven tragbar sind. So scheint der Abbildung zufolge

die größte Gefahr zu bestehen, wenn ein Staat eine militärische Bedrohung für eine andere Nation darstellt. Allerdings zeigen unter anderem neuzeitliche, menschen- und klimabedingte Katastrophen wie das Hochwasser im Ahrtal aus dem Juli 2021 oder der Hunger im Jemen oder Südsudan seit einigen Jahren, dass regionale, ökologische Risiken, die die Gesellschaft treffen oder nur treffen könnten, erodierende Traumata für große Teile eines Landes nach sich ziehen können und teils dramatische Realfolgen für die Menschen haben. Somit erlaubt der erweiterte Sicherheitsbegriff kein durchweg stringentes Klassament der Sicherheitsbewertung, in dem eine Gefahr stets schwerer wiegt als eine andere, ist aber als Hilfestellung gewinnbringend.

Insofern kann nicht das Suppositum eines stabilen Sicherheitsbegriffs zugrunde liegen, sondern Sicherheit ist als die fortschreitende und dynamische Produktion dessen zu verstehen, was eine Gesellschaft als Sicherheit festschreibt. Die schematische Vereinfachung offenbart, dass Sicherheit kein finiter Begriff ist, der auf allgemeingültige, determinierende Charakteristika reduziert werden kann. Er lässt sich vielmehr durch eingrenzende Fragen nach einem gesellschaftlichen Konsens erfassen: Was sollen Sicherheitsvorkehrungen schützen? Wie viel Sicherheit ist notwendig? Gegen welche Bedrohung ist vorzugehen? Welche Mittel müssen eingesetzt werden? Welcher Preis ist für die angestrebte Sicherheit zu zahlen? Auf welchen Normen und Werten beruht diese Sicherheit (vgl. Kaal et al. 2009, 83)? Die zugehörigen Antworten sind gleichermaßen divers und subjektiv. Sie sind etwa abhängig von der individuellen Gefahrensituation, dem Bedrohungsempfinden oder dem soziokulturellen Bezugsrahmen.

1.2. Kultur und Institution

Der Kulturbegriff im soziologischen Kontext ist ein nicht greifbares, nicht abschließend festgehaltenes Konstrukt. Kultur bricht vielmehr hervor, als dass sie geschaffen wird. Sie ist der Sammelbegriff für ein Potpourri aus Aktionen, Künsten, Gegenständen, Gedanken und Vergangenheitserzählungen einer begrenzten Personengruppe „im Rahmen eines historisch gegebenen, sozial konstruierten Wissensvorrates und der von ihm zur Verfügung gestellten Wahrnehmungs- bzw. Erfahrungs-, Deutungs- und Handlungsschemata“ (Keller 2005, 214). Ebenso wie eine spezifische Kultur nur eine limitierte Anzahl von Menschen widerspiegelt, ist sie lokal und chronologisch eingeschränkt. So beruhen Kulturen auf vergangenen Kulturen. Manche überdauern

länger als andere. Gewisse Kulturen breiten sich über ganze Kontinente aus, andere nur auf wenige einzelne Menschen. Hinzu kommen Kulturpraktiken, die supranational wie temporal Gültigkeit besitzen, andere Teile von Kulturen werden jedoch nicht weiter adaptiert. Raymond Williams greift auf Herder zurück, um darzustellen, dass es nicht die eine Kultur gibt. Stattdessen plädiert er dafür, stets von Kulturen im Plural zu sprechen, die national, aber auch regional, ökonomisch – und seit einigen Jahren muss man sagen, auch virtuell und transgeografisch – nebeneinander, miteinander oder untereinander existieren (vgl. Williams 1985, 89). Diese recht indifferente Skizze zeigt bereits, dass der Terminus der Kultur selbst mindestens so ungenau und fließend ist, wie der Umstand, den dieser beschreibt.

Der Duden teilt die Definition der Vokabel sogar und unterscheidet zwischen der „Gesamtheit der geistigen, künstlerischen, gestaltenden Leistungen einer Gemeinschaft als Ausdruck menschlicher Höherentwicklung“ und der „Gesamtheit der von einer bestimmten Gemeinschaft auf einem bestimmten Gebiet während einer bestimmten Epoche geschaffenen, charakteristischen geistigen, künstlerischen, gestaltenden Leistungen“ (Duden 2019). Es wird demnach einmal die vollständige, manifestierte Schaffenskraft eines irgendwie gesellschaftlich gearteten Konstrukts in Abgrenzung zu allem Tierischen wiedergegeben (vgl. Schipper 2017, 31). Zugleich bildet Kultur das Ergebnis einer abgesteckten Ordnung ab, bei der Ausgestaltung und historischer Augenblick in Relation zueinander stehen und nur innerhalb eines kurzen Moments als stabil wahrzunehmen ist.

Doch warum soll die kulturelle Perspektive bei der Untersuchung von Sicherheitsaspekten überhaupt eine bedeutsame Rolle spielen? Warum nicht lediglich den Zustand der IT-Sicherheit zweier Staaten untersuchen? Darauf gibt es im Wesentlichen zwei Antworten. Zuerst unterliegt die Wahrnehmung von Sicherheit offensichtlich der soeben beschriebenen möglichen Diskrepanz zwischen Objektivität und Subjektivität. Dieses Gefüge ist für jede Gesellschaft, für jede Gruppe individuell und ergibt sich aus unterschiedlichsten Faktoren, wie beispielsweise der wirtschaftlichen Leistungsfähigkeit, historischer Traumata oder geopolitischer Einfassung (vgl. Burri 2015, 250). Derartige Rahmenbedingungen, eben die Kultur mit ihren zahlreichen materiellen und immateriellen Institutionen, entscheiden schließlich darüber, wie eine Gesellschaft zum Beispiel mit Sicherheit umgeht und welche Relevanz sie dem Thema in der alltäglichen Verhandlung einräumt. Das wiederum ist

der limitierende Faktor für Ressourcen, finanzielle Mittel oder Kompetenzen, die in der Lage sind, die drängenden Herausforderungen anzugehen. Eine solch verstetigte Einfassung in repetitive Prozeduren weist einem Thema seinen Stellenwert innerhalb eines Diskurses zu. Zweitens umschreibt Kultur gewissermaßen die Begegnungsprozesse, die einsetzen, verworfen werden oder aushärten, wenn Akteure auf Beschaffenheiten, Netzwerke oder weitere Akteure treffen (vgl. Siedschlag/Jerković 2014, 307). Dies verdeutlicht, dass neben dem rein technokratischen Blick auf Informationstechnik eine soziale und kulturelle Perspektive mindestens ebenso zentral ist. Erst wenn das Gewicht eines Motivs allgemein bekannt, anerkannt und somit in kulturelle Prozesse gegossen ist, können Problemstellungen umfassend bearbeitet werden. Man kann daher wohl kaum leugnen, dass Kunst, Mode oder Architektur – um nur wenige kulturmanifestierende Praktiken hervorzuheben – immer von simultanen ökonomischen, ökologischen, kriegerischen, technologischen oder spirituellen Umständen der jeweiligen Gegenwart bedingt wurden und werden (vgl. Stauff 2014, 516). Zugleich jedoch wirken kulturelle Akte auch auf den zeitgenössischen Kontext und das Lebensgefühl einer Epoche ein und wirken daran mit, die kollektive Identität fortzuschreiben, in der sie verhaftet sind (vgl. Hansen 2006, 71f).

Raymond Williams ergänzt deshalb noch eine dritte Spezifizierung, die im Duden nicht zu finden ist: Er beschreibt Kultur als „way of life“ (Williams 1985, 89). Dies meint nach Williams eine Akkumulation von Werten und Vorstellungen, die sich in der Lebensweise ganzer Gruppe oder gar Epochen niederschlägt und sich so schließlich im Verhalten wie auch in Institutionen wiederfinden lässt (vgl. Williams 1961, 41). Von der ersten Definition von Kultur als Idealisierung des Menschseins grenzt sich Williams Lesart insofern ab, als sie nicht derart generalistisch gefasst ist und eine präzisere Untersuchung von strukturellen Wechselbeziehungen ermöglicht. In die Gegenwart übertragen, würde Williams beobachten, welche Serien die Menschen schauen, mit welchen Ritualen sie sich begrüßen oder in welchen sozialen Begegnungsmomenten sie auf ihr Smartphone schauen. Von der Kulturdefinition als Produkt künstlerischer Arbeit differenziert sich der Way of Life jedoch auch, da er sich vollkommen unbewusst vollzieht; ganz im Gegenteil etwa zu Akten der Hochkultur wie Kunst, Musik oder Literatur (vgl. Williams 1960, 253f). Stattdessen sind diese Kulturen nach Williams Phänotypen des Way of Life, den sie in der Inszenierung materialisieren und produzieren (vgl. Williams 1960, 254). Obendrein lässt diese Perspektive den

Leistungs- und Anspruchsgedanken außen vor und ist in dieser Konsequenz vollständig wertungsfrei.

Daraus muss der Schluss folgen – zu dem auch Williams kommt – dass der Kulturbegriff und die Kultur im deterministischen Sinn nicht existieren. Stattdessen stellen sie den Versuch dar, divergierende Gegenständlichkeiten, Phasen und kontextualisierende, subjektive Wirklichkeiten zu überschreiben und in einem vagen Hyperonym zusammenzufassen. Es gilt daher stets, Kultur und ihre

Texte im Kontext umfassenderer kultureller Praktiken und sozialer Machtbeziehungen zu betrachten, wie sie zum Beispiel durch den Produktionskontext und die damit verbundenen ökonomischen Beziehungen bestimmt sind. Deshalb rücken die Spannungen zwischen Text und Kontext ins Zentrum. Mediale Texte werden zu Momenten größerer kultureller Formationen (Winter 2011, 428).

Aus diesem Grund kann auch die Untersuchung einer Cybersicherheitskultur der späten 2010er und frühen 2020er-Jahre nur unvollständig sein und wie jeder Ansatz zur Untersuchung eines spezifischen gesellschaftlichen Feldes lediglich den Blick auf einen festgelegten Ausschnitt ermöglichen. Erschwerend muss erwähnt werden, dass die maximale kulturelle Speicherkapazität begrenzt ist, laut David Lyon durch Digitalität sogar geringer wird (vgl. Bauman/Lyon 2013, 178). Das bedeutet, dass Vergangenes aus dem Reservoir allgemein überlieferter Erinnerungen verschwinden kann und so irrelevant für die Prägung alles Zukünftigen wird (vgl. Rudolf 2018, 65). Nur über die Annäherung aus vielen Perspektiven kann sich ein imperfektes, aber möglichst approximatives Bild der begutachteten Konstellation zu erkennen geben. Genau wie „Medien nur in der Verflechtung mit kulturellen Praktiken zu verstehen sind“, sind technologische Praktiken, die mit ihnen verbundene Sprache oder die Interdependenzen nur zu begreifen, indem sie in einen Kontext mit den zeitgenössischen Medien und Technologien gesetzt werden (Stauff 2014, 519). Cornelius Castoriadis nähert sich der Kultur als „Verhältnis zwischen Institution und gesellschaftlichem Leben“, ergo als „*Momente* in einer Struktur, die niemals starr ist und in jeder Gesellschaft ihre unverwechselbare Spezifität besitzt“ (Castoriadis 1990, 214f). Es zeigt sich, dass nicht nur die Betrachtungsweise von Sicherheit im Laufe der Zeit stetiger Reformation unterliegt, sondern tatsächlich auch das vage Gebilde der Kultur.

Ein weiterer Grund für eine Untersuchung von (IT-)Sicherheit unter kulturellen Gesichtspunkten leitet sich aus der angeführten These selbst ab. Denn indem man davon

ausgeht, dass Unterschiede im Umgang mit IT-Sicherheit bestehen, schließt dies auch die verschiedenen Voraussetzungen ein, die in Deutschland und in den Niederlanden herrschen. Da zugleich davon auszugehen ist, dass die technischen Voraussetzungen aufgrund des vergleichbaren Wohlstands- und Bildungsniveaus nahezu identisch sind, ist insbesondere der gesellschaftlich-kulturelle Umgang mit Sicherheits Herausforderungen von Interesse.

Was in einem gesellschaftlichen Sinnhorizont als rationale sicherheitspolitische Maßnahme erscheint, gilt einem anderen Horizont als irrationales Risiko. Festzuhalten ist also, dass der bedeutungsorientierte, praxeologische Kulturbegriff soziales Handeln nicht *rational*, sondern *relational* definiert (Daase et al. 2014, 37).

Der Begriff *Kultur* unterliegt verschiedenartiger Verwendungen, die nicht den gleichen Bezugsraum abdecken. Dabei gibt es einerseits Kulturen, die nur begrenzten Personen in ebenso begrenzten Raum-Zeit-Situationen zugeschrieben werden. Beispiele hierfür sind die Kinokultur oder die Essenskultur. Bei dieser Zuschreibung besteht die Kultur immer nur im Moment der Aktion beziehungsweise der Teilnahme, also während des Kinobesuchs oder während des Essens. Sie ist damit spezifisch und kann wechselnde Personenkreise zeitweise aus- und wieder einschließen. Der zweite Typus von Kultur ist umspannender gefasst und entlässt teilhabende Akteure nicht vorübergehend. Diese Ausprägung von Kultur ist kaum limitierend und bezeichnet gesamtgesellschaftlich normierte und internalisierte Verhaltensmuster, Annahmen und Moralkonstellationen. Im Unterschied zum Gesellschaftsbegriff, für den unter anderem Stephan Moebius und Dirk Quadflieg die Gefahr sehen, er könne mit dem Kulturbegriff verschwimmen, ist Kultur hier eine handlungsbeschreibende, eine interaktionsbeschreibende Terminologie und keine gruppenderminierende (vgl. Moebius/Quadflieg 2011, 12). Mittels einheitsstiftender Attribute wie Moralität, Relevanz oder Ideal ordnet Kultur eine Gesellschaft und gibt über Konsens stillschweigend Leitplanken vor. Bernt Schnettler steuert den Versuch bei, zu illustrieren, wie Kultur aus relationalem Verhalten hervorgeht und stützt hiermit auch den praxeologischen Kulturbegriff nach Daase, Junk und Rauer:

In der Wiederholung typischer Interaktionssequenzen entwickeln sich jedoch automatisch auf der Basis der wechselseitigen Typisierungen wechselseitige Erwartungszwänge bei den beteiligten Handlungspartnern, aus denen wiederum Handlungsverpflichtungen erwachsen, die damit die einmal interaktiv gefundenen Problemlösungen für bestimmte Handlungsprobleme verfestigen (Schnettler 2011, 216).

Demzufolge generiert mutuelles Verhalten antizipative und damit ordnend-strukturierende Annahmen darüber, was sowohl das Gegenüber als Nächstes tun wird als auch darüber, was von einem selbst zu tun erwartet wird. Die Wiederholung dieses schauspielähnlichen Ablaufs zementiert Aktionen zu Gewohnheiten oder Automatismen. Reziproke Erwartungen fordern somit regulierte Interaktion ein und manifestieren auf diese Weise allgemein wünschenswertes Verhalten. W. Penn Handwerker stützt ebenfalls diese Feststellung, indem er zusammenfassend postuliert, dass die Interaktion zwischen Menschen, also Reaktion und empathiebegründete Teilhabe, zur Veränderung von Überzeugungen und damit auch zur Veränderung von künftigen Handlungen führt (vgl. Handwerker 2009, 79). Die Repetition dieser vernetzenden Handlungen mündet ihm zufolge in Verhaltensmustern und schafft konventionelle, universelle Überzeugungen. Ein solches in Rituale gegossenes Verhalten ist nach Handwerker sichtbare Kultur (vgl. Handwerker 2009, 79). Schnettler substituiert diese These, indem er herausstellt, dass nur gegenseitiges Wirken gesellschaftlich konsolidiert werden kann:

Wechselseitige, typisierte Handlungen verfestigen sich zu Gewohnheiten, die mit Handlungserwartungen verknüpft eine bestimmte interaktive Problemlösung institutionalisieren. Grundsätzlich kann jegliche Handlung routinisiert werden [...], für die Institutionalisierung gesellschaftlichen Handelns sind aber die rein subjektiven Relevanzen ungenügend (Schnettler 2011, 216).

Daraus folgt einerseits, dass kulturalisiertes Handeln sich nicht verfestigt, weil individuelle Präferenzen gewisse Aktionen favorisieren, sondern es im Gegenteil einer kollektiven Legitimierung durch repetitive Konformität bedarf. Zugleich lässt sich deduzieren, dass die Ausformung von Kultur, Sitte und Moral sich nicht erzwingen, wenngleich aber forcieren, lässt:

Als Technik des Liberalismus und Neoliberalismus schafft Sicherheit Bedingungen, die es ermöglichen, Individuen in einem freiheitlich-liberalen Rahmen mittels Marktmechanismen zu lenken (Meyer et al. 2008, 13f).

In seinen Erläuterungen zur grundlegenden Konstruktion von Security Awareness beispielsweise hält Stefan Beißel fest, dass Verhalten gelenkt werden kann, indem es in erwünscht und unerwünscht dividiert wird, um es entsprechend zu belohnen oder abzustrafen (vgl. Beißel 2019, 137). Er legt demnach nahe, dass zwischenmenschliches Verhalten zu konditionieren ist. Mit dieser Annahme reduziert er Dynamiken humaner Interaktion jedoch zu deutlich. Das mag in dem von Beißel skizzierten Verständnis der Security Awareness noch funktionieren, da hier sichtlich begrenzte Räume mit starken

Hierarchien vorherrschen und auch da wohl ehemals eine gewisse Einigkeit über die Herstellung von Sicherheit, zum Beispiel am Arbeitsplatz, besteht. Kann man sich aber nicht mehr auf diesen Raum beziehen, weil ein Motiv etwa jeden Bereich des Alltags durchzieht, so lässt sich erwünschtes Verhalten nur schwer pauschal festlegen, noch weniger lässt es sich durch einfachste Belohnungsmechanismen herstellen.

Wenn man Kulturbildung betrachtet, ist es unentbehrlich, auf Schnettlers ‚soziohistorisches Apriori‘ zu blicken und festzustellen, „dass Menschen immer in bestimmte und bereits vorexistierende historische und gesellschaftliche Strukturen hineingeboren werden“ (Snettler 2011, 214). Sie wachsen in einem vordefinierten politischen, geografischen, religiösen, ökonomischen, biografischen und temporalen Sinnzusammenhang auf und erfahren so eine Vielzahl von Orientierungen, die die von Beißel angeführten Kategorien Regelverhalten, Risikoverhalten oder Problemverhalten derart maßgeblich modellieren, dass die aus dem Behaviorismus bekannten Mechanismen positiver und negativer Verstärkung nur noch bedingt dirigierend wirken können (vgl. Beißel 2019, 137). Somit deklariert Snettler den Menschen zum Verwalter seiner biografischen Umstände. Er schließt keineswegs aus, dass das Individuum „als Teil eines individuenübergreifenden Wissenssystems“ zu Veränderung veranlagt ist, sondern hält fest, dass jeder Einzelne mit einem in der Vergangenheit begründeten Ausgangskontext konfrontiert wird, mit dem er auf die eine oder andere Weise umzugehen verdammt ist (Busse 1987, 226). Diese Rahmung ist weder selbstverursacht noch umkehrbar. Stattdessen ist sie ein unauflösliches Paradoxon, da die Voraussetzungen genauso wie die spätere Aneignung von Lebenserfahrungen in absoluter Einzigartigkeit verlaufen und unterdessen auf einer Perzeption von Gemeinschaft, Umwelt und Medien beruhen – die gesellschaftlich-geschichtliche Institution, wie Castoriadis diese historio-soziale Einbettung tauft (vgl. Castoriadis 1990, 369).

Die Regeln werden durch eine, durchaus auch institutionell gebundene, diskursive Praxis bestimmt, welche als historisch gebundene das in einer Epoche zu sagen, zu denken und zu tun Mögliche begrenzt (Busse 1987, 225).

Somit ist dieses Dispositiv zugleich Voraussetzung für jedes kulturelle Handeln wie auch dessen limitierender Faktor. In der gesellschaftlich-geschichtlichen Institution verbirgt sich „gegenwärtiges Wirken des ‚Vergangenen‘“ (Castoriadis 1990, 369). Aus dieser Sphäre, so Castoriadis, treten die Institutionen des *legein* und des *teukein* hervor; das „*λέγειν* als eindeutige[r] Kodex und das *τεύχειν* als funktionelle, instrumentale

Tätigkeit“ (Tassis 2007, 274). Castoriadis postuliert damit im Wesentlichen, dass sich Gesellschaften produzieren und reproduzieren, indem sie von sich sprechen und indem sie ihre Vorstellungen in Handlung stabilisieren (vgl. Castoriadis 1990, 449). Dabei kann die Sprache bekanntlich nur Abbilder der Umwelt schaffen, aber nicht die Umwelt sein. Für das Tun stellt er fest, dass es sich letztlich um die „Materialisierung“ der imaginären Bedeutungen der betreffenden Gesellschaft“ handelt, die sich „in wirklichen gesellschaftlichen Tätigkeiten verkörpern, ausgestalten, darstellen, [ihre] Werkzeuge“ verstetigen muss (Castoriadis 1990, 590/594). In *legein* und *teukein* drückt sich also das gesellschaftlich-Imaginäre aus: Das *Sagen* und das *Tun* ermöglichen erst die Verwirklichung „gesellschaftlicher Selbstinstitutionalisierungsprozesse“ (Maierhofer 2003, 62). Castoriadis zementiert damit auch die performative Natur von Kultur und Gesellschaft.

Nick Couldry trägt dem Rechnung, wenn er sagt: „Media cultures derive from what people do with media“ (Couldry 2012, 158). Zwar bezieht er sich hier ganz deutlich auf Medienkulturen, liefert aber eine Vorlage zum Transfer. Denn auch Sicherheitskultur, Popkultur, Essenskultur oder Theaterkultur erwachsen aus dem, was Menschen innerhalb wie auch mit der jeweils konstruktivistischen Lebenswelt tun und sind Teil des „way of life“ (Williams 1960, 344). Kultur ist unter dieser Prämisse kein starres Gebilde, sondern eine flüchtige, nicht zu fixierende Beschreibung multipler, gleichzeitiger Handlungen inmitten unübersichtlicher Sozialsysteme. Hier springt zusätzlich Luhmann erkenntnistheoretisch zur Seite, indem er festhält, dass Kultur – egal welcher Art – insbesondere durch menschliche Interaktion ausgestaltet und unentwegt neu verhandelt wird.

Interaktionssysteme können und müssen laufend aufgegeben und neu begonnen werden. Das macht eine übergreifende Semantik, eine Kultur erforderlich, die diesen Vorgang in Richtung auf Wahrscheinliches und Bewährtes steuert (Luhmann 1985, 588).

Und ebenjene Kultur ist nicht naturgegeben, sondern eine Schöpfung des gesellschaftlich-Imaginären, das sich in „kollektiv wirksamen diskursiven Fundierungsprozesse[n]“ ausbildet und sich en passant faksimiliert (Maierhofer 2003, 59).

Das (ontologische) Magma ist in dieser Formel das Sein, aus dem sich eine unendliche Zahl funktionaler, identitätslogischer Mengen sowie imaginärer Bedeutungen entnehmen lässt. Diese Mengen werden durch Sprechen und Handeln unterschiedlich

instituiert und tragen so wiederum zum Magma bei, ohne es gänzlich herstellen zu können. Institutionen, nach Castoriadis also Instituiertes wie auchstituierendes, entnehmen stetig aus dem Magma und fügen Neues zum Konvolut der imaginären Bedeutungen einer Gruppe hinzu. Das gilt unter anderem für staatliche Einrichtungen, Religion, die Ökonomie oder auch Sprachen. Sprache reinkarniert das gesellschaftlich-Imaginäre: Die tausenden heute und in der Geschichte hervorgebrachten Sprachen entspringen einem Magma, das all diese Möglichkeiten der Sprachausbildung bereithielt. Dieser Theorie folgend bildeten sich aus einer Art Ur-Magma über die Ausdifferenzierung regional und kulturell abweichender Gesellschaftsmodelle zahllose Magmen, aus denen sich unzählige Sprachen und Dialekte fortlaufend ausdifferenzieren und zum Projektionsergebnis ihrer jeweiligen kulturell-historischen Umstände werden konnten.

Aus nahezu unbedeutenden Anfängen heraus gewinnt die instituierende Tätigkeit der ‚coustume‘ in dem Maße, in dem ihre gesellschaftlichen Phantasmen von den Subjekten aufgegriffen und [...] immer wieder reproduziert werden, eine machtvolle Eigendynamik (Maierhofer 2003, 60).

Das gesellschaftlich-imaginäre ist demnach selbst Magma, da es Quell von Handlung und Sprache ist, und Institution, da es sich selbst wie auch das magmatische Feld nachhaltig verformt (vgl. Tassis 2007, 321). So können immer nur Konzepte von beispielsweise Religion, Heimat, Demokratie, Sicherheit oder jeder anderen imaginären Dimension, die auf dem Fundament des Imaginären stehen und sich in Sprache und Habitus konstituieren, betrachtet und besprochen werden; nicht die Ursprünge, die sie zu modellieren versuchen. Es handelt sich um Ideen-von, nicht um die Demokratie oder Religion selbst.

Nachdem soeben ein Bild davon entstanden ist, auf welche Weise Verhalten und Überzeugungen internalisiert und zu Kultur übersetzt werden, stellt sich noch die Frage nach dem Zweck von Kultur, nach dem *Warum*, auf das die Projektion eine Antwort zu geben scheint. Bauman registriert Kultur als konservierenden, archaischen Überlieferungsmechanismus, der Vergängliches gegen das Fortlaufen der Zeit bewahrt.

Die Leistung der Kultur bestand von Anbeginn in der Überführung flüchtiger und vorübergehender Phänomene aus dem Reich menschlichen Lebens und Handelns in dauerhafte Objekte, aus dem Flüchtigen sollte das Dauerhafte, aus dem Diskontinuierlichen das Kontinuierliche erwachsen, um so die Grenze der Sterblichkeit zu überwinden und das endliche Leben des einzelnen in der Unendlichkeit der Gattung Mensch aufzuheben (Bauman 2000, 150).

Angesichts der menschlichen Endlichkeit, so also Bauman, verkörpert Kultur den Versuch, auf der Basis von Repetition, Kreativität, Erzählung und Überlieferung gewisse Leitmotive von der Zeit zu entkoppeln, sie zu tradieren und insofern Bleibendes zu schaffen. Folglich objektiviert der Mensch also, er speichert Bedeutungen und Intentionen in Gegenständen, Texten und Medien, sodass sie Raum und Zeit überwinden können. So ist es möglich, dass etwa Archäologen mittels eines Fundstückes Schlüsse auf die Intention einer längst vergangenen Person oder Gruppe ziehen können (vgl. Berger/Luckmann 2018, 37f). Dieses Argument aber greift als alleinige Erklärung für den Bedarf an Kultur zu kurz. Vielmehr ist die Traditionsschilderung Baumans als additional Funktion zu verstehen. Der Begriff der Kultur stellt den Versuch einer Vereinfachung eines indefiniten, sozialen Ordnungsschemas dar,

durch das eine Gesellschaft ihre Umwelt erfährt, ihr gemeinsam eine bestimmte Bedeutung zuschreibt, und mit dessen Hilfe sie versucht, einerseits strukturelle Umwelteinflüsse zu bewältigen und andererseits angesichts einer sich ständig wandelnden, komplexen Umwelt anpassungsfähig und handlungsfähig zu bleiben (Siedschlag/Jerković 2014, 307).

Vilém Flusser verdichtet Tradition, soziohistorisches Apriori und historisches Gemeinschaftsgefühl in einer Anthropomorphisierung, die bekannt erscheinen dürfte. Er attestiert den Produkten menschlicher Schaffenskraft – also nicht dem Menschen selbst, sondern etwa Kunst oder Literatur, aber auch Möbeln oder Gebäuden – ein kulturelles Gedächtnis zu bilden, das späteren Jahrgängen Orientierung bietet (vgl. Flusser 1989, 41). Er zieht hier die Demarkation etwa zwischen Mensch und Tier, da sich der Mensch als einziges Wesen seiner Vorgeschichte bewusst ist, sich in seine jeweilige Gegenwart einfügt und sogar die Fähigkeit besitzt, Parahistorien zu erdenken. Für Luhmann bedeutet das kulturelle oder das Mediengedächtnis, dass gewisse Verhandlungen über Faktizität nicht mit jeder Generation neu begangen werden müssen, sondern als gegeben akzeptiert werden (vgl. Luhmann 2017, 83). Gleichzeitig erkennt auch er das fortwährende „Diskriminieren zwischen Vergessen und Erinnern. Frei werdende kommunikative Kapazitäten werden durch Wiederbenutzung benötigter Sinneinheiten ständig neu imprägniert“, sodass ein Erstarren unmöglich ist (Luhmann 2017, 54). Für Berger und Luckmann transferiert das kollektive Erinnerungsvermögen konkretes Wissen. So geht im Tod eines Individuums sein genetisches Wissen verloren, sodass es gezwungen ist, das Gedächtnis vorab zu externalisieren, es dann zu objektivieren, sodass es schließlich wieder von Weiteren internalisiert wird – der Mensch kulturalisiert sich selbst

(vgl. Berger/Luckmann 2018, 51f/139). Dabei ist Tradition als Kulturbrücke immer auch Selektion, wie Raymond Williams anschaulich macht: Der Mensch zeichnet in medialen Texten auf – seien es Dokumente, Videospiele, Podcasts oder Institutionen – was ihn gegenwärtig bewegt und differenziert im Produktionsprozess zwischen wenigstens subjektiv relevanten Informationen und Behaviorismen und solchen, die es nicht festzuhalten lohnt. Williams gibt zu bedenken, dass vor allem jene Gruppen den stärksten Einfluss auf tradierendes Wissen haben, die Kultur rearrangieren und eine gesellschaftliche Dominanz aufweisen (vgl. Williams 1960, 340).

Sie reproduzieren sich selbst in Wort, Text, Musik, Kunst, Gesetz, Medien und Institution und realisieren auf diese Weise strukturelle Gegebenheiten, die kulturprägend sein können. Eine Idee, an die unter anderem Schnettler und Busse später anknüpfen, wenn sie darlegen, wie Menschen unter gewissen, mehr oder minder institutionalisierten Rahmenbedingungen aufwachsen und agieren müssen. Damit differenziert Williams die individuelle Gestaltungsfähigkeit von Kultur also nach Klassen, wenngleich heute Bezeichnungen wie sozio-ökonomische Gruppen treffender wären.

Diese Untersuchung bewegt sich aus all den soeben genannten Gründen im Fachgebiet der Cultural Studies. Denn wie Hasse und Krücken feststellen, können die Cultural Studies stabile Demarkationen wissenschaftlicher Praxis überwinden und die Methodik der Annäherung an das Kernphänomen unterordnen (vgl. Hasse/Krücken 2009, 82f). Die zentrale Fragestellung wird zur Maxime, sodass die Werkzeuge sehr differieren dürfen und nur wenige Ordnungsparadigmen vorherrschen. Dies eröffnet unter anderem sogar die Möglichkeit, „theoretische und historische Entwicklungen [einzubeziehen], die Aufschluss über die Gegenwart geben und zu ihrer Analyse und Veränderung beitragen können“ (Winter 2009, 82f). Die Cultural Studies sind mithin wie Kultur und Institutionen selbst: multidimensional anschlussfähig, äußerst kontextualisierend und zugleich hochgradig vielfältig in ihrer Dimensionalität.

1.3. I'majə,nerē¹¹

Sheila Jasanoff gibt ein Theorem an die Hand, das auf die Methode des Vergleichs zugeschnitten zu sein scheint und das insbesondere den Begriff des Imaginären beziehungsweise des *Imaginary* präzisiert, welcher bis hierher so selbstverständlich verwendet wurde. Sie bemerkt, dass die höchst komplexen und multidimensionalen Interaktionen, die in ihrer Gesamtheit eine Kultur ausmachen, für jede Nation, Gruppe, Gemeinschaft und ihre anhängigen Diskurse individuell sind, da sie einem ebenso einzigartigen Mosaik aus Framing, Wissensfundus und auch Zukunftsbildern entspringen – hier lassen sich durchaus Verwandtschaften mit der Castoriadischen Idee des Magmas ausmachen (vgl. Jasanoff 2015b, 334). Mit dem Imaginary stellt Jasanoff ein Axiom auf: Menschen erzeugen in der Verarbeitung ihrer Umwelt ikonische, meist vereinfachende Abbilder ihrer Lebenswirklichkeit. In dieses Panorama projizieren sie ihre persönlichen Biografien, ihre gegenwärtigen subjektiven Umstände, aber auch ihre Erwartungen für die Zukunft. Sie gießen Hoffnungen, Erfahrungen, Fakten und Meinungen in ein zunächst höchst subjektives Porträt des Was-Ist und des Was-Wird. Mehr noch stellen Individuen und Gruppen Bilder her, die mit Bedeutung angefüllt sind: „Der elaborierteste Wahn ist ebenso wie die geheimste und verschwommenste Phantasie aus ‚Bildern‘ gemacht, doch diese Bilder stehen für etwas anderes, haben also symbolische Funktion“ (Castoriadis 1990, 218). Hierbei ruhen die Überlegungen Jasanoffs und Anderer vornehmlich auf dem, was Jean Baudrillard schon in den frühen 90er Jahren über Simulakren, Simulationen und Science Fiction formulierte:

It is no longer possible to manufacture the unreal from the real, to create the imaginary from the data of reality. The process will be rather the reverse: to put in place "decentered" situations, models of simulation, and then to strive to give them the colors of the real, the banal, the lived; to reinvent the real as fiction, precisely because the real has disappeared from our lives. A hallucination of the real, of the lived, of the everyday-but reconstituted, sometimes even unto its most disconcertingly unusual details, recreated like an animal park or a botanical garden, presented with transparent precision, but totally lacking substance, having been derealized and hyperrealized (Baudrillard 1991, 311).

Er konstatierte damals, dass die Fiktion das Reale nicht nur tangiert, sondern sie maßgeblich initialisiert. Nach Baudrillard wird gar die Fiktion als Summe von Simulakren zur Vorlage für die Bildung von Realität. Diese Kraft des Imaginären wusste

¹¹ Lautschrift: Imaginary

sich unter anderem der deutsche Faschismus zu eigen zu machen, sodass der nationalsozialistische Staatswissenschaftler Carl Schmitt 1938 skandierte:

Keine noch so klare Gedankenführung kommt gegen die Kraft echter mythischer Bilder auf. [...] Wer solche Bilder benutzt, gerät daher leicht in die Rolle eines Magiers, der Gewalten herbeiruft, denen weder sein Arm noch sein Auge noch das sonstige Maß seiner menschlichen Kraft gewachsen ist (Schmitt 1982, 124).

Noch früher und kompromissloser aber als Baudrillard formulierte Jacques Derrida den Gedanken, den er jedoch vornehmlich auf Schrift, Sprache und Text anlegte: Mit dem Zeichen konzentriert Derrida seine dekonstruktivistische Idee auf die untrennbare Bindung von grundlegenden Symbolen oder Glyphen mit der Realität. Ihm zufolge ist es nicht möglich, einen „einzigen destruktiven Satz [zu] bilden, der nicht schon der Form, der Logik, den impliziten Erfordernissen dessen sich gefügt hätte, was er gerade in Frage stellen wollte“ (Derrida 1972, 425). Der Satz etwa, der die Regeln der Grammatik zu examinieren versucht, fabriziert sich innerhalb ebenjener grammatikalischen Gesetze. Deshalb schließt Derrida, dass das Zeichen immer schon so angelegt war, dass es ein *Zeichen-von* etwas ist, also ohne den Bezug auf ein entsprechendes Signifikat keinen Bestand hat. Sprache, Text oder andere Symbolkategorien sind damit stets reduzierte Abbilder ihres naturalen Pendants (vgl. Derrida 1972, 425). Umgekehrt heißt das, dass die Veränderung eines Zeichensystems oder seiner Regeln immer auch die inhärente Bedeutung der Zeichen modifiziert und somit Einfluss auf ihre Verwendung sowie auf die Lebenswirklichkeit hat (vgl. Flaßpöhler 2018). Die allegorische Aufladung eines Gegenstandes, eines Aktes oder einer Institution stellt schließlich das Band zwischen Zeichen und Sache her, zwischen dem Faktisch-Realen und dem darauf verweisenden Signifikanten her (vgl. Castoriadis 1990, 219). So verbindet etwa das Wissen, dass ein rotes Kreuz als Zeichen für medizinische Hilfe fungiert, dieses simple und zunächst inhaltsarme Symbol mit ‚Krankenhaus‘, ‚Arzt‘ oder ‚Medizin‘ und transportiert damit wirkungsvoll erfahrungsbasierte Fantasien und Erwartungen.

Jasanoff ergänzt mit den soziotechnischen Imaginaries die Idee der Zukunftswirksamkeit kollektiv-kultureller Anschauungen. Sie schreibt etwa dem literarischen Genre der Science Fiction Attribute einer selbsterfüllenden Prophezeiung zu: Die Fiktion eines möglichen Futurums hat eine aktivierende Wirkung, weil sie dazu mobilisiert, dieses Szenario zu erreichen oder es zu vermeiden. Dabei ist es unerheblich, ob es sich um dystopische oder utopische Zukunftsphantasmen handelt

(vgl. Jasanoff 2015a, 1f). Denn der Mensch erdenkt Bilder von sich selbst, indem er beispielsweise Kunst oder Literatur erzeugt und „damit auch *sich selbst* erschafft“ (Castoriadis 1990, 233). Die reine Spekulation über Wirklichkeitsmöglichkeiten auf Grundlage gegenwärtiger Parameter trägt das Potenzial zur Konstitution solcher Annahmen in sich. Der polnische Schriftsteller Stanislaw Lem zeichnet ein einleuchtendes wie simplifizierendes Sprachbild: „Es kann keinen Flug geben ohne vorangegangene Träume vom Fliegen“ (Lem 1981, 72). Umgekehrt kann etwa neue Technologie eben solche Vorstellungen generieren und erweitern. Musterhaft zu erwähnen ist der Aufstieg des Computers in den frühen 80er Jahren des letzten Jahrhunderts. Wenngleich sich neue Chancen auftaten, beschlich viele Menschen eine Skepsis gegenüber dieser intelligent wirkenden Universalmaschine. Sogar gegen zeitgenössisch weit entfernte Technologien, wie der künstlichen Intelligenz, entwickelte sich ein allgemeines Unbehagen, das sich bis in die Popkultur durchschlug; gut zu erkennen an Filmerfolgen wie *Terminator*, *Tron*, oder *Zurück in die Zukunft*. Dadurch wurde die damals neue Technik mit sichtlicher Faszination als handelnder, kognitiver Akteur stilisiert. Koinzident entzieht sich dieser Protagonist aber jeglicher Kontrolle und ist schließlich die Ursache des kulturellen Phobos. Mit zunehmender Erfahrbarkeit der Computertechnik in den folgenden Jahrzehnten wurde das Neue zum Alltäglichen, die Befürchtungen traten nicht ein und die Potenziale verdrängten viele der Bedenken.

Jasanoff, Castoriadis und viele weitere nehmen mit den soziotechnischen Imaginaries in den Blick, auf welche Weise derartige Deutungen (un)möglicher Topoi die Produktion und Evolution von Technologie beeinflussen und wie diese sich dann wiederum auf Gesellschaft niederschlagen. Das, „woran sich die Gesellschaft anlehnt, [erfährt] aufgrund dieser Anlehnung eine Veränderung durch die Gesellschaft“ (Castoriadis 1990, 580f). In Entwicklung, Herstellung und Vertrieb solcher Produkte – in Jasanoffs Beispiel Auto, Smartphone oder Computer – finden unzählige intersubjektive, soziale Prozesse statt, die einen immanenten Teil der Technik determinieren. Jasanoff weist Technologien darum als „integral components of social order“ soziokulturelle Relevanz zu (Jasanoff 2015a, 2). Technologische Erzeugnisse und Gesellschaft sind somit verwoben und reizen sich reziprok. Indem sie nun das wechselseitige Geflecht von Imaginaries und Wirklichwerdung auf die programmierte Verkettung von Gesellschaft und Technologie anwendet, gibt Jasanoff den

soziotechnischen Imaginaries eine insbesondere medienwissenschaftliche Tragweite. Sheila Jasanoff verdichtet soziotechnische Imaginaries schließlich:

Taking these complexities into account, we redefine sociotechnical imaginaries [...] as collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology (Jasanoff 2015a, 4).

Damit attestiert auch sie dem Imaginary performative Wirkung, die sich im sozialen Gefüge, beispielsweise in Werten oder Institutionen, niederschlägt und zugleich aus diesen hervorgeht. Sie konstatiert, dass neue Technologien entstehen, weil die Menschen, die sie entwickeln, ihr Ideal eines Zukunftsbildes verfolgen. Diese Imagination ist dabei bereits ein Produkt existierender Technologien, sozialer Strukturen oder auch kontemporärer Umwelteinflüsse. Die „Erfahrbarmachung“ neuer Medientechnologie“ ist ein Sprungbrett für das Vorstellungsvermögen zukünftiger Medientechniken und -praktiken (Ernst/Schröter 2020, 108). Dabei spielt es nur eine untergeordnete Rolle, ob diese Erlebnissituation etwa über das unmittelbare Nutzungserlebnis aktueller Technologie oder über die Rezeption von Zukunftsliteratur erfolgt; in jedem Fall keimt die Fantasie einer Entwicklungsmöglichkeit (vgl. Ernst/Schröter 2020, 108). Ob diese Zukunft eintreten wird oder kann, ist jedoch im Erlebnismoment ungewiss, denn „[k]ein imaginary ist in der Lage, genau festzulegen, was wir in der Praxis tun oder was wir in etwas sehen“ (Ernst/Schröter 2020, 109). Diesen Einwand führte Raymond Williams schon 1960 ins Feld, als er davon sprach, dass wir die Zukunft nicht kennen können. Jedoch versuchten wir heute, die Gegenwart so zu gestalten, dass sie nach unserem Empfinden auf eine der möglichen (und erstrebenswerten) Zukünfte zulaufen muss (vgl. Williams 1960, 354). Allerdings können Imaginaries so desiderabel sein, dass breite Einigkeit besteht, diese Zielvorstellung auch erreichen zu wollen oder zu müssen – wie der Weg dorthin aussieht und ob dieser Weg dann erfolgreich ist, steht auf einem anderen Blatt.

Ernst und Schröter kondensieren aus dem Verständnis soziotechnischer Imaginaries von Jasanoff und Kim, Castoriadis, Williams, Baudrillard und all der anderen diverse nachvollziehbare Eigenschaften dieser Zukunftsprojektionen (vgl. Ernst/Schröter 2020, 48). Sie beschreiben etwa, dass sich Imaginaries neben den schon genannten Merkmalen dadurch auszeichnen, dass sie in der Interaktion verhandelt werden. Sie kommen in der gemeinschaftlichen Verflechtung auf und schreiben sich

zum Beispiel durch Medien oder Kommunikation fort. Imaginaries werden als Werkzeuge teils bewusst kreiert und dienen als Bindeglied zwischen Wissenschaft, Technologie und Gesellschaft. Sie erhärten und stabilisieren sich in Vorstellungen und Normen noch vor der Wirklichwerdung erdachter Technologie (vgl. Ernst/Schröter 2020, 48). Damit sind Imaginaries zwar individuell konstruierte Abbilder, können jedoch als solche ausschließlich aus interpersonellen Verhandlungsprozessen erwachsen; es „bedarf [...] kollektiv verfügbarer Signifikanten und vor allem Signifikate“, die sich wiederum über Sprache und Tun produzieren (Castoriadis 1990, 248). Nach dieser Auslegung fügt das Imaginary also der auf Wissen fixierten Wirklichkeitskonstruktion von Berger und Luckmann unter anderem Kontextualität und Intention hinzu (vgl. Keller 2005, 66). Es rekurriert auf das Kulturverständnis von Schnettler oder Luhmann und liefert ein Modell für die Nahtstelle zwischen Personen wie auch Generationen überschreitender Kultur und jedem einzelnen Teilhaber dieser spezifischen Gruppen. Das Imaginary verdeutlicht den Prozess innerhalb des Individuums nach Erhalt einer Botschaft und vor Weitergabe seiner individuellen Interpretation, ergo die Eingabe, Verwertung und Ausgabe überindividuellen Wissens. Zugleich steht es nicht für jede einzelne Vorstellung singulärer Personen, sondern verweist auf kulturell bedingte Wahrnehmungen der Realität (vgl. Jasanoff 2015a, 14).

Those imaginaries help explain why societies differ [...], how they evolve through time [...], how powerful vision spread through space [...], and how they in turn burrow into human identity and subjectivity [...] (Jasanoff 2015b, 338).

Das schließlich erlaubt, Imaginaries mit politischen Entscheidungen oder auch akzeptierten Institutionen in Relation zu setzen. So stehen hinter Reglementierungen, insbesondere innerhalb demokratischer Gemeinschaften, sich wandelnde Anschauungen des Wirklichen, die je auch den sozialen und politischen Zeitgeist einfangen. So zeigte sich etwa die Geschlechterungleichheit und das konservative Familienbild der frühen Bundesrepublik darin, dass man sich erst 1957 durchringen konnte, das Gesetz über die Gleichberechtigung von Mann und Frau ins Leben zu rufen, das noch bis in die frühen 90er-Jahre Lücken aufwies¹². Solche Referenzialität auf ursächliche Leitvorstellungen lässt sich heute wenig überraschend genauso entdecken: Wenn etwa das Bundesverfassungsgericht auf Initiative von Klimaaktivisten feststellt, dass „die

¹² Bis 1993 war bei Uneinigkeit in der Namenswahl zweier Ehepartner der Name des Mannes zum Familiennamen.

nationalen Klimaschutzziele und die bis zum Jahr 2030 zulässigen Jahresemissionsmengen insofern mit Grundrechten unvereinbar sind“, repräsentiert dieser Entscheid auch den progressiven Wandlungsprozess im Umgang mit den Herausforderungen der Umweltausbeutung (Bundesverfassungsgericht 2021). Das Wissen um eine herannahende Klimakrise manifestiert sich in dieser Korrektur der Politik und in einer neuen Lesart des Grundgesetzes, weil große Bevölkerungsgruppen die dystopischen Aussichten noch abzuwenden versuchen. Denn in der Regel verbergen sich in den Imaginaries allgemein anerkannte Konventionen, die von den übrigen Partizipanten der Gesellschaft überzeugt getragen oder mindestens geduldet werden.

Nun ist es ein Grundprinzip der Informationssicherheit, manch einer mag sagen ein Grundproblem, sowohl in technischer als auch in kulturell-habitueller Auslegung, exakt im sprunghaften Verhältnis von neuen und zukünftigen Medien gefangen zu sein. Ernst und Schröter unterscheiden nämlich zwischen Imaginationen, die zukünftige, noch nicht existierende Medien abbilden und „imaginaries, die sich entwickeln, wenn ein Medium ›neu‹ ist“ (Ernst/Schröter 2020, 15). Vorstellungen darüber, was bald durch Technologie möglich sein könnte, beruhen auf dem Wissen über bereits bestehende Technologien; sie induzieren der Zukunft folglich die Potenz der Gegenwart. „Securitization must be understood as both an existing reality and a continual possibility“ (Williams 2003, 522). Exemplarisch führt auf diese Weise erst die vage Fiktion einer bevorstehenden Wahrscheinlichkeit von künstlicher Intelligenz – auf der Faktenlage der gegenwärtigen Technologiedynamik – zu einem Spannungsfeld zwischen unerschöpflicher Progression und maximalem Unbehagen¹³. Ernst und Schröter berücksichtigen außerdem die performative Wirkkraft solcher Zukunftsformulierungen, die hier bereits zu Jasanoffs soziotechnischen Imaginaries behandelt wurde, und übertragen sie auf die fortwährende Medientransformation. Auf

der Ebene der Verbindung von Imagination und Medienwandel in konkreten Praktiken wirken zukünftige Medien ›performativ‹ auf den Medienwandel ein. Dies tun sie vor allem als sogenannte ›imaginaries‹ – historisch wandelbare und mitunter sehr spezifische Formationen des Imaginären, mit deren Hilfe man sich das oben genannte ›Bild‹ vom Medienwandel in einer möglichen Zukunft macht (Ernst/Schröter 2020, 15).

Das Imaginary ist damit ein Medium der Wirklichkeitskonstruktion, das sich aus Facetten der Realität synthetisiert und mittels dieser selektiven Kompilation simultan

¹³ Populäres Beispiel sind die Prophezeiungen des amerikanischen Futuristen Raymond Kurzweil über die *technologische Singularität*.

dazu beiträgt, die Wirklichkeit auf eine andere Weise zu betrachten und zu inszenieren (vgl. Ernst/Schröter 2020, 51). Ernst und Schröter haben bereits acht charakteristische Eigenschaften von Imaginaries herausgearbeitet, von denen an dieser Stelle drei im Besonderen von hervorragender Bedeutung sind (vgl. Ernst/Schröter 2020, 48). So erkennen sie erstens, dass Imaginaries zwar von Einzelnen getragen werden können, sie aber meist innerhalb von Gruppen aufkeimen und diese als Nährboden benötigen, um sich viral zu reproduzieren. Sie bekräftigen zweitens die kollektive Veranlagung der Imaginaries, indem sie festhalten, dass diese Wirklichkeitsvorstellungen auf Multiplikatoren wie Massenmedien, Politik oder auch Popkultur angewiesen sind. Imaginaries benötigen also diese Instrumente, um sich zu replizieren und einen relevanten Wirkungsbereich einzunehmen. Ernst und Schröter beschreiben zwar, dass sich Imaginaries interpersonell vervielfältigen. Sie stellen aber außerdem fest, dass Imaginaries nicht allein auftreten und „zu einem historischen Zeitpunkt [...] verschiedene imaginaries“ existieren. Gleichzeitig bedeutet das, dass Imaginaries damit Anschauungen und Bilder nivellieren, da sie stets in einer Art darwinistischem Wettbewerb um die kulturdominierende Exegese, mithin „um strittige Akzeptanz von Ereignisdeutungen, Handlungsoptionen, Geltungsansprüchen, Orientierungswissen und Werten in Gesellschaften“ stehen (Felder 2013, 21). Ekkehard Felder beschreibt diese Kontrarität, indem er nicht von Anschauungen oder Leitbildern, sondern von Wissensbeständen spricht. Er legt dar, dass Wissen, Tatsachen oder Wahrheiten einerseits aus unanfechtbaren Daten, beispielsweise dass Wasser unter Normdruck bei 100 °C siedet, und andererseits aus produzierten, aber streitfähigen Studiendeutungen, etwa dass Fleischkonsum ungesund sei, bestehen (vgl. Felder 2013, 14). Setzt sich ein Imaginary nun durch, entweder weil es durch Daten gestützt wird oder weil seine Versprechungen verlockender respektive überzeugender sind als andere, so reduzieren sich gesellschaftliche Diskrepanzen und Antithesen, sodass sich diese neue Faktizität als Konvention etabliert.

Hieran schließt das dritte wesentliche Charakteristikum von Imaginaries an, das Ernst und Schröter herausgearbeitet haben: Denn Imaginaries werden „von Nationalstaaten, Unternehmen oder sozialen Bewegungen (z. B. Umweltbewegung) hervorgebracht“ (Ernst/Schröter 2020, 48). Damit können Imaginaries intendierte Erzeugnisse sein, die bewusst installiert werden und ein spezifisches Resultat herbeiführen sollen. Die Bundestagswahl 2021 eignet sich als anschauliches Beispiel für die eben genannten

Eigenschaften von Imaginaries. Denn um die Wählerinnen und Wähler möglichst zahlreich von der eigenen Partei zu überzeugen, zeichneten die Akteure subjektive Bilder der Gegenwart und stellten diesen Bilder der Zukunft gegenüber. Allen voran nutzten sie die TV-Debatten der Kandidierenden für das Kanzleramt, um Unterschiede beispielsweise in der Umwelt-, Arbeits- oder Sozialpolitik zu unterstreichen. Die Union beschrieb Deutschland als stabil und wirtschaftlich stark, um so die Ergebnisse der letzten Regierungsperiode zu unterstreichen. Zugleich bat sie um Vertrauen und versprach Konstanz sowie Halt für die folgenden Jahre. Die Grünen hingegen betonten die globale Klimakrise und formulierten das Credo der letzten Chance für einen Umbruch. Dazu wiederholten sie stetig, dass eine nachhaltige Klimastrategie, damit die Wende im Umweltschutz, alternativlos sei und kreierten so einen endzeitlichen Abzug einer Zukunft ohne grüne Politik. Die SPD wiederum porträtierte Deutschland als zwar wohlhabendes, aber ungerechtes Land, in dem nur wenige stark profitierten. Daher gab die Partei aus, die Weichen für Umverteilung und mehr Solidarität zu stellen. Letztlich wurde in den letzten Wochen des Wahlkampfes deutlich, dass die drei größten Parteien verschiedenste Momentaufnahmen Deutschlands herstellten, um möglichst große Gruppe für die jeweiligen Zielvorstellungen einzunehmen, obgleich ihre Programme teils große Überschneidungen aufwiesen. Gleiches gilt für ihre figurativen Versprechungen für die Zukunft: Sie hoben singuläre Tatsachen hervor und ignorierten andere, um Bilder des Jetzt und des Werdenden zu erschaffen, die den Wählenden möglichst attraktiv erscheinen sollten. Ganz nach Castoriadis schuf man Bilder, deren Ursprünge zwar im Realen verhaftet waren, die aber subjektiv „unterschieden [...] zwischen dem, was geschehen soll, und dem, was nicht geschehen darf“ (Castoriadis 1990, 250). Ekkehard Felder leitet von solchen Praktiken ab, dass der Analyse von Diskursen unter Einbeziehung der diversen Perspektiven und Akteure besondere Bedeutung zukommt, da die Leitfiguren einer Debatte selektieren, welche Wissensbestände priorisiert zur Sprache kommen oder welchen Sachverhalten keine Beachtung zu schenken ist (vgl. Felder 2013, 15).

Ulrike Felt leitet aus der Wirkkraft der Imaginaries ab, dass Staaten als institutionalisierte Entitäten großer Menschengruppen auch technopolitische Identitäten ausbilden. Durch die (nicht-)Entwicklung von Technologieprojekten determinieren Nationen, ob sie technophil oder technophob auftreten und damit auch, ob sie ein innovationsfreundliches Klima bereitstellen oder Aversion zeigen (vgl. Felt 2015, 104).

Sie komprimiert ihre Idee in dem Begriff des „innovation governance“ (Felt 2015, 105). Demnach hat der Staat die Kraft, verschiedene Weichen so zu stellen, dass Anreize entstehen oder beispielsweise der ökonomische Druck zu einer Konzentration von schöpferischen Anstrengungen führt. Regierungen können mit solchen Maßnahmen regulieren, welche selbstreflexiven Impressionen sich durch geteilte rhetorische Figuren wiederholen und reproduzieren (vgl. Felt 2015, 105). Am Beispiel der österreichischen Ablehnung von Atomkraft illustriert Felt, dass die in einer historischen Reihe von Technologieskepsis verwurzelte Entscheidung gegen die Verwendung von Atomenergie ein anhaltendes Selbstverständnis der Bevölkerung geprägt hat, in dem nationale Souveränität, demokratisches Selbstbewusstsein, Nachhaltigkeit und viele weitere soziopolitische Felder langfristig eingefärbt wurden (vgl. Felt 2015, 109). Dabei schildert sie nicht nur ein gegenwärtiges soziotechnisches Imaginary, sondern steuert zusätzlich eine Erläuterung für Kriterien bei, mit denen eine Technologie aufwarten muss, um eine ausreichende Hingabebereitschaft der potenziellen Benutzer hervorzurufen: Entweder muss die Technologie als ursprünglich national zugehörig verstanden werden, also ein offenes Produkt der lokalen Traditionen sein, oder sie muss geeignet sein, in die Erzählung der Kulturgemeinschaft integriert zu werden, etwa durch ihre unwiderlegbaren Vorzüge sowie durch ihre Passung mit den regionalen Gegebenheiten (vgl. Felt 2015, 109). Auf diese Weise können relevante Akteure die Hoheit über die Diskursrichtung erlangen, also Macht ausüben, und gleichzeitig an der Kondensierung einer Individuen übergreifenden Identität Anteil haben.

In Conclusio sind Imaginaries zunächst Wirklichkeitsvorstellungen, die jede Person auf Basis ihrer Erfahrungen, Umstände oder zwischenmenschlichen Interaktionen aggregiert und zusammenfügt. Jedoch ist eine wesentliche Eigenschaft von Imaginaries, dass sie intersubjektiv große Schnittmengen, also zwischenmenschliche Similaritäten, aufweisen. Dies wiederum bedeutet, dass jene scheinbar subjektiven Vorstellungen miteinander in Verbindung stehen. Sie sind folglich Produkt und Produzent von Kultur zugleich, wenn sie aus Kommunikation erwachsen und wiederum in Kommunikation münden, ergo in der Weitergabe des individuell reproduzierten Imaginaries. Aber Jasanoff entdeckt in Imaginaries nicht nur das Ergebnis von willkürlichem, intersubjektivem Austausch, sondern macht das Idiom der Koproduktion aus (vgl. Jasanoff 2015a, 14). „[T]hese imaginaries are at once products of and instruments of the coproduction of science, technology, and society in modernity“

(Jasanoff 2015a, 19). Es zeigt sich, Imaginaries erleichtern die Untersuchung des oben beschriebenen, multiperspektivischen Zusammenspiels von Mensch und Technik. Sie lassen sich etwa in Gesetzen, politischen Entscheidungen oder massenmedialen Agenden ablesen und erlauben wieder neue Hypothesen über die kulturelle Verankerung dieser Codices. Dieses

ursprünglich strukturierende Moment, [...] dieser Träger aller Verknüpfungen und Unterscheidungen zwischen Wichtigem und Unwichtigem, dieser Ursprung der Seinsbereicherung, [...] – dieses Element ist nichts anderes als das Imaginäre der Gesellschaft oder der jeweiligen Epoche (Castoriadis 1990, 249f).

Sodann dient das Imaginary als methodisches Werkzeug zur Dechiffrierung abweichender Handhabungen von identischen technologischen Herausforderungen zweier Vergleichsgegenstände und stellt insofern ein nützliches Konstrukt dar, um die Besonderheiten der deutschen wie der niederländischen Cybersecurity Cultures zutage zu fördern.

1.4. Exegese des Begriffs *Sicherheitskultur*

Daase, Junk und Rauer unternehmen nicht den Versuch einer universellen Kulturdefinition, sondern wagen sich an die Subform Sicherheitskultur. Dabei bringen sie den Begriff der Hybridität nach Münkler ein, also ein „Bereich, in dem vermittelt über Kommunikation, Diskurse und Narrative darüber entschieden wird, was als eine Gefahr angesehen wird und wie ihr begegnet werden sollte“ (Daase et al. 2014, 43). Sie setzen voraus, dass Sicherheit immer Bezug zu einer Bedrohung voraussetzt – egal ob diese unmittelbar oder indirekt bevorsteht.

Nach dem soeben geschriebenen Zeilen sind Kultur und folglich auch Sicherheitskultur eine fließende Verhandlung dessen, was für angebracht, für notwendig oder auch für selbstverständlich gehalten wird. Die Sicherheitskultur oder Security Culture begründet sich in der Determinierung als

Summe der Überzeugungen, Werte und Praktiken von Institutionen und Individuen, die darüber entscheiden, was als eine Gefahr anzusehen ist und wie und mit welchen Mitteln dieser Gefahr begegnet werden soll, bietet einen Rahmen, soziale und politische Wandlungsprozesse zu verstehen und zu erklären (Daase 2012, 40).

Die Autoren haben die Sicherheitskultur aus Gründen der Eingängigkeit in eine Grafik gegossen, die die Schnittstellenaufgabe der Wortschöpfung veranschaulicht (siehe Abbildung 6). Im Bereich der politischen Kultur agieren dabei vorwiegend die

Bürger oder Wähler, ergo das Gros der Bevölkerung. Sie leben und handeln im Kontext tradierter, politischer Wertesysteme. Die politische Kultur ordnet „sektorale Subsysteme“ und stellt Individuen in Relation zu politischen Systemen (Daase et al. 2014, 39). Innerhalb dieses Kulturraums prallen Emotionen und Meinungen verschiedener politischer Strömungen direkt aufeinander und entladen sich in Konfrontation beziehungsweise durch unmittelbare Diskussion. Der Fokus richtet sich folgerichtig auf die zahlenmäßig überwiegende Population eines staatlichen beziehungsweise nationalen Gefüges.

Demgegenüber steht die strategische Kultur, innerhalb derer der Blick auf den lenkenden Akteuren liegt. Zu diesem Feld gehören schließlich Subkategorien wie Außenpolitik oder Kriminalprävention. Mehr noch als über die Elitenzuordnung definiert sich dieser Kulturbegriff über das strategische Vorgehen, ergo einer Top-Down-Aktion, die von der Planung über die Ausführung bis zur Erreichung eines von Beginn an festgeschriebenen Ziels stringenten, strategischen Horizonten folgt. Dabei sind Risikoabwägungen zu treffen und Entscheidungsoptionen komparativ abzuwägen (vgl. Daase et al. 2014, 42). Die strategische Kultur etabliert soziale oder politische Kontrahenten und legt taktische Vorgehensweisen fest. Diese stehen in einem „symbolischen Kampf um die Durchsetzung ihrer Weltdeutungen“ (Keller 2005, 73).

Letztlich fehlt es beiden genannten Ideen in dieser Vorstellung an Schnittmengen. Auf der einen Seite steht die politische Kultur als gesellschaftlich quantitatives Übermaß, das Agenden, im vorliegenden Fall Sicherheit, über Diskurse schafft und dabei zwangsläufig den Blick stets auf, teils gegen, die wirkmächtigen Eliten richtet. Diese wiederum entwickeln Sicherheitsstrategien, vielmehr Gefahrenvermeidungsstrategien, und legen sie der Mehrheit auf. Daase, Junk und Rauer lokalisieren in genau der Sphäre, in der sich nun beide Milieus oder mindestens ihre politischen Erzeugnisse treffen, die Sicherheitskultur. Dazu zeichnen sie das Bild „eines Scharniers, indem es den Umgang mit Gefahren, Unsicherheiten und Risiken jeweils als Ausdruck von bedeutungsgenerierenden Diskursen und Narrativen und als Teil eines Wechselspiels zwischen Staat und Gesellschaft begreift“ (Daase et al. 2014, 42).

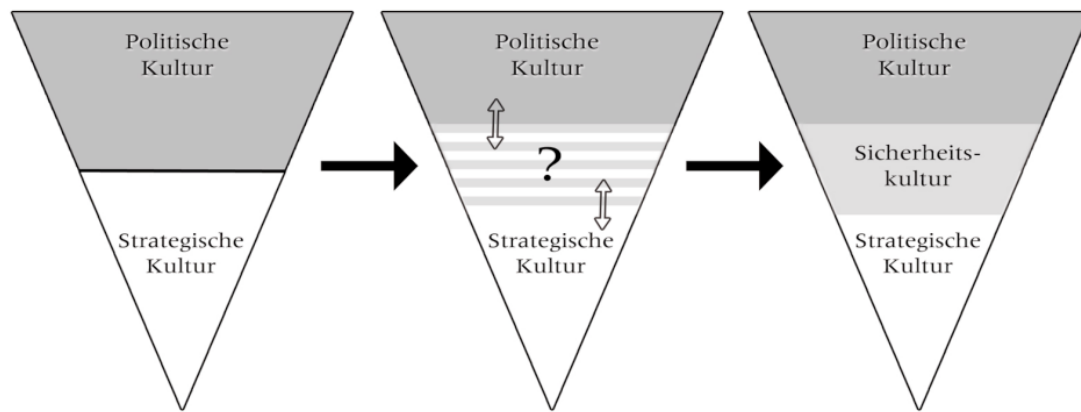


Abbildung 6: Wandel sicherheitskultureller Begrifflichkeit (Daase et al. 2014, 45)

Diese diffuse Sicherheitskulturdomäne wird unter anderem gekennzeichnet durch popkulturelle Leitmedien, technologische Innovationen, Krisen oder die Auseinandersetzung mit Diskursen. Intra- und intergesellschaftliche Kommunikation und Interaktion bilden wiederkehrende und wechselseitig bedingende Kontaktpunkte für politische wie auch strategische Kultur, in denen objektive und subjektive Sicherheit zusammentreffen, aber in denen auch eine Kultur der Bedrohungsvermeidung entsteht, indem der Umgang mit Gefahren wiederkehrend und auf bewehrte Weise verbalisiert, priorisiert und schließlich bewältigt wird. Christoph Gusy untermauert dieses Verständnis der basalen Eigenschaft von Kultur, insbesondere von Sicherheitskultur, indem er festhält:

Kultur ist primär Kommunikation. Sie besteht nicht aus den Dingen selbst, sondern schließt Kommunikation über die Dinge jedenfalls mit ein. Nur so tritt zum Wohnen die Wohnkultur, zum Bauen die Baukultur, zur Politik die politische Kultur. Und nur so tritt zur Sicherheit die Sicherheitskultur (Gusy 2010, 112).

Mittels dieser Kommunikation bildet sich demzufolge heraus, welche sicherheitsbezogenen Themen relevant werden, welche sich nachhaltig festschreiben und welche schließlich spürbare Konsequenzen haben. Dabei äußert sich Sicherheitskultur in diversen Formen wie beispielsweise Strategien, Zielen, exekutiven Maßnahmen oder medialem Framing. Sicherheit als kultureller Prozess ist immer eine herbei zu wünschende Konditio, die zur Zielgröße ausgerufen wird. Passend zu diesen Zielen lassen sich Handlungsmuster dann so adaptieren, dass sie zur Verwirklichung hinführen und umgekehrt (vgl. Daase et al. 2014, 37f). Zur Aufdeckung dieses Prozesses identifiziert Balzacq drei relevante Analyseeinheiten, verwandt mit den vier Dimensionen, die Daase mit seinem erweiterten Sicherheitsbegriff aufstellt

(siehe Abbildung 5): Erstens das Referenzobjekt, also jenes Objekt, über das Sicherheit verhandelt wird. Zweitens sieht er den *securitizing actor*, der Sicherheit artikuliert und damit definiert. Als dritte Einheit nennt Balzacq die funktionalen Akteure, also diejenigen, deren Handeln sich auf die Herstellung von Sicherheit auswirkt (vgl. Balzacq 2005, 178). Somit hängt Sicherheits- respektive Gefahrenempfinden nicht ausschließlich davon ab, welche Ereignisse augenblicklich stattfinden, sondern ebenso davon, welche Kommunikationsverläufe darum herrschen. „Therefore, how problems are ‘out there’ is exclusively contingent upon how we linguistically depict them“ (Balzacq 2005, 181). Die wesentliche Aufgabe der Sicherheitsgesellschaft besteht somit in der „Verwaltung des empirisch Normalen“, also in der Besprechung dessen, was nun als Sicherheitsstandard gilt und was darüber hinausgeht (Terberl/Wendekamm 2014, 331f). Die Feststellung in Erinnerung, dass Sicherheitskultur nie eine absoluter, sondern immer nur ein relativer und subjektiver Zustand sein kann, kann nicht nur von Belang sein, wie diese Sicherheit produziert wird. Stattdessen gibt die Verhandlung des übrigen Restrisikos ebenso viel über eine Gruppe oder eine Gesellschaft preis. „Es gilt, nicht nur den Begriff der Sicherheit, sondern den Blick auf Sicherheit zu erweitern“ (Endreß/Feißt 2014, 29). Notwendigerweise entstehen Imaginationen von Bedrohungen, Zielen und vermeintlich geeigneten Maßnahmen (vgl. Jasanoff 2015b, 338):

Zum einen gelingt den Menschen die Lösung realer Probleme gerade nur deshalb, weil sie zur Imagination fähig sind; zum anderen wären jene realen Probleme keine solchen, das heißt könnten sich nicht als diese Probleme stellen, die sich die jeweilige Epoche oder Gesellschaft gerade zu lösen vorgenommen hat, wenn es nicht ein zentrales Imaginäres der betreffenden Epoche oder Gesellschaft gäbe (Castoriadis 1990, 230).

Die oben beschriebenen Imaginationseffekte sind Jasanoff wie auch Castoriadis zufolge unerlässliche Bedingungen, um ein Problem angehen zu können; um eine gesamtgesellschaftliche Aufgabe zu kultivieren. Im Kontext der Sicherheit muss also ein übereinstimmendes Zielmaß an Sicherheit gegeben sein, das die Gesamtheit der Gesellschaft zu erreichen oder zu erhalten versucht und somit gewisse Diskurse und Entscheidungen erst möglich macht. Über Debatten, teils mittels Gewalt, als Folge einschneidender Ereignisse oder aber durch eine geopolitische Exposition setzen sich Ideale eines Soll-Zustands durch. Diese Zukunftsverheißungen leiten das gegenwärtige Weltbild sowie die aktuelle Sicherheitspolitik in ihrem Handeln an und haben das Potenzial, eine Gesellschaft zu stabilisieren und weniger bedeutsame Streitpunkte

vorerst beiseite zu legen (vgl. Schwarz 2014, 78). Denn Sicherheit respektive die Angst vor Unsicherheitszuständen zieht Demarkationen zwischen dem *Wir* und dem *Sie* und hat damit eine inhärent identitätsstiftende Implikation.

[...] security discourses draw boundaries around the "we" on whose behalf they claim to speak, and the "you's" who are simultaneously addressed by the linking of fears and threats to "feelings, needs and interests" (Hansen/Nissenbaum 2009, 1165).

In dem Augenblick aber, in dem sich „Konflikte von ihren tradierten und erprobten Lösungsmustern abkoppeln“, wird die bisherige Methodik obsolet (Schwarz 2014, 84). Die Akteure stehen dann vor der Herausforderung, Normalität neu zu entwerfen. Das Normale ist es dann auch, das bestimmt, wie wehrhaft sich eine Gesellschaft gegenüber Bedrohungen zeigt. „Das Ausmaß an Krisenfestigkeit und Besonnenheit handelnder Akteure kann mit dem Begriff Resilienz umschrieben werden“ (Giebel 2014, 368). Resilienz setzt voraus, dass der Einzelne die systemberührende Umwelt als solche begreift, ihre Prinzipien durchdringt und darauf einen Mechanismus zur Kontrolle dieser Umwelt aufbaut (vgl. Strohschneider 2010, 168f). Dementsprechend ist die Resilienz, obwohl sie schwer greifbar ist, ein entscheidender Indikator für die Leistungsfähigkeit einer Sicherheitskultur. Ist eine Gruppe auf gewisse Gefährdungen eingestellt, liegen objektive und subjektive Bedrohung beieinander. Und geht sie souverän mit zugehörigen Schutzmechanismen um, steigt die Wahrscheinlichkeit einer wirksamen und schützenden Reaktion (vgl. Giebel 2014, 370).

1.4.1 Der Staat als Garant für Sicherheit?

In seiner Ausarbeitung der flüchtigen Moderne identifiziert Zygmunt Bauman einen Verantwortlichen für diese Kluft des Sicherheitsempfindens: den Nationalstaat. Der Staat sei „als wichtigster (vielleicht sogar monopolistischer) Anbieter von Sicherheit und Gewißheit“ in den Hintergrund getreten und nehme „die Sorgen und Ansprüche seiner Untertanen nicht mehr ernst“ (Bauman 2000, 216). Er sieht die Ursache in der fortschreitenden Trennung von Staat als regulierender, sicherheitstiftender Institution und Nation als Identität und Gemeinschaft herstellendem Kulturkonstrukt (vgl. Bauman 2000, 216f). Baumans Skizze rührt aus einem Nationenverständnis, das seinen Ursprung in den politischen Verstrickungen des 19. und 20. Jahrhunderts hat. Hieraus zieht er konsequent die Gewissheit, dass der „Handlungsspielraum staatlicher Politik [...] durch globale Mächte zusehends eingeschränkt“ wird (Bauman 2000, 217). Dem ist jedoch entschieden zu entgegen, dass staatliche Autorität nicht an undefinierte

globale Mächte abgegeben wurde, sondern sich lediglich anhaltend neu ordnet – Bauman würde dies wohl ebenfalls flüchtig nennen (vgl. Williams 2003, 527f). Westliche Demokratien zum Beispiel geben Zuständigkeiten bereitwillig an die Europäische Union als friedensstiftende, übergeordnete Instanz ab; Angriffe auf Kritische Infrastrukturen erfolgen nicht mehr mit Raketen, sondern mit Ransomware; und der Wert gut ausgebildeter Spezialisten für innovative Technologien ist, entgegen Baumans Postulat, höher denn je. Dementsprechend nimmt Sicherheit weiterhin „für die Legitimation des modernen Staates einen hohen Stellenwert ein und ist daher eine zentrale politische Aufgabe“ (Terberl/Wendekamm 2014, 323). Macht und Gewalt liegen noch immer überwiegend bei Staaten, und zwar bei jenen, die ihre Ressourcen auf die dynamischste und schnellste Weise an neue Gegebenheiten adaptieren können. Während sich nationalstaatliche Gewalt mehr und mehr von physischer, militärischer Präsenz und teils körperlicher Repression löst, um zunehmend subtiler zu agieren, schwindet diese Gewalt nicht, sondern verlagert sich. Denn die Digitalisierung als ein Symptom und zugleich Treiber der gegenwärtigen Epoche löst das Abhängigkeitsverhältnis zwischen Ländern und ihren naturgegebenen Ressourcen auf: Im Informationszeitalter sind Wissen und Innovationsvorsprung die bedeutsamen Waren. Im Gegensatz zu Rohstoffen wie Öl oder Gold lassen sich Informationen nahezu beliebig replizieren und monetarisieren. Lene Hansen diagnostiziert den Konzepten Staat und Sicherheit, dass sie schicksalhaft miteinander verbunden sind, weil der Staat seine Legitimierung unter anderem aus dem Anspruch gewinnt, seine Bürger vor Gefahren aller Art zu bewahren:

Threats and insecurities are not just potentially undermining of the state and things that could be eliminated, they constitute the state: the state only knows who and what it is through its juxtaposition against the radical, threatening Other (Hansen 2006, 34).

Lyon folgt Baumans These, dass der Staat der hauptsächliche Garant für Sicherheit ist und verweist auf das bekannte Dilemma zwischen Sicherheit auf der einen Seite und Freiheit auf der anderen. „It is a highly contested concept, often constructed as being in conflict with claims to a right to privacy or to civil liberties“ (Lyon 2015, 122). Michaela Wendekamm und Christina Terberl gehen sogar so weit, einen neuen Panoptismus auszurufen, bei dem Sicherheit nur durch Unsichtbarkeit hergestellt werden kann (vgl. Terberl/Wendekamm 2014, 327f). Sie stellen fest, dass das moderne Individuum zunehmend transparenter für seine Mitmenschen wie auch für den Staat

wird, indem es fortlaufend Daten emittiert. Ein solch „technokratische[r] Sicherheitsansatz“, der „auf der Auswertung dieser exponentiell wachsenden Datenmengen“ basiert, blendet jedoch viele Aspekte einer ganzheitlichen Sicherheitsgesellschaft aus (Schaar 2017, 59). Die Autorinnen beziehen ihre Ausführungen sichtlich auf digitale Interaktionen, die die Nutzer bewusst oder unbewusst unverschlüsselt beziehungsweise ungeschützt vollziehen, lassen aber jene Handlungen weitestgehend außer acht, die sich vergleichsweise mühelos den Blicken von Behörden oder Mitmenschen entziehen. Dem liegt zusätzlich die Annahme zugrunde, dass die Bürger eines Sicherheit herstellenden Staates nicht oder nur passiv zum Bestehen der Sicherheitskultur beitragen. Denn wie jedes Individuum ein vom tatsächlichen Sicherheitszustand abweichendes Empfinden von Sicherheit hegt, wirkt auch jede dieser Persönlichkeiten, ob vorsätzlich oder nicht, auf ihre Weise an der Herstellung von Sicherheit mit. Sei es, indem sie sich an die Geschwindigkeitsbegrenzung hält, immer ihre Updates installiert, Unrechtsbewusstsein an ihre Kinder weitergibt oder schlichtweg selbst keine Straftaten begeht. Das offenbart einen Akteur, der mit dem Staat interagiert, aber nicht artverwandt ist: die Gesellschaft. Sie stellt Sicherheit her, indem nicht jeder Einzelne partikular definiert, was sicher ist und was nicht, sondern indem die Räume zwischen den Individuen mit Gemeinschaft angefüllt werden und auf diese Weise gemeinsame Ziele hervortreten. Dabei darf man nicht dem Irrtum erliegen, dass sich diese sozialen Interaktionsbereiche fakultativ mit Eintracht und Konsens anfüllen (vgl. Moravcsik 1997, 517). Sie sind vielmehr Konfrontationsräume, in denen ebenso gut Reibung und Kontroverse stattfinden. Die Gesellschaft der Gegenwart besteht nicht mehr nur aus einer längst überkommenen bourgeoisen Bürgerschaft. Stattdessen stellen Technologieproduzenten, Lobbyisten, Verbraucherschützer, Interessenverbände, Influencer, dynamische Bevölkerungsgefüge, Journalisten oder Großkonzerne je auf ihre Weise (Un-)Sicherheit her oder entwickeln subjektive Exegesen (vgl. Lange 2010, 337). Aufgrund dieser Vielseitigkeit und der damit verbundenen Pluralität von Bedürfnissen und Anforderungen an Sicherheit kann ein angestrebtes Schutzniveau, das möglichst wirksam und daneben undogmatisch sein soll, nur von allen Beteiligten gemeinsam getragen werden. „Die klassische Vorstellung, wonach Sicherheitspolitik beinahe ausschließlich »Staatspolitik« ist, bei denen gesellschaftliche Gruppen keine maßgebliche Rolle spielen, ist obsolet“ (Lange 2010, 337). Dem Staat obliegt demgemäß kein Sicherheits-, sondern ein

Gewaltenmonopol, in dessen Maßgaben er handeln kann. Er ist nicht alleiniger Anbieter von Sicherheit, nimmt aber eine zentralverantwortliche Rolle und eine Leitfunktion ein.

Andrew Moravcsik bringt Staat und Gesellschaft in eine nachvollziehbare Ordnung. Er umschreibt die Gesellschaft als Aggregation limitiert rationaler Persönlichkeiten mit unterschiedlichen Vorlieben, sozialen Einbettungen und Voraussetzungen (vgl. Moravcsik 1997, 517).

Socially differentiated individuals define their material and ideational interests independently of politics and then advance those interests through political exchange and collective action. Individuals and groups are assumed to act rationally in pursuit of material and ideal welfare (Moravcsik 1997, 517).

Moravcsik sieht in der Gesellschaft eine Sphäre, in der Absichten und Ziele entstehen, die dann in Staat und Politik umgesetzt werden, um schließlich wieder auf die Gesellschaft rückwirken zu können. Eingangs ließ sich schon bei Landwehr entdecken, das zumindest eine Komponente dieser Sphäre ein hochkomplexes, kommunikatives Netz ist, „in dem über Zeitungen, Briefe, mündliche Mitteilungen usw. Ereignisse durch Versprachlichung zu politischen Gegenständen gemacht werden. Die Wirklichkeit der Politik ist immer und kann nur eine sprachlich vermittelte Wirklichkeit sein“ (Landwehr 2008, 149). Daraus resultiert auch die Funktion des Staates als repräsentative Einrichtung. Er verkörpert Bevölkerungsgruppen, in deren Interesse dann die Verantwortlichen des Staates handeln. Der Staat selbst ist dem anhaltenden Wandel der Gesellschaft ausgeliefert und wird entsprechend der sich verändernden Anforderungen modelliert und bei Bedarf reformiert (vgl. Moravcsik 1997, 518).

Ausgerechnet das Feld der Cybersicherheit zeigt anschaulich auf, warum Staat und Gesellschaft trotz ihrer Ungleichheit untrennbar miteinander verwoben sind und einander bedingen. Mary Aikens Routine Activity Theory, kurz RAT-Theorie, besagt, dass Verbrechen dann begangen werden, wenn potenzielle Täter auf ein Machtvakuum, auf einen unbeobachteten Raum treffen. Begegnet dem Täter in dieser verborgenen Sphäre dann ein geeignetes Opfer, kohärieren Verlockung und Gelegenheit und machen die Straftat wahrscheinlicher (vgl. Aiken 2018, 456). Insofern zeichnet Aiken auch die Kehrseite des panoptischen Bildes von Terberl und Wendekamm. Sie schreibt der globalen Digitalisierung gewissermaßen zu, einen Ausweg aus Benthams Ordnungsvorstellung anzubieten. Aiken sieht in der Informationstechnologie einen Bereich, der sich dem Sichtfeld von Überwachung und Regulierung entziehen kann. Aiken und sogar Bauman diagnostizieren eine weitestgehende Absenz von staatlicher

Autorität im Online-Raum und assoziieren damit eine erhöhte Wahrscheinlichkeit für entsprechende Verbrechen. Gegen ihre Grundannahme, dass ein Machtvakuum respektive eine Kontrollabsenz Kriminalität begünstigt, lässt sich kaum protestieren. Sie deduzieren aber, dass es maßgeblich die Anwesenheit von staatlicher Aufsicht ist, an der es mangelt. Indes fehlt es in den unbeobachteten Räumen, in denen sich Unsicherheit beispielsweise mittels Kriminalität entfaltet, an einer intersubjektiven Observierung. Somit kann Aikens Beobachtung nicht auf das von Bentham und Foucault konstruierte panoptisch-delinquente Überwachungsjoch abzielen, sondern auf die Eingliederung dieser leeren Räume in die übrige Gesellschaft. Die gegenseitige Erfassung, besser gegenseitige Wahrnehmung, vermittelt ein Gefühl der Einbettung und schließlich der korrelierenden, gesellschaftlichen Verantwortung. Das Internet jedenfalls bietet zahlreiche Räume, die sich sowohl den Blicken der Strafverfolgungsbehörden als auch denen aller übrigen Mitmenschen entziehen. Genau hier steht insbesondere der „Gewährleistungsstaat“ als Konzentrat der bürgerlichen Gesellschaft in der Verantwortung, mit gutem Beispiel voranzugehen und verhältnismäßige Anreize zu setzen (Lange 2010, 336ff). Gleichzeitig ist es an den Individuen und speziell an deren Kollektiven, digitale Bedrohungen als solche zu akzeptieren, zu stigmatisieren und schließlich ihre Abwehr zu institutionalisieren.

1.4.2 Institutionalisation von Sicherheitskultur

Warum also erwähnt Castoriadis auf mehr als 600 Seiten nur einmal das Konzept Sicherheit? Warum sieht er darin weder eine gesellschaftliche noch eine imaginäre Institution? Für ihn ist ganz klar, dass der Mensch nicht ein Bedürfnis hat, dass sich von unendlich vielen anderen Bedürfnissen trennen ließe oder dass überhaupt nur zu befriedigen wäre. Dagegen gebe es ein Konglomerat an Bedürfnissen, darunter auch die Sicherheit, dessen Quantum den Menschen erst ausmache (vgl. Castoriadis 1990, 232f). Damit würdigt Castoriadis keineswegs die Bedeutung der singulären Bedürfnisbefriedigung herab und auch nicht die der Sicherheit, jedoch sind sie ihm für seine ontologische Theoriebildung zu unbedeutend.

Dabei sind Imagination und Sicherheit häufig miteinander verwobene und akademisch diskutierte Termini – beispielsweise in Michael C. Franks *Antizipationen des nächsten Anschlags*, in dem er herausstellt, dass die Vorstellung einer Wirklichkeit der tatsächlichen Wirklichkeit vorauseilt. Am Beispiel des 11. Septembers beschreibt Frank, dass die amerikanische und westliche Medienöffentlichkeit nachfolgend ein Porträt

einer Welt zeichnete, in der eine terroristische Omnipräsenz zu herrschen schien – obwohl die Risiken im gleichen Zeitraum nachweislich geringer wurden (vgl. Frank 2019, 135f). Frank führt dieses Phänomen auf eine „Empfindung gesteigerter Verletzlichkeit“ zurück; das Resultat einer noch jungen Daseinsverschiebung (Frank 2019, 136). Denn Risiken sind gegenwärtig Umweltfaktoren, die nicht eigenverantwortlich abzuwehren sind, sondern denen „wir passiv, ohne eigenes Zutun ausgeliefert sind, und zwar permanent – in dem Gefühl, die Risikofaktoren weder beherrschen noch vollauf verstehen zu können“ (Frank 2019, 136). Hierin liegt eine wesentliche Gemeinsamkeit von ideologischem Terrorismus und Cyberbedrohungen. Das Katastrophische ist diffus, nicht auf eine Person oder Gruppe referenzierbar, nicht abzuwenden und ist in seinen Konsequenzen unvorhersehbar. Demzufolge werden der Diskurs, die mediale Berichterstattung und die persönliche Erfahrung eines Geschehens machtvoller und sind mindestens so wichtig für die Sicherheitsrezeption wie die Fakten der Begebenheit selbst.

Wie bereits erkannt, ist Sicherheit selbst ein imaginäres Konstrukt, ein Gefühl, das nicht greifbar und nicht messbar ist. Kaum eine Domäne des öffentlichen Lebens ist so sehr von Bildern und Imaginationen geprägt wie die öffentliche Sicherheit: In Boulevard, Politik, Familie behandeln Menschen täglich Themen wie Krieg, Epidemie, gesellschaftlichen Bruch oder ökonomischen Abschwung und sie sehen sich Aufzeichnungen aus Konfliktgebieten an, zitieren Klimaberichte oder teilen Artikel über Anschläge auf Flüchtlingsunterkünfte. Dazu spielen nahezu alle Helden- und Actionfilme, weite Teile der belletristischen Literatur sowie eine große Zahl von Videospielen mit einer schier unüberwindbaren Bedrohung und inszenieren den Sicherheitszustand als maximal fragil, als abhängig von dem Wohlwollen und den Fähigkeiten weniger Personen oder Parteien. All diese fiktionalen oder non-fiktionalen Bedrohungen werden durch ihre Inszenierung und Reinszenierung erfahrbar und rücken näher an die Zusehenden. Damit fühlt sich die Bedrohung unmittelbar wie auch gewöhnlich an: Durch die Rezeption von Gewalttaten am anderen Ende der Welt entsteht der Eindruck einer persönlichen Gefährdung und damit steigt das Bedürfnis nach Sicherheit.

An diesem Punkt offenbart sich erneut die Wirkmacht des Imaginären. Mittels der „antizipativen Imagination“, also der Erwartung bestimmter, noch imaginärer Ereigniswahrscheinlichkeiten auf der Grundlage bisheriger Vorkommnisse, können

präventive Entscheidungen die bis dahin unberührte Gegenwart ändern (Frank 2019, 130). Es ist demgemäß kaum erstaunlich, „dass der sicherheitspolitische Diskurs trotz seinem programmatischen Rekurs auf die Vorstellungskraft Tatsachen schafft“ (Frank 2019, 145). Die obigen Kapitel zeigen zudem, dass jede Ausprägung von Sicherheitskultur, egal in welcher Form, solche bewusst oder unbewusst getroffenen Risikoabwägungen einschließt, die sich zudem in fortlaufendem Wandel befinden. Sie bilden die immanente Antwort auf die für jede Gesellschaft individuelle Frage nach dem jeweils richtigen Verhältnis zwischen innovationsförderndem Risiko und augenscheinlich sicherheitstiftender Kontrolle (vgl. Siedschlag/Jerković 2014, 308). Zugleich sind sie das Ergebnis kollektiver Erfahrungen, überlieferter Ängste und Hoffnungen wie auch einer intersubjektiv geltenden Auffassung von Sicherheit. Diese Prämisse ist insofern nachvollziehbar, als sie auf der Idee aufbaut, Unsicherheitsfaktoren, Gefährdungswahrnehmungen und akute Bedrohungslagen erzwingen neue Sicherheitsdebatten. Dieses Verständnis geht aber weder ausreichend auf den Ursprung des Gefahrenempfindens ein noch berücksichtigt es, dass Sicherheitsdebatten zwangsläufig auch immer Angstdebatten sind.

Bei Sicherheitsdebatten, sei es nun Terrorismus oder Gewaltkriminalität, ist davon auszugehen, dass der Höhepunkt eines Diskurses rund um ein kritisches Ereignis stattfindet. Wie eingangs dargelegt, kann ein Sicherheitsthema beispielsweise aufkommen, wenn extern induzierte Ereignisse auf eine Gesellschaft treffen. Das können Unfälle sein, wie etwa Flugzeugabstürze, in deren Folge dann über technische Verbesserungen und mehr Reglementierung gestritten wird. Oder es handelt sich um Kriminalität, Krieg oder andere menschlich herbeigeführte Szenarien (vgl. Balzacq 2005, 181f). Diese treten dann von außen an eine soziale Gruppe heran und setzen die Agenda. Jedoch können auch gruppeninterne Kräfte bewusst Sicherheitsdiskussionen erzeugen.

Das führt uns von der ‚attentiveness‘ zur ‚securitization‘ (zum Konzept siehe Balzacq 2011). Abhängig von ihrer formalen Stellung und ihrer Geschicklichkeit im Umgang mit wesentlichen politischen Manipulationsstrategien (Zahariadis 2007: 75f.) vermögen politische Unternehmer Ereignisse als wesentliche Sicherheitsprobleme zu deuten. Mit der Securitization der Ereignisse bzw. des Diskurses über sie ‚ko-produzieren‘ politische Unternehmer gewissermaßen die Sicherheitskrise (Müller 2012, 233f).

Thierry Balzacqs Begriff der *Securitization* reflektiert einen intersubjektiven Prozess (vgl. Balzacq 2005, 177). Für ihn manifestiert sich der Zustand von Sicherheit im

Sprechen darüber. Sicherheit ist ein gesprochener Akt, der Wirklichkeit erst im intersubjektiven Austausch erfährt (vgl. Balzacq 2005, 178). Darauf baut die Kopenhagener Schule auf, die Sicherheit als diskursiven Akt deutet, welcher mit rhetorischen Mitteln eine Wirkmacht umsetzt (vgl. Hansen/Nissenbaum 2009, 1156). Michael C. Williams entdeckt Securitization als gesprochene Performance unter anderem auch in Medien, politischen Dramen, Institutionen und in anderen Formen der Visualisierung und erweitert so das ursprüngliche Verständnis aus der Kopenhagener Schule (vgl. Williams 2003, 512).

Issues become ‚securitized‘, treated as security issues, through these speech-acts which do not simply describe an existing security situation, but bring it into being as a security situation by successfully representing it as such (Williams 2003, 513).

Das bedeutet, dass sich Sicherheitssituationen weitestgehend von der Wahrheit lösen können; man denke an die eingangs bemerkte Unterscheidung zwischen objektiver und subjektiver Sicherheit oder die These Franks, dass die Imagination die Information ersetzen könne (vgl. Frank 2019, 134). Das kann teils abstruse Auswüchse annehmen. So entfernten etwa viele Supermärkte kurz nach dem Angriff Russlands auf die Ukraine im Februar 2022 russische Produkte wie Wodka oder gesüßte Sahne aus den Sortimenten ihrer Filialen (vgl. Business Insider Deutschland 2022). Dieser Aktionismus, eine Art populistische Überreaktion, katalysiert eine pauschale Feindlichkeit gegen alles Russischstämmige und ändert nichts an der europäischen Sicherheitslage, sondern ist – wie die betreffenden Unternehmen selbst zugaben – ein symbolischer Akt. Ein weiteres Beispiel für die Diskrepanz zwischen Information und Imagination resultierte aus dem vielfach als Exempel herangezogenen 11. September 2001: Nach den Anschlägen wurden Ethnienzuschreibungen wie *Islam* oder *Muslim* neu formuliert, pauschalisiert und schließlich mit generalisierenden Gefährdungssentimenten verbunden. Es entstand eine neue Polarität zwischen *den Muslimen* und *uns Christen*, in gut und in böse. Aus dem asymmetrischen Angriff einer terroristischen Organisation konstruierte die amerikanische Bush-Administration einen NATO-Bündnisfall gegen den afghanischen Staat und erzeugte letztlich eine anhaltende Stimmung, die nicht zwischen dem islamistischen Fundamentalismus und der unbeteiligten, muslimischen Majorität unterschied (vgl. Wichmann 2014, 243). Diese mangelnde Differenzierung, die auf einer einfachen, populistischen Rhetorik ruhte, führte zu Vorbehalten und rassistischen Ressentiments, die bis heute nachhallen. Beide

Beispiele haben gemein, dass Fiktion und Wahrheit weitestgehend voneinander gelöst sind; und die Fiktion die Wahrheit sogar überschreibt.

Solche Vereinfachungsmechanismen – simplifizierte, teils verzerrte Abbilder der Realität – schüren wiederum Bedürfnisse nach Sicherheit, Abgrenzung oder Gesundheit und bewegen gesellschaftliche Gruppen dazu, Forderungen zu stellen und ihre Vorstellungen zu konsolidieren. Die Rufe nach Veränderung, nach Gegenmaßnahmen und Gesetzen, vielleicht sogar nach neuen Organisationen basieren auf einer Imagination und ihrer Nähe oder Entfernung zur Wahrheit. Es entsteht „ein symbolisches, gesellschaftlich sanktioniertes Netz, in dem sich ein funktionaler und ein imaginärer Anteil in wechselnden Proportionen“ befinden (Castoriadis 1990, 226). Indem diese Netze entstehen, kondensieren zunehmend robuste Lebenswelten, die wiederum auf die Perzeption von – in diesem Fall – Sicherheit einzahlen (vgl. Williams 1961, 117). Gehen wir zu vorherigen Seiten zurück, wird der Gedanke noch deutlicher: Sicherheit stellt sich als gesellschaftliches Konstrukt dar, das einerseits von tatsächlich bestehenden Gefahren determiniert, andererseits aber auch von dazugehörigen Protagonisten bewusst ausgefüllt wird. So bestimmen nicht nur höhere Gewalt oder gewaltsame Angriffe ein Bedrohungsempfinden, sondern ebenso die zirkulierende Kommunikation und die teilnehmenden Personen. Diese Akteure legen dann durch ihre gegebenen oder erlernten kognitiven wie linguistischen Ressourcen sowie auf Basis ihrer Absichten die Richtung fest, die eine Sicherheitsdebatte einschlagen kann (vgl. Balzacq 2005, 190). Vereinen sich genügend gleichdenkende politische oder gesellschaftlich relevante Menschen, die die notwendigen rhetorischen Kapazitäten besitzen, können sie die Sicherheitsagenda dirigieren oder mindestens eine Richtung aufzeigen. Daneben liegt auch in ihren Händen, ob eine Sicherheitsdebatte zur Angstdebatte verkommt, sie also nicht in den Mittelpunkt stellt, Sicherheit zu produzieren, sondern Angst zu wecken, um beispielsweise politische Intentionen zu verfolgen. In einem solchen Fall rückt die tatsächliche Schwere des Bezugsrahmens in den Hintergrund des Diskurses und wird ersetzt durch eine mehr oder minder abweichende Dramaturgie.

Highlighted in this context, the word ‘security’ does not point towards an objective reality; it is an agency in itself to the extent that it conveys a selfreferential practice instantiated by discourses on existential threats that empower political elites to take extraordinary measures to alleviate ‘insecurity’ (Balzacq 2005, 181).

Balzacq folgend verwendet man derartige Erzählungen, um außergewöhnliche Maßnahmen zu rechtfertigen. Erneut eignet sich die Corona-Pandemie als anschauliches Exempel: Um das Virus einzudämmen, beschlossen zahlreiche Staaten Ausgangssperren, Kontaktverbote oder griffen auf sensible Informationen ihrer Bürger zu, darunter Reise- und Bewegungsdaten (vgl. WDR 2020a). Das heißt, es wurden außerordentliche Reglementierungen bis hin zu Grundrechtseinschränkungen vorgenommen und größtenteils von den Bevölkerungen akzeptiert, da mit diesen Handlungsmustern das kollektive Ziel verfolgt wurde, gesundheitliche Sicherheit wiederherzustellen. In Zeiten terroristischer Gefährdung, finanzieller Krisen, Umweltkatastrophen oder anderer einschneidender medialer Ereignisse ist die Angst sehr verbreitet, persönlich Opfer zu werden. Immer dann ist der Ruf nach einem Handeln des Staates laut, sodass die Verknüpfung zwischen dem öffentlichen Bedürfnis nach Sicherheit und der Legitimierung staatlicher Exekutivmaßnahmen sichtbar wird.

In Fällen, in denen ein derartiger Vorstoß anhaltend gelingt, verfestigt sich die neue Zielgröße entweder als Gesetz oder als administrative Einrichtung, manchmal auch als politisches Leitbild. Die Sicherheitsdebatte mündet dann in einer Verstetigung ihrer selbst und schließlich in ihrer Institutionalisierung. „Kulturen der Politik wären dann auf Stabilität drängende, Konflikte unterbindende, auf Regelmäßigkeit und Routinen abzielende Praxisformen, die sicherlich auch eine Tendenz zur eigenen Institutionalisierung aufwiesen“ (Schölzel 2016, 51).

Beispielhaft hierfür ist unter anderem das bayerische Polizeiaufgabengesetz von 2018, mit dem die Landesregierung nach den Anschlägen in München und Ansbach aus dem Juli 2016 auf vermeintliche terroristische Bedrohungen zu reagieren versuchte – obwohl Gewalkriminalität seit Jahren bundesweit rückläufig war (vgl. Bundeskriminalamt 2020, 165). Mit dessen umstrittener Einführung erhielt die Landespolizei nach intensiver öffentlicher Debatte die Befugnis, präventive Maßnahmen schon vor Eintreten einer drohenden Gefahr einzuleiten (vgl. Bayerische Staatsregierung 2018). Mit ähnlichem Antrieb rief man die beim BKA angesiedelte Antiterrordatei 2007 ins Leben, auf die eine Vielzahl von Behörden seit dem Zugriff haben. Diese macht es unter anderem möglich, sogar Kontaktpersonen eines Verdächtigen in die Datenbank aufzunehmen und somit ihr Recht auf informationelle Selbstbestimmung einzuschränken (vgl. Schaar 2009, 153). Auch das Kommando Cyber- und Informationsraum der Bundeswehr begründet sich in der

Wahrnehmung einer diffusen Schutzlosigkeit, die schließlich ausreichend gewichtig war, um den Aufbau der neuen Organisationseinheit beibringen zu können (vgl. Bundeswehr 2020). Bei den Beispielen handelt es sich schlicht um eine Auswahl vielzähliger, institutionalisierter Angstmotive, von denen sich beliebig viele weitere finden ließen. Sie wurden über einen intensiv geführten politischen Diskurs mit Relevanz und letztlich kollektiver Billigung versehen, sodass der breite „Konsens und noch stärker die habituelle Unhinterfragtheit“ zu ihrer Verwurzelung führten (Gengnagel/Hirschfeld 2016, 104). Solche Maßnahmen vermitteln den politisch Handelnden, aber auch der Bevölkerung den Eindruck, dass sich die Situation fortan im eigenen Sinn verbessern wird und Beständigkeit einkehrt. Über die Repetition internalisieren sich Ansichten und Verhalten, sie werden habitualisiert und sind somit Teil des als natürlich wahrgenommenen Gesellschaftsspektrums. Berger und Luckmann beschreiben, dass die Wahrnehmung, also die Welt selbst, auf diese Weise objektiviert wird (vgl. Berger/Luckmann 2018, 61ff). „Nur so, als *objektive* Welt, können die sozialen Gebilde an eine neue Generation weitergegeben werden“ (Berger/Luckmann 2018, 63). Diese Institutionalisierung beziehungsweise Verhärtung ist also folgerichtig Teil der Sicherheitskultur. Diskurse und die Einordnung von Bedrohungen manifestieren sich in Gegenmaßnahmen, die dann nicht selten dauerhaft Bestand haben. Ihre Existenz wird zur Selbstverständlichkeit. Es wäre also umkehrbar: Sicherheitskultur muss eine imaginäre Institution sein. Der Institutionalismus bietet demgemäß kennzeichnende Eigenschaften von Organisationen und interpersonellen Grundsätzen an. Institutionen stellen in dieser soziologischen Disziplin verdichtete Wertvorstellungen mit normativer Funktion dar. Sie sind ein Sammelbecken aus homogenen, überindividuellen Werten und beschreiben einen Konsens, den der Querschnitt einer Bevölkerungsgruppe vertritt (vgl. Sandhu 2012, 96). Zusätzlich können mit dem Institutionalismus „größere Räume und historische Zeitspannen, also umfassendere institutionelle Kontexte“ in die Charakterisierung von Kulturen einfließen, da Institutionen in Retrospektiven wurzeln und Routinen stabilisieren (Keller 2005, 65).

Swaran Sandhu reduziert deshalb die Institutionen einer Gesellschaft auf zwei elementare Eigenschaften, nämlich „Dauerhaftigkeit“ und „Regelmäßigkeit“ (Sandhu 2012, 97). Als Beispiel für eine Institution führt er die Sprache ins Feld, die aufgrund ihrer Gesetzmäßigkeit interpersonell anwendbar ist und sich aufgrund ihrer

Dauerhaftigkeit generationenübergreifend fortschreibt. Demnach sind Paradigmen institutionalisiert, wenn sie objektiv nachvollziehbar in eine beständige, logische Form gegossen wurden, die sich nicht ohne weiteres von Einzelnen annullieren lässt. Sandhu betrachtet den Institutionenbegriff also als „*Verbindungsmechanismus* zwischen Organisation und Gesellschaft“ (Sandhu 2012, 96). Darum bedeutet Institutionalisierung nicht, dass sich eine Kulturpraxis zwangsläufig in einer materiellen Organisation konsolidiert. Es kann stattdessen oder zusätzlich auch heißen, dass sie sich markant verdichtet, sich also beispielsweise in Symbolen, Gesinnungen oder in Neologismen niederschlägt (vgl. Schönherr-Mann 2016, 29): *Corona-Pandemie*, *Respektrente*, *Heißzeit*, *postfaktisch*, *Flüchtlinge*, *GroKo* oder *Wutbürger* sind allesamt Begriffe, die seit 2010 von der Gesellschaft für deutsche Sprache zum Wort des Jahres gekürt wurden (vgl. Gesellschaft für deutsche Sprache e. V. 2021). Darunter befinden sich Komposita wie auch Abkürzungen; sie sind tendenziös, vom jeweiligen Zeitgeschehen verfasst und demonstrieren, wie sich neue Gegebenheiten in der Sprache niederschlagen und damit Identitäten verfestigen (vgl. Hansen 2006, 23).

Konsensuale Annahmen verdinglichen sich gleichwohl in Organisationen; koinzident schreibt die bloße Existenz zweckgerichteter Organisationen das kollektive Narrativ fort (vgl. Miller 2015, 278). Ein Bundesamt für Bevölkerungsschutz und Katastrophenhilfe begründet seine ganze Existenz in der Vorausnahme des Unheils; die Internationale Atomenergie-Organisation (IAEO) trägt inhärent das Gefahrenpotential von Kernenergie und -waffen; während die Centers for Disease Control and Prevention untrennbar mit der Angst vor Pandemien und Infektionskrankheiten verbunden sind. Immer wieder ist dieser Vorgang bei dem lauter werdenden Ruf nach einem deutschen Digitalministerium zu beobachten, der auf einer Angst vor Cyberattacken wie auch vor möglicherweise verpassten Chancen bei der Digitalisierung ruht (vgl. Digitalministerium.org 2021/Handelsblatt 2020b). Somit entstehen Organisationen, um Leitbilder zu prozessualisieren und kontrollierbare Schablonen zu modellieren. Das Ziel von Organisationsstrukturen ist es, „gesellschaftlich institutionalisierten Vorstellungen zu entsprechen, um darüber Legitimität in der gesellschaftlichen Umwelt der Organisation zu erzielen“ (Hasse/Krücken 2009, 239). Organisationen kontrollieren zum Beispiel die Einhaltung institutionalisierter Normen, zum Beispiel Behörden oder Gerichte, sie verwalten Regelsysteme, etwa Vereine, Gremien oder Verbände, oder sie sind die Reaktion auf tief verwurzelte Wunsch- oder

Angstvorstellungen, wie Unternehmen oder auch Polizeien. Insofern können Organisationen als ein mögliches Produkt von institutionalisierten Imaginaries verstanden werden. Denn „[o]rganisationale Handlungen und Entscheidungen sind nicht das Ergebnis autonomer Wahl. Sie sind ohne den Rekurs auf ihre gesellschaftliche Umwelt und die dort vorherrschenden Regeln gar nicht denkbar“ (Hasse/Krücken 2009, 239). Eine Institution ist das formalisierte Abbild soziologischer Stabilisierungsabfolgen und zugleich „aus makro-institutioneller Perspektive aber auch ein Produkt ihrer gesellschaftlichen Umwelt, die ihre Struktur durch bestimmte Erwartungen prägt“ (Sandhu 2012, 85). Organisationen, die aus dieser Konsolidierung hervorgehen, verfügen so über einen inhärenten Legitimierungsautomatismus, weil der Diskurs, der zu ihrer Entstehung führte, dann eine Nähe zu weiteren populären Diskursen der Systemumwelt aufweist (vgl. Sandhu 2012, 104).

Es verdeutlicht sich das reziproke Verhältnis zwischen System, hier der Organisation, und Systemumfeld, also der stets transformativen gesellschaftlichen Wirklichkeit, im Institutionalisierungsprozess. Denn wenngleich Organisationen und Institutionen zum Beispiel über Regulierungen auf Rezeptionen und Diskurse einwirken, sind sie selbst Ergebnis ebensolcher Leitmotive oder gemeinschaftlicher Deutungshorizonte:

Organisationen orientieren sich an gesellschaftlichen Erwartungsstrukturen, die ihren Handlungsspielraum ermöglichen aber auch begrenzen. Sobald Organisationen diese Anforderungen übernommen haben, spricht man von Institutionalisierung. [...] Organisationen gelten dann als institutionalisiert, wenn die Bedeutung ihrer Elemente oder Praktiken bzw. wenn die Organisation an sich nicht infrage gestellt, sondern als selbstverständlich angesehen wird (Sandhu 2012, 77).

Daraus folgt erstens, dass Institutionalisierung für sich nicht ideologisch ist, sondern allenfalls ein Vehikel zur Ausgestaltung ebenjener Ideologie. Deshalb haben Institutionalisierungsvorgänge das Potenzial, nicht nur vernunftbasierte Praktiken zu verfestigen, sondern auch jene zu legitimieren, die etwa auf irreführender Agitation beruhen. Die jeweilige Ideologie wird von relevanten Akteuren weitergetragen und als „Interpretationsrahmen (frames or packages) kommuniziert, das heißt bestimmte Themen werden ideologisch eingerahmt“ (Jahn 2013, 316f). Zweitens zeichnet sich ab, dass institutionalisierte Organisationen auf Konventionen errichtet werden, die letztlich gemeinschaftliche Paradigmen respektive „Regelwerke“ abbilden (Hasse/Krücken 2009, 237). Diese Regeln, die eigentlichen Institutionen, können stark formalisiert sein. Das heißt, sie exponieren sich beispielsweise in Gesetzen oder

Behörden. Sie können aber auch informell bestehen und sich vielmehr in der Kategorisierung von erwünschtem und unerwünschtem Verhalten äußern, sodass diese Regeln eine weitestgehend irritationsfreie zwischenmenschliche Verständigung ermöglichen (vgl. Hasse/Krücken 2009, 237). Das heißt, dass die Betrachtung von Institutionen nicht nur Informationen des übergeordneten Systems preisgibt, sondern ebenso aufzeigt, inwiefern Individuen innerhalb der spezifischen Organisation ihre gesellschaftliche Rolle einnehmen (vgl. Williams 1961, 102). Damit sind Institutionalisierungen stets auch anschlussfähig für mikrosoziologische Untersuchungen individueller Fenster zu jener regelhaften Umwelt (vgl. Buzan/Hansen 2010, 662).

Durch die permanente Wiederholung dieses Schemas – das sich auf verschiedensten Interaktions- und Relevanzniveaus en passant selbst reproduziert – trägt die Institutionalisierung zur Etablierung gruppenkohärenter, teils identitätsstiftender Kulturpraktiken bei. Swaran Sandhu bricht auf einen Satz herunter, welches Institutionenverständnis für die aufbauenden Ausführungen wichtig sein wird: „Institutionen sind dauerhafte Regelsysteme, sie ermöglichen soziales Handeln, beschränken es aber zugleich und werden durch routinisierte Handlungen reproduziert“ (Sandhu 2012, 76). Dabei erfindet jede makrosoziologische Gruppe ihre eigenen Regelwerke, die sich zwar nach isomorphen Prinzipien transnational angleichen können, aber grundsätzlich in der Lage sind, ihre eigenen Motivationen und Ordnungen auszubilden (vgl. Bonacker 2009, 190). Wenn also Reiner Keller davon spricht, dass „der Neo-Institutionalismus die Strukturierung des Möglichkeitsrahmens von Wirklichkeitskonstruktionen durch Machtverhältnisse hervor[hebt]“, dann bestätigt er die Überlegung von Sandhu (Keller 2005, 65f): Gesellschaften fixieren über ihre Institutionen eine immanente Palette aus Denk- und Handlungsoptionen, definieren damit zugleich aber auch die Grenze des Möglichen. Die gesellschaftsspezifischen Institutionen fußen folglich auf gesellschaftsspezifischen Imaginaries. Diese verändern sich zwar im Laufe der Zeit, jedoch sind sie stets die Genese vergangener und gegenwärtiger Kollektivprinzipien – ein „diskursiver Kern“, wie Swaran Sandhu es betitelt (Sandhu 2012, 102).

Der (Neo-)Institutionalismus stellt unter anderem den Versuch dar, den Institutionenbegriff in Bezug zu den elaborierten Imaginaries zu setzen und ist damit ein Theorieansatz, der die Konzentration von gesellschaftlicher Ordnung und Legitimierung

in Organisationen annimmt. Institutionen fungieren „als Klassifikations- und Unterscheidungskriterium für gesellschaftliche Strukturen, die überindividuell sind“ und eignen sich somit als Indikatoren in einem transkulturellen Vergleich (Sandhu 2012, 96). In ihnen verdinglichen sich Imaginaries zu begründeten Instanzen, sodass Felt gar den Schluss zieht, dass die Nation selbst nur eine imaginierte Gemeinschaft sein kann (vgl. Felt 2015, 103). Institutionen oder auch Organisationen sind dem folgend steingewordene Kultur; mindestens aber internalisierte, soziale Praxis. Die Untersuchung einzelner Organisationen kann deshalb nicht nur eine Analyse inhärenter Merkmale sein, sondern muss immer auch die Funktionen und Beziehungen der jeweiligen Institution innerhalb des Gesamtgefüges einschließen (vgl. Williams 1961, 46f). Die Identität, die aus der mutualen Relation von Institutionen und Imaginaries hervorgeht, ist nicht apodiktisch, sondern immer untrennbar mit dem akuten Gesellschaftssystem sowie der Systemumwelt verbunden, sodass selbst unverrückbar geltende Institutionen stets ihre Form wandeln (vgl. Felt 2015, 120). Für die Institutionen der Sicherheit, damit einhergehend für die Sicherheitskultur einer Gesellschaft bedeutet diese Erkenntnis, dass diese nicht a priori mit einer handfesten Gefahr einhergehen, sondern vielmehr auf den Sorgen, Ängsten und teils auf singulären Erlebnisdimensionen zurückgeführt werden können. Denn die Existenz gewisser Institutionen besitzt eine inhärente Botschaft darüber, was als Bedrohung gilt und welche Aufwände unternommen werden, um diese – vielleicht imaginären – Gefahren einzudämmen. Infolgedessen müssen sich Institutionen imaginärer Sicherheit stets ihrer Umwelt und der vorherrschenden Angstprojektionen beugen.

1.5. Sicherheitskultur trifft auf Informationstechnik: ein Spannungsfeld

Diese in Institutionen gegossene Sicherheitskultur von Nationen oder Staaten sieht sich mit der Digitalisierung Herausforderungen von besonderer Geschwindigkeit und Diversität gegenüber. Es mag paradox wirken, aber zu diesen Aufgaben gehört auch, dass Cybersicherheitsvorfälle gegenwärtig nur selten existenzielle Bedrohungen aufweisen und noch seltener die Folgen solcher Problemsituationen lange genug diskutiert werden, um alternative Handlungsgerüste herbeizuführen. Häufig sind Individuen oder vereinzelte Unternehmen äußerst schwer getroffen, weil beispielsweise intimste Informationen an die Öffentlichkeit gelangen. Ebenfalls häufig entstehen erhebliche finanzielle Schäden oder sensible Informationen zu beispielsweise

Produktionsgeheimnissen gehen verloren. Jedoch heißt das nicht, dass IT-Vorfälle bislang keine schwerwiegenden Schäden angerichtet haben, wie beispielsweise die Malware NotPetya vor wenigen Jahren mit einem Defizit von 10 Mrd. Dollar unter Beweis stellte (vgl. Welt 2018). Insgesamt bemisst sich der jährliche Schaden nach Angaben des Branchenverbands Bitkom für 2020 auf 223,5 Milliarden Euro – nur in Deutschland (vgl. Bitkom 2021a, 10).

Jedoch führten große Cyberzwischenfälle der Vergangenheit nie zu Leid in gesamtgesellschaftlichem Ausmaß; der Druck zu uniformen Sicherheitsanforderungen wurde nicht aufgebaut (vgl. Hansen/Nissenbaum 2009, 1165). Zusätzlich können Diskussionen um Informationssicherheit kaum das zuvor erklärte Kriterium der Zeitabhängigkeit verwerten. Während Terrorismus, Epidemien oder Kriege nur lokal oder zeitlich begrenzt stattfinden und einer Klimax folgend befristet nachhallen, ist die Unsicherheit von Informationstechnik eine andauernde und inhärente Eigenschaft ebendieser. Das kontinuierliche Dilemma aus Digitalisierungslust und Vulnerabilität verhindert die Ausbildung diskursiver Höhepunkte. Während also zum einen substanzielle Repressionen durch Cybervorfälle bislang ausgeblieben sind, besteht ein konstantes und stetig anwachsendes Bedrohungspotenzial, das aufgrund mangelnder Höhe- und Tiefpunkte nur gelegentlich seinen Weg in die öffentliche Besprechung findet. Die Öffentlichkeit entdeckt nicht den einen figurativen Anhaltspunkt, der Empörung nebst Widerstand einfordert und somit auf eine korrektive Wirkung hinauslaufen kann.

Wie sich auf den vergangenen Seiten gezeigt hat, sind sowohl der Sicherheits- als auch der Kulturbegriff zudem vielschichtige Felder – unzweifelhaft gilt dies auch für die Informationstechnik, sodass die Cybersicherheitskultur eine Aggregation von Komplexität darstellt. In der Psychologie gelten Situationen oder Problemstellungen bereits als komplex, wenn sie vier Merkmale besitzen: umfangreich, vernetzt, intransparent und dynamisch (vgl. Badke-Schaub et al. 2008, 83). Alle vier Kennzeichen treffen auf die Informationstechnik zu, sodass diese Technologien ein breites Wissen voraussetzen und Überforderung oder gar Ablehnung durch laienhafte Bediener hervorrufen. Eine Überforderung tritt auf, wenn die notwendigen Fähigkeiten die persönlichen Kapazitäten übersteigen und ein „mentales Modell der Funktionsweise“ fehlt (Badke-Schaub et al. 2008, 317). Die galoppierende Technologisierung zieht zwangsweise nach sich, dass vermehrt diejenigen Nutzer in

Kontakt mit komplexer Technik geraten, die nicht für die Bedienung ausgebildet sind (vgl. Strohschneider 2010, 167). Anwender „sind in diesem Fall nicht in der Lage, die wahrgenommenen Informationen richtig zu interpretieren und daraus Vorhersagen über die weiteren Prozesse abzuleiten“ (Badke-Schaub et al. 2008, 317).

Sich verändernde Bezugsrahmen, katalysierende Medieneffekte und fluktuierende Technologien, die jeweils auf eine stetige Assimilation der etablierten Lebensgewohnheiten hinwirken, katalysieren die Komplexität der Alltagswelt, weil sie stets unter anderem auf Moral, Selbstreflexion und Vergangenheitsbewusstsein treffen (vgl. Berger/Luckmann 2018, 51).

Der Moralpegel der öffentlichen Kommunikation steigt mit dem unkalkulierbaren Wirkungspotenzial von Hochtechnologien und Zivilisationsoptimierungen. Moralische Appelle und Warnungen sind als Gegenreaktion darauf zu verstehen, dass das eigene Vertrauen in die Lebenswelt regelmäßig ausgehebelt und mit Unwissen und Angst konfrontiert wird. Nichtwissen, Misstrauen und angsterregende Berichterstattung erzeugen in dieser Kombination alles andere als Technikoptimismus oder kollektive Gelassenheit (Ziemann 2011, 251).

Aus Andreas Ziemanns Postulat lässt sich folgern, dass ein Zusammenstoß von indoktrinierten, tradierten Gewohnheiten mit verunsichernden Gegebenheiten zu gesteigerter öffentlicher Aufmerksamkeit und erhöhter Erregung führt. Je unvorhersehbarer die Folgen neuer „Hochtechnologien und Zivilisationsoptimierungen“ desto offener sind Diskussionsbedarf und Ruf nach Sicherheiten. Im Umkehrschluss ist diese Verstimmung eine bedeutende Triebfeder zur Einleitung reformierender Bemühungen. Obwohl Marshall McLuhan vor der Hochzeit von Internet und Vernetzung verstarb, stellte er bereits 1964 fest: „Thus the age of anxiety and of electric media is also the age of the unconscious and of apathy“ (McLuhan 1964, 47). Ziemann und McLuhan erkennen hier eine Konfusion, die in einem ähnlichen Maß ansteigt, wie die Technologiekomplexität zunimmt. Obendrein identifiziert Niklas Luhmann das Dilemma als „Komplexitätsgefälle zwischen Umwelt und System“, das er unter anderem auf die moderne Anforderung der Gleichzeitigkeit zurückführt (Luhmann 1985, 256).

Währenddessen stellt man fest, dass Informationstechnik und Digitalisierung nicht abgelehnt, sondern kulturübergreifend vermehrt eingefordert und forciert werden. Es scheint also ein Phänomen zu existieren, dass die Steuerung komplexer Systeme ermöglicht, sie zugänglich macht und einer Überlastung der User vorbeugt – die Black

Box. Dieser Terminus ist deshalb hier so gewinnbringend, weil er verdeutlicht, wie Menschen diffizile soziale und technische Herausforderungen bewältigen, ohne übermäßige Expertise anhäufen zu müssen. Die Idee der *doppelten Kontingen*z nähert sich der Black Box unter sozialwissenschaftlichen Gesichtspunkten: Talcott Parsons führte die doppelte Kontingenz ein, um das Scharnier zwischen individueller Interaktion und gesellschaftlicher, schließlich kultureller Manifestation benennen zu können (vgl. Parsons et al. 1951, 16). Der Begriff beschreibt einen Augenblick zwischenmenschlicher Interaktion, in dem beide Akteure nichts tun müssen, aber zugleich alles tun könnten. Sie kennen ihr Gegenüber nicht und können nicht sicher wissen, welche Handlung die andere Person als nächste unternimmt. Die Black Box meint eben das auf gegenständliche Weise: Ein System, dessen Funktion, Algorithmen, Gedanken oder Schaltungen für dessen Umwelt nicht nachvollziehbar sind. „Das, was von ihr sichtbar wird, ist deshalb notwendig Reduktion“ (Luhmann 1985, 156). Die Interaktion beschränkt sich auf die für eine Kommunikation unausweichlichen Anschlusspunkte der Box. Die Innereien der Box selbst sind dabei nicht determinierbar. Auf diese Weise blendet das Bildnis der geschlossenen Dose zunächst aus, dass die Beteiligten innerhalb eines sozialen oder technologischen Kontextes aufgewachsen beziehungsweise programmiert sind und bereits ein erwartbares Verhalten erlernt haben. Diese Akteure setzen dann voraus, dass externe Systeme, seien es nun Personen, Tiere oder leblose Gerätschaften im Rahmen des Repertoires agieren, das schon in der Vergangenheit zu beobachten war. Dies unterstreicht Parsons doppelte Kontingenz: Auf Basis wechselseitiger Beobachtung sowie eines erlernten normativen Fundaments wählen die beteiligten Akteure, ob und wie sie interagieren möchten. Für einen intersubjektiven Dialog müssen sie den Zustand der Kontingenz überwinden, wodurch Kommunikation zunächst eher unwahrscheinlich wird. Jedoch führt die Beobachtung des Gegenübers und die vorausgehenden Interaktionserfahrungen zu Erwartungen, die das jeweils andere System reduziert und erst ordinär begreifbar macht. Damit zeigen sowohl Parsons als auch Luhmann, dass internalisierte Automatismen notwendig sind und gleichzeitig dokumentieren sie, dass diese Konnexionsmomente in härtenden System-Umwelt-Handlungen aufgehen. Es entsteht eine „immanente Zirkularität“, die ein Zusammenspiel erlernbar macht (Luhmann 1985, 150). Systeme eignen sich dann an, was sie an ihrer Umwelt „als Input und Output beobachten können, und lernen jeweils selbstreferentiell in ihrer je eigenen Beobachterperspektive“ (Luhmann 1985, 157). Luhmann versucht die Schiefelage später mit dem Konzept der

Interpenetration aufzulösen. So hat ein penetrierendes System nicht nur Einfluss auf das aufnehmende System, sondern auch umgekehrt. Ohne die Autonomie der jeweiligen Systeme zu beschädigen, entstehen durch Kommunikation und Interaktion Unordnungen, die zu neuer Strukturbildung beitragen (vgl. Luhmann 1985, 290).

Als naheliegendes Beispiel eignen sich Computer. Sie sind für die meisten Bediener nicht zu durchdringende Unbekannte, deren Funktionsweise völlig mysteriös bleibt und die sie dennoch täglich viele Male verwenden. Die Eingaben mittels der wenigen intuitiven Schnittstellen erfolgen im Flow, in einem Zustand schematisierter Abfolgen und sind dabei doch für alle Bedienenden gleich. Die technologische Black Box normiert und standardisiert Bedienung, Kommunikation und Kulturpraxis, unabhängig von Herkunft und Vorwissen der Anwender (vgl. Hallin/Mancini 2004, 260). Gedanken über Hintergrundprozesse oder gar über Bedrohungen sind für die reibungsfreie Funktion des Geräts kontraproduktiv. Horkheimer und Adorno präzisieren in ihrer ‚Dialektik der Aufklärung‘ das Phänomen:

Der Zuschauer soll keiner eigenen Gedanken bedürfen: das Produkt zeichnet jede Reaktion vor: nicht durch seinen sachlichen Zusammenhang – dieser zerfällt, soweit er Denken beansprucht – sondern durch Signale. Jede logische Verbindung, die geistigen Atem voraussetzt, wird peinlich vermieden (Adorno/Horkheimer 2019, 145).

Natürlich beziehen sich die Autoren an dieser Stelle weder auf moderne Notebooks noch auf Smartphones oder vernetzte Autos. Ihr Argument bleibt jedoch bestehen. Technologien sind Werkzeuge, die den Nutzer unterstützen, bestenfalls unterhalten sollen. Dabei kann es völlig undienlich sein, wenn die Konsumenten mit der detaillierten Funktionsweise des jeweiligen Produkts vertraut sind. Das Ziel des Produzenten besteht im Gegenteil darin, dem Nutzer die Bedienung möglichst angenehm zu gestalten, sodass das Produkt bei jeder Verwendung die mit ihm verbundenen positiven Assoziationen verstärkt. Zusätzlich vergrößert eine vereinfachte Bedienung die Zahl möglicher Käufer, die wiederum als Multiplikatoren und unwissentliche Werbeträger wertvoll sein können – die Massenproduktion stellt Uniformität her (vgl. Williams 1960, 344). Auch deshalb stehen moderne Gesellschaften an einem Punkt, an dem sich Informationstechnik nicht mehr in einzelne Sphären des Lebens wie den Beruf einordnen lässt, sondern stattdessen organisations-, länder- und kulturübergreifende Reize setzt.

Die Vorteile von Vereinfachungsmechanismen erkannte auch Niklas Luhmann. Obwohl er sein Theorem zur Interdependenz von System und Umwelt bevorzugt auf soziale Entitäten anwendet, lassen sich viele mindestens sinnkongruierende Eigenschaften der Systemtheorie auch in maschinelle Systeme respektive Umwelten übersetzen. Luhmann errichtet Umwelten, die aus einer nicht determinierbaren Zahl von geschlossenen Systemen bestehen und bricht seine Theorie selbst auf ein zentrales Paradigma herunter: „Alles, was vorkommt, ist immer zugleich zugehörig zu einem System (oder zu mehreren Systemen) und zugehörig zur Umwelt anderer Systeme“ (Luhmann 1985, 243). Er schließt, dass die Simplifizierung einer Systemeigenschaft zur Vereinfachung der Umwelt aller anderen Systeme führt. Folglich bedeutet dies, dass die Banalisierung des technologischen Systems Computer seit den späten Zwanziger Jahren des 20. Jahrhunderts endlosen, divergierenden Umwelten und Systemen den Umgang mit dem Computer erleichtert und gar erst ermöglicht hat.

Zugleich führt diese Annäherung der Systeme unweigerlich zu Abstrahierungen, sodass die angeeigneten Automatismen als Interaktionszugang genügen und das Wissen über den detaillierten Inhalt des Systems Computer verzichtbar wird. Das entspricht dem Geheimnisprinzip der Informatik, welches die Idee verkörpert, dass Informationen zum Beispiel in Klassen verborgen werden, um freiwillige oder unfreiwillige Manipulation zu verhindern (vgl. Parnas 1985, 19). Es entstehen aus dem Blickwinkel der umliegenden Systeme Black Boxes, deren Qualitäten, Prozesse und Potenziale unsichtbar sind. Ebendiese Verpackung eines komplexen Systems in einer differenzierbaren, uniformen Hülle der unbewussten Handhabbarkeit macht soziale Gruppen, Automobile oder Computer erst erlebbar.

Für die Funktion einer Black Box ist also die gezielte Abwesenheit detaillierter Information damit von entscheidender Bedeutung. Luhmann erklärt die Simplifizierungsfunktion der Black Box mit einer sichtbaren Normativität des Verhältnisses aus Reiz und Reaktion. Ein immer gleicher Input hat einen vorhersagbaren Output zur Folge, was bedeutet, dass die eigentliche Komplexität des Systems nachgeordnete Relevanz erfährt (vgl. Luhmann 1985, 156). Auf diese Weise wird der Anwender vor Überforderung bewahrt und zugleich das System von Bedienfehlern weitestgehend isoliert. Zugleich setzt diese Idee voraus, dass die große Mehrheit der umgebenden Akteure ihre eigene, zumindest bedingte Unwissenheit akzeptieren muss.

Einerseits umreißt dies ein unabdingbares Konstruktionsprinzip verschachtelter Systeme, da sonst alle Benutzer eines Computers tiefgehende Kenntnisse im Bereich der Informatik oder Elektrotechnik aufweisen müssten. Andererseits dient die Black Box als Vorhang, der im Falle von Rechenmaschinen vor Platinen, Laufwerken und Registry-Datenbanken hängt. Dies führt dazu, dass Bediener nicht befähigt sind, souverän Probleme zu detektieren und zu normalisieren; ihre Position wird durch die Detailverhüllung geschwächt, indem sie schwindende Mündigkeit mit erhöhtem Komfort aufwiegen. Die Verbraucher legitimieren den Produzenten und räumen diesem einen Vertrauensvorschuss ein. Der Experte einer spezifischen Black Box hingegen gewinnt an Bedeutung für das Funktionieren des vorgeordneten Systems. Der Experte visualisiert ein Hemmnis, benennt und beseitigt es. So öffnet ein Mediziner den Korpus der Box (des Menschen), um die vorgesehene Dienstfähigkeit zu erhalten. Laien geraten auf diese Weise notgedrungen in ein Abhängigkeitsverhältnis, aus dem sich zu befreien, aufgrund der Vielzahl gleichartiger Abhängigkeiten hoffnungslos erscheint. Ist dann auch noch, wie im Fall der Informationstechnik, der zum Expertentum erforderliche Sachverstand offenkundig umfassend, erscheint dem Laien das Begreifen der verborgenen Prozesse noch unwahrscheinlicher. Wenn der Bediener nicht weiß, wie das Gerät funktioniert, wo dessen neuralgische oder disponierte Winkel liegen, ist der Schutz des Gesamtsystems eine zweifelhafte Herausforderung. Boaru und Iorga unterstützen die Bedeutung eines mündigen Bedienenden, indem sie veranschaulichen, dass der Mensch die Schnittstelle zwischen dem physischen und dem virtuellen Raum bildet:

We breath – we navigate, we speak – we socialize online, we feed ourselves – we simulate, we go to school – we are e-learning clients, we compose letters – we are sending an e-mail, we make investments – we make online transactions, all these are just a few elements that coexist in those two totally different spaces according to their characteristics, but that are linked by the integrating human part – the one that has generated, develops and exploits them (Boaru/Iorga 2015, 32).

Es sind die Anwender, die selbstverständlich zwischen den Räumen wandeln und derweil zumeist nicht über die notwendige Autonomie verfügen, die interdependente Sicherheit beider Räume selbstbestimmt zu verwalten. Luigi Lo Iacono und Matthew Smith fordern aufgrund dieser Komplexität und gleichzeitigen Verschllossenheit informationstechnischer Systeme zusätzlich zur Qualitätseigenschaft *Sicherheit* auch das Attribut der *Usability*, also der allgemeinen Nutzbarkeit. Zwar sehen Lo Iacono und

Smith die Gefahr, dass beispielsweise eine Steigerung der Sicherheit eine Beeinträchtigung der Bedienbarkeit zur Folge haben könnte. Jedoch nehmen sie an, dass es ebenso realisierbar ist, „den gewünschten Grad an Sicherheit zu erreichen, ohne dass die Benutzbarkeit hierdurch beeinträchtigt wird“ (Lo Iacono/Smith 2018, 101). Mit dem Stichwort *Usable Security* benennen die Autoren deshalb ihre Annahme, die darauf abzielt, dass „Nutzer jeglicher Couleur (insbesondere aber auch Laien und technikferne Endanwender) in die Lage versetzt werden, Sicherheitsfunktionen und deren Notwendigkeit zumindest grundlegend zu verstehen und diese in der dafür vorgesehenen Weise zu verwenden“ (Lo Iacono/Smith 2018, 101). Mit dieser Idee leisten Lo Iacono und Smith exemplarisch einen Beitrag zu ebenjener IT-Sicherheitskultur. Sie zeigen auf, dass Informationstechnik zugleich Secure und Usable sein kann und stellen koinzident die gegebene Rollenverteilung infrage, indem sie Verantwortung von den Nutzern auf die Produzenten der Technologie verlagern.

In der Nahtstelle zwischen vermeintlich sicherer Technologie und den teilweise digital unaufgeklärten Anwendern zeigt Cybersicherheitskultur des Weiteren integrierende Wirkung. Eine ausgeprägte, offene Sicherheitskultur kann die Berührung mit Informationstechnik erleichtern und korrelative Effekte lostreten. Als breit angelegte, öffentliche Debatte über ein IT-Problem löst sie bestenfalls nicht nur die technische Fragestellung, editiert also das maschinell-digitale, sondern manifestiert durch die inkludierende Diskussion mindestens basale Kenntnisse und führt punktuell zu nachdrücklichem Interesse. Unter teils unbewusster Berücksichtigung eigener wie auch fremder Standpunkte entscheidet der Bediener im Augenblick der Anwendung, ob er den gängigen Einsichten folgt. Er kann durch die (nicht-)Nutzung von Technologie zu ihrer Verbreitung beitragen und er formt durch seine Art des Konsumierens und Rezipierens, wie das Umfeld die Bedeutung von IT-Sicherheit wahrnimmt – ein im Grunde hochgradig demokratischer Hergang. Auf diese Weise können anspruchsvolle, überwiegend akademische Komplexe nachhaltig in gesellschaftliche Faktizität überschrieben werden.

Security culture can be defined as the first line of cyber defense and is the sum of values, norms, attitudes and actions in the virtual environment, which determines the understanding and assimilation of cyber security concept and other secondary concepts: information security, physical security, document security, personnel security, communications security, political security, insecurity etc. (Boaru/Iorga 2015, 40).

Das ist wohl auch jener Moment, den Vilém Flusser meinte, als er schrieb, dass sich jeder Einzelne als „Funktion aller anderen“ erkennt und darüber die Verantwortung die individuelle Freiheit ersetzt (Flusser 1989, 54). IT-Sicherheit gewinnt durch Diskurs, Innovation, Vermarktung und vielzählige weitere Faktoren an Relevanz, da die beschriebene Internalisierung zu erhöhter Akzeptanz sowie potenziertem Engagement führen kann. IT-Sicherheitskultur ist somit mehr als nur die unmittelbare Mensch-Maschine-Interaktion. Sie hilft, das Wissen von dem *was ist* zu ordnen, indem sie jedem Teilhaber der Gesellschaft eine Rolle zuweist, die jedes Individuum mit erlernten Routinen anfüllt (vgl. Berger/Luckmann 2018, 45). Eine Untersuchung von Cybersecurity Culture bedeutet sogar, die Technik nicht zu zentrieren, sondern ihre Wirkung auf den Menschen und den Umgang des Menschen mit den Unsicherheits Herausforderungen der Technologie zu beobachten. Alle vorausgegangenen Zeilen lassen nur den Schluss zu, dass das Paradigma einer zeitgemäßen IT-Sicherheitskultur, gar von Kultur überhaupt, sein muss, „Technik nicht mehr als Subsystem, sondern als integralen Bestandteil des gesellschaftlichen Systems von Kulturfertigkeiten und sozialen Praktiken zu konzipieren“ (Siedschlag/Jerković 2014, 309). Aus vielen, nicht eindeutig zu umreißen Wesenszügen einer sozialen Gruppe und einer unzählbaren Menge möglicher Einflüsse – beispielsweise ein breiter Konsens oder Dissens, gruppenäußere wie -innere Dynamiken, durch vergangene individuelle wie kollektive Erfahrungen sowie wiederkehrende, gravierende Impetus – erwächst ein kausales Wechselspiel von Aktion und Reaktion, das sich schließlich in Institutionen und Organisationen niederschlägt. Wenn Sicherheitskultur nun den fortschreitenden Disput über das Sichere und das Unsichere verkörpert, sich dieser Austausch in Organisationsgerüsten und Handlungsnormativen verfestigt, und er schließlich zu partikularen Determinationen des Möglichen führt, dann kann für die anschließende Untersuchung unterstellt werden, dass Sicherheitskultur auch von diesen strukturell-institutionellen Gegebenheiten evoziert wird. Indem es gelingt, dieses gruppenspezifische Echo als Essenz relationaler, routinierter Erfahrungen und imaginierter Zukunftserwartungen einzufangen, entspinnen sich charakteristische Abbilder von IT-Sicherheitskultur.

1.5.1 Medium *IT-Sicherheitskultur* in den Medien

Mehr und mehr kommt zum Vorschein, warum diese Arbeit unter dem Dach der Medienwissenschaften verfasst ist. Denn offenbar besteht eine korrelative Beziehung

zwischen gerade erklärten komplexen, technischen Medien aus dem Umfeld der IT-Sicherheit und den mit diesen interagierenden Gesellschaften und Kulturen. Jedenfalls kursieren von statischen Dogmen bis hin zu abstrakteren, aufnahmefähigen Deutungen unzählige Ansichten darüber, was unter Medien zu verstehen ist, sodass im Laufe der Zeit nahezu alles schon ein mal zum Medium erkoren wurde (vgl. Ernst/Schröter 2020, 11). Nun hilft es der Argumentation wenig, zu tief in die Terminologiedebatte einzutauchen. Stattdessen genügt es, zwei approximative Medieninterpretationen zu destillieren, die im Fortlauf unentbehrlich sind. Dazu bietet sich die Unterscheidung in öffentliche und infrastrukturelle Medien nach Erhard Schüttpelz an, der sich Jens Schröter bei seinem Brückenschlag von Medien und Ökonomie ebenso bediente:

1. Die Diskussion um die jeweiligen Cybersicherheitskulturen verhandelt selbstverständlich Medien im klassischen Sinne, also etwa Computer, das Internet oder auch distribuierende Massenmedien wie Zeitungen oder Rundfunkanstalten. Dieses Verständnis zentriert Technologien und haptisch begreifliche Medien, die ihre mediale Vermittlerfunktion insbesondere dadurch ausüben, dass sie Nachrichten und Botschaften über Entfernungen respektive Zeiträume hinweghelfen. Sie sind öffentlich in gleich mehrfacher Hinsicht.

2. Medien sind nicht nur maschinelles Werkzeug zur Übertragung von Informationen, sondern ein Konstitutionsinstrument. Sie schaffen Abbilder und Versionen von Realitäten und sind qua ihrer Selektion und Verwertungsqualität stets performativ. Sie sind bei Schröter die Ökonomie, allgemeiner gesprochen eben die Infrastruktur, für die oben stehenden Medien (vgl. Schröter 2019, 14). Zu dieser Gattung gehören folglich der Markt und das Geld, als Träger und Vermittler von Informationen wie Wert oder Nachfrage (vgl. Schröter 2019, 15ff). Durch ihre Transferleistung wirken derartige Medien auf Empfängergruppen ein und besitzen das Potenzial, Reaktionen hervorzurufen, die wiederum das Medium verändern. Um bei dem genannten Beispiel zu bleiben, denke man nur an eine breite Vermehrung des Infrastrukturmediums Geld. Dieses Phänomen, bekannt als Inflation, hat schon so manche Regierung und noch mehr persönliche Schicksale sabotiert. Schüttpelz selbst fasst unter infrastrukturelle Medien „lokalisierte Interaktionsketten mit ihren situierten »skills«, »communities of practice« und »gängigen Verfahren«, genauso wie etablierte und weitestgehend universell gültige Normen und Prozesse, „die eine Anonymisierung und Vervielfältigung der

zirkulierenden Dokumente und Daten“ ermöglichen (Schüttpelz 2016, 15). In diesem Sinne lassen sich dann Ökonomien, Bindestrichkulturen, die Politik oder womöglich die Medienwissenschaften selbst als Medien erfassen.

Christoph Ernst und Jens Schröter schlagen gar die Brücke zwischen beiden Perspektiven, wenn sie auf Friedrich Kittler verweisen. Obwohl nach wie vor zwischen infrastrukturellen und öffentlichen Medien differenziert werden kann und muss, zeigen sich naturgemäß übereinstimmende Attribute:

Medien machen Objekte wahrnehmbar, mit ihrer Hilfe werden Informationen verarbeitet, sie ermöglichen die Kommunikation, sie sind das Gedächtnis einer Kultur und einer Gesellschaft (Kittler 1993a, S. 8). Als solche unterliegen Medien aber auch einem konstanten Wandel. Ebenso wie Kultur und Gesellschaft dafür sorgen, dass sich die Medien wandeln, wirkt sich umgekehrt der Medienwandel auch auf Kultur und Gesellschaft aus (Ernst/Schröter 2020, 9f).

Vor wenigen Seiten zeigte sich, dass auch die Kultur primär ein Destillat von Kommunikation ist. Da Medien Botschaften tragen beziehungsweise Botschaften sind, liegt hier nahe, dass auch Kultur ebenso Medium ist. Medien selektieren, naturalisieren, imitieren, konkurrieren und individualisieren Nachrichten und Botschaften. Sie sind zugleich Behältnis und Formgeber von Interaktion. Erst Medien, und sei es nur die Stimme, erlauben Kommunikation, die wiederum notwendig zur Herstellung von Kultur ist.

Medien haben in diesem Zusammenhang ihren Stellenwert, indem durch sie Kommunikationsprozesse in Gang gesetzt werden. Medienangebote sind damit die zentralen Elemente der Kopplung von Kognition (des psychischen Systems) und von Kommunikation (als Basis des Sozialsystems). So müssen kognitive Operationen in Medienangebote transformiert werden, um Kommunikation auszulösen, und umgekehrt Medienangebote in kognitive Operationen überführt werden, um neue Kommunikationen zu ermöglichen (Hepp 2011, 24).

Andreas Hepp, der sich bei dieser Aussage auf Siegfried Schmidt bezieht, entdeckt Parallelen zwischen den Begriffen *Medien* und *Kultur*. Er nimmt an, dass Kultur und Medien deckungsgleich in ihrer Funktion sind und deshalb nur ein und dasselbe sein können, weil sie, wie Bauman oben schon zitiert wurde, „aus dem Flüchtigen [...] das Dauerhafte, aus dem Diskontinuierlichen das Kontinuierliche“ modellieren (Bauman 2000, 150). Schmidt erkennt, dass Medien stets ein untrennbarer Teil von Kultur sind, weil sie es sind, die erst die kollektive Reproduktion vieler einzelner Wirklichkeiten erlauben (vgl. Schmidt 2000, 41). Eine nach allgemeinen, sozialen Regeln funktionierende Medienkultur ist die Voraussetzung für Interaktion, die dann

wiederum Konsolidierung und Progression zwischenmenschlicher Erwartungen und Normative erwirkt. Somit ist die Kultur das, was bei Schröter der Markt ist – ein infrastrukturelles Medium, auf dessen Fundament „überall Informationen aufgespeichert, übertragen, verarbeitet und dargestellt werden“ (Schröter 2019, 14).

Andreas Ziemann steuert zur Verbindung von Medien und Kultur bei. Er verknüpft beide in dem Versuch, die Funktionen von Massenmedien respektive öffentlichen Medien zusammenzutragen und nennt Attribute, die genauso gut auf Kultur zutreffen: „Moralisierung und Alarmierung“, „Sozialisationsfunktion, Informations- bzw. Wissensfunktion, kollektive Gedächtnisfunktion und Gratifikations- bzw. Unterhaltungsfunktion“ (Ziemann 2011, 252). All diese Aufgaben, die Kultur ergo Medium erfüllen soll, sind leicht nachvollziehbar. Gleichzeitig sind sie eine Bestätigung dessen, was schon vor einigen Seiten als ‚soziohistorisches Apriori‘ vorgestellt wurde: Der Versuch Kultur nahezukommen, kann nur unter Berücksichtigung der sozialen wie zeitlichen Verortung des zu untersuchenden Kulturgebildes und „nur innerhalb der jeweiligen theorie- und disziplinabhängigen Konstruktion von Gegenständen und Fragestellungen kohärent“ vollzogen werden (Moebius/Quadflieg 2011, 13). Der Resonanzraum, in dem Medienkultur verhandelt wird, setzt dem folgend die Grundbedingungen für die Reproduktion von Wertvorstellung, Ethos und Agenda Setting fest. Gleiches gilt, wie zuvor erkannt für Sicherheitskultur.

Wenn sich Kultur über Kommunikation, Relation und Resonanz konstituiert, nehmen Medien und mediale Praktiken zwangsläufig eine tragende Funktion ein. Online-Foren, Talkshows, Bücher, Zeitungen, Podcasts, aber auch Volksfeste, Kneipen oder Büros sind Medien, in denen sich Menschen begegnen und innerhalb derer sie Kultur generieren. Passend dazu formuliert Nick Couldry einen weiteren grundlegenden Gedanken, der erahnen lässt, wie Medien in den Prozess der Kulturinternalisierung eingewoben sind und führt dazu den Begriff der ‚Naturalisierung‘ an. Damit verfolgt er die These, dass Medien Bilder der Welt naturalisieren beziehungsweise etablieren. Essenziell hieran ist, dass sie dies nicht einheitlich tun, sondern für jedes Individuum subjektive Aspekte ausblenden, Bedeutungsebenen verbinden und gewisse Standpunkte stärken, während sie andere schwächen. Diese Filtration von Inhalten und Botschaften liegt unter anderem in den individuellen Erfahrungen und der persönlichen Rezeptionsweise begründet. „[...] Naturalization is not a property exclusively of media: it is an effect of all forms of power that construct a distinctive map of ‘what is’“ (Couldry 2012, 84f).

Demnach erzeugen Medien, aber zum Beispiel auch populäre Vorbilder oder Regierungen in höchstem Maße selektive Stimulanzien. Die naturalisierenden Kräfte forcieren einander und porträtieren dabei niemals eine universelle und objektive Reproduktion der Wirklichkeit.

Auf der einen Seite der Medialisierung steht also die individualisierte, subjektive Wahrnehmung.

Zum anderen greift die Integrationskraft, dass notwendiges Wissen, Neues und Sinnorientierungen durch Massenmedien und Populärkultur vermittelt sind und diese die Basis sozialer Ordnung und geteilter Wirklichkeitserfahrungen herstellen wie auch garantieren (Ziemann 2011, 226).

Der Mensch vor dem Fernseher, der Zeitung oder dem Tablet rezipiert folglich völlig allein unter den Bedingungen seiner gänzlich subjektiven Sinneswahrnehmung und befindet sich gleichzeitig in einer parasozialen Ordnung. Er erfährt also in dem Bewusstsein, dass die Medienbotschaft simultan viele weitere Personen erreicht, eine Form paralleler Homogenisierung (vgl. Wenzel 1998, 120). Darin ist keinesfalls ein Widerspruch zu entdecken. Vielmehr überschneiden sich beide Erfahrungsflächen: Die jeweilige Wahrnehmung determiniert, mit welcher Intensität das Individuum die doch gemeinschaftliche Rezeption des Medienempfangs als solche apperzipiert. Das angeführte Vertrauenskapital, das Wenzel 1998 besonders dem Fernsehen zuschreibt, ersetzt ihm zufolge die sozialen Orientierungsmächte, also jene orthosozialen Beziehungen, die Menschen im direkten, stofflich-realen Kontakt erleben. Dieser Vorschuss an Integrität und Vertrauen ermöglicht es medialen Botschaften, zum Einzelnen im Rahmen seiner singulären Rezeption vorzudringen. Im McLuhan'schen Sinn steckt insofern in jedem Medium auch eine spezifisch immanente Qualität seiner Glaubwürdigkeit und Überzeugungskraft, die jedoch mit der Zeit großen Schwankungen unterliegen kann. Niklas Luhmanns Idee einer „Individualisierung der moralischen Referenz“ fügt dem eine weitere Ebene hinzu (Luhmann 1997, 248). Abhängig von Beruf, Stellung oder Erziehung gehen innerhalb einer sozialen Gruppe Meinungen und Vorstellungen von Moralität auseinander, die dazu führen können, dass ein und dieselbe Situation von mehreren Personen höchst unterschiedlich bewertet wird. Insbesondere die mediale Vielfalt und die damit verbundene Möglichkeit zur Auswahl der persönlich präferierten ‚konkurrierenden Öffentlichkeit‘ im Habermas'schen Verständnis hat das Potenzial, Debatten entweder neu zu ordnen oder radikale Lagerbildung zu zementieren (vgl. Habermas 1990, 344).

Nach der Feststellung, dass sich kulturelle Muster unmittelbar durch die eingangs genannten klassischen Massenmedien fortpflanzen, also beispielsweise durch Internet, Videospiele, Podcast oder Fernsehen, wird die Kongruenz von Sicherheitskultur und Medium noch sichtbar. Gleichzeitig verdeutlicht sich, dass die Securitization der Kopenhagener Schule weiter zu fassen sein muss und die Limitierungen der reinen Sprache überwindet: „[T]he speech act of securitization [...] is a broader performative act which draws upon a variety of contextual, institutional, and symbolic resources for its effectiveness“ (Williams 2003, 526). Ohne lokal oder temporal am gleichen Ort sein zu müssen, können einander unbekannte Menschen den identischen Inhalt in ihrer subjektiven, individuellen Erfahrungswelt rezipieren. Das verleiht Medien eine besonders machtvoll Position: Sie bilden eine Brücke, wie es Hubert Kleinert nennt, zwischen dem teilweise singularisierten Publikum und dem aktuellen Zeitgeschehen, sodass ihre Darstellung der Ereignisse zur Wahrheit wird (vgl. Kleinert 2020, 639). „Im Ergebnis spielen persönliche Netzwerke und Verbreitungsmedien also ineinander, wenn es um die Entstehung und Verbreitung von kulturellen Mustern geht“ (Fuhse 2011, 34). An dieser Stelle schließt sich der Kreis und man gelangt erneut zu Schnettlers soziohistorischem Apriori, das sich auf Michel Foucaults historisches Apriori stützt.

Die Wahrheit ist von dieser Welt; in dieser wird sie aufgrund vielfältiger Zwänge produziert, verfügt sie über geregelte Machtwirkungen. Jede Gesellschaft hat ihre eigene Ordnung der Wahrheit, ihre 'allgemeine Politik' der Wahrheit: d. h. sie akzeptiert bestimmte Diskurse, die sie als wahre Diskurse funktionieren lässt (Foucault 1978, 51).

Verschiedenerlei biografische wie auch soziale Kontexte stellen ebenso zahlreiche Lesarten her. Die enthaltenen Botschaften werden dann individuell im Rahmen einer kulturellen Einbettung entschlüsselt und reproduziert. Walter Benjamin formulierte schon Jahre vor Foucault, dass Kognition kein rein biologischer Vorgang ist, sondern innerhalb eines historisch bedingten Mediums verläuft (vgl. Benjamin 2010, 18). Seine darauffolgenden Schilderungen zu Kunst und Reproduktion zeigen deutlich, dass Benjamin mit diesem Medium zeitgenössische Kulturmodi bedenkt. Zu ebendiesen gehört freilich auch die Sicherheitskultur, da der Druck von Kriegen, Krankheiten oder anderen Bedrohungen seit jeher den Rahmen für die Lebenswirklichkeiten formt und damit fundamentalen Einfluss zum Beispiel auf den sozialen oder politischen Kontext der Menschen ausübt.

Um es in einem Bild auszudrücken ist Kultur, in ihrer spezifischen Ausprägung Cybersicherheitskultur, die Bühne zur anhaltenden Neuverhandlung dessen, was sicher ist. So zeigt das Szenenbild dem Publikum Ausschnitte aus dem, was weithin als gegeben gilt. Es repräsentiert das verbreitete Verständnis über das Dilemma, die Problemstellung, vor der das Theater stattfindet. Die Schauspieler in dieser Allegorie kolportieren Botschaften und wirken auf die Wahrnehmung des Szenenbilds ein. Ihr Spiel beeinflusst maßgeblich, wie das Stück wahrgenommen wird und welche Interpretation der Realität sich nachhaltig durchsetzt. Sie sind Meinungsmacher, Sender, Funktionäre oder auch Freunde. Dem Publikum dieses Stücks kommt nicht nur eine rezeptive Funktion zu. Es wirkt aktiv an der Geschichte mit und dient vielmehr als Spiegel für die Schauspieler. Das Publikum, im obigen Verständnis auch die politische Kultur, geht mit individuell biografischen Prägungen in das Stück und verlässt es mit einem weiteren Impetus. Es reagiert auf die Handlung der Figuren und drückt Einverständnis oder Missmut aus. Nebenbei sprechen die Besucher des Stücks sogar miteinander und verwerten das Spiel unmittelbar. Diese horizontale Kommunikation festigt Meinungen und äußert sich schließlich in vertikalen Antworten. Schauspieler und Publikum agieren in einer Art Improvisationstheater miteinander und schreiben die Erzählung fort. Wenngleich die vorausgegangenen sowie die noch folgenden Kapitel aufschlüsseln, dass die soeben gezeichneten Abläufe deutlich komplexer sind, illustriert diese Metapher, dass (Sicherheits-)Kultur nicht nur einen Phänotyp medialer Hergänge darstellt. Stattdessen ist sie selbst Bedeutungsträger, indem sie kollektive Annahmen, Urteile und Visionen speichert und verbreitet.

Dennoch werden Medien selbst häufig nicht als Botschaft gelesen, sondern als Überbringer von Bild, Ton und Text. Jedoch ist schon seit Ende der 50er Jahre nicht zu bestreiten, dass Medien auch selbst Nachrichten und nicht nur ihre Träger sind (vgl. McLuhan 1964, 29). Die Form der Botschaftsvermittlung hat nach diesem Axiom entscheidenden Einfluss auf den Inhalt selbst. Die Übertragungskraft des Mediums, also die Darreichungsform einer Information, hat substanziellen Einfluss auf die Information (vgl. Floren 2006, 84). Das Medium ist somit wichtiger Bestandteil der übermittelten Nachricht. Deutlich wird diese Doppelfunktion, indem man „ihre Effekte wiederum als Ursachen begreift“ (Sprenger 2017, 40). Das bedeutet, dass der Aggregatzustand einer Botschaft maßgeblich beeinflusst, wie diese Botschaft empfangen und entschlüsselt wird. Überträgt man diesen Gedanken auf die Sicherheitskultur, stellt man unweigerlich

die identische Besonderheit fest. Denn ganz eindeutig hängt die Verankerung neuer Sicherheitsmechanismen davon ab, wie sich die Sicherheitskultur zur vorliegenden Problemstellung verhält. Die Ausprägung der Sicherheitskultur, ergo der Medien, mit denen sich Sicherheitsempfinden und -verständnis über eine Gesellschaft ausbreitet, beeinflusst grundlegend, welche Themen der Sicherheit aufgegriffen werden, welches Kolorit sie einnehmen und schließlich auch, wie sie auf die bestehende Sicherheitskultur zurückwirken. Sicherheitskultur ist dann entsprechend selbst Träger von Erwartungen, Hoffnungen und Botschaften – also Medium, und so im konstituierten Zustand eine Nachricht an alle Protagonisten dieser Kultur.

Denn die Kulturpraxis der Sicherheitsherstellung konstruiert subjektive und intersubjektive Wirklichkeitsvorstellungen; eine Eigenschaft, die Hepp eigentlich der Medienkultur zuschreibt (vgl. Hepp 2011, 25). Erst vor wenigen Seiten steht, dass sich Sicherheitskultur durch das wiederholende Begegnungsmoment auszeichnet, in dem Annahmen über Sicherheit und Gefahr als solche lokalisiert werden. Damit bildet sich Sicherheitskultur, gleiches gilt für Medien, niemals ausschließlich intentional aus. Sie werden aus unendlichen Richtungen kollektiv gestaltet und senden auf ebenso vielen Wegen zurück. Security Culture ist also „ein diskursives Element, das aus verschiedenen Richtungen besetzt werden kann und gleichwohl einen minimal-homogenen Kern besitzt“ (Schröter 2014, 8). Die Beobachtung dieser Wirkrichtungen ermöglicht für die Sicherheitskultur im Wesentlichen zwei generalisierte Annahmen: Erstens trägt die Kategorisierung von Umweltsystemen in sicher und unsicher Botschaften über die Konstitution einer Gesellschaft in sich. Ruft man sich das Sicherheitsquadrat in Erinnerung, wird deutlich, dass die gemeinschaftlich wahrgenommene Sicherheit in solchen Fällen von der tatsächlich bestehenden oder nicht bestehenden Gefahrensituation abweicht. Das Ausmaß dieser Abweichung kann dann Rückschlüsse auf pauschale Sehnsüchte, tradierte Ängste oder Zögerlichkeiten – man denke nur an die berühmte *German Angst* – oder eine politische Agenda zulassen (vgl. Krüger 2017, 10). Zweitens bedingt die Installation gewisser Bezugsrahmen als unsicher oder sicher, wie diese Gegebenheiten fortan wahrgenommen werden. So zeigt zum Beispiel das Digitalbarometer des BSI, dass sich der Glaube aus den Anfangszeiten der privaten Computernutzung hartnäckig hält, ein Virenschutzprogramm sei der beste Schutz für das eigene System, obwohl es mittlerweile effektivere Abwehrmechanismen gibt (vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI)/Polizeiliche

Kriminalprävention der Länder und des Bundes (ProPK) 2020, 5). Die daraus sprechende Befürchtung zu relativieren und nun aufzuzeigen, welche Maßnahmen bereits präventiv helfen könnten, lässt sich nur schwer nachhaltig realisieren. Das Label *unsicher* oder *sicher* kann zuweilen nur mühsam entfernt oder verändert werden.

Unter ebendiesen Voraussetzungen nimmt Sicherheitskultur katalysierende Funktion ein und kann sogar ein intendiertes Werkzeug sein, um Kollektivbilder zu schaffen, Motive geschickt zu platzieren und eine Agenda aufzubauen. „Diese Medien-Agenda wirkt sich dann auf die Publikums-Agenda aus, wenn die Medienthemen tatsächlich in der sozialen Anschlusskommunikation aufgegriffen werden“ (Beck 2014, 456). Die Kulturalisierung kollektiver Sicherheitsannahmen respektive -Imagines durch Medien stellt also einen wichtigen Resonanzkörper zur Erzeugung von Diskurs, Meinung und Urteil bereit. Denn Medien wirken nicht in eine prädestinierte Richtung, sondern bedürfen Widerhall und Interaktion, die dazu führen, dass „sich Wirkungen und Rezipienten während des Kommunikationsprozesses aufgrund der Intra- und Intertransaktionen selbst verändern“ (Beck 2014, 456). Auf ebendiese Weise können sich nützliche Verhaltensweisen popularisieren. Genauso gut schreiben sich so Annahmen und Mythen fort, nicht ausschließlich, weil sich eine Stimme der Debatte mit Argumenten durchgesetzt hat, sondern möglicherweise, weil sie die lauteste oder die beständigste war.

Bedrohungslage, Gefahrenwahrnehmung oder aber politische Kultur wandeln sich im Laufe der Zeit und mit Ihnen die Sicherheitskultur, in der sich diese Momente befinden. Gleiches gilt für Spezifika wie der Cybersicherheitskultur. Neue Ereignisse erfordern Reaktionen und lassen Debatten entflammen, die wiederum die Wahrnehmung von Bedrohung modifizieren. Folglich unterliegt Security Culture, ergo das Medium Security Culture, temporal-abhängigen Mechanismen, denn „[s]owohl Rezeptions- als auch Kommunikationsformen der Gesellschaft verändern sich im Zuge des Mediatisierungsprozesses“ (Giebel 2014, 369). Mehr noch wurde in den vorstehenden Kapiteln bereits erkennbar, dass es vom gegenwärtigen Kontext, dem Nachrichtenwert oder von der Aussicht auf Klicks abhängt, wie eine medial-öffentliche Debatte verläuft und mit welcher Intensität diese geführt wird. Denn Medien sind keine Abbilder einer objektiven Realität, sondern Selektionsinstrumente, die gewissen Regelmäßigkeiten folgen. Die Sicherheitskultur, also die Verhandlung dessen, was Sicherheit bedeutet und welches Niveau erstrebenswert erscheint, dient als Vehikel für Diskurs, teils für Streit

und Eskalation. Denn der kulturalisierte Umgang mit Sicherheitsanforderungen, aber auch mit Politik oder anderen bestimmenden Topoi schließt immer alle Ebenen sozialer Konstruktionen ein. Dabei ist es irrelevant, wie sehr eine Teilmenge versucht, eine andere auszuschließen, denn auch über Exklusion wird Kultur geformt und verändert. Sicherheitskultur kann dementsprechend als Bedeutungsträger dienen, mit dessen Hilfe politische und strategische Kultur ihre jeweiligen Interessen in der gegenwärtigen Mediendemokratie platzieren und Illustrationen des Hier und Jetzt schaffen können (vgl. Floren 2006, 82).

Wenn man sich nun abschließend in Erinnerung ruft, dass Sicherheit per definitionem immer als Utopia für ein näheres oder ferneres Futurum entsteht, zeigt sich die Bedingtheit der IT-Sicherheitskultur durch ebensolche Illustrationen von Gegenwart und Zukunft. Auf den vorausgegangenen Seiten ist zu lesen, dass Imaginaries ein bedeutsames Werkzeug zur Fabrikation und Dispersion von Kultur sind. Ihnen kommt eine „*Vermittlungsfunktion* [...] für die Koordination in der Entwicklung neuer Medien und die soziale Akzeptanz dieser Technologien“ zu. Das bedeutet, Imaginaries sind ein mandatorischer Bestandteil von IT-Sicherheitskultur mit identitätsstiftendem Potenzial (vgl. Ernst/Schröter 2020, 49). Somit haben Imaginaries eine zutiefst technische Komponente, da sie die gesellschaftlichen Bedürfnisse und kollektiven Wünsche für den anhaltenden Fortschritt katalysieren, um sie etwa in Halbleiter und Quellcode zu transformieren. Zugleich sind die Imaginaries aber ein allzu soziokulturelles Phänomen, welches mittels der gegenwärtigen Technik-, Konsum- und Medienlandschaft die Vorstellungen des künftig Möglichen installiert. In dem Geflecht/Terminus der Sicherheitskultur kumulieren die zirkulierenden Bilder, relevante Akteure, Medienagenden, politische Gremien und unvorhersehbare Zwischenfälle schließlich, sodass von einer komplexen Plattform der multidirektionalen Einflussnahme, letztlich von einem Medium gesprochen werden kann. Geht man von den justament zusammengestellten Prämissen aus und berücksichtigt man dazu noch, dass in den Niederlanden und Deutschland beispielsweise weitestgehend gleiche Werte, Technologien und extrinsische Umstände vorherrschen, müssen feststellbar unterschiedliche Ansätze in der kulturellen Verarbeitung dieser Gegebenheiten begründet liegen. Umgekehrt heißt dies, dass sich verschiedenartige Imaginaries materialisieren, die die IT-Sicherheitskultur zu einem wirklichkeitsproduzierenden Medium machen.

Hiermit gelangt man nun also zurück zum Beginn des Textabschnitts und zu der Frage, inwiefern IT-Sicherheitskultur mit Medien in Verbindung steht. Offensichtlich ist, dass Medien in ihrer offensichtlichsten Form als Rundfunk oder Text etwa unbestreitbar tief im Prozess der Meinungs-, Kultur- und Identitätsbildung verankert sind. Nicht nur, dass Berichterstattung über mediale Kanäle die Verbreitung von Informationen drastisch beschleunigt: Mit jeder Meldung oder Kommentierung fügen sowohl die gewählten Worte als auch die Selektion der Übertragungstechnik der Botschaft weitere Informationen hinzu. Das vielfach angesprochene Imaginary erhält also im Moment seiner Reproduktion neue Facetten. Es zeigte sich, dass Sicherheitskultur von der Fähigkeit der öffentlichen Medien abhängig ist, Distanzen zu überwinden und die Rezeption von einem transitorischen Zeitpunkt zu lösen.

Die vergangenen Zeilen haben darüber hinaus festgestellt, dass IT-Sicherheitskultur aus vielerlei Gründen selbst als Medium zu betrachten ist. So war erkennbar, dass Cybersicherheitskultur fortlaufend Varianten der Realität konstituiert. IT-Sicherheitskultur ist Transporter für Erwartungen, Befürchtungen, Wirklichkeitsbewältigung und Interaktionspraktiken – durchweg immanente Attribute, die gleichermaßen den öffentlichen Medien zugeschrieben werden. Wie sich herausgestellt hat, ist Cybersecurity Culture also selbst ein infrastrukturelles Medium mit performativer Kraft. Sie stellt die Bühne zur Inszenierung von Sicherheit, auf der die von Schüttpelz benannten *Communities of Practice* mit eigenen Regeln, Rollen und immer neuen Zielgrößen elaborieren, welches Verhalten gemeinhin als angemessen oder gar als zwingend erforderlich kategorisiert wird. Aus diesen Gründen wird die Cybersecurity Culture in der Folge als Medium betrachtet sowie als Reibungspunkt, an dem die Dichotomien des Added Values-Ansatzes aufeinander stoßen.

Was also ist Cybersecurity Culture? Wie sich gezeigt hat, ist IT-Sicherheitskultur kein spekulatives Konstrukt, sondern ein feststellbares Phänomen, das die technologisierte Gesellschaft von heute vollständig durchdringt. Auf den letzten Seiten konnte nachgezeichnet werden, dass Kultur und Imaginaries per se flüchtig sind, da sie nur im Moment der Inszenierung sichtbar sein können und nachfolgend nur widerhallen. Zugleich stellte sich heraus, dass Kultur – in diesem Fall IT-Sicherheitskultur – Standards und Denkweisen institutionalisieren kann, indem sie Ideen der Wirklichkeiten konsolidiert, also in bleibende Strukturen überführt. Solche Institutionen aller Art transformieren dann parallel mit der weiter emergierenden Kultur oder härten aus, um

schließlich gar jenseits eines kulturellen Konsenses zu stehen. Gleichzeitig zeigen die vielen Gesetzgebungsverfahren beider Länder in den vergangenen Jahren, dass man versucht, mit hoher Geschwindigkeit auf die hochdynamischen Techniksysteme zu reagieren, die für ihre (kulturellen) Umweltsysteme stets wirksam sind.

National technopolitical identities are therefore neither stable nor monolithic. Rather, they have to be seen as developing out of a complex blend of intertwined histories, as being in a continuous process of reenactment and in need of nourishment and caring (Felt 2015, 120).

Dieses Tun ist dort abzulesen, wo es sich verstetigt und reproduziert, nämlich in Institutionen, einvernehmlichen Regeln oder Texten und anschließend Hinweise auf die zugrundeliegende Kultur liefern.

Das bedeutet ebenfalls, dass die IT-Sicherheitskultur stets von den Menschen eines Landes oder einer Gesellschaft gebildet und geformt wird, die wiederum auf interne wie auch externe Wirkkräfte reagieren. Und so sind es auch diese Menschen, die Gesetze gegen Cyberkriminalität beschließen, die Standards für sichere Onlinezugänge einführen oder die neue Behörden zum Aufbau einer robusten Digitalinfrastruktur begründen – oder nun einmal nicht.

Die Wertvorstellungen in Bezug auf schützenswerte IT-Güter und IT-Sicherheitsmaßnahmen sind in den unterschiedlichen Staaten verschieden und schlagen sich in den nationalen Gesetzen und Normen nieder. Sie geben somit auch Aufschluss über die nationale IT-Sicherheitskultur eines Landes (Pohlmann 2016, 39).

Eine Untersuchung der existierenden, menschengemachten Strukturen zur Herstellung von IT-Sicherheit sowohl staatlichen als auch gesellschaftlichen Ursprungs ermöglicht es dann, Rückschlüsse auf die IT-Sicherheitskultur ziehen. Folgerichtig sollten sich ungleiche Kulturen in unterschiedlichen Zielsetzungen, Gesetzen oder Organisationsprinzipien niederschlagen. An dieser Stelle lohnt es, sich eine Hypothese dieser Arbeit in Erinnerung zu rufen: Die eng verwandten Kulturräume Deutschland und Niederlande weisen trotz all ihrer Gemeinsamkeiten wesentliche Unterschiede in den Ausprägungen ihrer Cybersicherheitskulturen auf.

Damit sich diese Annahme aber letztgültig als korrekt erweisen kann, müssen im Folgenden strukturell verschiedene Phänotypen der IT-Sicherheit nachgewiesen sein, die sich nicht auf Zufälle oder einzelne Abweichungen stützen, sondern sich stattdessen auf substanzielle, kulturelle Divergenzen zurückführen lassen. Denn eines zeigen die

Beschreibungen von IT-Sicherheitskultur wie von Imaginaries gleichermaßen: Beide Ebenen, die abstrakte Kultur und das konkrete Imaginary, vollziehen sich im Tun. Daher ist das formulierte theoretische Fundament der Unterbau für einen Vergleich der niederländischen mit der deutschen Cybersicherheitskultur.

2 Wie organisieren die Vergleichsländer IT-Sicherheit?

2.1 Querschnitt: Deutschland zwischen 1945 und 2022

Bei der Betrachtung der historischen Disposition Deutschlands und der Niederlande sowie den daraus abzuleitenden Handlungen zeigt sich eine Dichotomie. Einerseits steht das aus Tradition und Historie erwachsene Kultur- und Interaktionsverhalten innerhalb beider Nationen, das den Mittelpunkt der Untersuchung bildet. Die Menschen dieser Gruppen werden demnach durch die Handlungen ihrer eigenen Vergangenheit wie auch ihrer kollektiven Prägung determiniert. Gleichzeitig unterliegt der Lesende, der Betrachtende, der Forschende genauso seiner auf Erlebnissen und Gelerntem basierenden Vorurteile. Wobei Vorurteil hier nicht negativ konnotiert zu verstehen ist, sondern vielmehr als wertfreie, a priori gefällte Beurteilung, die abermals aus Vergangenheitserzählungen gespeist ist. Entsprechend karambolieren auch die in der Vergangenheit ruhenden kollektiv-kulturellen Eigenarten der Forschungsobjekte mit den subjektiven, individuellen Erfahrungen des Betrachters zu einem genuinen Mosaik. Die Herausforderung besteht nun offenkundig darin, trotz allem eine axiomatische Plausibilität zwischen Historie und Präsens herzustellen und jegliche Eingenommenheit weitestmöglich außen vorzulassen. Die deutsche Vergangenheit seit 1945 ist eine Geschichte von Verdrängung und Aufarbeitung, aber auch von neuer Verantwortung, wiederkehrendem Wohlstand und von rasanter Technologisierung. Für diese Arbeit ist insbesondere diese jüngere deutsche Historie bedeutsam, da die Umwälzungen der Periode nach dem Krieg bis heute nachhallen und das kollektive Selbstverständnis der Deutschen nachhaltig beeinflussen. In dieser Phase vollzieht obendrein die gesamte Nordhemisphäre einen epochalen Wandel vom Industrie- zum Informationszeitalter, der im Grunde noch heute beobachtet werden kann.

Um aber die untenstehenden kulturellen und politischen Entwicklungen zwischen 1945 und heute verorten zu können, ist ein knapper Exkurs in den Nationalsozialismus, also vor 1945, unumgänglich. Der Aufstieg der Nationalsozialisten besiegelte zugleich das Ende der nie völlig konsolidierten Weimarer Republik und läutete 1933 mit der Ernennung Adolf Hitlers zum Reichskanzler eine 12 Jahre währende Zeit des Terrors, der Unmenschlichkeit und des Krieges ein. Im Gegensatz zu den Wirren um 1914 ist der Kriegsbeginn 1939 eine unbestreitbar deutsche Schuld. Vor allem in den Kriegsjahren hat das Dritte Reich durch heimtückische Kriegserklärungen, Holocaust und

unvergleichliche Gewalt gegen Fremde sowie gegen die eigene Bevölkerung Verbrechen gegen die Menschlichkeit in bis dahin nie dagewesenem Ausmaß begangen. Im Unterschied zum ideologisch geführten Feldzug 25 Jahre zuvor, ging Deutschland dieses Mal auch gegen nahezu wehrlose Nationen wie Norwegen oder eben die Niederlande militärisch, repressiv wie auch antisemitisch-genozidal vor (vgl. Lademacher 1993, 580ff). Damit waren die Beziehungen zu den bis dato weitestgehend neutralen Niederlanden irreparabel beschädigt (vgl. Wielenga 2004). Am Ende des vom nationalsozialistischen Deutschland losgetretenen Völkermordens sind mehr als 60 Millionen Menschen weltweit tot und 6 Millionen Juden in Vernichtungslagern ermordet (vgl. Bundeszentrale für politische Bildung 2021). Die Erfahrungen der Deutschen und ganz besonders ihrer Nachbarn in Europa und auf der Welt haben das Bild Deutschlands für Jahrzehnte erschüttert. Spätestens seit 1945 bedingt dies maßgeblich die Identität der Menschen in Deutschland.

In den Jahren bis 1949 sortierten sich die Bundesländer innerhalb der unterschiedlichen, alliierten Besatzungszonen neu und gaben sich im Zuge dessen erste Landesverfassungen (vgl. Kleinert 2019, 17). Der anschwellende Dissens zwischen den Westalliierten und der Sowjetunion fand seinen vorläufigen Höhepunkt in der Währungsreform 1948, mit der die D-Mark eingeführt wurde und sich zeitgleich zwei separate Wirtschaftszonen etablierten, die sich im Folgejahr in zwei Staaten manifestierten (vgl. Kleinert 2019, 40ff). Mit dieser Teilung ging auch eine ideologische Reorientierung der jungen Bundesrepublik, eine „Anpassung an westliche Ordnungssysteme“, einher, mit der das kulturelle, moralische und ökonomische Leitbild für Westdeutschland schon in dieser Frühphase determiniert war (vgl. Schulz 2005, 98). Die 50er-Jahre zeichneten sich durch den Wiederaufbau und die Wiederbelebung der Wirtschaft aus. Die Bonner Republik stabilisierte sich innenpolitisch, indes wurde im Privaten der Rückzug in einen „kulturellen Konservatismus“ vollzogen, „der neben vielen Elementen von Kontinuität auch biedermeierliche Züge trug“ (Kleinert 2019, X). Während die Deutschen selbst sich also ins eigene Heim zurückzogen und ihre Kriegsvergangenheit zu verdrängen versuchten, erkannten ihre ehemaligen Feinde der westlichen Welt mehr und mehr an, dass die Bundesrepublik ein souveräner, demokratischer Staat war. So wurde Deutschland 1957 sogar zu einem der Gründungsmitglieder der Europäischen Wirtschaftsgemeinschaft (EWG) und sah sein ökonomisches Gewicht anerkannt.

Es zeigte sich bald, dass Deutschlands Entwicklung weiterhin vom Verlauf bewaffneter Konflikte abhing. So war der Korea-Krieg eine von vielen Krisen, die in den Folgejahren bevorstanden. Die Stellvertreterauseinandersetzung in Asien ist rückblickend einer der Gründe für die frühzeitig einsetzende Wiederbewaffnung Deutschlands (vgl. Mai 1977, 173). Kurze Zeit später entflammte zusätzlich der Vietnam-Krieg, ein weiterer Ost-West-Konflikt, der in einem Drittstaat ausgetragen wurde. In Deutschland führten diese rücksichtslosen Großmachtdemonstrationen der USA und der Sowjetunion vor allem zu einer Politisierung von Gesellschaft, Kunst und Kultur. Der offen zutage getretene Rassismus gegen Afroamerikaner trug zusätzlich dazu bei, die Vereinigten Staaten als Leitkultur in Zweifel zu ziehen (vgl. Klimke 2010, 25). Das Image der USA als Befreier und Friedensstifter, damit auch als wegweisender Archetyp, begann zu bröckeln. Die Demonstrationsbewegungen der 68er gegen das Vorgehen der USA zog in Deutschland obendrein einen Widerstand gegen das sogenannte Establishment nach sich. Im berühmten Protestruf „Unter den Talaren der Muff von tausend Jahren“ konzentrierte sich der Konflikt zwischen der konservativen, teils alt-nationalsozialistischen Elite und einer jungen, antiautoritären Studentenschaft (Kleinert 2019, 221). Nachdem 1961 eine physische Mauer mitten durch Deutschland errichtet worden war, um Ost und West zu trennen, zog sich zum Ende des Jahrzehnts ein Graben zwischen politischer Rechte und politischer Linke, respektive zwischen Restauratoren und Revisionisten. Zu dieser Zeit sind Nachrichten über die atomare Aufrüstung beider Blöcke regelmäßig zu lesen und das allgegenwärtige Eskalationspotenzial des Konflikts ist ein ständiger Begleiter. Auch die deutsche Außenpolitik war auf nukleare Abschreckung ausgerichtet und die Bundesrepublik, wenngleich sie nicht über eigene Sprengköpfe verfügte, wurde zum Lager amerikanischer Atomwaffen. Als Transitstaat zwischen Ost und West wäre das Land erster Austragungsort und damit existenziell von der atomaren Bedrohung betroffen gewesen. Die vorläufige Zuspitzung des Kalten Krieges in der Kubakrise, im Vietnam-Krieg und später im Jom-Kippur-Krieg induzierte in Deutschland die Angst vor neuerlichen Weltkriegsszenarien.

Trotz allem setzte mit dem *Wandel durch Annäherung* zum Ende der 60er-Jahre eine Verständigungspolitik zwischen Ost- und Westdeutschland ein, die unter anderem das Reisen nach Ostdeutschland ermöglichte, ständige Vertretungen einrichtete und die DDR partiell auf der Grundlage des Völkerrechts anerkannte (vgl. Kleinert 2019, 286f).

Wenngleich der Grundlagenvertrag auf eine Näherung beider deutscher Staaten hindeutete, zementierte er für viele Zeitgenossen die Trennung Deutschlands. Obwohl beide deutschen Nationen noch von einer Vielzahl von Krisen bewegt wurden, darunter der RAF-Terrorismus, der Streit um die atomare Aufrüstung der BRD oder der NATO-Doppelbeschluss, zeichnete sich doch im Laufe der Jahre ab, dass ideologische Abgründe abnehmen könnten. Währenddessen behielt die Sowjetunion ihre politische und kulturelle Einbahnstraße noch bei; in der Bundesrepublik änderte sich das Lebensgefühl dagegen: Die anhaltende atomare Gefahr, die Ölkrise oder aber die schwindende Bedeutung der klassischen Kernfamilie für die individuelle Entfaltung weckten Unsicherheiten und beendeten die Illusion eines auf Jahrzehnte planbaren Lebensverlaufs (vgl. Kleinert 2019, 416ff). Hinzu kommt die innerdeutsche Zerrissenheit, die sich nicht nur mitten durch das Land zog, sondern ebenso durch zahllose Ortschaften, Familien oder Freundschaften. Indem beide Staaten ideologisch weiter auseinanderdrifteten, war die Konfliktgefahr nicht nur von sowjetischer oder amerikanischer Seite spürbar, sondern auch andere Deutsche wurden zum Feindbild und womöglichen Aggressor. Zudem wurde Westdeutschland mit dem Wirtschaftswunder neuerlich zu einem bedeutenden Technologie- und Industriestandort – konnte sich also ökonomisch zunehmend vom Weltkrieg entfernen, während sich die DDR in anhaltender Rezession befand und vielerorts nie die Kriegsschäden beseitigen konnte. Unter anderem in diesem Aufschwung lag die westdeutsche Überheblichkeit begründet, die sich nach dem Durchsetzen des kapitalistischen Systems mit der späteren Wiedervereinigung der deutschen Staaten vollends manifestierte.

Die DDR litt in den 70er- und 80er-Jahren zunehmend unter den Limitierungen der Planwirtschaft und insbesondere unter den Einschränkungen ideologischer Überzeugungen. Mit dem Aufstieg Honeckers setzten vereinzelte Zugeständnisse an die Bevölkerung ein, die Konsum, Medienrezeption und Importe aus dem Westen weniger stark beschnitten (vgl. Kleinert 2019, 305f). Die ökonomische Trendwende war damit aber nicht zu erreichen, sodass die DDR Anfang der 80er Jahre sogar hohe Kredite der Bundesrepublik annehmen musste, um den Haushalt stützen zu können. Gleichzeitig kam es zu Spannungen zwischen der UdSSR und der DDR-Administration, während viele Menschen in Ostdeutschland verstärkt Fluchtversuche unternahmen. Als schließlich die Macht der Sowjetunion nachließ, die Deutsche Demokratische Republik vor der Insolvenz stand und zudem die Grenze zu Ungarn nahezu ungehindert

überwunden werden konnte, war der Weg frei für den Fall der Mauer (vgl. Ritter 2009, 299f). Wenige Monate später schon erfolgte das alternativlose Angebot der Bundesrepublik, mit der DDR eine Währungsunion zu bilden (vgl. Ritter 2009, 304). Mit der Währungsreform 1990 stand die Tür zur Wiedervereinigung ein gutes Stück weiter offen. Der Vollzug am 03. Oktober 1990 war in gewisser Weise aber eine Einverleibung der DDR durch die Bundesrepublik. Ab diesem Punkt bestimmte der politische Sieger des Ideologiestreits über die Integration des Verlierers in das vermeintlich überlegene System. So gründete die BRD etwa die sogenannte Treuhand, um die volkseigenen Betriebe zu zerschlagen, zu privatisieren oder auf eine rentablere Grundlage zu stellen. Die Menschen in den damals neuen Bundesländern sahen sich plötzlich der rücksichtslosen Profitorientierung und der Ungewissheit des freien Marktes ausgesetzt; man verlangte ihnen erneut die eilige Anpassung an ein fremdes politisches System ab. Sicherheitspolitisch bedeuteten diese radikalen Umbrüche, dass die Menschen, vor allem im Osten Deutschlands, ihren wirtschaftlichen, kulturellen und sozialen Halt verloren. Indem die Sowjetunion zerfiel, war zugleich ihre über Jahrzehnte gepflegte kommunistische Doktrin passé. Die Menschen sollten sich wiederholt in eine Gesellschaft einfügen, die sich als überlegen verstand. Obwohl die reale Kriegsgefahr durch die Vereinigung zweier ideologischer Konfliktparteien abnahm, waren vor allem Ungewissheit, Klassismus und spürbare kollektive Vorbehalte Risiken für die öffentliche Sicherheit in Deutschland. Politische Eliten, Ökonomie und Weltanschauung konnten nicht länger apodiktisch vorgehen; diese Erkenntnis galt für den Osten wie für den Westen. Während vor allem die Menschen der ehemaligen DDR mit allerlei Umstellungen zu kämpfen hatten, zerbrach für die NATO und die BRD zusehends die ideologische Binarität (vgl. Kleinert 2020, 186). Mit dem Ende der Sowjetunion war anstelle von Konfrontation plötzlich Integration gefragt. Gerhard Ritter hebt die Leistungen dieser Zeit deshalb hervor, statt die Unzulänglichkeiten zu betonen, wenn er postuliert, dass „die friedliche Revolution, die eine Diktatur in eine Demokratie verwandelte und Millionen Menschen Freiheit und mehr Wohlstand gab, eine der Sternstunden der an solchen leider nicht gerade reichen deutschen Geschichte“ ist (Ritter 2009, 338).

Die Jahre rund um die Jahrtausendwende waren erneut von tiefgreifenden Veränderungen wirtschaftlicher wie auch sozialer Art gekennzeichnet. Im Kosovo-Konflikt entsendete Deutschland 1998 erstmalig seit dem Zweiten Weltkrieg Soldaten in

einen Kampfeinsatz. Auf die pogromartigen Angriffe auf ein Wohnheim für vietnamesische Gastarbeiter in Rostock-Lichtenhagen Anfang der 90er-Jahre folgte am Ende des Jahrzehnts der sogenannte Nationalsozialistische Untergrund. Mit drei Sprengstoffanschlägen und zehn Morden terrorisierte die Gruppe Menschen mit Migrationshintergrund in ganz Deutschland, indem sie existenzielle Ängste schürte. Gleichzeitig war der NSU der unübersehbare Beweis, dass rechtsradikales Gedankengut in Deutschland weiter auf Nährboden stieß und nicht marginalisiert werden konnte. Nahezu gleichzeitig schlugen in New York Flugzeuge in das World Trade Center ein und erodierte die bestehende Weltordnung. An diesem Punkt setzte eine Diffusion von Gefahr ein: Das über Jahrzehnte gepflegte Feindbild des Kommunisten hatte sich aufgelöst und an diese Stelle traten nun Narrative über Bedrohungen aus dem In- und Ausland, die plötzlich hervorstießen, deren Motivlage eingangs zumeist uneindeutig war und die nicht staatlich organisiert oder diplomatisch interessiert waren. Ebenfalls zu dieser Zeit kamen erstmals in der Breite Berichte über Malware auf, da Loveletter, Code Red, Slammer oder Sobig.F auf spektakuläre und teils kreative Weise je Schäden in Höhe mehrerer Milliarden Dollar anrichteten. Die nebulöse Bedrohungslage und das Gefühl, jederzeit und auf jegliche Art angreifbar zu sein, wurde auch durch die aufkommenden IT-Bedrohungen weiter verstärkt, die damals weder greifbar noch abwehrbar waren.

Weitere Verunsicherung erlebten im Besonderen die Ostdeutschen, die mit dem Euro die sechste Währung innerhalb eines Jahrhunderts und die dritte innerhalb von nur etwas mehr als einem Jahrzehnt erfuhren. Die ‚Agenda 2010‘ und die umstrittenen Hartz-Gesetze trugen ihren Teil zur fortschreitenden Ungleichheit zwischen Arm und Reich bei, während Internet und Mobilkommunikation parallel neue Räume zur Individualisierung und Beschleunigung öffneten (vgl. Fehr/Vobruba 2011, 216). Erste Gerüchte einer Industrie 4.0 tauchten auf, in der besonders geringqualifizierte Berufe einem hohen Automatisierungsrisiko ausgesetzt sein sollten. Parallel jedoch war der Breitbandausbau in der Phase zwischen 2005 und 2015 ein kaum prosperierendes Infrastrukturprojekt (vgl. oecd.org 2019). In dieser Zeit der Weichenstellung agierte Deutschland zögerlicher als viele andere Länder und verpasste so die Gelegenheit, sich frühzeitig als digitaler Technologie-Leader, wie in der Automobil-, Maschinenbau- oder Chemieindustrie, zu positionieren. Damit liegt die Rolle des digitalen

Technologietreibers mittlerweile bei anderen Nationen wie den USA, Israel, China oder Japan.

Trotz seiner außenpolitisch führenden Funktion innerhalb der Europäischen Union bei der Bewältigung der Finanzkrise, der wirtschaftlichen Stabilisierung Griechenlands oder aber auch bei den Verhandlungen mit der Türkei über die Sicherung der EU-Außengrenzen nach 2015, blieb das deutsche Engagement auf dem interkontinentalen Parkett häufig hinter den Erwartungen der Bündnispartner zurück. So stellt Hubert Kleinert fest, „[ö]konomisch sei das Land ein Riese, politisch aber ein Zwerg“ (Kleinert 2020, 672). Als freiheitlich-soziale Demokratie nach dem Dritten Reich sah man sich über viele Jahre der außergewöhnlichen Situation gegenüber, besetzt, geteilt und schuldbehaftet inmitten von Nachbarn zu leben, über die man zuvor Terror und Not gebracht hatte, indem man sie überfallen, ebenfalls besetzt und gewaltsam ausgebeutet hatte. Aus dieser prägenden Schuld erwuchs, statt einer wuchernden Verbitterung über das Kriegsende wie nach 1918, dieses Mal eine Kollektivverantwortung zu europäischem Engagement (vgl. Deutsche Welle 2019). Die später wiedervereinte Republik präsentierte sich sogar als Sinnbild „eines supranational gedachten europäischen Einigungsprozesses“ (Kleinert 2020, 669). Zugleich ruhte auf dieser Verantwortung, dass sich Deutschland in militärischen Angelegenheiten zumeist zurückhielt und sicherheitspolitische Belange dagegen mithilfe des über Jahrzehnte gewachsenen, diplomatischen Gewichts aufzulösen versuchte. Die erfolgreiche Flucht nach vorn durch eine glaubhafte Rehabilitation impliziert bis heute eine gewisse gesellschaftliche Sensibilität gegenüber jeder Gestalt aufkeimenden Nationalismus. Insofern stiftete diese Patriotismusnegierung eine neue Form der nationalen Identität und stellte sich als „ein positiv besetzter Teil des Deutschland-Fremdbildes bzw. des deutschen Images“ heraus (Grabbe 2014, 225).

Aufgrund dieser Komposition bundesdeutscher Beschaffenheiten ist es schwierig, die eine greifbare, deutsche Kultur festzustellen. Deutschland ist als Ergebnis seiner Historie ein Land der Gegensätze zwischen Tradition und kultureller Vielfalt, zwischen sparsamer Sachlichkeit und wirtschaftlicher Tatkraft, zwischen Erneuerung und Trägheit. Somit ist es wohl ebendiese Disparität, die – wenn man so will – typisch deutsch zu sein scheint.

2.2 Deutschland heute

Auf den vorausgegangenen Seiten zeigt sich, dass die Bundesrepublik in ihrem gegenwärtigen Charakter das Ergebnis eines Jahrhunderts der Kriege, der Besatzung, des Genozids, der Teilung, aber dennoch auch Resultat eines Säkulum des Fortschritts, der Europäisierung, der Solidarität und der Annäherung ist. Das Land sah sich in der Vergangenheit mehrmals radikaler Umbrüche gegenüber, die immer wieder Adaption verlangten und ist dennoch weiter auf der Suche nach seiner Rolle im internationalen Staatengefüge. Obwohl der für die Bundesrepublik fundamentale Föderalismus regelmäßig unter Kritik steht, bleibt das Subsidiaritätsprinzip und die Souveränität der Bundesländer über schwerste Krisen hinweg als unverrückbares, charakteristisches Organisationsprinzip deutscher Staatlichkeit und Bürokratie erhalten.

Dabei steht Deutschland vor einer Vielzahl von Schwierigkeiten, während diese Zeilen geschrieben werden. Angesichts des vorherigen Kapitels mag diese Erkenntnis wie ein Déjà-vu erscheinen. Einige der Herausforderungen der Gegenwart teilt sich Deutschland mit seinen Nachbarn wie den Niederlanden: Der erhebliche Migrationsdruck, der europaweite Aufstieg politischer Extreme von innen und außen oder die vierte industrielle Revolution sind nur eine kleine Auslese der Schwierigkeiten, denen sich Deutschland und die Niederlande gleichermaßen gegenübersehen. Nicht wenige Unwägbarkeiten aber, die teils auch in der eben beschriebenen Historie begründet liegen, betreffen singulär Deutschland. So ist es wie kein anderes Land mit der europäischen Idee mehr noch Verpflichtung verwachsen und auf ihr Gelingen angewiesen. Überdies hat sich die deutsche Exportwirtschaft in ein ökonomisches Abhängigkeitsverhältnis mit China und den USA begeben, das mit Blick auf diplomatische Verwicklungen zu Interessenkonflikten führen kann. Die gegenwärtige Energiewende ohne Atomstrom sowie der nicht von der Hand zu weisende Digitalisierungstau tun ihr übriges, um zu unterstreichen, dass Deutschland zwischen Verstetigung und Fortschritt verharrt.

Selbstverständlich definiert sich die Bundesrepublik nicht nur anhand ihrer Schwierigkeiten. Sie ist etwa die größte Volkswirtschaft der EU, ein renommierter Wissenschaftsstandort und erfährt allgemeine Anerkennung für ihr starkes Sozialsystem. Deutschland gilt als ein Land, das humanistische Maxime anlegt und sich selbst als ethisch-moralische Instanz begreift (vgl. Burri 2015, 247). Regelmäßig betritt die

Bundesrepublik das internationale Parkett, indem sie eine Vermittlerfunktion einnimmt, beispielsweise zwischen Russland und den westlichen Staaten oder mit der Berliner Konferenz im libyschen Bürgerkrieg. Der Wunsch nach globaler Verantwortung und nach einem Platz zwischen Großmächten wie China oder den USA ist erkennbar. Während Deutschland nach außen also auf der Suche nach seiner Rolle zu sein scheint, tritt es innenpolitisch gefestigt auf. Deutschland ist seit Jahrzehnten ein Einwanderungsland, ursprünglich begründet in ökonomischem Kalkül, mittlerweile verstärkt durch weltweite Krisen oder den demografischen Wandel. Daraus leiten sich, häufig aus (rechts-)konservativen Lagern, Debatten über Migrationspolitik, Leitkultur und Identität ab (vgl. Deutschlandfunk Kultur 2017). Vielmehr noch aber haben die letzten Dekaden gezeigt, dass die Zuwanderung vielzählige Bereiche des Alltags, darunter Musik, Kulinarik oder Kunst diverser und vielschichtiger werden ließ. Die politische Landschaft hat dennoch – wie in nahezu allen anderen europäischen Staaten – eine Radikalisierung und ein Erstarken nationalistischer Kräfte vollzogen. Gleichzeitig lahmen etablierte Parteien wie die CDU, die über 16 Jahre die Kanzlerin stellte und eine Große Koalition mit der SPD anführte. Die kleineren Parteien der Mitte konnten zuletzt davon profitieren und werden von vielen Wählern als taugliche Alternative zu den Volksparteien wahrgenommen. Trotz des Nachlassens bisheriger Parteien schaffen es Rechte wie die AfD nicht, ähnlichen Rückenwind zu erhalten, wie es in Frankreich, den Niederlanden oder Polen zu beobachten war und ist. Die Historie und die anhaltende Aufarbeitung der nationalsozialistischen Vergangenheit, das föderalistische System und nicht zuletzt womöglich der Terror von rechts unterbinden immense Zugewinne. Attentate auf Walter Lübcke, auf eine Synagoge in Halle, auf neun Menschen in Hanau oder die Anschlagsserie des NSU haben aufgezeigt, dass der Terrorismus weniger ein außen- als ein innenpolitisches Phänomen extremistischer Täter ist.

Aber nicht nur die Politik befindet sich in einem Wandlungsprozess, sondern ganze Regionen Deutschlands durchlaufen augenblicklich tiefgreifende Umbrüche. Die Kohlereviere und alten Industrielandschaften in Rheinland und Ruhrgebiet, einige Teile der ostdeutschen Bundesländer und rurale Gegenden mit starker Abwanderung in die Städte sehen sich einem schwachen Arbeitsmarkt und einer alternden Infrastruktur gegenüber. Während 1980 noch mehr als 41 % der Erwerbstätigen der Bundesrepublik im sekundären, also produzierenden Sektor, beschäftigt waren, waren es 2020 lediglich noch 24 % (vgl. Destatis 2021c). Damit besitzt Deutschland im Vergleich zu vielen

anderen Wohlstandsstaaten immer noch eine gewichtige Industrie, hat aber in den vergangenen vier Jahrzehnten eine ökonomische Umstrukturierung erlebt, wie es sie zuletzt im 19. Jahrhundert zur Zeit der industriellen Revolution gab. Nach wie vor nehmen alternde Branche wie der Automobil- oder Stahlbau für die Wirtschaft und das Image Deutschlands eine große Bedeutung; ihre Wandlung in einen digitalen und klimaneutralen Sektor ist jedoch schwerfälliger als in nicht produzierenden Gewerken.

Bei der Lösung von Problemen dieser Größenordnung verließen sich die Deutschen in den vergangenen zwei Jahrhunderten vor allem darauf, dass die Wissenschaft Antworten findet (vgl. Burri 2015, 236). In Marken und Bildern wie *Made in Germany* verdichtet sich der Blick anderer Länder auf deutsche Erzeugnisse und Ideen. Ohne Prüfung gelten Produkte, die mit solchen Floskeln versehen sind als hochwertig. Dabei beruht diese Annahme lediglich auf Erfahrungen der Vergangenheit. Diese Draufsicht aber bestimmt zugleich das deutsche Selbstbild. Im Bundestagswahlkampf 2021 beispielsweise wurde wiederholt von den Deutschen als ein Volk der Tüftler und Denker gesprochen (vgl. Redaktionsnetzwerk Deutschland 2021). Und dabei entspricht dieses deutsche Eigenporträt teils der Realität: Die bedeutsamsten Fortschritte in der Erstellung eines mRNA-Impfstoffes gegen COVID-19 kamen aus Mainz und der Chemie-Nobelpreis 2021 ging unter anderem an einen Deutschen. Dagegen stammen Hochtechnologie-Innovationen häufig aus anderen Ländern. So belegt der Global Innovation Index (GII) der WIPO, dass Deutschland lediglich Platz 10 erreicht und in einzelnen Kategorien gar deutlicher zurückliegt. Die vorderen Plätze gehören der Schweiz, Schweden und den Vereinigten Staaten; auch die Niederlande liegen insgesamt vor Deutschland (vgl. Weltorganisation für geistiges Eigentum 2021, 22/30). Es zeichnet sich „neben einer generellen Risikoscheu, auch eine gehörige Portion Skepsis gegenüber neuer Technik – ausgerechnet in einem Land, das für seine technologischen Standards legendär ist“ – ab (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 2018, 4).

2.2.1 Staatsprinzip: Föderale Republik

Für alle nachfolgenden Entitäten, die in Deutschland im Rahmen einer demokratisch-staatlichen Ordnung handeln und bemächtigt sind, Aufgaben öffentlicher Verwaltung wahrzunehmen oder gar freiheitliche Rechte zu beschneiden, gilt, dass sie gesetzlichen Rahmungen unterliegen – damit auch das BSI und alle weiteren Sicherheitsbehörden (vgl. Bundesregierung 2019, 69). Der sogenannte *Vorbehalt des Gesetzes* besagt, dass

Institutionen öffentlichen Rechts eine gesetzliche Legitimierung benötigen, um gewisse Tätigkeiten durchführen zu können. Fehlt einer Behörde die juristische Grundlage für eine Handlung, so darf diese nicht ausgeführt werden. Es ist etwa der Polizei unter definierten Gegebenheiten erlaubt, den Straßenverkehr zu regulieren, dem Bundesamt für Strahlenschutz steht die gleiche Maßnahme jedoch nicht zu. Konsensuelle Standards, also parlamentarisch beschlossene Gesetze, bestimmen exekutive Instanzen, die realiter evident und kohärent Abwägungen vorzunehmen haben (vgl. Rieckhoff 2007, 24).

Dieser Vorbehalt des Gesetzes gilt damit auch für alle staatlichen Einrichtungen, die sich mit der IT-Sicherheit in Deutschland befassen und zieht sich über die Organe des Bundes hinunter bis zu den kleinsten kommunalen Institutionen. Dieses fundamentale Dogma mündet darin, dass die Legitimität exekutiver Handlungen zugewiesen sein muss, bevor die jeweilige Aktion ausgeführt werden kann. Die Gesamtheit nationaler Gewalt verteilt sich infolgedessen auf diverse Einheiten des Staatswesens. Bestenfalls führt diese Regelung dazu, dass öffentliche, kompetente Anlaufstellen entstehen, die dann mit den notwendigen Befugnissen ausgestattet werden. So wird sichergestellt, dass verliehene Macht begrenzt ist und stets auf dem Prüfstand steht. „Der Gesetzesvorbehalt grenzt lediglich die Kompetenzsphären ab zwischen dem demokratisch unmittelbar gewählten Parlament und der regelmäßig nur mittelbar demokratisch legitimierten Exekutive“ (Rieckhoff 2007, 22).

Die obige Erklärung sei eingangs dieses Kapitels gestattet, um die Zielsetzung zu verdeutlichen, denn der Vorbehalt des Gesetzes sowie die darin festgeschriebene Allgemeingültigkeit von Grundrechten nimmt maßgeblich Einfluss auf den Föderalismus und umgekehrt. So sind gesetzgebende und gesetzessvollziehende Organe auf die legitimierende und ebenso machtbegrenzende Funktion des Gesetzes angewiesen, um die Durchlässigkeit föderaler Vertikalmechanismen zu gewährleisten (vgl. Rieckhoff 2007, 38). Zugleich müssen die Akteure in stets voranschreitenden Gesellschaften fortlaufend sicherstellen, dass Grundrechte und Gesetze auf allen erdenklichen Ebenen modernisiert und umgesetzt werden – selbstverständlich auch bei Fragen und Herausforderungen der Cybersicherheit. Daher legen die folgenden Absätze dar, wie Deutschland unter den Gegebenheiten von Föderalismus und Gesetzesvorbehalt versucht, ein tragfähiges Gerüst der Informationssicherheit herzustellen.

Mit Blick auf die gesamtstaatlich, administrative Organisation der Bundesrepublik enttarnt sich der grundlegende Unterschied der deutschen Interpretation von Demokratie im Vergleich zu vielen anderen Staaten Europas: Der Föderalismus, dessen Ordnung teils noch auf den oben beschriebenen Beschlüssen von 1815 fußt. Deutschland baut aus historisch gewachsenen Ursachen auf das sogenannte Subsidiaritätsprinzip, also der Bemächtigung möglichst kleiner Einheiten, um lokale Problemstellungen sachgerecht und regional zu behandeln. Daraus folgt, dass etwa überschaubare Entitäten wie Kommunen ihre Belange weitestgehend souverän verwalten können. Erst bei Angelegenheiten, die über die Kommune hinaus Wirksamkeit haben oder welche die Gemeinde selbst nicht bewältigen kann, greift das Bundesland ein. Für dieses Land gilt dann das identische Prinzip: Alle Themen, die nur auf das jeweilige Land wirken, werden ohne Zustimmung der nächsthöheren Gewalt betreut. So ordnen sich unter anderem die Polizeien oder die Kultusministerien auf Länderebene ein. Übergeordnete Probleme werden dann im Bundesrat vorgebracht oder bei eindeutiger Zuständigkeit direkt vom Bund bearbeitet.

Holger Kastler vereinfacht das Prinzip und bricht es auf ein für den vorliegenden Zweck verständliches, wenn auch idealisiertes Maß herunter: Er illustriert die

Föderation als eine Union von Gruppen (Staaten, Organisationen und Menschen), die von einem oder mehreren gemeinsamen Zielen, welche ihre Wurzel in gemeinsamen Werten, Interessen oder Überzeugungen finden, vereint werden, gleichzeitig aber ihre eigene [sic!] Gruppencharakter für andere Zwecke bewahren. Eine solche Föderation vereinigt, ohne zu zerstören und bestärkt die sich vereinigenden Gruppen, die gleichzeitig wesentlichen Einfluss auf das föderale System haben (Kastler 2015, 81).

Dieser Hoffnung folgte wohl auch der Parlamentarische Rat 1948/49, denn im Grundgesetz findet sich der Föderalismus als fundamentales Organisationsprinzip der BRD: „Die Bundesrepublik Deutschland ist ein demokratischer und sozialer Bundesstaat“ -Art. 20 Abs. 1 GG (Bundesregierung 2019, 73). Artikel 31 schreibt den Vorrang des Bundesrechts fest, Artikel 51 reglementiert die Zusammenstellung des Bundestages und die Artikel 83 bis 91 bestimmen über die Ausführung der Bundesgesetze und die Bundesverwaltung. Das Beziehungsgeflecht zwischen dem Bund und seinen untrennbar verwobenen Bundesländern zieht sich durch das gesamte Grundgesetz. Rechte und Pflichten, Autonomien und Heteronomien sind dort festgehalten und tangieren alle Belange von Politik, Verwaltung oder Rechtsprechung in Deutschland.

So geht Artikel 23 des Grundgesetzes zwar im Wesentlichen auf das Verhältnis der Bundesrepublik zu Europäischen Union ein, veranschaulicht aber damit das für Deutschland und seinen Föderalismus signifikante Subsidiaritätsprinzip. So ist dort festgehalten, dass zum Beispiel in Dingen der Kultur, der Bildung oder des öffentlichen Rundfunks das Urteil der Länder, ergo nicht des Bundes, maßgeblich ist (vgl. Bundesregierung 2019, 76). Genauer steckt hinter der Subsidiarität, dass immer die möglichst kleinste entscheidungsbefugte Ebene einen Sachverhalt reguliert. Erst wenn Kompetenzen oder Handlungsmöglichkeiten dieser Stufe erschöpft sind, kann die nächsthöhere Einheit legitimiert agieren (vgl. Bundeszentrale für politische Bildung 2020). Das bedeutet, die jeweils höhere Ebene verfügt über limitierte Befugnisse, wohingegen sich die konkrete Ausführung meist durch das Wirken der niedrigeren Ebene vollzieht (vgl. Rieckhoff 2007, 41).

Möchte man die Kompetenzverteilung in Deutschland zwischen den einzelnen Bundesländern und dem Bund überschaubar reduzieren, lässt sich festhalten, dass das Grundgesetz dem Bund überwiegend gesetzgebende und den Ländern vermehrt administrative Kompetenzen überträgt, wenngleich diese Feststellung nicht ausschließlich zu lesen ist (vgl. Reutter 2020, 40f). Die verfassungsmäßige Definition der Befugnisse sowie die weitreichende Autonomie der Länder in zahlreichen Angelegenheiten spricht deutlich gegen eine Überordnung des Bundes als maßgebliche Entität für die Länder. Vielmehr handelt es sich um ein Nebeneinander der Gefüge, in dem der Bund den umschließenden, aber nicht absorbierenden Korpus bereithält. Dies lässt sich dadurch erhärten, dass kleineren Organisationseinheiten wie den Ländern Mittel gegeben werden, der höheren Ebene, hier dem Bund, zu widersprechen oder Akzente zu setzen. Die Länder sind legitimiert, bundesweite Gesetzesrahmen in ihrem Sinne auszulegen oder im Bundesrat zu anderen Beschlüssen zu kommen als das Bundeskabinett und damit auch als Korrektiv aufzutreten (vgl. Klenk 2019, 79). Ferner steht ihnen unter bestimmten Voraussetzungen sogar das Recht zu, per konkurrierender Gesetzgebung souverän Gesetze zu erlassen (vgl. Bundesregierung 2019, 111).

Hier zeichnet sich ab, dass es nicht den einen Weg gibt, die Idee des Föderalismus juristisch oder organisatorisch auszudeuten und zum Beispiel im bundesrepublikanischen Alltag umzusetzen (vgl. Schäffer/Vorländer 2013, 57ff). Während der deutsche Föderalismus nach das intrastaatliche Modell baut, also auf Integration und die „Herstellung gleichwertiger Lebensverhältnisse“ abzielt, existieren

durchaus föderalistische Staatenmodelle, die sich nicht hinsichtlich rationaler Funktionen zusammenstellen, sondern nach historischen Souveränitäten sortieren (Bundesregierung 2019, 111). In den USA beispielsweise herrscht eine interstaatliche Konstellation vor, die „die Autonomie der Einheiten und die Vielfalt der Lebensbedingungen“ fördert (Broschek 2009, 46). In der kooperativen Praxis bedeutet dies, dass US-amerikanische Bundesstaaten mehr Souveränität besitzen und ihnen damit nicht nur weitgehend administrative Kompetenzen anhaften. Sie verfügen je über eine eigene Gesetzgebung sowie Rechtsprechung, die der Bund nur bedingt beeinflussen kann. Das amerikanische Modell ist ein Bund souveräner Staaten, die sich in Anerkennung der jeweils anderen Staaten verbündet haben, um insbesondere militärisch oder wirtschaftlich gemeinsam aufzutreten. Im deutschen Föderalismus hat der Bund eine bedeutendere Funktion und dient sowohl als verbindendes Glied zwischen den Bundesländern als auch als Richtschnur bei legislativen Fragen. Artikel 71 des Grundgesetzes fasst den Unterschied zum amerikanischen Föderalismus, in dem alle nicht eindeutig dem Bund zugeschriebenen Kompetenzen den Ländern obliegen, in wenigen Zeilen zusammen. Denn demzufolge können deutsche Bundesländer nur dann Gesetze erlassen, „wenn und soweit sie hierzu in einem Bundesgesetze ausdrücklich ermächtigt werden“ (Bundesregierung 2019, 111). Die politisch-demokratische Autorität kann sich also in föderalen Systemen an unterschiedlichen Positionen verdichten. Im amerikanischen Beispiel liegt die Macht bei den selbstbestimmten Teilstaaten, die sich im Senat konzentriert; hierzulande fungiert der Bund als Direktive für die in ihm organisierten assoziierten und wertentsprechenden Länder.

Dabei haben beide Gefüge das Potenzial, Bürgernähe und regionale Flexibilität herzustellen, können im Gegenzug allerdings auch kompliziert und verworren wirken. So wäre nach dem Prinzip der Subsidiarität beispielsweise anzunehmen, dass die jeweiligen Kommunen in Deutschland die Hauptakteure im Bereich der Sozialpolitik sind, diese also für Arbeitslosengeld, Sozialhilfen und Jugendzentren aufkommen. In der Realität jedoch trägt der Bund große Teile der Rentenkosten sowie der Erwerbslosenunterstützung (vgl. Bundesministerium für Arbeit und Soziales 2019). Die Sozialhilfe hingegen wird durch Länder und Gemeinden finanziert, wohingegen die Kommunen die Jugendzentren verwalten. Man sieht, der deutsche Föderalismus ist nicht immer trennscharf oder leicht verständlich und spricht daher vom „kooperativen Exekutivföderalismus“ (Klenk 2019, 79).

Dennoch lässt diese Struktur gegenüber zentralistischer Staatsschemata entscheidende Vorteile, aber zugleich bemerkenswerte Defizite erkennen. So kann Deutschland mittels des föderalen Systems sehr genau auf örtlich vorliegende Unterschiede mit individuellen Maßnahmen und Vorgaben reagieren. Der bundesrepublikanische Föderalismus bringt gesamtstaatliche und legislative Aufgaben mit lokal ausdifferenzierten administrativen Operationen zusammen. Dieses dezentrale Organisationsprinzip weist die übergeordnete Richtung für alle Mitgliedsländer an. Es unternimmt mithin den Versuch der Homogenisierung verbindender Interessen, und sorgt bestenfalls ebenso für „die Erhaltung und Pflege regionaler Identitäten und Besonderheiten in einem gemeinsamen Staats- und Gemeinwesen“ (Edelmann 2014, 10). Politisch wie juristisch klar erkennbare Ansprechpartner und zuständige Verwaltungen ermöglichen zivile Gestaltungsräume beziehungsweise nehmen sie gewisse Hürden bei der Wahrnehmung demokratischer Beteiligungsmöglichkeiten.

Was hier genuin demokratisch im Wortsinn zu sein scheint und geradezu unerreichbar klingt, birgt bei inadäquater Anwendung zugleich das Potenzial für Korruption, Fehlwirtschaft oder übermäßige Bürokratie. Denn eine derart breite und auf Subsidiarität aufbauende Staatenkonstruktion fußt zwangsläufig auf einem beachtlichen Verwaltungsapparat. Der soeben noch als bürgernah und basisdemokratisch ausgezeichnete Föderalismus offenbart sich bei näherer Betrachtung als möglicherweise träge oder ausufernd kompliziert (vgl. Edelmann 2014, 7). So ist es möglich, dass die Beteiligung aller notwendigen, föderalen Gremien zu einer Verzögerung teurer Großprojekte führt oder Finanzmittel nicht rechtzeitig dort ankommen, wo sie benötigt werden. Eine Uneinigkeit zwischen Bund und Ländern hat im äußersten sogar die Wirkmacht, gewisse Entscheidungsprozesse gänzlich zu behindern (vgl. Bundestag.de 2020). Wo zentralistisch geprägte Demokratien nationale, parlamentarische Entscheidungen auf das ganze Land übertragen können, sehen sich föderalistische Gesellschafts- und Politiktraditionen im Allgemeinen einer aufwendigeren Debattenherausforderung gegenüber. Bei „bestimmten Gegenständen der konkurrierenden Gesetzgebung und der Verwaltungsangelegenheiten“ haben Länder das Recht, für sich jeweils passende und vom Bund abweichende Gebote zu erlassen (Reutter 2020, 41). Das ermöglicht zwar eine breitere Partizipation und regionale Differenzierungen, kann unter gewissen Gegebenheiten aber zu Verlangsamung und

Verteuerung führen, wie das gesellschaftliche Brennglas Corona-Pandemie mit seinen stetigen Ministerpräsidentenkonferenzen, unterschiedlichen Länderbeschlüssen und dezentralen Beschaffungen medizinischer Hilfsmittel vergegenwärtigt hat.

Gerade der Umgang mit Informationstechnik ist im Grundgesetz, Artikel 91c, uneindeutig gefasst und steht somit vor dem Risiko, nicht mit der angemessenen Geschwindigkeit und Befugnis bedacht zu werden. In Artikel 91c ist festgehalten, dass Bund und Länder bei Betrieb und Planung von IT-Systemen zusammenarbeiten oder gemeinsame Sicherheitsanforderungen entwickeln können, wobei die genaue Ausgestaltung in Vereinbarungen zu regeln ist (vgl. Bundesregierung 2019, 139). Solche Freiräume bieten Flexibilität, können aber auch über Koordinationsprobleme und Parallelität zu einem Stadium übergreifender Nichtverantwortlichkeit führen.

Die expliziten Regelungen zur IT-Sicherheit im deutschen Föderalismus weist schließlich die Cybersicherheitsstrategie von 2021 und das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme näher aus. Dort wird zum Beispiel auf das Nationale Cyber-Abwehrzentrum als überregionale Verbindungsstelle und auf eine gegenseitige Verpflichtung von Bund und Ländern „zur gemeinsamen Abwehr von Angriffen auf Informationsinfrastrukturen in der öffentlichen Verwaltung“ hingewiesen, um ein einheitliches Lagebild zu erschaffen und eine koordinierte Zusammenarbeit über föderalistische Limitierungen hinweg zu etablieren (Bundesministerium des Innern 2016, 27/36).

2.2.2 Internationale Rolle in Europa und der Welt

Deutschland nahm und nimmt eine geografische wie politische Zentralposition in Europa ein und steht damit nicht nur unter der Last, der historischen Verantwortung gerecht werden zu müssen, sondern besetzt innerhalb der kontinentalen Gemeinschaft eine bemerkenswerte Rolle. Mit der Wiedervereinigung 1990 und dem kurz darauffolgenden Artikel 23 des Grundgesetzes zur „Verwirklichung eines vereinten Europas“ legte die Bundesrepublik den Grundstein für ihre heutige ökonomische und politische Bedeutung (Bundesregierung 2019, 76). Unter anderem über die EU-Osterweiterung von 2004 stärkte Deutschland seine geopolitische Mittellage in Europa und unterstützte das Export-Kapital der nationalen Wirtschaft. Die Finanz- und Eurokrise ab etwa 2008 sowie der daraus erwachsene Europäische Stabilitätsmechanismus erhärteten den Eindruck von der Führungsnation Deutschland

innerhalb der EU. In den Jahren 2012 und 2013 legten die wohlhabenden Staaten Europas – unter der Anleitung Deutschlands – den schwerer getroffenen Staaten wie Griechenland eine katonische Austeritätspolitik auf, die vielerorts als hegemonial, teils autoritär aufgefasst wurde. Man fing das griechische Haushaltsdefizit mit gemeinschaftlichen Krediten auf und stellte Bedingungen wie Kürzungen der Sozialleistungen, Steueranpassungen und einer Beschränkung der finanziellen Souveränität (vgl. Kundnani 2016, 9). Zwar erwuchs so, insbesondere mit der Erinnerung an deutsche Großmachtvorstellungen des 20. Jahrhunderts, großer Unmut gegen die Gläubigerstaaten der EU; jedoch entwickelte sich zugleich eine finanzpolitische Patronatsstellung der Bundesrepublik. Während Deutschland in diesen Jahren von Teilen der Europäischen Union als restriktiv und bevormundend wahrgenommen wurde, wandelte sich das Bild mit der zugänglichen Migrationspolitik 2015 und dem mittlerweile ikonischen Ausspruch der Bundeskanzlerin: „Wir schaffen das“ (Bundesregierung 2015).

Eine aktuelle Befragung des European Council on Foreign Relations unter EU-Bürgern hat ergeben, dass etwa ein Drittel der Europäer Deutschland in einer Führungsposition sehen, wenn sie an Wirtschafts- und Finanzpolitik sowie an die Verteidigung von Demokratie und Menschenrechten denken (vgl. Buras/Puglierin 2021, 5f). Im Gegensatz dazu schätzen die Befragten das internationale Gewicht der Bundesrepublik eher gering ein. Im Umgang mit Großmächten wie China trauen sie Deutschland nur wenig Durchsetzungsvermögen zu.

Berlin has the confidence of more than one-third of EU citizens in handling economic issues and standing up for democratic values, but only 17 per cent of them believe that Germany can lead the bloc in its relations with China. In handling the EU's relations with Russia and the US, only one-fifth and one-quarter of Europeans trust Germany respectively (Buras/Puglierin 2021, 9f).

Auch deshalb nennt Hans Kundnani Deutschland eine „Halbhegemonie“; eine Position, „die das Land schon zwischen 1871 und 1945 in Europa innehatte – diesmal aber in «geoökonomischer» und nicht in geopolitischer Form“ (Kundnani 2016, 15). Kundnani schließt, dass Deutschland in seiner augenblicklichen Beschaffenheit gleichzeitig zu stark und zu schwach ist: Auf europäischer Ebene sei die Bundesrepublik vor allem ökonomisch unantastbar, auf der globalen Bühne bleibe das Land noch hinter seinen Möglichkeiten zurück (vgl. Kundnani 2016, 15). Eine Erhebung der GIZ aus dem Jahr 2018 bestätigt diese Wahrnehmung. Die internationale Befragung ergab, dass man die

„Führungsrolle für Deutschland nie im Alleingang, sondern immer im Kontext der Europäischen Union“ erwarte (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 2018, 40). In Belangen der Sicherheitspolitik setze Berlin auf eine vernetzte Sicherheit, etwa unter dem Schutz der NATO, und weniger auf eigene militärische Kapazitäten, sodass man gar nur über sekundäre Souveränität verfüge (vgl. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 2018, 29). Auch deshalb attestiert Kundnani der Bundesrepublik, ein Paradoxon zu sein: Deutschland ist „zwar ökonomisch innerhalb Europas ausgesprochen bestimmend, doch außerhalb Europas bleibt es auffallend zögerlich und zeigt deutlich weniger Ambitionen zur Machtprojektion als Frankreich oder Großbritannien“ (Kundnani 2016, 15).

Damit hat sich seit und mit der Wiedervereinigung ein Richtungsgeber für Europa entwickelt, der darüber hinaus nur begrenzte Wirkmacht besitzt. Jedoch verwendet beziehungsweise zitiert die GIZ in ihrem überschaubaren Bericht ganze 22 Mal das Wort *Vorbild*. Deutschland werde international als Anker für Klimaschutz, Moral und Sozialstaatlichkeit wahrgenommen – daher formulieren die Autoren der Studie ein mögliches Credo für die Bundesrepublik: „Führen durch Vorbild“ (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 2018, 34/35). Deutschland gilt mit seiner stabilen Wirtschaft, seiner ausgeprägten Zivilgesellschaft und nicht zuletzt der langen Kanzlerschaft Angela Merkels als beständiger Fels innerhalb der EU. Mit Ursula von der Leyen ist seit 2019 eine Deutsche Präsidentin der Europäischen Kommission, die somit das auf die Bundesrepublik projizierte Leitungsparadigma verkörpert.

2.3 Wie ordnet sich Cybersicherheit in Deutschland?

Dieses Kapitel dokumentiert die Rollen der wichtigsten öffentlichen Protagonisten der Informationssicherheit in Deutschland und setzt diese in Relation zu den jeweils anderen. Am Ende dieses Prozesses sind die Anschlussstellen zwischen den Institutionen sichtbar, sodass sich diese Fixation als Vergleichsgröße anbietet, nachdem die niederländischen Gegebenheiten auf gleiche Weise vorliegen.

Die untenstehende Skizze bildet ab, wie Cybersicherheit in Deutschland organisiert ist und welche staatlichen, aber auch privat-öffentlichen Akteure entscheidenden Anteil daran haben. Als Grundstein für diese Analyse dienen die zugrundeliegenden Gesetze

und Strategien, die die Weichen für die Ausgestaltung von Informationssicherheit stellen.

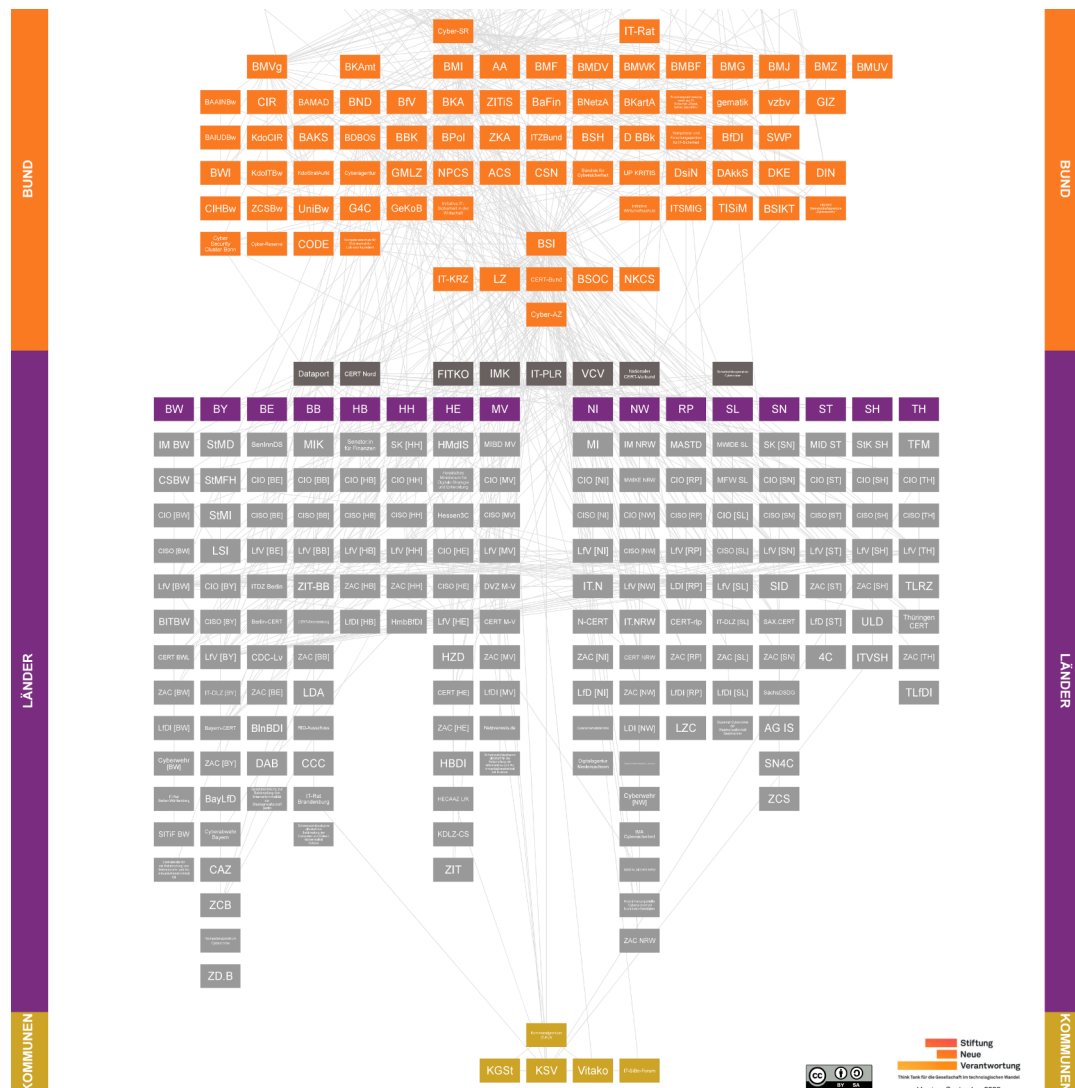


Abbildung 7: Deutschlands staatliche Cybersicherheitsarchitektur (Herpig/Rupp 2022)

Dabei handelt es sich bei oben stehender Darstellung nur um einen Ausschnitt der gesamten Grafik. Internationale Schnittstellen sind hier außerdem ausgeblendet. Doch schon so lässt sich leicht erkennen, dass die Zuständigkeit für Cybersicherheit in Deutschland auf viele Schultern verteilt ist. Zugleich ist festzustellen, dass es innerhalb der Sicherheitsarchitektur Knotenpunkte gibt, die von besonderer Relevanz sind und Zentralstellen zur Koordination, Aufsicht oder Weisung im Verantwortungsbereich der Cybersecurity bilden. Mit ihrer ausführlichen Arbeit haben Herpig und Rupp eine Draufsicht erstellt, die hier nicht wiederholt wird. Stattdessen ist die Leistung der Autoren eine gehaltvolle Grundlage, die folgende Absätze sinnvoll ergänzen. Nicht die Vollständigkeit, wie bei Herpig und Rupp, ist das Ziel, sondern eine neue Sichtachse,

die Strategien, Lücken, Prioritäten oder auch Mängel innerhalb der Cybersicherheitsarchitektur offenbart.

2.3.1 Staatliche Institutionen des Bundes

Die Digitalisierung und Technologisierung der unterschiedlichsten Lebenswelten in Deutschland gestalten etliche oberste und obere Bundesbehörden, wozu unter anderem die zahlreichen Ministerien gehören. So unterhalten die Bundesregierung, das Bundesministerium für Wirtschaft und Klimaschutz (BMWi), das Bundesministerium der Verteidigung (BMVg), das Bundesministerium des Innern und für Heimat (BMI), das Bundesministerium für Digitales und Verkehr (BMDV) und das Bundeskanzleramt (BkA) ganze Einrichtungen oder auch Organisationseinheiten, die sich mit Digitalthemen, ihrer Implementierung oder ihrer sicheren Ausgestaltung befassen.

Bundesministerium für Wirtschaft und Klimaschutz / Bundesnetzagentur

Das Bundesministerium für Wirtschaft und Klimaschutz schreibt sich auf die Fahne, den „digitalen Wandel gestalten“ zu wollen (Bundesministerium für Wirtschaft und Energie 2020). Deshalb fällt in das Ressort des BMWi die Bundesnetzagentur (BNetzA), die sich mit der Telekommunikation als eines von vier Fachthemen befasst. Insbesondere der Aufbau und die Marktregulierung zugrunde liegender Netzinfrastrukturen obliegen der Behörde. Die derzeit bekanntesten Beispiele für die Tätigkeiten der BNetzA ist die Regulierung der 5G-Netzkonstruktion und des Breitbandausbaus (vgl. Bundesnetzagentur 2020a). Die Behörde soll sicherstellen, dass Betreiber die Netze marktneutral, zuverlässig, zugänglich und sicher errichten und unterhalten. Daraus ergibt sich die Position der Bundesnetzagentur als ressortübergreifende Schnittstelle. Für die Vergabe der 5G-Frequenzen beispielsweise verfasste die Agentur vorab Sicherheitskriterien, an die die Betreiber von Telekommunikations- und Datenverarbeitungssystemen unumgänglich gebunden sind (vgl. Bundesnetzagentur 2020b). Dazu griff die BNetzA auf die Expertise des Bundesamts für Sicherheit in der Informationstechnik und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zurück, um die Kriterien so zu formulieren, dass sie den Anforderungen aus den Perspektiven Datensicherheit, Datenschutz und Infrastruktur standhalten können. Diese Geschäftsbereich und Ministerien übergreifende Zusammenarbeit ist ein Kennzeichen der deutschen Umsetzung der Digitalisierung, wie sich im Folgenden wiederholt zeigen wird.

Bundesministerium für Digitales und Verkehr

Das Bundesministerium für Digitales und Verkehr (BMDV) behandelt die „bedarfsgerechte Planung der Bundesverkehrswege“, den öffentlichen Nahverkehr, Elektromobilität, Luftfahrt, Wasserverkehr sowie „die Weiterentwicklung der Mobilitäts- und Kraftstoffstrategie“ (Bundesministerium für Verkehr und digitale Infrastruktur 2020). Daneben beansprucht das Ministerium, wie es der Name schon sagt, eine grundlegende Rolle bei der Verwaltung der digitalen Infrastruktur. So beschäftigt sich die Abteilung *Digitale Gesellschaft* des BMDV mit „dem automatisierten und vernetzten Fahren“, der „Digitalisierung des ÖPNV“, der „künstliche[n] Intelligenz in der Mobilität“ sowie der Förderung des Breitbandausbaus (Bundesministerium für Verkehr und digitale Infrastruktur 2020). Diese Zuständigkeiten betreffen zuvorderst das Kraftfahrt-, das Luftfahrt- und das Eisenbahn-Bundesamt. Die Behörden benötigen zur Entwicklung und Instandhaltung smarter Verkehrssysteme und zuverlässiger Glasfasernetze die Beratung und Unterstützung anderer Administrationen, etwa des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder des BSI.

Bundeskanzleramt / Bundesnachrichtendienst

Die Funktion des Bundeskanzleramts (BKa) in Bezug auf die deutsche Informationssicherheit wird erst auf den zweiten Blick deutlich. Als Unterstützungsbehörde des Bundeskanzlers ist die Herstellung von Cybersicherheit keine Kernaufgabe des Bundeskanzleramts. Bei genauerer Betrachtung fällt jedoch auf, dass dem Bundeskanzleramt lediglich eine Behörde nachgeordnet ist, nämlich der Bundesnachrichtendienst. Der deutsche Auslandsnachrichtendienst hat indessen eine gewichtige Funktion für die Informationssicherheit in Deutschland. So hat er etwa die alleinige „Befugnis und die technischen Möglichkeiten zur strategischen Erfassung internationaler Datenverkehre“ (Bundesnachrichtendienst 2021). Damit ist der BND mit Privilegien ausgestattet, um wichtige Informationen zu gewinnen, zu analysieren und im Rahmen des Nationalen Cyber-Abwehrzentrums (NCAZ) mit den übrigen Sicherheitsbehörden des Bundes zu teilen. Die Beobachtung internationaler Datenströme, des Darknets und terroristischer Bedrohungen liefert bedeutende Erkenntnisse für die Lageeinschätzung und die Antizipation möglicher Angriffsvektoren.

Neben dem BND gehörte bis Dezember 2021 auch die Beauftragte der Bundesregierung für Digitalisierung dem Bundeskanzleramt an. Diese Funktion ist in Deutschland mit keinem eigenen Ministerium hinterlegt. Stattdessen war die Staatsministerin damit beauftragt, aktuelle Impulse zur Digitalisierung des Staates und zur Digitalstrategie in der Bildung zu setzen, die über die Ressorts hinweg aufgegriffen werden sollten. Damit hatte sie eine verstärkt repräsentative Funktion ohne festgeschriebenes Budget oder nachgeordnete Behörden. Trotzdem geriet das Amt im Sommer 2020 in die Schlagzeilen, als Dorothee Bär den Vorstoß zu einer Bundeszentrale für digitale Aufklärung wagte (vgl. Bundesregierung 2020). Die neue Bundeszentrale war der Versuch, die „Bürgerinnen und Bürger auf allen Feldern der digitalen Transformation zu begleiten, auf der einen Seite technisch, aber auf der anderen Seite vor allem auch persönlich“ (Behörden-Spiegel 2020). Im Dezember 2021 wurden die Aufgaben der Digitalstaatsministerin ersatzlos eingestellt.

Informationstechnikzentrum Bund

Das Informationstechnikzentrum Bund ist seit 2016 der zentrale IT-Dienstleister für die deutsche Bundesverwaltung und untersteht dem Bundesministerium der Finanzen. Ein Hauptauftrag des ITZBund liegt darin, die IT-Konsolidierung des Bundes umzusetzen. Damit sollen Dienste vereinheitlicht und in eigenen Rechenzentren administriert werden, sodass der Bund die Kontrolle darüber behält, wo Daten gespeichert sind und wie sie geschützt werden. Das bedeutet auch, dass das ITZBund Server und digitale Dienste für seine Kundenbehörden verwaltet und bereitstellt (vgl. Informationstechnikzentrum Bund 2021a). Die Einrichtung hostet Webseiten, pflegt Server und entwickelt IT-Produkte, um den Leistungsbedarfen der Bundesbehörden gerecht zu werden. Daraus wiederum ergibt sich, dass das Informationstechnikzentrum Bund eine potenziell vulnerable Infrastruktur bereitstellt und aufgrund der Zentralisierung der Dienste und Daten hohe Sicherheitsstandards anlegen muss. Dies sichert das ITZBund unter anderem durch externe Kontrollen und interdisziplinäre Konsultationen:

Unser Umgang mit Daten und Informationen wird regelmäßig extern überprüft, z. B. durch den Bundesrechnungshof (BRH), den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), das Bundesamt für Informationstechnik (BSI) [sic!] oder auch durch den kritischen Blick unserer eigenen Kunden (Informationstechnikzentrum Bund 2021b).

Durch ihre Positionierung als Dienstleister unter ressortübergreifenden Aufsichtsmechanismen besitzt die Behörde geringen Gestaltungsspielraum. Stattdessen ist das ITZBund eine der wenigen Bundesinstitutionen, die sich auf eine konkrete und deutlich zu umreisende Aufgabe berufen kann.

Bundesministerium des Innern und für Heimat

Das Ministerium des Innern und für Heimat fällt durch die Vielzahl der zugeordneten Aufgaben auf: So zählen Gebiete wie Migration, Sicherheit, öffentlicher Dienst, Digitalisierung, Wohnen und sogar Sport zum Geschäftsbereich des Innenministeriums (vgl. Bundesministerium des Innern, für Bau und Heimat 2021b). Diese unterschiedlichsten Aufgaben gibt das BMI an 19 nachgeordnete Behörden wie dem Statistischen Bundesamt, dem Bundesverwaltungsamt (BVA), dem Technischen Hilfswerk (THW) oder dem Bundesamt für Migration und Flüchtlinge (BAMF). Da das Ministerium durch die zahlreichen nachgeordneten Behörden sowohl die zivile Sicherheit Deutschlands herstellt als auch die IT des Bundes pflegt, obliegt auch die allgemeine Sicherheit des deutschen Cyberraums dem BMI.

Zu den wichtigsten Aufgaben der Innenpolitik gehört es, die öffentliche Sicherheit zu gewährleisten. Sie umfasst den Schutz der Bürgerinnen und Bürger vor Gewalt, Verbrechen und Terror sowie den Schutz unserer verfassungsmäßigen Ordnung (Bundesministerium des Innern, für Bau und Heimat 2020a).

Aus diesem Schutzauftrag leitet das Ministerium die Aufgaben der Kriminalitätsbekämpfung und Gefahrenabwehr, der Spionageabwehr und der Extremismus- wie auch Terrorbekämpfung ab (vgl. Bundesministerium des Innern, für Bau und Heimat 2020a). Da diese Bedrohungen der öffentlichen Sicherheit im Digitalraum und mithilfe digitaler Werkzeuge stattfindet, befassen sich gleich mehrere Einrichtungen des BMI mit Aspekten der Cybersicherheit. Dazu zählen insbesondere das Bundesamt für Sicherheit in der Informationstechnik, das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, die Bundespolizei, das Bundeskriminalamt oder die Zentrale Stelle für Informationstechnik im Sicherheitsbereich, auf die mitunter im Folgenden noch näher eingegangen wird. All diese Institutionen stehen im Austausch miteinander, der teilweise institutionalisiert ist, wie zum Beispiel im Nationalen Cyber-Abwehrzentrum. Zusätzlich ist im Bundesinnenministerium der Beauftragte der Bundesregierung für

Informationstechnik angesiedelt, der eine Schnittstellenfunktion zwischen dem Bund, den Ländern und der Wirtschaft wahrnimmt. Diese Aufgabe ist von überwiegend beaufsichtigender Natur, da der „Beauftragte bei allen strategischen Fragen des IT-Einsatzes in der Bundesverwaltung und an allen Gesetzgebungsverfahren und anderen Regierungsvorhaben zu beteiligen [ist]“ (Der Beauftragte der Bundesregierung für Informationstechnik 2021). Diese Vielfalt macht das BMI zum versatilsten und personell größten Ministerium der Bundesrepublik.

Die eminente Bedeutung des Innenministeriums und seiner nachgeordneten Behörden für die Informationssicherheit ist augenfällig, da sich das BMI sowohl für die deutsche Cybersicherheitsstrategie wie für das IT-Sicherheitsgesetz 2.0 hauptverantwortlich zeigt. Damit aggregiert das Ministerium einen wesentlichen Teil der Steuerungsbefugnisse für die Cybersicherheit in Deutschland und setzt regelmäßig den Ton zu Digitalthemen. Mit seiner Kommunikation vermittelte das Ministerium in der Vergangenheit häufig Dringlichkeit und zeichnete stets anwachsende Unsicherheitslagen. Bei der Veröffentlichung des Lageberichts des BSI 2021 sagte der damalige Innenminister Horst Seehofer etwa, die „Gefährdungslage im Cyber-Raum ist hoch. Wir müssen davon ausgehen, dass dies dauerhaft so bleibt oder sogar zunehmen wird“ (Bundesamt für Sicherheit in der Informationstechnik 2021c). Der ebenfalls ausgeschiedene BSI-Präsident Arne Schönbohm rief sogar eine „Alarmstufe Rot“ aus (Bundesamt für Sicherheit in der Informationstechnik 2021c). Anfang 2021 erklärte Dr. Markus Richter, Staatssekretär im Ministerium, zum Start einer Aufklärungskampagne von BMI und BSI für Endanwender: „Nicht jedem ist bewusst, welche konkreten Risiken in sozialen Netzwerken und beim Online-Shopping bestehen und welche Schäden, sei es finanzieller Art oder schlicht durch Bekanntwerden persönlicher Daten, entstehen können“ (Bundesministerium des Innern, für Bau und Heimat 2021d). Die Angst vor individuellem Schaden fungiert hier als Hebel, um Aufmerksamkeit zu erlangen, in Handlung umzusetzen und um die Aktivitäten des Ministeriums als zwingend notwendig zu inszenieren.

Bundesamt für Sicherheit in der Informationstechnik

Schon dem Namen nach liegt der Schluss nahe, dass dem Bundesamt für Sicherheit in der Informationstechnik eine herausgehobene Position bei der Informationssicherheit auf Bundesebene zukommt und es deshalb kontinuierlich weitere Aufgaben und Zuständigkeiten bündelt. Die Verortung des Nationalen Cyber-Abwehrzentrums

(NCAZ), des Lagezentrums Bund sowie des CERT-Bund innerhalb des BSI schaffen ein Kompetenzzentrum zur Abwehr von digitalen Gefahren für den Bund. Das IT-Sicherheitsgesetz in seiner zweiten Fassung, das unter anderem die Rolle des BSI im digitalen Verbraucherschutz stärkt, untermauert diese Ableitung. Damit zementiert das Bundesinnenministerium die Stellung des BSI für die IT-Sicherheit auf Bundesebene. Zu den Kernaufgaben des Bundesamts gehört die „Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes“, der Schutz Kritischer Infrastrukturen, die Warnung bei Schwachstellen, Entwicklung technischer Standards und die Zertifizierung von Produkten, Beratung in der Digitalisierung anderer Behörden (Bundesgesetzblatt 2009, 2823).

Das BSI wird durch die Ansiedlung in Freital, im Saarland und mittels diverser Verbindungsbüros in ganz Deutschland als nationale Schaltstelle etabliert, kann umfassender warnen als je zuvor, greift in die IT-Standards Kritischer Infrastrukturen ein und besitzt nun auch aktive Befugnisse gegen Cyberkriminelle. Dass das BSI eine Vielzahl von Aufgaben zu bewältigen hat, spiegelt sich in dessen Leitbild beziehungsweise in der zugehörigen Absichtsformulierung wider:

Unser Ziel ist der sichere Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft. Mit unserer Unterstützung soll Informationssicherheit als Voraussetzung der Digitalisierung verstanden und eigenverantwortlich umgesetzt werden. Wir wollen bewirken, dass Sicherheitsaspekte schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden. Denn Informationssicherheit und Digitalisierung gehören untrennbar zusammen (Bundesamt für Sicherheit in der Informationstechnik 2022).

Die Behörde verfolgt hier eine ganzheitliche Vorgehensweise. Das BSI möchte nicht nur Technologien, sondern ebenso ihre Nutzung sicher machen, indem sie Resilienz bei den Anwendenden hervorruft und zugleich Sicherheitsmechanismen schon bei der Entwicklung von Informationstechnik implementiert. Das Bundesamt will Informationen und Technologien schützen, die Bevölkerung sensibilisieren, die Sicherheit der Bundes-IT gewährleisten und Cyberangriffe abwehren. Somit adressiert das Bundesamt etliche Ziel- und Interessengruppen mit diversifizierten und gegebenenfalls gegenläufigen Anforderungen wie Problemen. Mit etwa 1400 Mitarbeitenden¹⁴ kann diese Fülle an Aufgaben und die damit verbundenen Erwartungen aus Politik und Öffentlichkeit als sehr herausfordernd betrachtet werden.

¹⁴ Stand Anfang 2022

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)

Dabei stellt das Bundesamt für Sicherheit in der Informationstechnik keinesfalls den einzigen länderübergreifenden Akteur im Geschäftsbereich des BMI dar. Neben dem BSI beschäftigen sich weitere Institutionen, Behörden und Personen mit Anforderungen der IT-Sicherheit. So rief der damalige Bundesinnenminister Thomas de Maizière 2017 die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) ins Leben. Diese Bundesstelle legt den Fokus auf Forschung und Entwicklung und grenzt sich auf diese Weise von den Tätigkeiten des BSI ab. Die Mitarbeiter der ZITiS befassen sich vornehmlich mit „digitale[r] Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse wie auch technische[n] Fragen der Kriminalitätsbekämpfung, Gefahren- und Spionageabwehr“ (ZITiS 2020). Sie forschen an neuen Technologien, erkennen Trends und entwickeln Lösungen, um schließlich die übrigen Behörden mit Sicherheitsfunktion entsprechend beraten und ausstatten zu können. Damit positioniert sich ZITiS als Dienstleister für Ministerien, Bundeswehr und Polizeien, wie dem Bundeskriminalamt.

Bundesamt für Verfassungsschutz

Mit dem Bundesamt für Verfassungsschutz verfügt das Innenministerium, wie auch das Bundeskanzleramt, über einen nachgeordneten Nachrichtendienst. Während der BND allerdings äußere Risiken und die Aktivitäten anderer Staaten ins Visier nimmt, befasst sich das BfV vornehmlich mit Bedrohung von innen oder gegen die grundrechtliche Ordnung der Bundesrepublik. Das bedeutet, das Amt geht gegen Extremismus, gegen staatsfeindliche Bemühungen oder gegen Demokratiefeinde vor, indem es Daten sammelt und auswertet, um die Informationen anschließend der Justiz oder der Polizei zukommen zu lassen. Dazu setzt der Nachrichtendienst mit mehr als 4200 Mitarbeitenden¹⁵ auf klassische Methoden wie die Beobachtung von Verdächtigen, den Mitschnitt von Kommunikation oder aber die Nachverfolgung im Internet (vgl. Bundesamt für Verfassungsschutz 2021). Indem man entweder „einschlägige Seiten des Internets [...] systematisch und kontinuierlich beobachtet und ausgewertet“ oder das Internet als Quelle „für die verdeckte Informationsbeschaffung, etwa in den sozialen Medien“ einsetzt, erlangt das BfV gegebenenfalls auch Erkenntnisse über die

¹⁵ Stand Ende 2021

Informationssicherheit in Deutschland und Europa
(Bundesamt für Verfassungsschutz 2021).

Nationales Cyber-Abwehrzentrum

In seinen Ausführungen zur Cybersicherheit verweist das Bundesministerium der Verteidigung (BMVg) auf die ressortübergreifende Zusammenarbeit, die in der nachfolgend erläuterten Cybersicherheitsstrategie veranlasst ist. Dieser kooperative Ansatz findet Ausdruck im Nationalen Cyber-Abwehrzentrum, in dem die Bundeswehr mit dem Kommando Cyber- und Informationsraum sowie dem Bundesamt für den militärischen Abschirmdienst vertreten ist. Das Cyber-AZ ist eine institutionalisierte Kooperationsplattform diverser Sicherheitsbehörden mit IT-Aufgaben. Dort können unter anderem Berichte der Bundeswehr über abgewehrte Aggressoren für innen gerichtete Behörden, wie BSI, Bundespolizei oder Verfassungsschutz, hilfreich bereitgestellt werden und umgekehrt. Das Abwehrzentrum dient dem Informationsaustausch mit dem Ziel, Bedrohungen frühzeitig zu erkennen und gemeinsame Schritte zur Gefahrenabwehr abzustimmen. Neben nachgeordneten Stellen des BMVg sind deshalb

am Cyber-AZ das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), das Bundespolizeipräsidium (BPOLP) [...] als Kernbehörden sowie das Zollkriminalamt (ZKA) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als assoziierte Stellen beteiligt (Bundesamt für Sicherheit in der Informationstechnik 2020b).

Die Koordination des Cyber-AZ wechselt alle zwei Jahre, sodass das Gremium nicht durch die Anleitung einer einzelnen Behörde seinen fachübergreifenden Charakter verliert. Das Cyber-Abwehrzentrum kommt in den Bonner Räumlichkeiten des BSI zusammen, da dort unter anderem auch das IT-Krisenreaktionszentrum verortet ist.

Bundeskriminalamt

Das Bundeskriminalamt ist die Kriminalpolizei des Bundes und ermittelt mit 7800 Beamten¹⁶ unweigerlich auch gegen digitale Kriminalität. In der Abteilung Cybercrime führt das BKA Untersuchungen gegen Kriminelle oder kriminelle Gruppierungen durch, die in Deutschland straffällig werden (vgl. Bundeskriminalamt 2022b). Dazu vernetzen

¹⁶ Stand Mitte 2021

sich die Kriminalbeamten aus Wiesbaden mit den Landeskriminalämtern und Polizeien der Bundesländer. Ihre Erkenntnisse und Informationen tauschen sie dann als eine von acht Kernbehörden des Cyber-Abwehrzentrums in täglichen Lagebesprechungen und Arbeitsgruppen mit den Verbindungspersonen der übrigen Ämter aus, darunter das Kommando Cyber- und Informationsraum, das BSI oder der BND. In jährlich erscheinenden Berichten, dem *Bundeslagebild Cybercrime* zeigt das BKA seit 2011 nicht nur die Resultate seiner Arbeit auf, sondern dokumentiert die Entwicklungen verschiedener Kriminalitätsdimensionen im Digitalraum. Ebenso in jedem Jahr veranstaltet das BKA mit dem ESMT Berlin die Cybercrime Conference (C³), um Erfahrungen, aber auch wirkungsvolle Strategien mit etwa der Politik oder der Wissenschaft zu diskutieren. Damit nimmt die Polizeibehörde überwiegend detektierende und reaktive Aufgaben wahr, konzentriert sich also auf die Bekämpfung von begangenen Gesetzesverstößen und ihrer Wiederholung. Zur Prävention, also zur Vermeidung von Straftaten bevor sie entstehen können, bringt sich das BKA in das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) ein. Dort entstehen Sensibilisierungsprodukte und -kampagnen wie Videos oder Broschüren. In enger Zusammenarbeit mit dem BSI erarbeitet ProPK beispielsweise Anwenderumfragen wie das Digitalbarometer. In Anbetracht des Gesamtengagements des BKA liegt das Hauptaugenmerk allerdings nicht in der Prävention, sondern in der Reaktion auf bereits erfolgte Straftaten mit herausgehobener Bedeutung für die Bundesrepublik.

Bundesministerium der Verteidigung

Das Bundesministerium der Verteidigung (BMVg) identifiziert im Zuge der voranschreitenden Digitalisierung, dass die Souveränität Deutschlands durch digitale Mittel bedroht ist und daher der Bundeswehr eine tragende Rolle bei der Verteidigung im Cyberraum zukommt (vgl. Bundesministerium der Verteidigung 2021a). Daraus leitete das BMVg 2017 ab, den Organisationsbereich Cyber- und Informationsraum (CIR) der Bundeswehr ins Leben rufen zu müssen. Dieser soll besonders der Verteidigung gegen externe, digitale Bedrohungen militärischer Dimension dienen und vereint herkömmliche Strukturen der Bundeswehr mit den Herausforderungen virtueller Verteidigung (vgl. Bundesministerium des Innern 2016, 33). Das militärisch agierende CIR ist folglich eine Einrichtung, die vergleichsweise wenig spürbar in die zivile IT-Sicherheitsstruktur hineinwirkt und ist aufgrund der florierenden Digitalisierung

zugleich ein Produkt ebendieser. So tragen die Mitarbeiter der Bundeswehr durch die Abwehr militärischer Cybergefahren nach eigener Aussage „in einer digitalisierten Umgebung zu einer gesamtstaatlichen Sicherheitsvorsorge bei und stärken die Cyber-Sicherheitsarchitektur“ (Bundeswehr 2020). Als Motivation zur Gründung des CIR nennt die Bundeswehr einerseits den Schutz der eigenen IT und andererseits die Detektion und Abwehr von Angriffen militärischer Akteure oder fremder Nachrichtendienste. Wie für die gesamte Bundeswehr gilt auch für den Organisationsbereich Cyber- und Informationsraum die verfassungsgemäße Maxime, nur im Verteidigungsfall und zur „Abwehr einer drohenden Gefahr“ militärisch aktiv werden zu dürfen (Bundesregierung 2019, 130).

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Der BfDI stellt die Einhaltung der nationalen wie europäischen Datenschutzvorgaben sicher. Dabei orientiert sich der Beauftragte im Wesentlichen an den Bestimmungen der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG), um die digitale Privatsphäre der Bürger gewährleisten zu können. Dazu nimmt der BfDI als unabhängige, eigenständige oberste Bundesbehörde unter anderem die Pflichten wahr, die Öffentlichkeit für den Datenschutz zu sensibilisieren oder alle öffentlichen Einrichtungen des Bundes zu kontrollieren. Der Grundgedanke dahinter: Der Schutz sensibler Daten und die Werbung für Datensparsamkeit sind ein wesentlicher Beitrag für die Datensicherheit. Denn personenbezogene Daten, die nie erhoben und akkumuliert wurden, können nicht missbraucht werden oder in die Hände von Kriminellen fallen.

Der Nationale Cyber-Sicherheitsrat

Unter der Leitung des Beauftragten der Bundesregierung für Informationstechnik kommen im nationalen Cyber-Sicherheitsrat alle tangierten Ministerien sowie Vertreter der Länder und der Wirtschaft zusammen. Die Mitglieder beraten die Bundesregierung bei strategischen Fragen und geben Anregungen, um neuen Entwicklungen rechtzeitig begegnen zu können. Die Denkanstöße sollen auf diese Weise in die Ressorts gelangen und zur Umsetzung kommen. Im Wesentlichen fokussierte sich der mindestens dreimal jährlich tagende Rat bislang auf den Schutz Kritischer Infrastrukturen und auf außenpolitische Angelegenheiten der Informationssicherheit (vgl. Bundesministerium der Verteidigung 2021b). Die Ergebnisse des Gremiums sind nicht mit Verpflichtungen

für die Ressorts verbunden, sondern sind ein Instrument, um einen Konsens jenseits föderalistischer Grenzen abzustimmen.

Agentur für Innovation in der Cybersicherheit

Mit der Agentur für Innovation in der Cybersicherheit GmbH haben das Bundesinnenministerium und das Verteidigungsministerium eine Ministerien übergreifende Institution zur Förderung von Forschungsprojekten und innovativen Technologien begründet (vgl. Bundesministerium des Innern, für Bau und Heimat 2021b). Mit dem zugewiesenen Budget beschäftigt die Agentur zu Beginn etwa 20 Menschen¹⁷ damit, Forschungsvorhaben zu stützen, die dem Cybersicherheitsstandort Deutschland zugutekommen sollen. Damit verbunden ist die Hoffnung, vermehrt Sicherheitslösungen entwickeln zu können, die nicht importiert werden müssen, sodass Deutschland die Abhängigkeiten in diesem Bereich reduzieren und autarke Produkte bereitstellen kann. Die Agentur ist eine GmbH mit der Absicht, Forschungsmittel an zukunftsweisende und sicherheitsfördernde Projekte zu verteilen, ohne dabei selbst zu forschen. Dadurch soll die Innovationskraft der Cybersicherheitsbranche befördert werden, sodass mehr und bessere Produkte im Inland entstehen und sich folglich die Abhängigkeit von beispielsweise amerikanischen Zulieferern reduziert.

Organisationen auf Landesebene

Aufgrund der Vielzahl der Einrichtungen, die auf Bundesebene mit der Cybersicherheit betraut sind oder zumindest Aufgaben bedienen, die der Informationssicherheit zuarbeiten, kann der Eindruck entstehen, dass die Datensicherheit ausschließlich den Bund betrifft. Jedoch ist dieser Schein trügerisch, da die föderale Staatsorganisation mit sich bringt, dass einige Bundeseinrichtungen in die Länder gespiegelt wurden, um fehlende Bundesbefugnisse zu kompensieren. So führt der bayrische Verfassungsschutz das Cyber-Allianz-Zentrum Bayern (CAZ). Ebenfalls in Bayern existiert das einzige Landesamt für Sicherheit in der Informationstechnik (LSI) sowie das einmalige Staatsministerium für Digitales. Baden-Württemberg möchte einen ähnlichen Weg gehen und errichtete 2021 Cybersicherheitsagentur Baden-Württemberg (CSBW), die analoge Funktionen ausfüllt wie das LSI für Bayern. Nordrhein-Westfalens Innenministerium besitzt indes eine ganze Digitalabteilung, die wiederum die

¹⁷ Stand Ende 2021

Koordinierungsstelle für Cybersicherheit verwaltet (vgl. Ministerium für Verkehr des Landes Nordrhein-Westfalen 2021). Während Hessen das Landes-CERT¹⁸ aufgrund seiner Funktion für die öffentliche Sicherheit im Innenministerium verankert, wurde das Bremer CERT dem Senator für Finanzen zugewiesen und zu einem Dienstleister ausgelagert (vgl. Hessisches Ministerium des Innern und für Sport 2021/Freie Hansestadt Bremen 2021). Für diese Heterogenität lassen sich zahlreiche weitere Beispiele finden, sodass von einer vollständigen Auflistung an dieser Stelle abgesehen wird. Sie zeigt aber, dass es weder einheitliche Standards noch vergleichbare Sicherheitsniveaus über die Bundesländer hinweg gibt.

Gleichzeitig existieren Zuständigkeitsprinzipien, die zwar auf Länderebene verwaltet werden, aber in jedem Bundesland gleich organisiert sind. Beispielsweise verfolgen 16 Landeskriminalämter Straftaten der Cyberkriminalität. Genauso betreuen 16 Landesverkehrsministerien die Digitalisierungsinfrastruktur. Gleiches gilt für die sogenannten Chief Information Officer (CIO), die sich in der Hauptsache für die Digitalisierung der jeweiligen Landesverwaltung verantwortlich zeigen. Jedes Bundesland in Deutschland ernennt einen solchen Beauftragten der Landesregierung für Informations- und Kommunikationstechnik¹⁹ selbst. Diese sind darüber hinaus zugleich die Vertreter ihres Landes im IT-Planungsrat. Dort kommen die Abgesandten mehrmals jährlich mit dem Bund zusammen, um die Reibungspunkte der föderalen Zusammenarbeit im Bereich der Informationssicherheit zu diskutieren (vgl. IT-Planungsrat 2019). Nicht zuletzt verantworten die Bundesländer über ihre Kultusministerien selbst, inwiefern Informatik und Informationssicherheit an Schulen und Universitäten gefördert werden. Damit nehmen sie entscheidenden, wenngleich verschiedenartigen, Einfluss auf die Ausbildung zukünftiger Fachkräfte sowie auf die Ausprägung einer allgemeinen IT-Kompetenz und -Resilienz in Deutschland.

Regionale Polizeidienststellen und Kriminalämter der Länder

Bei der Betrachtung der Cybersicherheitsarchitektur werden die Landespolizeien häufig übersehen, füllen aber eine elementare Funktion innerhalb dieser aus. So sind Institutionen wie das BSI oder ZITiS in der Gewaltenteilung nicht befugt, strafrechtlich gegen Täter vorzugehen oder Persönlichkeitsrechte einzuschränken. Die Polizeien der Länder beginnen genau hier mit ihrer Arbeit und reagieren auf begangene

¹⁸ Abkürzung: Computer Emergency Response Team

¹⁹ Der Titel kann je nach Bundesland abweichen.

Digitalstraftaten, indem sie diese erfassen und gegebenenfalls Ermittlungen als ersten Schritt des rechtsstaatlichen Prozesses einleiten. Angesichts dessen sind die lokalen Polizeibehörden und die Landeskriminalämter von essenzieller Bedeutung zur Identifizierung von Tätergruppen, Angriffsmustern und für ein aussagefähiges Lagebild. Diese Fallerfassung hilft dann beispielsweise dem BKA und weiteren Behörden, ihre Arbeit auf ebenjene Erkenntnisse abzustimmen. Damit ist die Polizei, im Gegensatz zu den meisten übrigen Einrichtungen des Staates, unmittelbar ansprechbar für die Bevölkerung.

Wie zu erwarten, sind die staatlichen Institutionen in Deutschland mehrheitlich auf den Ausbau, den Betrieb oder die sichere Ausgestaltung von Infrastruktur bedacht und haben weniger einzelne Nutzer oder Nutzergruppen im Blick. Zudem wird ebenso erwartungsgemäß deutlich, dass diese Strukturen die innerdeutsche Absicherung zum Ziel haben und lediglich BND und CIR nach außen gerichtet arbeiten. Insgesamt zielt der (Cyber-)Sicherheitsapparat darauf ab, den jetzigen Lebens- und Sicherheitsstandard zu erhalten, um Gesellschaft und Wirtschaft im Innern eine ungestörte Entfaltung zu ermöglichen. Progression oder Innovation sind für diese Einrichtungen zwar notwendige Triebkräfte, um mit den Herausforderungen Schritt halten zu können, als wegweisende Impulsgeber fallen die Institutionen allerdings nicht auf. Stattdessen treten die Behörden und Funktionsträger apodiktisch auf. Allein ihre schiere Anzahl, ihre ähnliche Benennung und die kaum zu durchschauende, zuständigkeitsbedingte Verkettung der Einrichtungen ermöglicht es Bürgern kaum, sich einen Überblick zu verschaffen oder die akademisch respektive bürokratisch formulierten Aufgabenfelder zu erfassen. Daraus folgt ein Mangel, mindestens eine fehlende Sichtbarkeit, an direkten Ansprechpartnern für die Bevölkerung.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	O		O	O		O		O			O

Die Aufgaben der Organisationen geben an dieser Stelle keinen Hinweis auf eine durch Befürchtungen angeleitete Sicherheitskultur. Wenngleich das BSI und andere Amtsstellen mehr und mehr Kompetenzen erhalten und sich auf Landesebene eigene Cybersicherheitsbehörden herausbilden, entstehen solche Strukturen nach wie vor aufgrund demokratischer Entscheidungsprozesse auf der Basis objektiver Parameter und nicht erkennbar durch populistische Aneignung. Gleichwohl gründen alle zuvor

benannten Institutionen ihre Legitimierung im Kampf gegen Unsicherheit und Risiko, nicht in der Analyse oder Nutzbarmachung von Möglichkeiten. Neue Technologien wie 5G oder KI werden durch die Behörden reguliert statt potenziert; Risiken werden eingedämmt, statt Chancen zu kultivieren.

2.3.2 Institutionen der Gesellschaft

Die Zivilgesellschaft darf im Kontext der Informationssicherheit keinesfalls als unorganisierte, zerstreute Masse gesehen werden. Stattdessen manifestieren sich gesellschaftliche Vertreter in Vereinen, Verbänden, Presse, Handelskammern, Unternehmen oder Bildungseinrichtungen. Mit der Cybersicherheitsstrategie 2016, später auch mit der CSS 2021 bekräftigt, erkannte die Bundesregierung die Bedeutung institutionalisierter Interessengemeinschaften, indem sie vier Handlungsfelder ausmachte, von denen gleich drei ein intensives Mitwirken nicht staatlicher Player verlangten (vgl. Bundesministerium des Innern 2016, 9). Denn aus staatlicher Perspektive haben diese repräsentativen Organisationen für gewöhnlich zwei instrumentelle Funktionen inne. Sofern es nämlich gelingt, Gesellschaftsvertreter von einer Idee zu überzeugen, helfen diese in der Regel dabei, das befürwortete Konzept in die Breite zu tragen. Nach dem Atomausstieg 2011 zeigten sich etwa zahlreiche Umweltverbände äußerst positiv gestimmt. Gleichzeitig setzte eine umfangreiche Anschlusskommunikation ein, mit der einerseits der Erfolg des Verbandengagements betont und nebenbei weitergehende Forderungen ergänzt wurden (vgl. Greenpeace 2011). Zweitens legitimiert das Zutun dieser Organisationen in Entscheidungsprozessen und Gremien den getroffenen Beschluss. Auf diese Weise sehen die Menschen, die von einer politischen Entscheidung betroffen sind, ihre Perspektive im Beschlussprozess berücksichtigt – und neigen so dazu, das Ergebnis anzuerkennen. Organisierte Gruppen können aber auch auf die entgegengesetzte Wirkrichtung abzielen: Die Stimme des Einzelnen verstärkt sich, indem sich Individuen zusammenschließen und gemeinsame Überzeugungen vertreten, um sie an den entsprechenden Machtpositionen vorzubringen. Damit nehmen Institutionen der Gesellschaft als Vertretungen großer Bevölkerungsgruppen eine wesentliche Funktion unter anderem für die Akzeptanz, Partizipation und Verbreitung von Cybersicherheitsfahrplänen ein. In Deutschland zeigt sich diese Landschaft sehr vielfältig und lässt sich aufgrund des Umfangs hier nur beispielhaft nachzeichnen.

Im Zusammenspiel mit der Politik existieren einerseits diverse, sehr potente Verbände, die häufig gar vom Staat konsultiert werden; andererseits gibt es Vereine, die wenig Wert auf einen Konsens mit dem Staat legen, sondern sich unter anderem der Netzfreiheit oder der digitalen Souveränität verschreiben. Beginnend mit den staatsnahen Interessenvertretungen fällt auf, dass diese Verbindung zwischen Staat und Gesellschaft eine institutionalisierte Form angenommen hat. Im oben genannten Nationalen Cyber-Sicherheitsrat sprechen unter anderem der Bundesverband der deutschen Industrie e. V. (BDI), der Deutsche Industrie- und Handelskammertag (DIHK) und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) für ihre jeweiligen Mitglieder aus der Privatwirtschaft. Sie haben damit in regelmäßigen Abständen Gelegenheit, Impulse zu platzieren, die der eigenen Branche zugutekommen und die Sicherheitspolitik in ihrem Sinne gestalten. Dort nehmen neben den großen Verbänden auch einzelne Unternehmen teil, die etwa wichtige IT-Strukturen unterhalten, bedeutende Informationstechnik herstellen oder die sogenannten Kritischen Infrastrukturen betreiben, also etwa Kraft- und Wasserwerke. Wenngleich nicht Teil des Cyber-Sicherheitsrats wirbt der VDE, der Verband der Elektrotechnik Elektronik Informationstechnik e. V., mit der politischen Einflussnahme offensiv auf der eigenen Webseite:

Der VDE ist hierbei Mittler und Motor zugleich. Mit Repräsentanzen in Berlin und Brüssel aber auch auf Landesebene berät der VDE die Politik mit seiner neutralen Expertise zu Technologie, Bildung, Normung und Verbraucherschutz (VDE 2021).

Diese Verbände als repräsentative Beispiele für unzählige mehr dieser Art sind Teil eines interessen- und branchenübergreifenden Lobbyismusnetzwerks, das sich nicht nur auf die Bundesrepublik, sondern auch auf transnationale Strukturen wie die Europäische Union erstreckt. Die Definition von Stefan Schwaneck zeigt, wieso schon die oberflächliche Untersuchung dieser Organisationen ausreicht, um diese Aussage gesichert treffen zu können:

Lobbying bezeichnet direkte und indirekte Versuche von Vertretern gesellschaftlicher Akteure auf politische Entscheidungsträger in Legislative und Exekutive sowie andere am politischen Willensbildungsprozess beteiligte Stakeholder durch Information, argumentative Überzeugung oder die Ausübung von Druck einzuwirken, um mehr oder weniger partikulare Interessen in Gesetzen oder staatlichem Handeln zu verankern (Schwaneck 2019, 25f).

Andere Gruppierungen wie eco, der Verband der Internetwirtschaft, oder BVDW, der Bundesverband Digitale Wirtschaft e. V., haben derzeit keine ständige Beteiligung in

einem konstituierten, politischen Gremium, sind deshalb jedoch nicht weniger aktiv auf diesem Gebiet. So fokussiert sich eco auf die Vernetzung der über tausend internationalen Branchenmitglieder und stellt auf diese Weise eine strategische Größe dar, um mit Ideen, Forderungen oder auch Anklagen an staatliche Stellen heranzutreten. In der Initiative Europäischer Netzbetreiber (IEN) vereinen sich, wie der Name es erahnen lässt, viele relevante Kommunikationsdienstleister, etwa Vodafone oder Orange, um sich gemeinsam „insbesondere zu Fragen der Gestaltung des nationalen und internationalen Regulierungsrahmens“ zu positionieren (Initiative Europäischer Netzbetreiber (IEN) 2019). Solche Vertretungen existieren nicht nur für Großkonzerne, sondern genauso für kleine und mittelständische Unternehmen, wie etwa der Bundesverband IT-Mittelstand e. V. (BITMi) belegt. Auch diese Gruppe probiert sich, wie schon die zuvor genannten, an politischer Intervention. Dieses Ziel führt der Verband ganz offen auf der eigenen Webseite noch vor Zwecken wie „Mittelstandskommunikation“ oder „Netzwerkbildung und Synergieeffekte“ (Bundesverband IT-Mittelstand e. V. (BITMi) 2021a). Der BVDW pflegt ein ähnliches, dezentrales Konzept für teilnehmende Unternehmen mit digitalem Geschäftsmodell, legt dabei aber einen Schwerpunkt auf die Vermarktung sowie Reichweitensteigerung der Unternehmen und „des BVDW als öffentliche Bühne“, um so Botschaften zu platzieren (BVDW 2021). Insgesamt zeigt sich hier, dass sich die Bundesregierung und die Ministerien im Alltag mit einer Vielzahl gesellschaftlicher und im speziellen ökonomischer Interessenvertretungen konfrontiert sehen und alle diese Zusammenschlüsse ihre jeweils subjektiven Erwartungen an die Entscheidungsträger herantragen.

Zu diesen vorwiegend monetär getriebenen Vereinigungen gesellen sich noch Organisationen, die gemeinnützig agieren und sich hauptsächlich einer Vorstellung, etwa der des freien Internets, verschrieben haben. Solche Zusammenschlüsse arbeiten nicht unter dem Druck, den Profit der Mitglieder maximieren zu müssen und können finanzielle Interessen, die nicht immer mit ideellen, moralischen Absichten einhergehen müssen, außen vor lassen. Sie dienen aus diesem Grund eher als kritische Beobachter und als korrektiv. Zu diesem Typus gehören in Deutschland etwa die Landes- und Bundesverbände der Verbraucherzentralen, die sich dem Schutz der Verbraucherinteressen widmen und deshalb auf Missstände und undurchsichtige Geschäftsmodelle aufmerksam machen. Seit vielen Jahren sprechen die

Verbraucherzentralen Warnungen vor unsicheren Digitalprodukten aus, geben Hinweise zum Datenschutz oder helfen Anwendern dabei, sich sicher in sozialen Netzwerken zu bewegen. Indem sie zusätzlich individuelle Beratungsleistungen anbieten und stellvertretend für Verbraucher in Rechtsstreitigkeiten ziehen, zum Beispiel gegen Google oder Facebook, tragen die Verbraucherzentralen eine maßgebliche Schnittstellenfunktion zur Aufklärung der Zivilgesellschaft bei und geben ihr eine regulative, demokratische Stimme (vgl. Verbraucherzentrale NRW 2020, 18f). Auch der Chaos Computer Club (CCC) hat eine solche Stimme. Jedoch vertritt die Nichtregierungsorganisation keine Verbraucher, sondern setzt sich für Informationssicherheit und -freiheit, Datenschutz, Netzneutralität sowie Digitaletik ein und versteht sich als Beobachter des Staates (vgl. Chaos Computer Club 2021a). Dafür hat der Club einzelne Mitglieder wie Linus Neumann zu Testimonials gemacht, die dann in Fernsehen, Zeitung oder Internet über Digitalthemen sprechen und Kritik an den Maßnahmen der Bundesregierung üben. So steuern sowohl der CCC als auch die Verbraucherzentralen den oft Nutzen-getriebenen Technikdebatten einen oppositären Standpunkt bei. Indem sie dabei häufig verwandte Positionen formulieren, beispielsweise als sich CCC und VZBV in einem offenen Brief gemeinsam gegen die Uploadfilter als Teil der europäischen Urheberrechtsreform aussprachen, verleihen sie den mutmaßlichen Interessen der Privatanwender mehr Nachdruck (vgl. Chaos Computer Club 2018).

Weniger als Korrektiv denn als Interessenvertreter digitaler Grundrechte treten etwa die Stiftung Neue Verantwortung, Digitale Gesellschaft e. V. oder LOAD e. V. auf. Alle drei wieder nur exemplarischen Vereine verstehen sich als „Denkfabrik und Interessenvertretung und förder[n] die aktuellen und zukünftigen Netzbürgerinnen und Netzbürger bei der Verwirklichung ihrer Grundrechte“ (LOAD e. V. 2021a). Damit sind diese Vereine nicht weniger Lobbyisten als die Industrie- und Handelskammern oder als der VDE, jedoch streiten sie nicht für bestimmte Personen- respektive Unternehmenskreise, sondern sehen sich von idealistischen Vorstellungen getrieben. So trägt das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) die altruistische Idee bereits im Namen. Die Mitglieder widersetzen sich allen Bestrebungen, Informationstechnik zur Überwachung, zur Kriegsführung oder zur Diskriminierung von Menschen anzuwenden, damit IT nach eigener Aussage „im Dienst einer lebenswerten Welt steht“ (Forum InformatikerInnen für Frieden und

gesellschaftliche Verantwortung e. V., 2021a). Die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) folgt auch einer Maxime, in diesem Fall der Aussicht auf einen skalierbaren und praxisnahen Datenschutz sowie auf informationelle Selbstbestimmung. Dazu bewertet der Verein Datenschutzgesetze, berät die Politik oder stellt Vertragsmuster zur Verfügung, die den teils sehr mühsamen Datenschutz vereinfachen (vgl. Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) 2021). Hinzu kommen Vereine wie Transparency International Deutschland, die nicht per definitionem von Digitalisierung und Cybersicherheitsfragen angetrieben werden, aber dennoch gelegentlich mit Nachdruck in diese Felder vordringen. Denn während sich Transparency International eigentlich der Korruptionsbekämpfung widmet, berühren einige ihrer Bemühungen die Digitalpolitik. So kritisierte der Verein im Sommer 2020, dass „die mit den neuen Gesetzen verbundene Sammlung und zentrale Speicherung von Patienten- bzw. Arztgeheimnissen sehr missbrauchsanfällig ist“ (Transparency International Deutschland 2020). Gleichzeitig engagiert sich Transparency gemeinsam mit unter anderem dem Bundesverband der Deutschen Industrie (BDI), dem Naturschutzbund Deutschland (NABU) und dem VZBV in der Allianz für Lobbytransparenz, um auf die Einführung eines Lobbyregisters hinwirken zu können (Transparency International Deutschland 2021). Damit wiederum soll mehr Transparenz bei der Zusammenarbeit von Staat und Wirtschaft, ergo auch bei der Regulationen neuer und sicherer Technologien oder bei Priorisierungen von Infrastrukturen, hergestellt werden. Bei dieser Betrachtung fällt ins Auge, dass gesellschaftliche Institutionen, ob profitorientiert oder staatlich gefördert, ihrer je eigenen Programmatik folgen: Sie versuchen, möglichst dezidiert Beziehungen zu Entscheidungsträgern und Einrichtungen zu unterhalten, um die größtmögliche Wirkung generieren zu können. Dabei ist Lobbyismus kein per se negativ zu konnotierender Begriff, sondern nach Patzelt sogar ein Bestandteil von Demokratie, die sich nur mit „dem Lernen aus Erfahrungen, also in der Praxis oft dem Lernen von jenen, die ihrerseits reichlich Erfahrung haben“, fortentwickeln kann (Patzelt 2019, 29).

Die in diesem Kapitel erkundeten Repräsentanten von Ökonomie, Privatpersonen, Verbrauchern, Kindern oder Berufstätigen unterscheiden sich nicht nur hinsichtlich ihrer Top-Down- oder Bottom-Up-Naturelle, sondern adressieren korrelierende Verantwortlichkeiten. Dabei zeichnet sich ab, dass sich einige der Gruppen an den Staat wenden, um der Legislative ihre Fürbitten vorzutragen. Sie messen somit dem

Bundestag und anderen Gremien unumgänglich Geltung bei und verweisen auf die Responsibilität der Regierung für maßgebende Gesetze und Bescheide. Insbesondere die politiknahen Verbände, wie die IHKs oder Bitkom, schieben Verantwortlichkeit um, indem sie durch öffentliche Einforderungen den Ball in die Hälfte der Bundesregierung spielen. So wies der DIHK am 23. Februar 2021 in einer Pressemitteilung auf eine „Lücke im geplanten Corona-Steuerhilfegesetz hin“ (Deutscher Industrie- und Handelskammertag e. V. (DIHK) 2021). Diese Mitteilung führte aus, inwiefern der Deutsche Industrie- und Handelskammertag die Pläne der Regierung als unzureichend identifiziert und schließt mit einer Empfehlung für besagtes Steuerhilfegesetz. Der Verband lokalisierte damit die Verantwortung nicht nur beim Staat, sondern er nahm sie zumindest kommunikativ von seinen Mitgliedern. Diese machten nun die Bundesregierung zum Entscheider über den Erhalt ihrer Zahlungsfähigkeit und sahen die Ursache weniger in ihrem persönlichen Wirtschaften. Zumindest in dieser Herangehensweise sind sich lobbyistische Verbände und Korrektive wie der Chaos Computer Club oder die Verbraucherzentralen einig. Sie sehen die Verantwortung für wesentliche Weichenstellungen zumeist bei staatlichen Stellen (vgl. Chaos Computer Club 2010). Die Eigenverantwortlichkeit von Privatanwendern ist sowohl bei den Unternehmensvereinigungen als auch bei CCC oder GDD nur von marginaler Bedeutung.

Diesem politischen Lobbyismus stehen Onlinemedien wie zum Beispiel netzpolitik.org, heise.de oder golem.de mit teils bemerkenswerter Reichweite gegenüber. Solche Portale bündeln Neuigkeiten aus der Welt der Informationstechnik, testen Hard- und Software und machen auf Mängel aufmerksam. Dabei verfolgen diese Medien eigene Agenden: So nimmt netzpolitik.org insbesondere Defizite der Regulierung und Gesetzgebung unter die Lupe. Die Redakteure loten vor allem aus, „wie die Politik das Internet durch Regulierung verändert und wie das Netz Politik, Öffentlichkeiten und alles andere verändert“ (Netzpolitik.org 2021a). heise.de, golem.de und ähnliche Onlinemagazine suchen vorwiegend nach News und technischen Innovationen, die Technikinteressierte ansprechen. Dabei setzen diese Portale mehr als netzpolitik.org auf journalistische Neutralität und verstehen sich weniger als Aufsichtsregime für staatliche oder internationale Akteure (vgl. golem.de 2020). Dennoch übernehmen diese Medien, ebenso wie noch viele weitere, die Funktion der begrifflichen publikativen Gewalt. Gemeinsam mit den zuvor genannten operativen Interessenverbänden figurieren sie als

Kontrollmechanismus, als meinungstiftendes Gegengewicht gegen oktroyierte Entscheide. Insofern sind diese Einrichtungen essenzielle Kanäle des demokratischen Austauschs und zur Beteiligung an der Digitalisierung in Deutschland – und damit obligatorisch für die Breite und Diversität der Cybersicherheitskultur. Sie informieren ihr Publikum über Pflichtverletzungen sowohl seitens des Staates als auch der Wirtschaft. So fanden sich auf [golem.de](#) und [heise.de](#) am 06. März 2021 Berichte über ein neues Jugendschutzgesetz, über eine Sicherheitslücke in einem Apple-Ortungsdienst, zum Stopp des Smart-Meter-Gateway-Rollouts durch ein Gerichtsverfahren, über einen Produkttest einer smarten Brille, über Kritik zur IT-Konsolidierung des Bundes, eine Meldung zum iOS-Update 14.5, eine Warnung vor einer SMS-Betrugsmethode oder eine Warnung über ein Datenleck bei einem Zahlungsdienstleister (vgl. [golem.de 2021/heise online 2021a](#)). Es zeigt sich, dass diese Plattformen nicht nur einer Aufsichtsfunktion nachkommen, sondern sie sind politische wie thematische Filter für die Diskurse rund um Informationstechnik und Digitalisierung.

Wer in der Lage ist, Themen in der Mediengesellschaft festzulegen, verfügt über einen entscheidenden Vorteil, da er so auch das entsprechende „framing“, d. h. die Art der Darstellung, Wahrnehmung und Interpretation eines Themas, die inhaltliche Perspektive des Gegenstandes sowie die auszuschließenden Aspekte, bestimmen kann (Piontek/Kopka 2019, 240).

Die Medien, die die komplexe Informationstechnologie für die Breite der Gesellschaft nahbar und erfahrbar machen, entscheiden darüber, wie sie diesen Zugang zum Thema herstellen und den Rahmen setzen. Indem sie informieren, aber dem Leser zumeist auch einen Adressaten der Botschaft – man könnte auch sagen, einen Schuldigen – implizit oder explizit präsentieren, schreiben sie Staat wie Wirtschaft Verantwortlichkeiten zu und belegen sie mit Pflichten. Es ist unter anderem an diesen und weiteren Medien, die Digitalisierung als Chance oder als Risiko abzubilden. Ihre Wortwahl entscheidet mit darüber, ob Deutschland von der eigenen Bevölkerung als gewappnet oder als unvorbereitet wahrgenommen wird.

An einer möglichst großen Teilhabe arbeiten darüber hinaus gemeinnützige Initiativen, die Bedürfnisse einer Bevölkerungsgruppe in den Blick nehmen. So richtet die Webseite [fragfinn.de](#) seinen Auftritt auf Kinder aus, indem sowohl die Sprache als auch die Inhalte den Bedürfnissen der jüngsten IT-Nutzer entsprechen. [Checked4you.de](#) möchte Jugendliche adressieren und sensibilisiert für Cybermobbing, den Datenschutz bei

Social-Media-Accounts oder die Fallstricke rund um Messenger. Dagegen wendet sich bagso.de explizit an Senioren, liefert fassbare Informationen und fordert, „dass digitale Technologien gut handhabbar, möglichst selbsterklärend und sicher sein müssen“ (BAGSO 2021). Dabei achten die Redakteure in allen drei Fällen darauf, mit Beispielen aus der anzunehmenden Lebensrealität zu arbeiten, intellektuell nicht zu unter- oder überfordern und die Auftritte so zu gestalten, dass sie bestenfalls zum Weiterlesen animieren. Jenseits dieser altersgruppengerichteten Akteure zieht es etwa mobilsicher vor, Anwendungsfälle zu behandeln und stellt so dar, worauf es bei der sicheren Smartphone-Nutzung ankommt. In beiden Ansätzen erlaubt die Konzentration auf ein eng umrissenes Themengebiet, Kommunikationsmaßnahmen alters- und bildungsübergreifend aufzubereiten. Damit unterscheidet sich der Ansatz von den zuvor genannten, obwohl die Zielsetzung, also der Aufbau von Resilienz durch Aufklärung, die Gleiche ist.

Neben Verbänden und Vereinen, für die Cybersicherheit und Digitalpolitik den Kern ihres Engagements darstellen, setzen sich seit der Corona-Pandemie vermehrt auch die großen Gewerkschaften für ein arbeitnehmerfreundliches, aber auch sicheres Homeoffice ein (vgl. verdi 2021). Die Gewerkschaften sehen ihre Kernkompetenz auf diesem Gebiet im Schutz der privaten Daten der Angestellten sowie in der Herstellung konstruktiver und gesunder Arbeitsumfelder im heimischen Büro. Mit dieser Betrachtungsweise tragen die Gewerkschaften weitere Aspekte in die gesamtgesellschaftliche Debatte ein, die zwar nicht originär der Sphäre der Cybersicherheit entspringen, diese jedoch ebenfalls bewegen und erweitern.

Nicht zuletzt sind es Universitäten, Schulen und Kultusministerien, die entscheidend an der Qualität der Cybersicherheitskultur in Deutschland beteiligt sind. Während die Schulen vor allem einen Beitrag für die Wahrnehmung von Informationssicherheit in der Breite leisten können, sind es die Universitäten und Berufsschulen, die der digitalen Bildung Tiefe verleihen können. Die Bildungseinrichtungen haben das Potenzial, sowohl Interesse für das Fach und die Technologie zu wecken als auch ein basales Gefühl für Gefahren, Risiken und Chancen der Digitalisierung zu vermitteln. Solche Medienkompetenzen können dann im Studium, im Beruf oder im Alltag weiter ausgeprägt werden. Während sich bei den Schulen noch eine große Kluft zwischen den Bundesländern, Schulformen, aber auch zwischen einzelnen Schulen zeigt, ist das Angebot an Universitäten bereits deutlich weiter vorangeschritten. So waren im

Sommersemester 2020 etwas mehr als 225.000 Studierende im ersten Semester Informatik an mehr als 200 Hochschulen eingeschrieben (vgl. Statistisches Bundesamt 2021b, 22/Wissenschaftsrat 2020, 17). Schon hier lässt sich also eine Divergenz zwischen der Schul- und der Hochschullandschaft erkennen. Das deutsche Bildungswesen, das die digitalen Fachkräfte hervorbringen soll, sieht sich seit Jahrzehnten großer Kritik ausgesetzt. Demzufolge sei Bildung hierzulande ungleich verteilt, nicht digital und stark unterfinanziert (vgl. OECD 2020, 359). Insbesondere in dem sich schnell wandelnden Sektor der Informatik sind eine gute materielle Ausstattung, interessierte Lernende über alle Schulformen hinweg sowie eine intensive Weiterbildung der Lehrkräfte wichtig für die Ausbildung späterer Innovationstreiber. Die Lehre der Grundlagen legt das Fundament für das Verständnis von Computern, Vernetzung und Digitaltechnologie: Der Informatikunterricht „entmystifiziert Netzwerke, Datenbanken, Verschlüsselung und ebnet ihnen [den Lernenden] den Weg zum mündigen Informationsbürger“ (Friedrich et al. 2020, 11). Eine Analyse der länderspezifischen Lehrformen durch die Universität Rostock Ende 2020 zeigt, wie es um die Ausbildung dieser kommenden Digitalbürger steht. So kommen die Autoren zu dem Schluss, dass es deutschlandweit keinen einheitlichen Informatikunterricht gibt und sowohl die Quantität als auch die Qualität der Bildung innerhalb dieses Fachgebiets sehr stark schwankt. Häufig werde Informatik nur als Wahlfach oder erst in höheren Jahrgangsstufen angeboten. Ein flächendeckendes Angebot wie in anderen Naturwissenschaften, etwa der Biologie oder Physik, bestehe aktuell nicht (vgl. Friedrich et al. 2020, 10). Die Gesellschaft für Informatik kommt zu dem Schluss, dass es „noch ein weiter Weg bis zu einer nachhaltigen und verbindlichen informatischen Bildung in der Schule in allen Bundesländern“ sei (Gesellschaft für Informatik e. V. 2021, 9). Ein völlig anderes Bild zeigt sich zunächst in der Hochschulbildung. Die Informatik in ihren unterschiedlichen Ausprägungen ist ein stark nachgefragtes Studienfach. Diese Nachfrage ist „zwischen den Wintersemestern 2009/2010 und 2018/2019 um fast 75 % gestiegen“ (Wissenschaftsrat 2020, 18). Der Wissenschaftsrat stellt fest, dass die Interdisziplinarität des Informatikstudiengangs sowie der verwandten Studienfächer wie etwa „Eingebettete Systeme, Visual Computing oder Human Computer Interaction“ ansteigt (Wissenschaftsrat 2020, 22). Wenngleich in nahezu allen Belangen Wachstum zu registrieren ist, zeigt sich bei genauerer Betrachtung, dass die Zahl der Studierenden im Verhältnis zur Bevölkerungsgröße nicht wirklich groß beziehungsweise noch ausbaufähig ist; Finnland

oder die Niederlande liegen in diesen Kategorien deutlich weiter vorn (vgl. Wissenschaftsrat 2020, 23f). Und auch die Quote der Studienabbrüche stagniert auf sehr hohem Niveau; knapp 45 % der Bachelorstudierenden bringen ihre Ausbildung nicht zu Ende (vgl. Wissenschaftsrat 2020, 23f). Daher ist anzunehmen, dass die Spezialisierung des Angebots nicht gleichbedeutend damit ist, dass den Erwartungen und dem Leistungsvermögen der Studienanfänger zielgenauer entsprochen wird. Obwohl in den vergangenen Jahren mit jedem Semester mehr Einschreibungen für Informatikstudiengänge zu verzeichnen waren, wuchs die Zahl der Lehrenden um ein Vielfaches langsamer (vgl. Wissenschaftsrat 2020, 27). Daraus folgt, dass jeder Lehrende mehr Studierende unterrichten und durch ihr Studium begleiten muss, womit die Betreuungskapazitäten für jeden einzelnen Studierenden sinken. Der Kreis schließt sich, wenn man in Augenschein nimmt, wie viele der mehr als 225.000 Informatikstudierenden einen Lehramtsabschluss anstreben. Lediglich 1578 Neustudierende möchten nach Erkenntnissen des Statistisches Bundesamt über das Sommersemester 2020 in Zukunft Informatik unterrichten (vgl. Statistisches Bundesamt 2021b, 23). Stellt man dieser Zahl die 8.062.083²⁰ Schülerinnen und Schüler an berufs- und allgemeinbildenden Schulen gegenüber, ist der Weg zu einem flächendeckenden Informatikunterricht durch qualifiziertes Fachpersonal noch ein weiter (vgl. Destatis 2020). Dieser aber ist eine Voraussetzung dafür, Folgegenerationen anzuleiten, für Informationstechnik zu begeistern und sie auf eine berufliche oder universitäre Ausbildung vorzubereiten.

Die Fülle der ausgewählten zivilgesellschaftlichen Beispiele zeigt im Wesentlichen zweierlei: Erstens, und hier liegt die Stärke der nicht kommerziellen Verbände und Vereine, dokumentieren die obigen Beispiele eine große Diversität der Interessenvertretungen, ihrer Mitglieder und ihrer Zielgruppen. Damit bilden sie vielzählige Perspektiven ab und demokratisieren die Entscheidungsfindung. In der Reibung mit Entscheidungsträgern und den ökonomisch motivierten Verbänden bringen sie eine zwingende Beteiligung großer Gesellschaftsgattungen ein. Da lediglich eine möglichst gleichwertige Partizipation aller Betroffenen eine debattenorientierte Cybersecurity Culture auszeichnet, könnte nach diesen Zeilen der Eindruck entstehen, dass eine solche Ausgewogenheit in Deutschland besteht. Das ist allerdings nur eingeschränkt der Fall,

²⁰ Eigene Berechnung anhand der Daten des Statistischen Bundesamts; Gesamtschülerzahl abzüglich der Vorklassen, Schulkindergärten und Grundschüler

denn zweitens zeigte sich, dass die Einflussnahme der Wirtschaft auf die Politik oder Regierungsorganisationen in verschiedenen Gremien institutionalisiert ist, wohingegen gemeinnützige Interessengruppierungen zumeist nur temporäres oder unregelmäßiges Mitspracherecht erhalten. Daher kann die dominante Wirkkraft der Ökonomie bei regulativen Entscheidungen nicht geleugnet werden. Erschwerend kommt hinzu, dass einige der großen Organisationen wie etwa die Bundeszentrale für politische Bildung mit staatlicher Förderung unterfüttert sind, teils sogar unter staatlicher Schirmherrschaft stehen und dadurch nicht völlig unabhängig agieren können. Indem diese von Bund oder Land gestützten Gruppen den öffentlichen Raum mit Publikationen und Meinungsbeiträgen anfüllen, verkleinert sich durch die Konkurrenz das Publikum für unabhängige nicht-gewerbliche Organisationen, sodass diese potenziell weniger Gehör bekommen.

An dem Punkt, an dem die staatliche Regulation nicht ausreicht oder das Zutun der Anwender erforderlich ist, setzt die Arbeit wiederum anderer gesellschaftlicher Interessenverbände ein. BAGSO, mobilsicher oder andere versuchen sich an der Sensibilisierung und Aufklärung großer Bevölkerungsgruppen – eine Hilfe zur Selbsthilfe. Wenngleich sie die Verantwortung des Staates ebenfalls nicht ignorieren, legen sie den Nutzern Werkzeuge in die Hand, um Informationstechnik selbstbestimmt bedienen zu können und sich dort emanzipieren zu können, wo der staatliche Schutz endet. Indem sie die technischen wie legislativen Umstände als weitestgehend gegeben ansehen, verhelfen solche Initiativen den Rezipienten zu Mündigkeit. Sie multiplizieren Wissen und ermöglichen vielen Laien auf diese Weise erst eine Teilhabe an Technik- oder Sicherheitsdiskursen. Nebenbei erlangen die Lernenden demokratische Verantwortung. Denn sobald sie befähigt sind, mittels Wissen einen Diskurs zu verfolgen und daran teilzunehmen, also ihres „in einer intelligiblen Ordnung der Dinge bestimmbaren Daseins bewußt“ sind, liegt auch die Verpflichtung zur Teilnahme bei ihnen – selbst im Moment der gewählten Nichtteilnahme (Kant 2011, 57).

Anhand dieser exemplarischen Auswahl gesellschaftlicher Stellvertreter ist abzulesen, wie vielfältig das Spektrum des Engagements im Bereich der Cybersicherheit in Deutschland ist. Dabei offenbart sich, dass die Organisationen diverse Interessen verfolgen und korrelierend auf je andere Schwerpunktadressaten für ihre Anliegen abzielen. Indes ist nicht nur die Quantität der Verbände auffällig, die ihre Intentionen primär über politischen Einfluss geltend machen wollen, sondern auch das Gewicht, das

diesen Gruppen zugesprochen wird. Sie sind in wiederholtem, institutionalisiertem Austausch mit staatlichen Verantwortlichen, um ihre Positionen mit Dringlichkeit zu versehen und sie gegenüber anderen Motiven zu priorisieren. Damit verfügen sie im Gegensatz zu den übrigen Formen gesellschaftlichen Engagements in der Cybersicherheit über einen unmittelbaren Kanal zu legislativen und exekutiven Administrationen. Zusätzlich stellt sich heraus, dass sich die aufgezählten Organisationstypen zumeist entweder an den Staat oder zum Beispiel mittels Sensibilisierungskampagnen direkt an Endanwender richten und diesen dadurch verschiedene Verantwortungsqualitäten zuweisen. Währenddessen spricht sich nur wenig zivilgesellschaftliches Eifer gegen Produzenten oder Ökonomie aus.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	O	O			O		O	O		O	

Zwar liegt das größte Engagement darin, die Politik zu beeinflussen und so insbesondere den regulatorischen Rahmen im eigenen Sinne zu setzen. Jedoch können diese Einflüsse an dieser Stelle inhaltlich nicht bewertet werden, da sie größtenteils undokumentiert bleiben. Die Arbeit der sensibilisierenden Akteure wie mobilsicher, klicksafe oder den Bildungseinrichtungen ist als wichtiger Beitrag zur Entwicklung einer handlungsfähigen Digitalgesellschaft sichtbar, beschränkt sich jedoch auf die Beratung und Anleitung der Bedienenden; die Sicherung durch technische Maßnahmen spielt hier nahezu keine Rolle. Während sich also manche Vereine tatsächlich für eine Sensibilisierung und Weiterbildung jedes einzelnen Anwenders einsetzen, um ihnen eine souveräne Verwendung des Internets zu erlauben, betrachtet ein Großteil der Organisationen Staat und Politik als Werkzeug, um Partikularinteressen durchsetzen zu können. Dabei arbeiten die Akteure mit höchst subjektiven Narrativen dessen, was wichtig und sinnvoll ist. Während der BDI etwa in zahlreichen Publikationen und Statements Investitionen, Innovationsprogramme und Wirtschaftsreformen für die Industrie forderte, veröffentlichte der CCC eine umfassende Stellungnahme zum IT-SiG 2.0, äußerte sich zur Speicherung von Biometriedaten und insistierte auf den Abbau sogenannter Staatstrojaner (vgl. Bundesverband der deutschen Industrie e. V. (BDI) 2021/Chaos Computer Club 2021c). Dennoch verlangen beide Vereine – und dieses Ansinnen ist bei näherer Betrachtung zumeist anzutreffen – Fortschritt statt Stagnation oder Rückbau. Die gesellschaftlichen Interessenorganisationen in

Deutschland streben nach Progression, wenngleich die Auffassung ebendieser sehr unterschiedlich sein kann. Sie benennen überwiegend Chancen und nutzen Risikobeschreibungen als Mittel, um die gleichzeitigen Möglichkeiten deutlicher hervorzuheben. Obwohl einige Institutionen auszumachen sind, die sich selbst als Mahner verstehen, unter anderem die Verbraucherzentralen, der CCC oder netzpolitik.org, und stetig auf Risiken und Sicherheitslücken hinweisen, ist die Summe der Einrichtungen als eher chancenorientiert zu bewerten. Insbesondere die Vertreter der Wirtschaft betonen, welche Potenziale bei einer in ihren Augen richtigen Digitalpolitik geweckt werden könnten und sehen sich im Vorteil, wenn sie auf Verbesserungen hinweisen, statt das Schlaglicht unumwunden auf Defizite zu lenken.

2.3.3 IT-Sicherheitsgesetz

Das BSI-Errichtungsgesetz (BSIG) von 1990 schrieb dem Bundesamt für Sicherheit in der Informationstechnik die Rolle einer Bundesoberbehörde unter dem Bundesinnenministerium zu. Weil das BSI zudem von Beginn an mit zahlreichen Schnittstellenaufgaben betraut wurde, um die Informationstechnik des Bundes zu schützen, schuf man unmittelbar mit der Gründung eine Zentralstellung für die Behörde. Zu den damals zementierten und seitdem weitreichend expandierten Pflichten und Funktionen gehören unter anderem die „Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik“, die „Zulassung von informationstechnischen Systemen“ sowie die „Unterstützung a) der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben, b) der Verfassungsschutzbehörden bei der Auswertung und Bewertung von Informationen“, aber genauso die „Beratung der Hersteller, Vertreiber und Anwender“ (Bundesgesetzblatt 1990, 2834). Es wird offenbar, dass die Behörde bereits von Beginn an als Sammelbecken für allerlei Aufgaben der digitalen Sicherheit installiert wurde. Zur Klientel gehören bis heute Unternehmen, Bürger, Nachrichtendienste, Politiker sowie andere Amtsstellen.

Die Kompetenzen, Befugnisse und Richtlinien für die Handlungsfähigkeit des BSI sind also in demokratischen Leitplanken festgeschrieben. Das bedeutet, dass das BSI als Teil der staatlichen Exekutive durch die weiteren Gewalten der Bundesrepublik mit Aufgaben betraut, aber auch kontrolliert wird. Diese Aufgaben, Kompetenzen und Zuständigkeiten sind im BSI-Gesetz determiniert. Ursprünglich formuliert am 17.12.1990 als Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik wurden die Paragraphen im Laufe der Jahre durch weitere

Artikelgesetze stetig entwickelt und abgeändert. So erfuhren die Regelungen 2009 mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes eine bedeutende Revision, die die Behörde zur zentralen Meldestelle für IT-Sicherheitslücken machte oder dem BSI die Möglichkeit verlieh, Warnungen vor Schwachstellen in Informationstechnik öffentlich auszusprechen (vgl. Bundesgesetzblatt 2009, 2822ff). 2015 erweiterte die Legislative mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, dem sogenannten IT-Sicherheitsgesetz, diese Kompetenzen nochmals deutlich. Dort wurden beispielsweise Betreiber Kritischer Infrastrukturen verpflichtet, bei Störungen ihrer Systeme an das BSI zu melden. Außerdem befähigt die rechtliche Regelung das BSI, Informationstechnik anlasslos auf ihre Sicherheit zu untersuchen (vgl. Bundesgesetzblatt 2015, 1325ff). Am 18. Mai 2021 dann wurde das BSI-Gesetz durch das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, oft als IT-Sicherheitsgesetz 2.0 bezeichnet, erneut ausgeweitet und kontrovers diskutiert.

Das am 17. Juli 2015 beschlossene IT-Sicherheitsgesetz umfasst 17 Aufgaben, die im Verantwortungsbereich des BSI liegen und damit bereits zehn Betätigungsfelder mehr als zur Gründung des Amtes. Diese machen das Bundesamt für Sicherheit in der Informationstechnik zur hauptverantwortlichen Institution für die Gefahrenabwehr der IT des Bundes. Das BSI hat den Auftrag, Soft- sowie Hardware zu testen und darauf basierend Warnungen beziehungsweise Empfehlungen zu veröffentlichen (vgl. Bundesgesetzblatt 2015, 1325). Daran knüpft die Direktive, „Kriterien, Verfahren und Werkzeug[e]“ zu entwickeln, die der Prüfung von IT-Sicherheit dienen (Bundesgesetzblatt 2009, 2822). So obliegt es dem Bundesamt, die Relevanz von Sicherheitstechnologien einzuordnen, Bewertungsattribute festzuschreiben und grundlegende technische Vorrichtungen zur Erhöhung der IT-Sicherheit bereitzustellen. Das bedeutet, das BSI besitzt regulierende Kompetenzen und kann mit einer strengeren Richtlinie oder mit verhaltenen Vorgaben markieren, wo die einzuhaltenden Grenzen von Informationssicherheit liegen.

Seit dem IT-Sicherheitsgesetz von 2021 ist das BSI die „Nationale Behörde für die Cybersicherheitszertifizierung“ nach EU-Verordnung 2019/881 und damit befähigt, digitale Angebote zu kennzeichnen, die gewisse Kriterien einhalten (Bundesgesetzblatt 2021, 1131). Das bedeutet, dass das BSI einerseits selbst Produkte oder Dienste zertifizieren, aber auch sogenannte Konformitätsbewertungsstellen

ernennen kann, die dann stellvertretend solche europäischen Sicherheitszertifizierungen vornehmen (vgl. Bundesgesetzblatt 2021, 1131f). Mit dieser Änderung des Paragraphen 9 geht einher, dass das BSI Betreibern Kritischer Infrastruktur den Einsatz von Komponenten untersagen kann, die die Behörde als kritisch einstuft. Das geschieht zum Beispiel, wenn „der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird“ oder wenn anzunehmen ist, dass das Bauteil „nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland“ hat (Bundesgesetzblatt 2021, 1132). Dieser Passus – in manchen Medien gar „Huawei-Klausel“ genannt – schafft die Grundlage, um beispielsweise Netzwerkkomponenten des chinesischen Herstellers Huawei aus dem deutschen 5G-Mobilfunknetz auszuschließen und erlaubt dem Bundesinnenministerium, spezifische Hersteller grundsätzlich als „nicht vertrauenswürdig“ zu deklarieren (Bundesgesetzblatt 2021, 1133/heise online 2020a). Auf Verbraucherseite trägt der Paragraph die Verpflichtung an das BSI heran, ein IT-Sicherheitskennzeichen zu entwickeln, das Produkte und Dienste kennzeichnet, die „für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen“ erfüllen (Bundesgesetzblatt 2021, 1133). Wenn diese freiwillige Selbsterklärung des Herstellers erfolgreich das Antragsverfahren durchlaufen hat und die „Herstellererklärung plausibel“ ist, „ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt [...] anzubringen“ (Bundesgesetzblatt 2021, 1134). Mit dem Kennzeichen sollen Kunden erkennen können, ob ein Produkt wesentliche Sicherheitseigenschaften besitzt und für ihre individuellen Anforderungen geeignet ist, sodass sie nicht bereits mit dem Kauf anfällige Hard- und Software erhalten.

Gleichzeitig ergänzte die Novelle 2021 auch die Befugnisse zur Warnung der Öffentlichkeit: Das BSI kann nun vor Schadprogrammen, vor Sicherheitslücken oder vor unbefugten Zugriffen „unter Nennung der Bezeichnung und des Herstellers“ warnen, wenn „Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen“ (Bundesgesetzblatt 2021, 1126). Neu hieran ist insbesondere, dass das BSI aktivere Autorisierungen als bislang erhält. So können als Mittel zur Schwachstellenerkennung sogenannte Portscans „an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen“ durchgeführt werden, wenn der Verdacht besteht, dass

Strukturen ungeschützt oder gefährdet sein könnten (Bundesgesetzblatt 2021, 1127). Einerseits verleiht das dem Bund mehr Schlagkraft gegen Cyberkriminalität, andererseits führen Kritiker an, dass die Kompetenzen des BSI zu weit gingen und den Datenschutz nicht ausreichend achteten. Grünen-Politiker von Notz mahnte Anfang 2021 an, dass das BSI „zu einer Art Ersatznachrichtendienst“ ausgebaut werde (Bündnis 90/Die Grünen 2021). Mithin unterstützt Paragraf 11 diese Annahme, denn dieser schränkt das Fernmeldegeheimnis und damit Grundrechte nach Artikel 10 des Grundgesetzes ein (vgl. Bundesgesetzblatt 2021, 1135). Dabei gehen die Befugnisse weiter: Das BSI kann von diesem Zeitpunkt an Methoden verwenden, die Hackern und Kriminellen vortäuschen, ihr Angriff sei erfolgreich gewesen, damit die Bundesrepublik Informationen über Angriffsverhalten oder neue Schadsoftware erhält. Mit diesen Honeypots kann das Bundesamt gezielt Fallen stellen und damit Konter gegen Aggressoren vornehmen (vgl. Bundesgesetzblatt 2021, 1127f).

Zugleich bestellt die gesetzgebende Gewalt das BSI, um die informationstechnischen Schnittstellen Kritischer Infrastruktur zu schützen. Hier eingeschlossen ist die „Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit [...] im Verbund der Privatwirtschaft“ (Bundesgesetzblatt 2009, 2822). Dieser Paragraf verpflichtet Betreiber solcher Infrastrukturen, Störungen oder voraussichtliche Störungen an das BSI zu melden. Das Bundesamt ist wiederum angewiesen, Informationen transparent mit Betreibern und Aufsichtsbehörden zu teilen und in eintretenden Störfällen bei der Problembehebung unterstützend tätig zu werden. Zum 1. Mai 2023 sind die Betreiber außerdem zum „Einsatz von Systemen zur Angriffserkennung“ gezwungen (Bundesgesetzblatt 2021, 1129). Ferner kann das BSI seit 2021 von ihnen „die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen“ (Bundesgesetzblatt 2021, 1130). Teilweise werden die Pflichten der Betreiber Kritischer Infrastruktur auch auf „Unternehmen im besonderen öffentlichen Interesse“ übertragen (Bundesgesetzblatt 2021, 1123). Dazu gehören insbesondere Unternehmen, die für die deutsche Wirtschaft unverzichtbar sind.

Überdies umfassen die vielzähligen Aufgaben seit 2015 auch die Unterstützung des Bundesbeauftragten für den Datenschutz. So hat das Bundesamt explizit die „Regelungen des Bundesdatenschutzgesetzes anzuwenden“ (Bundesgesetzblatt 2015, 1326). Dazu gehört, dass persönliche Daten, die

beispielsweise bei der Auswertung von Protokolldaten anfallen, „nach erfolgtem Abgleich sofort und spurlos gelöscht werden“ (vgl. Bundesgesetzblatt 2009, 2823). Zudem muss das BSI im Sinne öffentlicher Transparenz einen jährlichen Bericht verfassen und das Bundesministerium des Innern und für Heimat über alle Belange in Kenntnis zu setzen. Die Neuerung 2021 definierte Ausnahmen von dieser strengen Auslegung: So kann in besonders dringlichen Fällen die Pseudonymisierung personenbezogener Informationen aus Protokolldaten aufgehoben oder die Betreiber von Telekommunikationsdiensten zur Auskunftserteilung verpflichtet werden, sofern dieses Wissen „zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes“ notwendig ist (vgl. Bundesgesetzblatt 2021, 1125). Das schließt auch ein, dass per Anordnung Datenverkehr direkt an das BSI umgeleitet werden muss und das BSI uneingeschränkter Zugang für bis zu drei Monate erhält (vgl. Bundesgesetzblatt 2021, 1128). Gleichzeitig schränken noch geltende Paragraphen der Fassung von 2009 die Unterstützung strafverfolgender Behörden und nachrichtendienstlicher Stellen umgehend ein und autorisieren das BSI ausschließlich, „Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen“ (Bundesgesetzblatt 2009, 2822). Dies schließt ein, dass das BSI berechtigt wird, Informationen über Sicherheitsrisiken zu sammeln, zu bewerten und mit „andere[n] Stellen“ zu teilen (Bundesgesetzblatt 2009, 2823).

Seit März 2002 fächert das BSI sein Informationsangebot nach Zielgruppen auf und bedient nachfolgend neben öffentlichen Verwaltungen, Bundesinstitutionen und wissenschaftlichen Einrichtungen auch Privatanwender (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019b). Mit seinem Angebot stellt das BSI auf einer eigenen Webseite, bei Veranstaltungen, mit Print-Publikationen, aber auch bei Social Media und YouTube, Inhalte bereit, die sprachlich und inhaltlich an solche Bediener gerichtet sind, die über kein Vorwissen oder lediglich über basale Kenntnisse in der Informationssicherheit verfügen. Der Koalitionsvertrag der Bundesregierung aus dem Jahr 2017 fügt diesem Spektrum hinzu, „den Verbraucherschutz als zusätzliche Aufgabe des BSI [zu] etablieren“ (Bundesregierung 2018, 44). Schließlich veranlasst das IT-Sicherheitsgesetz 2.0 2021 das BSI, sich im digitalen Verbraucherschutz zu engagieren (vgl. Bundesgesetzblatt 2021, 1123). Dazu erweiterte das Amt die Maßnahmen der Präventionsarbeit, etablierte eine Marktbeobachtung, führte das genannte IT-

Sicherheitskennzeichen ein und schuf mehr als 20 Stellen in einem neuen Fachbereich (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021b).

Abseits der Rechte und Pflichten, die das Gesetz wiederholt ordnet, haben die neuen Vorschriften symbolische Wirkung: Sie machen deutlich, dass die digitale Infrastruktur ebenso bedeutsam und schutzbedürftig ist wie der analoge Raum und der Staat seiner Sicherheitsverantwortung nachzukommen versucht. Denn wie in 1.4.1 festgestellt, schließt diese staatliche Verpflichtung ein, Sicherheit nicht nur im Sinn von Unversehrtheit herzustellen, sondern auch als Gewissheit (vgl. Bauman 2000, 216). Dieses Stabilitätsversprechen findet sich auch im IT-Sicherheitsgesetz wieder und vervollständigt ein Narrativ, das die Grundlage für Planungssicherheit, wirtschaftliches Handeln und die Integrität von Informationsaustausch darstellt. Schon der ursprüngliche Gesetzestext mit der Gründung des BSI 1991 trägt die Erzählung von einer unsichtbaren Bedrohung in sich, um welche man sich jetzt auf nationaler Ebene kümmern werde. Damit öffneten die Verantwortlichen eine zusätzliche Gefahrendimension und nahmen im selben Schritt die Last auf sich. Der Staat konnte sich durch das Gesetz als Aufpasser positionieren, der den Status quo zu erhalten versuchte. Dieser Mechanismus greift auch in den redigierten Fassungen, beispielsweise wenn die Legislative ankündigt, ungeschützte Systeme künftig beobachten und die Betreiber warnen zu wollen. Das Gesetz beschreibt damit, dass Betreiber von Telekommunikationssystemen häufig Schuld an Vorfällen tragen, der Staat die Aufsicht haben sollte und Abhilfe schaffen kann. In dieser Erzählform etwa werden Portscans zu einem notwendigen Arrangement, um das identifizierte Problem zu lösen. Wenn nun der digitale Verbraucherschutz und offensive Befähigungen den Aufgaben des BSI hinzugefügt werden, verdichtet das Gesetz seine intrinsische Erzählung eines passiven, schutzbedürftigen Endanwenders sowie einer Exekutive als handelnde Schlüsselfigur, die sich nicht lediglich als reagierende Instanz versteht, sondern entschlossen Lösungen herbeiführt.

Das IT-Sicherheitsgesetz ist nicht nur ein legislativer und ein symbolischer, sondern ebenso ein medialer Akt, der einem überarbeiteten Sicherheitsvorhaben eine gesellschaftlich-kommunikative Schicht verleiht. Bereits seit 2019 kursierten Entwürfe und Auszüge des zuletzt erschienenen Gesetzestextes, die die Öffentlichkeit diskutierte. So hob das ZDF hervor, dass man mit dem IT-SiG in der Lage sei, Huawei aus dem deutschen Mobilfunknetz auszuschließen. In der entsprechenden Meldung ist die Rede von einer neuen möglichen „Prüfung auf politische Vertrauenswürdigkeit“.

Währenddessen beklagte der Chaos Computer Club kurz darauf ebendiesen § 9 und warf der Politik „Hilflosigkeit, Strategielosigkeit und Ahnungslosigkeit“ vor (ZDF 2020/Chaos Computer Club 2021b). Der Deutschlandfunk kritisierte den schwerfälligen Legislaturprozess (vgl. Deutschlandfunk Kultur 2021). Und der Bitkom sprach im April 2021 gar von einem Gesetz mit „fragwürdigem Mehrwert für die IT-Sicherheit“, mit dem „Kollateralschäden in Kauf genommen“ würden (Bitkom 2021b). Ein ähnliches Bild ergaben die Debatten im Bundestag: Die Große Koalition stimmte für das Gesetz, wogegen die Opposition geschlossen gegen die Reform des IT-SiG war. Manuel Höferlin, FDP, störte sich bei der ersten Lesung des Gesetzestextes vor allem an der anhaltenden Abhängigkeit des BSI und forderte die Abkopplung vom BMI:

Das BSI gerät zunehmend in die Schere zwischen Schließen von Sicherheitslücken und [...] Offenhalten von Sicherheitslücken, um Staatstrojaner, Online-Durchsuchungen et cetera weiter durchsetzen zu können. [...] Nehmen Sie das BSI endlich aus dem BMI raus (Bundestag 2021a).

Diese Geschichten, etwa von neuen Möglichkeiten, um gegen ausländische Interessen vorzugehen; von einer unzureichenden Sicherheitspolitik bis hin zu den Vorwürfen, der Staat nehme mit dem Gesetz Begleitschäden in Kauf und das BSI halte Schwachstellen bewusst offen, können auf drei wesentliche Narrative heruntergebrochen werden:

- 1. Deutschland hat nun ein Gesetz, das wirksam sichtbare Mängel angeht.*
- 2. Die Gesetzgebung verläuft zu langsam und wird zu wenig fachlich geführt, ähnlich wie in anderen Bereichen des Technologie- und Infrastrukturausbaus.*
- 3. Der Staat handelt vorsätzlich zum Nachteil seiner Bevölkerung, indem er Hintertüren für Sicherheitsbehörden einbaut und ein Gesetz ohne Mehrwert für Anwender erlässt.*

Diese Erzählweisen zeigen: Die Ebene der technischen oder juristischen Regulierung wurde längst verlassen. Gemein haben diese publik vorgetragenen Positionen, dass sie performative, gesprochene Akte sind, die in Anlehnung an Balzacqs Securitization eine Sicherheitswirklichkeit konstruieren, welche sich nicht am tatsächlichen Gesetzestext aufhängt. Dieses heterogene Gemisch aus Erzählungen hinterlässt den Nachgeschmack eines Pyrrhussiegs, bei dem zwar Fortschritte für die Sicherheit errungen, aber dafür Verluste für die individuelle Freiheit eingefahren wurden. Das wiederum kann in Zeiten ohnehin schon großer Skepsis gegenüber Staat und Regierung das Misstrauen befeuern. Simultan verhindert der gesäte Argwohn eine positive Konnotation der neuen Möglichkeiten zur Absicherung.

Das Bundesamt für Sicherheit in der Informationstechnik wird auf Grundlage der Gesetzesänderungen 2009, 2015 und schließlich 2021 zur zentralen Meldestelle für IT-Sicherheit in Deutschland (vgl. Bundesgesetzblatt 2009, 2822). Das hat zur Folge, dass das BSI von allen Behörden, öffentlichen Institutionen und Kritischen Infrastrukturen über jegliche relevanten Vorgänge der Sicherheit der Informationstechnik informiert werden muss. Nachrichtendienstliche Stellen, wie der Bundesnachrichtendienst oder der Verfassungsschutz werden von diesem Paragraphen ebenso tangiert wie gleichrangige Bundesbehörden oder sogar Ministerien. Auf diese Weise laufen bundesweite Erkenntnisse zur Informationssicherheit gebündelt in Bonn auf. Die oben aufgezählten juristischen Bestimmungen geben die zentrale Bedeutung des BSI für die IT-Sicherheit des Bundes, aber auch für die übrigen Akteure der Informationssicherheit in Deutschland wieder.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	O		O	O		O		O			O

Zugleich sind diese Ermächtigungen klar eingeschränkt, sodass militärische Cyberangriffe, Spionage oder die Entwicklung von Angriffsvektoren nicht im Geschäftsbereich des BSI, sondern bei Bundesnachrichtendienst, Bundeswehr oder dem Militärischen Abschirmdienst verortet und insgesamt nur zurückhaltend statthaft sind. Allen voran aber die Reform des IT-Sicherheitsgesetzes von 2021 stärkt die Relevanz des BSI, indem das Gesetz wichtige Kompetenzen, wie die Einsicht in Protokolldaten oder die Legitimierung zu Portscans, in diesem Bundesamt zusammenträgt. Gleichzeitig wurden damit andere Protagonisten der IT-Sicherheit, beispielsweise Betreiber Kritischer Infrastrukturen, mit mehr Pflichten beladen, die dem BSI oder verwandten Behörden die Aufsicht erleichtern. In Summe bezwecken alle angeführten Maßnahmen, dass Sicherungsaktionen wirkungsvoller, zeitgerechter und professioneller umgesetzt werden können; Aktionismus oder eine allzu extrinsisch getriebene Agenda lassen sich nicht erkennen. Darin drückt sich aber genauso aus, dass technische Lösungen im Vordergrund stehen und die Akteure trotz aller Neuerungen zuvorderst auf veränderte Aufgabenstellungen reagieren, statt Informationssicherheit als Innovationstreiber zu deklarieren.

2.3.4 Die Lage der IT-Sicherheit in Deutschland 2019–2021

Der Bericht über die Lage der IT-Sicherheit in Deutschland erscheint alljährlich und wird vom BSI erstellt und herausgegeben. Das je 80- bis 100-seitige Papier umfasst den jeweiligen Berichtszeitraum von Juni bis Mai und wurde als Report über Cybervorfälle, aber auch als Arbeitsnachweis des BSI angelegt. Es gibt zugleich Veränderungen, Trends und Prognosen zur Sicherheitsdimension aus wie auch strukturelle und strategische Richtungsänderungen der IT-Behörde. Der Lagebericht ist ein bemerkenswertes Untersuchungsobjekt, weil er zugleich objektivierte Daten enthält, die die Lage der Cybersicherheit in Deutschland spiegeln, aber auch strategische Botschaften trägt, die eng mit den zusammengetragenen Informationen verwoben sind. Zu Beginn eines jeden Berichts steht zum Beispiel das Vorwort des Ministers, welches als Lob an das BSI, aber auch als Träger politischer Aussagen fungiert. Während des Kabinetts Merkel IV 2019 und 2020 finden sich hier Ausblicke in die Zukunft der deutschen Cybersicherheit und Ankündigungen davon, was das BSI oder der Minister vorhaben. 2021 dagegen, zum Ende der Legislaturperiode, steht hier ein Blick auf die Leistungen der zurückliegenden Jahre, sodass sich anhand des Dokuments selbst politische Zyklen ausmachen lassen.

Im Berichtsteil setzt das BSI stets auf eine Zweigliederung des Reports: Die erste Hälfte des Berichts etwa führt die Bedrohungen des vergangenen Beobachtungszeitraums aus. Dabei gehen die Ersteller auf mögliche Ursachen für Verschiebungen ein oder erläutern gegebenenfalls Motive der Tätergruppen. Die zweite Hälfte listet dann auf, welche Leistungen das BSI im gleichen Zeitraum für die Adressatengruppen Staat, Wirtschaft und Gesellschaft erbracht hat, um diesen Gefährdungen zu kontern. Im Lagebericht deduziert das BSI seine Bedrohungsbewertung jeweils aus dem Rückblick. Auf 24 bis 30 Seiten blicken die Autoren zurück auf das Berichtsjahr, stellen die Auffälligkeiten dar und beschreiben die Gefahr, die darin lag oder liegt. Sie unterstützen ihre Interpretation, indem sie Zahlen und Fakten anführen, die zumeist in Grafiken und Diagrammen aufbereitet werden. Der Argumentationsstrang schließt in einem realen Fallbeispiel aus dem Berichtsjahr, das die Theorie begreiflich macht. Der Lagebericht 2019 etwa widmet sich unter anderem dem Phänomen Distributed Denial of Service. An dieser Stelle führt das BSI zunächst aus, was DDoS bedeutet und was die Konsequenzen dieses Angriffsszenarios sein können. Schließlich kommen die Autoren auf den Grund zurück, weshalb explizit DDoS-Angriffe in den Bericht aufgenommen

wurden. Demnach mache „die stetige Spezialisierung bei der Ausführung von Angriffen durch Anwendung neuer Angriffsvektoren [...], durch zielgerichtete Zusammensetzung von DDoS-Angriffen (Multivektor-Attacken) oder durch den Einsatz neuer Angriffswerkzeuge (DDoS aus der Cloud)“ DDoS-Angriffe wirkungsvoller und damit noch attraktiver für die Täterseite (Bundesamt für Sicherheit in der Informationstechnik 2019a, 19). Dem BSI zufolge seien 59 % aller DDoS-Vorfälle Ende 2018 sogenannte Multivektor-Attacken gewesen und ebenfalls 59 % der Angriffe erfolgten mittels Cloud-Servern, die eigens für diesen Zweck gekapert wurden (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a, 19).

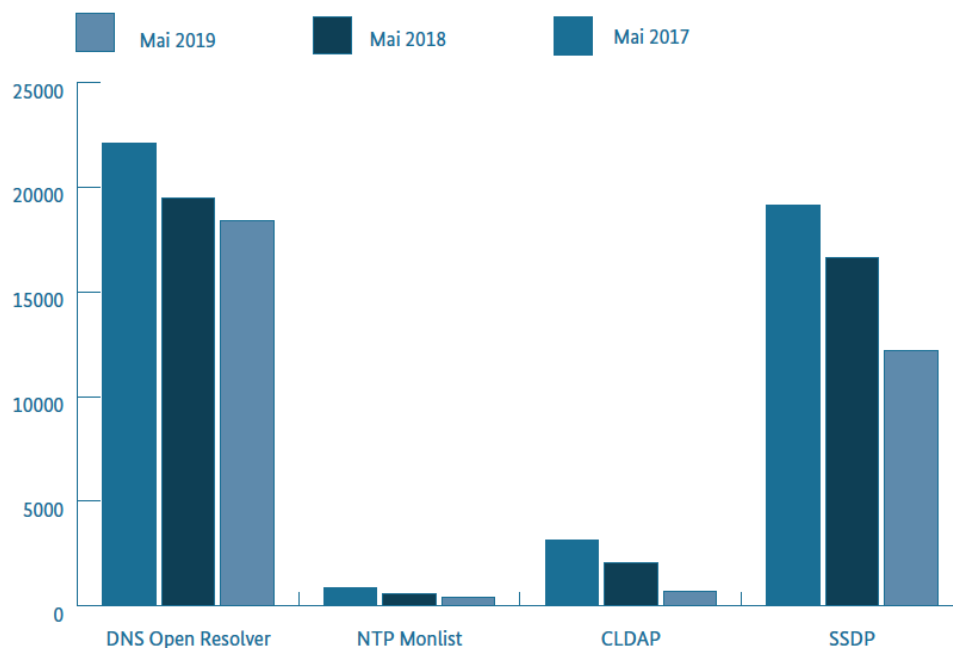


Abbildung 05 BSI, europol, security-insider

Abbildung 8: Darstellung der Angriffsvektoren von Multivektor-DDoS-Attacken (Bundesamt für Sicherheit in der Informationstechnik 2019a, 19)

Ergänzend zu diesen Daten stellt das BSI in einem Balkendiagramm dar, welche die häufigsten Angriffsvektoren sind und wie sich ihre Verbreitung in den vergangenen Jahren verändert hat. Das Themenfeld DDoS schließt mit einer Einordnung der Statistiken, indem die Schreiber erklären, dass erst die Cloud-Anbindung von DDoS-Attacken die Leistungsfähigkeit der Methode potenziert und somit ermöglicht, DDoS-as-a-Service, also DDoS als bezahlbare Dienstleistung, für Laien anzubieten. Das mache die Angriffstechnik für einen, wenn auch illegalen, Massenmarkt verfügbar (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a, 20). 2020 beziehen sich die Berichterstatter auf den Bericht von 2019 und zeigen, dass der Anteil von Multivektor-Angriffen auf 65 % gestiegen ist. Zudem nennen sie die noch junge Methode des Carpet

Bombing als Werkzeug für Täter, die Schutzmaßnahmen der Internetprovider zu umgehen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 29f). 2021 stellt der Berichterstatter an gleicher Stelle einen Zusammenhang zwischen der rascheren Digitalisierung aufgrund von COVID-19 und der größeren Angriffsfläche für DDoS-Angriffe her (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 32). Die Pandemie habe den Breitbandausbau beschleunigt und Prozesse aus gesicherten, professionellen Umfeldern in private Heimnetze verlagert. Liegen die Jahre 2019 bis 2021 nebeneinander, wird sichtbar, wie sich die Bedrohungslage im Bereich DDoS fortwährend entwickelt, auf welche akuten Gefahren es zu reagieren gilt und welche begünstigenden Umweltfaktoren zur je aktuellen Situation beitragen. Diese Argumentationsstringenz des Lageberichts ruht unter anderem in einer bemerkenswerten technischen Detailtiefe. Im zugehörigen Angriffsbeispiel des DDoS-Kapitels 2021 heißt es etwa: „Die Angriffe basierten auf UPD-Floods, TCP-Floods und SYN-Floods. Zur Steigerung der Angriffsvolumina setzten die Täter auf die Reflection-Amplification-Vektoren WS-Discovery und Apple Remote Control sowie DNS“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 34). Das BSI bedient sich Fachtermini selbstverständlich, statt sie zu erläutern. Damit demonstriert die Behörde einerseits ihre Kompetenz wie auch Glaubwürdigkeit gegenüber einer wissenden Teilöffentlichkeit, wendet sich andererseits keineswegs dem Gros der Anwenderinnen und Anwender zu, um ihnen die Bedrohungslage geläufig zu machen.

Stattdessen setzen die Autoren des Berichts auf Multiplikatoreffekte, also auf versierte Menschen, Medien oder Organisationen, die die Kernbotschaften des jeweiligen Reports für wiederum ihre Zielgruppen übersetzen sowie vervielfachen. Besonders deutlich wird dies bei Betrachtung der zentralen Doppelseite einer Jahresausgabe. Diese zwei Seiten lesen sich wie ein Management-Report: Dort befinden sich ausgewählte Statistiken mit oft hohen Fall- oder Betroffenenzahlen, die prominentesten Cybervorfälle wie auch kuratierte, zitierfähige Botschaften, die in Pressemeldungen aufgegriffen werden sollen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 42f). Aus dem Bericht 2019 zitierte die Zeitung Welt als eine von vielen die Doppelseite: „Zwischen Juni 2018 und Mai 2019 wurden rund 114 Millionen neue Schadprogramm-Varianten registriert“ (Welt 2019). Angaben der Berichtsdoppelseite 2020 fanden sich unter anderem im Handelsblatt: „In insgesamt 419

Fällen wurde das BSI im Berichtszeitraum (1. Juni 2019 bis 31. Mai 2020) über Probleme im Bereich der sogenannten kritischen Infrastruktur informiert“ (Handelsblatt 2020c). Und 2021 entwarf die Computerwoche neben vielen anderen Medien eine Schlagzeile aus ebenjener Botschaftensammlung des Berichts:

Etwa 14,8 Millionen Meldungen zu Schadprogramm-Infektionen übermittelte die Behörde an deutsche Netzbetreiber, mehr als doppelt so viel wie im Jahr zuvor. Auch der Tagesspitzenwert an Bot-Infektionen deutscher IT-Systeme hat sich von 20.000 auf 40.000 verdoppelt (Computerwoche 2021).



Abbildung 9: Seiten 36 und 37 des BSI-Lageberichts 2020 (Bundesamt für Sicherheit in der Informationstechnik 2020a, 36f)

Die Doppelseite, die jedes Jahr am Ende des Kapitels *Gefährdungslage* wesentliche Daten zusammenfasst, nimmt auch eine Doppelfunktion ein. Im ersten Sinne ist dieses Stilmittel eine Übersicht über jene Zahlen und Fakten, die das BSI aus einem professionellen Standpunkt für bedeutsam hält. Daneben ist diese Doppelseite ein Instrument zur Anleitung der Medienberichterstattung, eine dankbar angenommene Zusammenfassung, aus der sich Kennziffern – abhängig vom Zielgruppenbedarf oder der Agenda des Mediums – wörtlich wiedergeben lassen. Bei näherer Betrachtung der ausgewählten Statistiken wird deutlich, dass es sich um stets steigende Angaben

handelt. Um nur wenige Beispiele herauszugreifen, stieg die Zahl der registrierten Schadprogramm-Varianten in den drei Jahren von 114 auf 144 Millionen. Die Vorfallmeldungen der Kritischen Infrastruktur verdoppelten sich von 2019 auf 2020 nahezu mit 419 im Gegensatz zu 252. 2021 existiert im gesamten Bericht keine Angabe zu Meldungen aus dem KRITIS-Sektor. Auf den Doppelseiten 2020 und 2021 findet sich dagegen die Information, dass sich die Zahl der durch das BSI an Netzbetreiber gemeldeten Schadprogramminfektionen von sieben auf über 14 Millionen verdoppelt hat. Dass bereits 2019 mehr als elf Millionen Meldungen erfolgten, findet im Verlauf der Reporte keine Erwähnung mehr. Demgegenüber führt die Doppelseite in jedem Jahr die Menge der Mitglieder der Allianz für Cyber-Sicherheit auf, die zwischen 2019 und 2021 von 3700 auf 5100 anwuchs (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 43). Mit der zielbewussten Anordnung der gemessenen Daten kann das BSI suggerieren, dass die Bedrohungslage und das Interesse an der Arbeit des BSI fortlaufend zunehmen. Hierdurch kann die Behörde ihre ursächliche Legitimität untermauern. Nicht nur die jährliche Doppelseite, sondern der gesamte Lagebericht kann im Sinne einer BSI-Agenda gelesen werden, die zum Ziel hat, weitere Gelder oder Personal zu akquirieren, Zuständigkeiten zu festigen oder ein gewünschtes Image auszubilden.

Im weiteren Verlauf des Berichts stellen die Berichterstatter vor, welche Maßnahmen das BSI unternimmt, um der zuvor beschriebenen Gefahren Herr zu werden. Dabei gliedern die Verfasser die Maßnahmen entlang der Zielgruppen Staat, Wirtschaft und Gesellschaft. Bei der Analyse des Kapitels *Staat* fällt auf, dass sich einige der Textpassagen über die Jahre sehr ähneln. Alljährlich berichtet das BSI beispielsweise über das Cyber-Abwehrzentrum: Der Lagebericht beschreibt, was das Cyber-AZ ist, welche die federführende Behörde im Berichtszeitraum war und stellt schließlich knapp vor, welche gegenwärtigen Geschehnisse das Abwehrzentrum besonders beschäftigt haben (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a, 66). Dabei treffen die Berichterstatter keine nennenswerten Aussagen über die Leistungen oder über explizite Prozesse in und um das Cyber-Abwehrzentrum. Ähnlich unkonkret bleibt das BSI auch im Bereich des nationalen Verbindungswesens. Mit Formulierungen wie „Die Kooperationen zwischen dem BSI und den Bundesländern werden aktuell weiter ausgebaut. Hierfür wurden seitens des BSI spezielle Kooperationsfelder im Bereich der Cyber-Sicherheit entwickelt“ (Bundesamt für Sicherheit in der

Informationstechnik 2020a, 68) oder „Im vergangenen Jahr konnte die Zusammenarbeit zwischen Bund, Ländern und Kommunen weiter ausgebaut und bei der Entwicklung praxisorientierter Lösungsansätze vertieft werden“ liefert der Lagebericht zwar jährlich eine Vorstellung von den Bemühungen des BSI auf diesem Feld, äußert sich aber kaum oder nur anlassbezogen über dezidierte Resultate (Bundesamt für Sicherheit in der Informationstechnik 2021a, 75). Dagegen gibt der Bericht über Verschlusssachen-Zulassungen immer wieder exakte Daten heraus: 2019 erteilte das BSI 50 Zulassungen, 2020 wurden 66 Zulassungen erteilt, 2021 waren es 91 (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 71). Es existiert folglich keine einheitliche Berichtsform quantifizierbarer Arbeitsnachweise. Stattdessen unterscheidet sich die Informationstiefe innerhalb des Reports deutlich. Mal treffen Leser empirisch begründete Faktenaufreihungen an, mal stoßen sie auf tendenziell erzählende Magazinbeiträge.

Auch deshalb lohnt sich der Blick auf die Differenzen zwischen den jährlichen Ausgaben. Diese Abweichungen zeigen auf, welche Themen und Aufgabenfelder sich addierten und welche mit der Zeit an Relevanz gewonnen haben. So gesellt sich 2020 zu Überschriften wie „Nationales Cyber-Abwehrzentrum (Cyber-AZ)“, „Informationssicherheitsberatung“, „Lauschabwehr“ oder „Smart Borders und hoheitliches Identitätsmanagement“ auch „Computer Emergency Response Team für Bundesbehörden“, das es im Vorjahr noch nicht in den Lagebericht schaffte (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 6). Dabei stellt CERT-Bund eine der Kernarbeitsbereiche dar, indem präventive, aber auch akute Maßnahmen für den Notfall entwickelt und dem Bund als Unterstützungsleistungen angeboten werden. Das können Hinweise zu Sicherheitslücken oder wichtige Fähigkeiten zur Schadensbegrenzung sein. In Ausnahmesituation kann das CERT zudem sogenannte Mobile Incident Response Teams aussenden, die der Bundeseinrichtung oder Infrastruktur vor Ort bei der Bewältigung einer Notlage zur Seite stehen. Erstmals im Lagebericht 2020 stellt sich das CERT-Bund vor und arbeitet seine Schlüsselrolle für die deutsche IT-Sicherheit heraus. Das BSI legt dar, dass CERT bei einer entdeckten Sicherheitslücke auf den sogenannten Coordinated Vulnerability Disclosure-Prozess (CVD) setzt. Das bedeutet unter anderem, dass dem Betreiber eines Produkts eine Frist eingeräumt wird, in der er den Mangel beseitigen kann und das BSI den Fund noch nicht publiziert. Dabei liegt in der Verantwortlichkeit von CERT-Bund, „eine

verbindliche Kommunikation und verlässliche Reaktionsprozesse“ zu gewährleisten (Bundesamt für Sicherheit in der Informationstechnik 2020a, 67). Mehr als 20 Fälle habe das BSI im Berichtszeitraum bearbeitet; 2021 waren es bereits 25 Vorfälle von nationaler Relevanz (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 71). 2021 findet sich im Lagebericht dann ein sehr ähnlicher Beitrag, der allerdings mit deutlich mehr Statistiken aufwartet, die die Größe des Arbeitsfeldes belegen. So habe man 1.050 Meldungen zu Schwachstellen veröffentlicht, 70 Notfälle bearbeitet und dafür zehnmal ein MIRT entsendet (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 71).

Zur Sicherung der staatlichen Cybersicherheit zählt der Lagebericht 2021 außerdem erstmalig die Absicherung von Satellitensystemen. Da diese Systeme oft transnational betrieben werden, konzentriert sich die Arbeit des BSI auf das europäische Satellitensystem GALILEO. „Zusammen mit anderen Mitgliedsstaaten wurde unter der Federführung des BSI ein Anforderungskatalog erstellt, um Satellitensysteme und deren Kommunikationsinfrastrukturen zukunftssicher zu machen“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 82). Als Nachweis dieses Engagements gibt das BSI an, an der Kryptografie für die kommende Satellitengeneration Europas führend beteiligt gewesen zu sein und die Technik vor allem widerstandsfähiger gegen Quantenangriffe gestaltet zu haben. Ebenfalls erstmals beschreibt das BSI an dieser Stelle seine Arbeit für sichere Messenger-Dienste, mit denen Ämter und Bevölkerung verschlüsselt und zuverlässig miteinander in Kontakt treten können, „sei es zur flexiblen Erreichbarkeit im Homeoffice, zum behördenübergreifenden Austausch bei Sicherheitsvorfällen oder zur Kommunikation mit Wirtschaft, Bürgerinnen und Bürgern oder europäischen Partnerbehörden“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 78). Hierbei legte man das Augenmerk auf moderne kryptografische Standards sowie Datenschutz. Obendrein setzte sich das BSI dafür ein, das sogenannte MLS-Protokoll zu etablieren und wirkte somit aktiv auf eine Interoperabilität der verschiedensten Messenger-Dienste hin.

Der Lagebericht folgt hier stets einer Formel: In einem ersten Schritt stellt das BSI alljährlich Kernbereiche für die Cybersicherheit der Bundesverwaltung vor. Im weiteren Verlauf betonen die Verfasser besondere Erfolge, die mit entsprechenden Daten unterfüttert werden, beispielsweise über bewältigte IT-Sicherheitsvorfälle. Schließlich führen die Berichterstatter Leuchtturmprojekte ins Feld, mit denen sich das BSI

augenblicklichen wie auch zukunftsgerichteten Anwendungsfeldern widmet – darunter Messenger-, KI-, Quanten- oder Satellitenprojekte. Das bedeutet, der Lagebericht folgt im Abschnitt zum *Staat* nicht der Form eines Berichts, da ausschließlich Erfolge präsentiert, konturlose Tätigkeitsbeschreibungen aufgelistet oder ausgewählte Progressivvorhaben publiziert werden. Stattdessen handelt es sich bei diesem Kapitel um eine Prioritätendarstellung.



Abbildung 10: Die hervorgehobenen Themenfelder des Lageberichts spiegeln sich auch auf der Webseite des BSI wider (Bundesamt für Sicherheit in der Informationstechnik 2022e)

Es finden vornehmlich solche Arbeitsbereiche und Botschaften ihren Weg in den Bericht, die im Interesse des BSI stehen. So gibt der Report neben den aufgeschlüsselten Messgrößen vor allem Aufschluss darüber, welche Themen respektive Herausforderungen für das BSI von besonderer Wichtigkeit und welche weniger bedeutsam sind. Dem selbst gezeichneten Bild folgend ist das BSI in der Lage, angemessen auf die steigende Bedrohungssituation zu reagieren, die relevanten Kompetenzen anzuhäufen und aufkommende Kontexte zu antizipieren; mehr noch, diese frühzeitig zu prägen. In diesem Zuge fallen auch jene Themenbereiche auf, die weniger Priorität genießen. Beispielsweise wird erkennbar, dass der grenzüberschreitenden Zusammenarbeit immer nur wenige Seiten, teils Absätze, gewidmet sind. Dabei setzen die Autoren auf wiederholende Aussagen wie: „Ziel des BSI ist, neben seiner nationalen Rolle als Cyber-Sicherheitsbehörde des Bundes, Cyber-Sicherheit auch international mitzugestalten sowie die eigene technologische Beurteilungsfähigkeit zu stärken“ (Bundesamt für Sicherheit in der Informationstechnik 2020a, 73/2021a, 79). Obwohl Cybersicherheit ein unbestritten kooperatives, multilaterales Vorhaben sein muss, um sich wirksam gegen Gefahren

schützen und Angriffe zurückverfolgen zu können, räumt das BSI der europäischen und interkontinentalen Zusammenarbeit an dieser Stelle wenig Raum und damit schließlich Bedeutung ein. Andere Fachgebiete, die im BSI zum Schutz des Staates angesiedelt sind, werden im Bericht gänzlich vernachlässigt. Dazu gehören unter anderem die zahlreichen Penetrationstests zur Prüfung von durch den Bund eingesetzten Technologien und Produkten. In Summe ist der Fokusteil Staat des Lageberichts über die untersuchten Jahre hinweg eine unscharfe Darstellung der akuten Gefahrenabwehr für den Bund wie auch der zugehörigen Beratungsleistungen für Politiker und Entscheider. Über die Zusammenstellung der Berichtsgegenstände können die Autoren die Innovationskraft des BSI exponieren und Erfolge hervorheben, um so die Relevanz des BSI für die IT-Sicherheitsstruktur der Bundesrepublik aufzuzeigen.

Für die Zielgruppe Wirtschaft bietet das BSI ebenso vielfältige Sicherungsmaßnahmen an. Schon im ersten Betrachtungsjahr, 2019, setzt das BSI auf die teils unspezifischen Schwerpunkte „Zertifizierung“, „Digitalisierungsprojekte“, „5G“, „Grundschutz“, „IT-Sicherheitsgesetz & Umsetzungsplan Kritische Infrastrukturen“, sowie „Allianz für Cyber-Sicherheit“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 51ff). Der Lagebericht 2019 stellt die unterschiedlichen Zertifizierungsinstrumente vor, mit denen das BSI Produktzertifizierungen oder Zertifizierungen von Managementsystemen vergeben kann. Hersteller oder Betreiber dieser Systeme können dann mit dieser Zertifizierung werben und nachweisen, dass ihr Produkt den Prüfkriterien des BSI entspricht (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a, 51ff). Im Lagebericht werden diese Methoden, die das BSI als Dienstleister anbietet, auf zwei Seiten beschrieben. Erst zum Ende des Kapitels findet sich ein Absatz mit Berichtcharakter. So wurden „im Rahmen der CC-Zertifizierung beim BSI im Berichtszeitraum insgesamt 119 Zertifikate [...] ausgestellt“ – 2020 waren es dann 97 Zertifikate, im darauffolgenden Jahr 120 (Bundesamt für Sicherheit in der Informationstechnik 2019a, 52). Ähnlich nah an der Datenbasis bleibt auch die Dokumentation der Allianz für Cyber-Sicherheit. 2019 vermeldet die ACS 3700 teilnehmende Unternehmen mit 120 aktiven Partnern sowie mehr als 90 Multiplikatoren mit relevanten Netzwerken (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a, 60). 2020 zeigt das BSI, dass diese Zahlen weiter deutlich gestiegen sind. Im Jahr 2021 ist die Zahl der Partner auf 150 gestiegen; die der Mitglieder bereits auf mehr als 5000 (vgl. Bundesamt für Sicherheit in der

Informationstechnik 2021a, 67). Durch diese wiederkehrenden Messeinheiten ist über die Jahre ein Verlauf erkennbar, wodurch das BSI in diesem Fall Transparenz herstellt und zugleich für Externe überprüfbar macht, ob die jeweiligen Arbeiten zielführend sind.

Während das BSI also Zahlen und Fakten zu Produktzertifizierungen in der Wirtschaft sowie zur Allianz für Cyber-Sicherheit aufzählt, liest sich der Lagebericht im Bereich Telekommunikationsinfrastruktur, also 5G, merklich deskriptiver. Die Autoren beschreiben 2019 den Stand des bevorstehenden 5G-Rollouts und dokumentieren, dass das BSI hierzu die Sicherheitsanforderungen erarbeitet, an die sich die Mobilfunkanbieter wiederum halten müssen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a, 57). Nachdem die eigene Rolle determiniert ist, stellt der Bericht die Vorteile der Technologie dar, um schließlich hervorzuheben, dass das BSI den Netzausbau, dem es bescheinigt, „zum größten Infrastrukturvorhaben des kommenden Jahrzehnts“ zu werden, von Beginn an mitzugestalten (Bundesamt für Sicherheit in der Informationstechnik 2019a, 58). Über alle drei Berichtsjahre hinweg signalisiert das BSI, dass es den Trend, technologisch wie auch gesellschaftlich, erkannt hat und installiert die Behörde selbst als Teil des Fortschritts. So heißt es 2019: „Das BSI begleitet diesen Prozess von Anfang an. Das BSI ist als eine von wenigen staatlichen Organisationen weltweit Mitglied der maßgeblichen Dachorganisation der Mobilfunkbranche GSMA [...]“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 58). Im Folgejahr unterstreichen die Autoren diese Position und weisen ihrer Organisation eine Schlüsselrolle für den 5G-Ausbau zu, wenn sie sagen, es sei am BSI, die Grundbedingungen für den Schutz der Netze zu schaffen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 57). 2021 schließlich hebt der Bericht hervor, dass das BSI seine Bemühungen im Bereich 5G eigens an einem Standort in Freital zusammenziehe und man bereits zukünftige 6G-Netze bedenke (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 61).

Ebenso unspezifisch trägt das BSI jährlich zum *Umsetzungsplan KRITIS* vor. 2019 beschreibt der Lagebericht lediglich, was der UP KRITIS ist, nämlich eine „öffentlich-private Partnerschaft von KRITIS-Betreibern, ihren Verbänden und dem Staat“, in der Branchenstandards, sogenannte B3S, „in gemeinsamen Arbeitsgruppen entwickelt“ werden (Bundesamt für Sicherheit in der Informationstechnik 2019a, 59). 2020 stellen die Autoren dagegen eine Risikomatrix in die Mitte ihrer Berichterstattung, mit deren

Hilfe die Teilnehmenden Risiken und Anpassungsbedarfe visualisieren und austauschen können (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 55f). Schließlich findet diese Matrix 2021 nur noch knapp Erwähnung; stattdessen berichten die Verfasser von Themenarbeitskreisen, die beispielsweise zu Detektion oder zu Informationsaustausch beraten, sowie von der reformierten Gremienstruktur des UP KRITIS (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 59). Schon an diesen Beispielen zeigt sich, dass der Lagebericht auch für die Wirtschaft nur vereinzelt einem Berichtformat folgt und stattdessen jährlich abweichende Schwerpunkte setzt, die miteinander kaum vergleichbar sind. Sowohl im Fall 5G als auch UP KRITIS ist für Leser nicht nachvollziehbar, ob die Aussagen des Berichts objektiv zutreffen oder ob sie ein eigen formuliertes Programmpapier bilden. Gleichwohl greift das BSI in seinen Maßnahmen für die Wirtschaft stets gegenwärtige Umstände auf. So legen die Berichtersteller dar, dass das BSI bereits zu Pandemiebeginn im März 2020 mit Empfehlungen zum Umstieg ins Homeoffice an die Öffentlichkeit ging und im April ein Kompendium veröffentlichte, „um den gesamten Lebenszyklus organisationsinterner Videokonferenzsysteme sicher zu gestalten“ (Bundesamt für Sicherheit in der Informationstechnik 2020a, 62). 2021 führt der Bericht gleich mehrere Themengebiete neu ein: Das BSI stellt dar, dass es mit dem Kraftfahrt-Bundesamt kooperiert, um vor dem Hintergrund der zunehmenden Vernetzung der Verkehrsinfrastruktur technische Standards entwickeln und Cybersicherheit als Kriterium für Typgenehmigungen etablieren zu können (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 61f). Auch das Engagement des BSI für Cybersicherheit im Luftverkehr findet in diesem Zuge Eingang in den Bericht. Diese Beschreibung ist jedoch weniger eine Bestandsaufnahme, sondern eine Absichtserklärung: „Das BSI wird für die Informationssicherheit in der Luftsicherheit Vorgaben und Anforderungen für die [...] regulierten Unternehmen erarbeiten“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 62). Ähnlich neoterisch beziehungsweise zukunftsgerichtet liest sich die Erklärung zu mehr Cybersicherheit in der Industrie. Man arbeite an Tipps und Hinweisen für kleine und mittlere Unternehmen. Daneben „wirkt das BSI an der Standardisierung einer Programmierschnittstelle für Sicherheitselemente in Industriegeräten mit“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 63). Zwar schildert der Bericht, woran das BSI für seine Zielgruppe Wirtschaft arbeitet, legt jedoch nahezu keine Ergebnisse dar, sodass die vorgestellten Initiativen uneinheitlich scheinen. Für Außenstehende ist schwer einzuschätzen, wie intensiv oder umfangreich

das jeweilige Engagement ist. Erneut kann also festgehalten werden, dass sich die Inkonsistenz der Form fortsetzt und der Bericht heterogen konstruiert ist, da sowohl die Art der gemeldeten Informationen als auch ihre Dichte stark variieren.

Im Abschnitt *Gesellschaft* lässt sich eine der wohl größten strukturellen Veränderungen des BSI in den vergangenen Jahren ablesen. Denn der Koalitionsvertrag des Kabinetts Merkel IV sah vor, dass das BSI den digitalen Verbraucherschutz als eine seiner Kompetenzen hinzugewinnt – und somit nicht mehr nur den Schutz von Staat und Wirtschaft in den Blick nimmt. Damit geht eine neue, umfassendere Sichtweise des BSI und des BMI einher, die Informationssicherheit nicht nur als Herausforderung versteht, der mit technischen Mitteln beizukommen ist. Von der überwiegenden Beobachtung von Gefahren und der Veröffentlichung einiger Sicherheitstipps auf dem Online-Portal [bsi-fuer-buerger.de](https://www.bsi-fuer-buerger.de) noch im Jahr 2019 hin zur ganzheitlichen Erarbeitung von Lösungen in Form von Standardisierungen, Herstellervorgaben und Handlungsempfehlungen 2020 vergingen sichtbar nur wenige Monate. 2019 erhält der Bereich *Gesellschaft/Bürger* noch fünf Normseiten, um dort sowohl die Bedrohungslage als auch die Schutzmaßnahmen darzulegen. Mehr als drei dieser Seiten schildern, dass dem Smarthome „ein besonderes Gefahrenpotenzial und eine besondere Schutzfunktion zuzuschreiben“ sei, dass diverse digitale Medizinprodukte zum Teil schwerwiegende Sicherheitslücken aufweisen, oder dass Finanzinstitute bis dato selbst über die Form des Authentifizierungsverfahrens ihrer Kunden entscheiden konnten, sodass die Benutzerfreundlichkeit oft den Vorzug vor der Sicherheit erhielt (Bundesamt für Sicherheit in der Informationstechnik 2019a, 63ff). Als eines von drei Lösungsangeboten präsentiert das BSI den Dialog für Cybersicherheit; ein Projekt, in dem relevante zivilgesellschaftliche Akteure regelmäßig in den Austausch mit dem BSI gehen und direkt Einfluss auf gewisse Themen nehmen können. Mit dem IT-Sicherheitskennzeichen soll zudem eine „verbrauchergerechte Darstellung der Sicherheitseigenschaften“ von vernetzten Produkten gelingen (Bundesamt für Sicherheit in der Informationstechnik 2019a, 67). Hier erlaubt sich der Lagebericht, ein Zukunftsbild zu zeichnen, in dem das BSI technische Richtlinien und das BMI den Rechtsrahmen vorgibt, um Geräte oder Software prüfbar und für die Kunden verständlich aufzusetzen. Als dritte Initiative, um Verbraucher in Deutschland zu digitaler Sicherheit zu verhelfen, benennt das BSI sein „breites Informations- und Beratungsangebot für Privatanwender unter dem Namen ‚BSI für Bürger‘“ (Bundesamt

für Sicherheit in der Informationstechnik 2019a, 68). An dieser Stelle zählt der Bericht die Medien und Formate auf, mit denen das BSI den Bedürfnissen der Anwender zu begegnen versucht. Darunter sind eine eigene Verbraucherwebseite, ein abonnierbarer Warndienst, mehrere Broschüren sowie Social Media-Auftritte und Kooperationsvereinbarungen mit Verbraucherzentralen oder dem Verein Deutschland sicher im Netz zu finden. Diese Dienstleistungen sind die einzigen Angebote im Bereich Gesellschaft, die einen Rückblick auf den Berichtszeitraum zulassen und die zudem noch mit quantifizierbaren Daten, beispielsweise über Follower oder Newsletter-Abonnenten, angereichert sind. Alle diese Angebote schreiben den Anwendern eine Holschuld zu. Sie müssen zunächst eine, vielleicht zukünftige, Problemsituation erkennen, zum Beispiel dass ihre unsicheren Passwörter sie gefährden könnten, um einen Anreiz zu verspüren, die Informationen des BSI in Anspruch nehmen zu wollen. Die Kooperation mit oder die Regulation von Herstellern, um so Digitalprodukte bereits sicher auf den Markt zu bringen, spielt hier keine nennenswerte Rolle. Ganz im Gegenteil: Das Kapitel *Gesellschaft* schließt 2019 damit, dass den Endanwendern eine entscheidende Mitverantwortung attestiert wird: „Unnötig verschärft wird die ohnehin angespannte Cyber-Sicherheitslage durch die in vielen Fällen festzustellende digitale Hilflosigkeit aufseiten der Anwender“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 75).

Schon 2020 ist solch eine Aussage im Lagebericht nicht mehr zu finden. Zwar wollte man Verbrauchern helfen, sich selbst helfen zu können, allerdings wird der Schutz der Anwender fortan differenzierter betrachtet. Der Bericht führt Schlagworte ins Feld, wie „staatliche Rahmen“, „Cyber-Sicherheit verbraucherfreundlich“, „sichere Verbraucherprodukte und -dienste“, die zeigen, dass das BSI die Verbraucher nicht länger nur befähigen, sondern im tiefsten Sinne schützen möchte (Bundesamt für Sicherheit in der Informationstechnik 2020a, 41). Dazu steigen die Berichtersteller mit einem Update zum IT-Sicherheitskennzeichen ein, welches allerdings 2020 weiter auf seine Erstveröffentlichung wartet. Im Übrigen aber erfährt der Bericht mit der neuen Aufgabe des digitalen Verbraucherschutzes einen Aufwuchs innerhalb des Berichts von etwa fünf auf 12 Seiten. Darunter befinden sich nun auch Beschreibungen von anschaulichen Beispielen dafür, was das BSI tut, um die Sicherheit der Verbraucher zu erhöhen. So entdeckte das Amt bei einer Smart Watch für Kinder derart schwerwiegende Sicherheitslücken, dass Außenstehende die Kommunikation zwischen

App und Server des Herstellers einfach abfangen können. Die Verfasser zeigen auf, wie das BSI erwirkt hat, dass die Uhr vom Markt genommen wurde, bis die Lücke geschlossen war (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 44). Im Bericht ist dies als ein Exempel von vielen aus der Alltagswirklichkeit im Umgang mit smarten Geräten deklariert. Nur wenige Absätze später illustrieren die Autoren, wie das BSI im Hintergrund auch an einem technischen Verbraucherschutz arbeitet. Denn um die Sicherheit von Bezahlverfahren mittels biometrischer Sensoren zu stärken, „entwickelt das BSI Prüfkriterien für biometrische Authentisierungsmechanismen“ (Bundesamt für Sicherheit in der Informationstechnik 2020a, 47). Als kontemporäres Projekt ist hier außerdem die Corona-Warn-App zu finden, bei deren Entwicklung durch die Deutsche Telekom und SAP das BSI begleitete und dabei die Einhaltung des Sicherheitskonzeptes sicherstellte (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 46). Es ist augenfällig, dass es sich bei den hier genannten um äußerst eindringliche Arbeitsproben des BSI handelt, da es entweder um den Schutz von Kindern geht, die Sicherheit des privaten Geldes thematisiert oder eine prominente Gegenwartscausa wie die Corona-Warn-App adressiert wird. Abschließend legen die Verfasser sogar nach, wenn sie die Arbeit der Behörde an fortschrittlichen Trendthemen wie Biometrie und KI ausführen. Demnach untersucht das BSI die „verschiedenen Aspekte von Angriffen und Verteidigungsmaßnahmen [...] in Kooperationen mit führenden nationalen Forschungseinrichtungen“ (Bundesamt für Sicherheit in der Informationstechnik 2020a, 51). Dennoch enthalten auch die Kapitel zu Gesellschaft und digitalem Verbraucherschutz über die Berichtsjahre hinweg Schilderungen von Studienaufbauten ohne konkrete Ergebnissenennung, wie beispielsweise im Projekt OPTIMOS 2.0 über elektronische Identitäten auf Smartphones (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 50).

2021 baut auf den Themen der Vorjahre auf und ergänzt nur wenig Neues. Gleichzeitig ist der Anteil jener Beiträge nochmals reduziert, die lediglich einen Ausblick geben oder noch ergebnislose Projekte vorstellen. Das im BSI noch junge Arbeitsfeld des digitalen Verbraucherschutzes kann in diesem Jahr mit ersten Ergebnissen aufwarten. Bei einer Studie zur Sicherheit von Gesundheitsapps stellt der Lagebericht fest, dass bei „84 betrachteten Anbietern [...] der Grundsatz Security by Design nur in Teilen des Entwicklungsprozesses berücksichtigt wurde“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 48). Zusätzlich konnte nachgewiesen werden, dass einige

dieser Apps Kennwörter unverschlüsselt übertragen und dabei der Kommunikationsweg zwischen App und Hersteller nahezu ungesichert ist. Aus einem weiteren Projekt, dieses Mal zu digitalen Medizinprodukten, berichtet das BSI von „mehr als 150 Schwachstellen in zehn Produkten aus fünf Kategorien (implantierbare Herzschrittmacher, Defibrillatoren und deren Zubehör, Insulinpumpen, Beatmungsgeräte, Patientenmonitore und Infusionspumpen)“ und demonstriert damit eindrücklich, welche Wirkung der Blick auf Endverbraucherprodukte entfalten kann, die bislang unkontrolliert blieben (Bundesamt für Sicherheit in der Informationstechnik 2021a, 51). Die Berichtersteller zeigen das BSI als Institution, die die Anwender multiperspektivisch zu schützen versucht, indem sie fortsetzen, dass die Behörde zahlreiche technische Richtlinien für Verbraucherprodukte veröffentlicht. Technische Richtlinien sind Empfehlungen, die Kriterien zur Herstellung oder zum Betrieb sicherer IT-Komponenten und -systeme enthalten. Darunter sind etwa Richtlinien für Online-Wahlen, Breitbandrouter oder auch elektronische Identitäten (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 55). Das flankieren die Autoren mit Daten aus der direkten Verbraucherkommunikation und Sensibilisierungsarbeit. Demnach betreibt das BSI einen Podcast namens *Update verfügbar*, einen YouTube-Kanal, Facebook oder auch einen Newsletter, zu denen der Lagebericht relevante Kennzahlen publiziert. Auch einzelne Produkte dieser Kanäle finden Erwähnung, etwa wenn angesichts der US-Wahlen 2021 mehrere Livestreams zu Desinformation im Internet produziert werden (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021a, 49).

Insgesamt zeigt sich der Lagebericht des BSI in dieser mehrjährigen Betrachtung intransparent und transparent zugleich. Er ist transparent, weil er eine große Menge quantifizierbarer und prüfbarer Fakten enthält; intransparent ist er dagegen aufgrund seiner zu komplexen Sprache bei variierender Detailtiefe. Dabei lässt sich eine wesentliche Sachlichkeit in der nüchternen Schilderung von Tatsachen feststellen, etwa wenn die Verfasser von neuen Methoden der Kriegsführung schreiben und dabei jegliche Form fachfremder Benennung auslassen: „Die weltweit fortschreitende Digitalisierung ist ein entscheidender Treiber der Dynamik hybrider Bedrohungen, da sich neue potenzielle Verwundbarkeiten von Staat, Wirtschaft und Gesellschaft eröffnen“ (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020a, 32). Koinzident zelebrieren die Autoren womögliche Gefahren ausgiebig, um die

Notwendigkeit des eigenen Tuns zu stützen. So „sind Identitätsdiebstähle an der Tagesordnung“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 7). An anderer Stelle heißt es: „Aufgrund dieser Beobachtungen ist davon auszugehen, dass die Trends anhalten und die Vielzahl und Größe von Botnetzen weiterhin zunehmen. Maßnahmen zur Prävention und Detektion sind zwingend erforderlich“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 25). Generell verwendeten die Täter „Angriffsstrategien, die leicht skalierbar sind und sich massenhaft gegen verschiedene Opfer anwenden lassen“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 12). Hierbei handelt es sich um bewertende Stellungnahmen, die allesamt aussagen, dass die digitale Sicherheitslage wenig kontrollierbar ist und sich fortwährend schwieriger gestaltet. Diese Gefahr wird dann zumeist von einer Beschreibung dessen flankiert, was das BSI in diesem Feld unternimmt oder bereits getan hat.

Der Bericht über die *Lage der IT-Sicherheit in Deutschland* enthält dem folgend durchgehend viel Datenmaterial, ist in der Auswahl der Zahlen aber wenig einheitlich. Des Weiteren offenbaren die letzten Seiten, dass der Bericht zwar teils empirisch aufgebaut ist, teils aber auch deskriptive Passagen einschließt, die für gewöhnlich in einer Broschüre oder einer Pressemitteilung zu finden sind. Statt tatsächlich Auskunft über Entwicklungen innerhalb des Berichtszeitraums zu geben, dienen diese Absätze vielmehr dazu, eine Position des BSI zu verdeutlichen:

Die Einführung des Mobilfunkstandards 5G hat das Potenzial, sich zum größten Infrastrukturvorhaben des kommenden Jahrzehnts zu entwickeln und die Digitalisierung von Staat, Wirtschaft und Gesellschaft auf eine vollkommen neue Basis zu stellen. Das BSI begleitet diesen Prozess von Anfang an (Bundesamt für Sicherheit in der Informationstechnik 2019a, 58).

Diese Textabschnitte stellen entweder eine Herausforderung neben eine Aufgabe des BSI oder sie rücken die Behörde in einen direkten Zusammenhang mit Motiven des Fortschritts oder der Sicherheit: „Zusammen mit den anderen durch das BSI wahrgenommen Aufgaben [...] wird gewährleistet, dass Angriffe erkannt und dass schnell [...] darauf reagiert werden kann“ (Bundesamt für Sicherheit in der Informationstechnik 2020a, 67). Die Verfasser der Lageberichte platzieren kontinuierlich eigene Leuchtturmprojekte und die damit verbundene Vorreiterrolle. Das ist aus strategischer und markenbildender Sicht nachvollziehbar, ist aber auch eine weitere Ursache dafür, dass sich eine erkennbare Inkonsistenz durch die Berichte zieht.

Dennoch erfasst der Lagebericht Statistiken und Fakten über IT-Sicherheit in Deutschland, teils auch international. Die Publikation ist zumeist nüchtern formuliert und stets komplex in Sprache und Inhalt. In der Folge sind die Lagebeschreibungen und abgeleitete Handlungsempfehlungen überwiegend an Staat, Wirtschaft und Organisationen gerichtet, die die Verfasser wiederum in der Pflicht sehen, ihre Mitarbeiter zu schulen. Das heißt, die Texte sind exklusiv und offenbaren eine Kultur des nicht-Informierens von Laien. Denn so eingängig die politischen Botschaften und Erfolgsgeschichten der Berichte auch sind, so wenig greifbar und mit dem Alltag verknüpft sind die technischen Analysen und Statistiken, die sich mit Fachbegriffen und der Aufreihung von Expertenwissen nicht zurückhalten. Daraus resultiert die Annahme, dass Leser keine unmittelbare individuelle Selbstwirksamkeit herstellen können, da sich nicht konsequent manifestiert, welche Wirkung eine mangelhafte Informationssicherheit für jeden Menschen einer Gesellschaft haben kann. Der Lagebericht würde demnach, trotz der vielen Gefahrenschilderungen, kein Gefühl der Dringlichkeit von Cybersicherheit auslösen und ist auf die Zweitverwertung, beispielsweise durch die Fachpresse, angewiesen, um Menschen mit geringen Technikenntnissen zu informieren. Demgemäß lässt sich gleichermaßen festhalten, dass der Report ein technozentriertes Produkt ist. Zwar ziehen die Abschnitte über den digitalen Verbraucherschutz auch Schutzmaßnahmen in Betracht, die Anwender selbst umsetzen können; ein folgerichtiger Ausbau dieser Nutzerresilienz bleibt im direkten Vergleich zu den übrigen Kompetenzen des BSI aber eine Nebensächlichkeit.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	O		O		O	O		O			O

Wenngleich der Lagebericht primär technische Umstände beziffert, bleibt am Ende doch haften, dass das Dokument als Abbild der Arbeit des BSI ein umfassendes Portfolio und Aufgabenspektrum wiedergibt, das sich stets im Wandel befindet und schnell auf Veränderungen der Lebenswirklichkeit reagiert. Insofern ist die Publikation durchaus Ausdruck eines gewissen Anpassungsvermögens und dient mitunter als nützliches Instrument, um jährlich Themen zu setzen, sie von Neuem mit Priorität zu versehen und die Interpretationshoheit über Sicherheitsdiskurse einzunehmen. Schließlich gestaltet das BSI mit der Informationsauswahl im Lagebericht, seinem sprachlichen Ausdruck oder der Reproduktion in den Medien die öffentliche Imagination von Cybersicherheit mit.

2.3.5 Cybersicherheitsstrategie für Deutschland 2021

Vorweg sei gesagt, dass Strategien und Agenden nur existieren, weil es langfristige Problemstellungen oder verbreitete Befürchtungen gibt. Sie dienen dazu, diese Vorahnungen mit einem Maßnahmenpaket zu beherrschen und Unwägbarkeiten in Kalkulierbares zu formalisieren. Die Vorstellungen eines erwarteten Problems manifestieren dann ein Gegensteuern; auch als Instrument der Legitimierungs- und Machtverhandlung (vgl. Miller 2015, 294f). Entsprechend formulierte das damalige Bundesministerium des Innern im November 2016 die Sicherheitsstrategie für die digitalen Lebensbereiche von Staat, Wirtschaft und Gesellschaft. Infolge der zu diesem Zeitpunkt bestehenden Rahmenbedingungen wurden vier Handlungsfelder identifiziert, die im Strategiepapier weiter segmentiert sind. Zuerst soll stets die Handlungsfähigkeit, ohne Manipulation oder Fremdeinwirkung, im Cyberraum sichergestellt sein. Punkt zwei stellt eine kooperative Verantwortung für das Gelingen einer sicheren Digitalisierung zwischen Staat und Wirtschaftsakteuren her. Handlungsfeld drei widmet sich der Etablierung einer belastbaren und gewappneten Sicherheitsinfrastruktur, die auch im Krisenfall dienstfähig und reliabel bleibt. Abschließend führt das BMI die Stärkung der deutschen Rolle in der internationalen Gemeinschaft an (vgl. Bundesministerium des Innern 2016, 10). Die substanzielle Leistung der Cybersicherheitsstrategie besteht insofern darin, gegenwärtige und zukünftige Bedarfe der IT-Sicherheit auszumachen, von denen sich schließlich diese vier Handlungsfelder ableiten. Die Absichten sind zunächst eine unkonkrete Projektionsfläche für allerlei mögliche Maßnahmen und Umsetzungspläne; diese wiederum können politisch nahezu beliebig befüllt werden.

Indes lassen die Handlungsfelder zu berücksichtigende Zielgruppen erkennen. Feld eins zielt selbstverständlich auf die Gemeinschaft aller Nutzerinnen und Nutzer von Digitaltechnik ab, weist zugleich aber einen klaren Bezug zur Zivilgesellschaft auf. Dahinter steht der Auftrag, die Bürgerinnen und Bürger im privaten Raum zu schützen und sie als Akteure der Cybersicherheit zu involvieren. Als Konsequenz sollen die Anwenderinnen und Anwender für Bedrohungen sensibilisiert und zugleich mit eindeutigen, marktregulierenden Kennzeichnungen zu einem reflektierten Technologiekonsum angeleitet werden. Das unbedingte Verhindern „digitaler Sorglosigkeit“ ist in der Strategie ein bedeutender Eckpfeiler für den Ausbau einer resilienten Bevölkerung (Bundesministerium des Innern 2016, 13). An dieser Stelle

formuliert das BMI konkrete Vorstellungen und strebt die Einführung eines Gütesiegels für IT-Sicherheit an, das die in Produkten und Dienstleistungen inkludierten Sicherheitseigenschaften offenlegt und sie anhand dieser kategorisiert, um somit Sicherheit zu einem Kriterium in der Kaufentscheidung der Kunden zu machen (vgl. Bundesministerium des Innern 2016, 17).

Daneben soll die frühzeitige Umsetzung von Sicherheitsanforderungen rechtlich eingefordert werden können, um deren Berücksichtigung bereits am Beginn einer technischen Entwicklung (Security-by-design) sicherzustellen (Bundesministerium des Innern 2016, 18).

Hier verfolgt das BMI also einen zweigleisigen Ansatz. Die Bürger sollen mehr Hilfe zur Selbsthilfe erhalten, während Unternehmen und Anbieter zu höheren technischen Standards verpflichtet werden sollen. In dieses Bild passt auch die Vorstellung des Innenministeriums, den Unternehmen und Bürgern eine assoziierte Verantwortung für Cybersicherheit zuzuschreiben (vgl. Bundesministerium des Innern 2016, 9).

Um die Wirtschaft bei der Digitalisierung zu unterstützen, spricht das BMI davon, die IT-Wirtschaft voranzutreiben, indem beispielsweise die Gründung von Start-ups erleichtert werde (vgl. Bundesministerium des Innern 2016, 21). Ferner zielt die beabsichtigte kooperative Zusammenarbeit von Wirtschaft und Staat auf die Konstituierung eines auszeichnenden Siegels mit der Bezeichnung „IT-Security Made in Germany“ ab (Bundesministerium des Innern 2016, 23). Auf diese Weise sollen deutsche Produkte für zuverlässige IT-Sicherheit stehen und infolge internationaler Anerkennung einen stark vermehrten Absatz finden.

Mit Handlungsfeld drei strebt das Innenministerium auf staatlicher Ebene an, die Kompetenzen und Ressourcen des Nationalen Cyber-Abwehrzentrum zu erweitern. Dazu gehört die Verbesserung fortschrittlicher Analyse- und Auswerteverfahren genauso wie die Handlungsfähigkeit vor Ort im Bedarfsfall (vgl. Bundesministerium des Innern 2016, 29f). Diese im Bundesamt für Sicherheit in der Informationstechnik angesiedelten Kapazitäten dienen der zeitnahen Entdeckung von relevanten Vorfällen und sollen durch schnelle Reaktion mögliche Schäden minimieren respektive Störfälle beheben. Sogenannte Mobile Incident Response Teams, die MIRTs, unterstützen Einrichtungen von besonderer öffentlicher Relevanz sofort und lokal. Die mobilen Einsatzgruppen, egal ob sie vom BSI, vom BKA oder dem Militärischen Abschirmdienst unterhalten werden, dienen der Auflösung bedeutsamer Zwischenfälle und der Eindämmung digitaler Epidemien (vgl. Bundesministerium des

Innern 2016, 29). Analog zu den dezentral agierenden MIRTs sieht die Strategie eine Stärkung des CERT-Bund wie auch nicht staatlicher CERTs vor. Bei dieser Stelle gehen Vorfallmeldungen ein, werden Krisenfälle bewertet und die Kommunikation mit weiteren Sicherheitsakteuren übernommen. Die CERT-Infrastruktur soll laut Strategie gestärkt und ein tragendes Element der IT-Sicherheitsarchitektur sein. Dazu sieht das BMI eine länder- und staatenübergreifende Vernetzung vor, die Reaktionszeiten verkürzen und international um sich greifende Infektionen sichtbar machen soll (vgl. Bundesministerium des Innern 2016, 34). Die Strategie von 2016 hält in diesem Handlungsfeld schließlich auch fest, dass die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) einzurichten ist, die zwar nicht operativ an der IT-Sicherheit arbeitet, dafür aber die „Entwicklung, Unterstützung und Beratung der Sicherheitsbehörden“ forcieren soll (Bundesministerium des Innern 2016, 32).

Feld vier führt staatenübergreifende Interdependenzen an und kennzeichnet das Internet als zugleich segmentierten und weltweiten Cyberraum. So sagt das Ministerium, der

Cyber-Raum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann (Bundesministerium des Innern 2016, 46).

In dieser Definition scheint die Annahme durch, dass der Cyberraum als supranationales Gebilde in keiner Relation zu regional divergierenden juristischen, politischen oder soziokulturellen Rahmungen steht. Im Fließtext befindet sich dann die staatliche Aufgabe, die verfassungsgemäßen Werte und Rechte „in unserem Land auch im Cyber-Raum“ abzubilden (Bundesministerium des Innern 2016, 27). Das Internet erlangt hier eine regionale Ausdeutung und es entsteht der Eindruck eines abgrenzbaren, deutschen Digitalraums, der sich aus dem globalen Netz mindestens abheben könnte. Hier postuliert das BMI einen europäischen Cyberraum, der die Funktion innereuropäischer Märkte und hoheitlicher Verwaltungen sicherstellen soll (vgl. Bundesministerium des Innern 2016, 39). Folglich spiegelt die variierende Verwendung des Begriffs *Cyberraum* eine inkonsistente Auffassung des abstrakten Gebildes.

Konsistenz besteht hingegen bei der Erkenntnis, dass die Schutzaufgabe für informationstechnische Systeme international getragen werden muss. Weltweit verteilte Server sowie ein vernetztes Wirtschafts- und Staatenkonglomerat lassen die Bildung virtueller Mauern nicht zu. Daher sieht die Strategie vor, die überstaatliche

„Entwicklung von Normen, Regeln, Prinzipien“ zu erarbeiten und kooperativ auf eine Potenzierung von Sicherheitsmechanismen hinzuwirken (Bundesministerium des Innern 2016, 41). Zwar scheint das Ministerium gewillt, Entwicklungshilfe auch im Bereich digitaler Technologien zu leisten, um „die Potenziale der Digitalisierung weltweit zu ermöglichen und damit verbundenen Risiken entgegenzuwirken“ (Bundesministerium des Innern 2016, 42). Es formuliert dabei jedoch nie den Anspruch, als Leader vorweg zu schreiten und so als Vorbild für andere Nationen zu dienen, um schließlich den ökonomischen Vorteil eines Innovationstreibers auszunutzen.

Die *Cybersicherheitsstrategie für Deutschland* in ihrer aktuellen Fassung wurde im September 2021 durch das Bundeskabinett beschlossen und ersetzt die Strategie von 2016. Damit möchte die Bundesregierung die Weichen für die kommenden fünf Jahre stellen. Die Überarbeitung wirft die bisherige Strategie nicht über Bord, sondern aktualisiert Variablen und passt sie an veränderte Gegebenheiten an. Dazu trennt das Bundesinnenministerium 2021 konsequenter zwischen den Handlungsfeldern und den vier neuen, sogenannten Leitlinien, die als Intentionen zu lesen sind. Zwei dieser Leitlinien stechen signifikant hervor. Eine Maßgabe lautet etwa, die digitale Souveränität „von Staat, Wirtschaft, Wissenschaft und Gesellschaft“ sicherzustellen (Bundesministerium des Innern, für Bau und Heimat 2021a, 22). Darunter versteht das BMI, die deutsche IT-Sicherheitsforschung auszubauen, sich von Produkten und Komponenten aus Drittstaaten zu lösen sowie Technologieanbieter aus der Europäischen Union zu bevorzugen (vgl. Bundesministerium des Innern, für Bau und Heimat 2021a, 22). Man strebt mit der Cybersicherheitsstrategie an, „eine gemeinsame Vision und Strategie der EU für Cybersicherheit und europäische Digitale Souveränität“ zu entwickeln (Bundesministerium des Innern, für Bau und Heimat 2021a, 23). Mit der zweiten Leitlinie verpflichtet sich das Ministerium erstmalig, die „Ziele messbar und transparent aus[zu]gestalten“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 26). Einhergehend wurden die Handlungsfelder so formuliert, dass der Fortschritt der Strategie jederzeit mess- und nachvollziehbar sein soll und zum Ende des Plans eine abschließende Evaluierung vorgenommen werden kann. Unter dem Strich stellt das BMI im Rahmen der besagten vier Handlungsfelder 44 strategische Ziele auf, die nach eigenen Angaben „SMART (spezifisch, messbar, aktiv beeinflussbar, realistisch und terminiert) definiert“ sind (Bundesministerium des Innern, für Bau und Heimat 2021a, 130). Um eine Erfolgsmessung zu erlauben, weisen die Verfasser den

Zielen wiederum Kriterien zu, die das Erreichen der Vorsätze abbilden sollen. Bei der Betrachtung dieser Kriterien lassen sich drei vorrangige Gattungen der Zielformulierung identifizieren. So sind einige Punkte aus der Rubrik „Woran lassen wir uns messen?“ quantifizierbar und lassen jederzeit auch Überprüfungen von außerhalb des Ministeriums zu (Bundesministerium des Innern, für Bau und Heimat 2021a, 31). Zu diesen Kriterien zählen exemplarisch:

Die Zahl der von Cyberangriffen betroffenen Privatpersonen ist rückläufig (Bundesministerium des Innern, für Bau und Heimat 2021a, 32).

Bürgerinnen und Bürger sowie Unternehmen verwenden mehr sicher verschlüsselte Kommunikationsmittel (Bundesministerium des Innern, für Bau und Heimat 2021a, 49).

Die Verfügbarkeit hochspezialisierter Expertinnen und Experten in den Kernthemen ist gestiegen (Bundesministerium des Innern, für Bau und Heimat 2021a, 106).

Wenn auch als messbar ausgewiesen, bleiben dann einige Kriterien unspezifisch, zum Beispiel:

Cybersicherheitsvorfälle und Cyberlagen werden schnell und effektiv bearbeitet (Bundesministerium des Innern, für Bau und Heimat 2021a, 92).

Für das Strafgesetzbuch werden, sofern eine Überprüfung entsprechenden Bedarf ergibt, Gesetzgebungsvorschläge vorgelegt (Bundesministerium des Innern, für Bau und Heimat 2021a, 98).

IT-Sicherheitsforschung in Deutschland ist international anerkannt (Bundesministerium des Innern, für Bau und Heimat 2021a, 70).

In Abstimmung mit ihren europäischen Partnern reagiert die Bundesregierung angemessen auf Cybervorfälle (Bundesministerium des Innern, für Bau und Heimat 2021a, 116).

Diese Kriterien lassen Raum für Interpretationen und geben keineswegs zweifelsfrei objektivierte Untersuchungsparameter vor. Sie wurden ohne greifbare beziehungsweise mit frei wählbaren Messgrößen formuliert, sind abhängig von willkürlichen Variablen oder sie sind an interne Bedarfe geknüpft, die sich jederzeit verändern können. Damit sind Untersuchungen, die auf diesen Maßen ruhen, nicht eindeutig reproduzierbar. Vielmehr noch können Messungen anhand derartiger Konditionen beliebig politisch aufgeladen und mit Erfolgen oder Misserfolgen assoziiert werden, sodass kommende Auswertungen undurchsichtig beziehungsweise tendenziös anmuten können.

Drittens fallen insbesondere Kriterien auf, die schon mit Erscheinen der Cybersicherheitsstrategie 2021 erfüllt oder wenigstens teilweise erfüllt waren:

Handlungsempfehlungen aufgrund der Forschungsergebnisse liegen vor (Bundesministerium des Innern, für Bau und Heimat 2021a, 70).

Vertrauenswürdige IT-Produkte werden im Markt erfolgreich angeboten (Bundesministerium des Innern, für Bau und Heimat 2021a, 72).

Die Integrität der Telekommunikationsnetze ist gewahrt (Bundesministerium des Innern, für Bau und Heimat 2021a, 82).

Zielgruppen des politischen Raumes werden für Belange der Cybersicherheit im Umfeld von Wahlen sensibilisiert (Bundesministerium des Innern, für Bau und Heimat 2021a, 95).

Solche Größen sind Garanten dafür, dass die Cybersicherheitsstrategie retrospektiv mindestens als Teilerfolg verbucht werden kann, da diese bereits zur Veröffentlichung des Papiers nahezu abgeschlossen oder längst gängige Praxis sind. Damit hebt sich zwar nicht das Cybersicherheitsniveau in Deutschland, politisch können diese Kriterien jedoch in die Bilanz eingehen, sofern etwa manche der konkreten Zielvereinbarungen verfehlt werden sollten.

Abseits der drei aufgezählten Kategorien steht die Cybersicherheitsstrategie – ähnlich dem IT-Sicherheitsgesetz 2.0 – in der Kritik, weil sie die Absicht dokumentiert, den staatlichen Sicherheitsbehörden mehr Möglichkeiten zur Abwehr von digitalen Bedrohungen an die Hand zu geben. So möchte das BMI etwa „[t]echnische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation“ entwickeln (Bundesministerium des Innern, für Bau und Heimat 2021a, 102). Mit dem Ziel 8.3.9 der Strategie soll zugleich die Privatsphäre eines Jeden durch wirksame Kryptografie gewahrt bleiben und die Sicherheitsbehörden befähigen, diese Verschlüsselung zur Kriminalitätsabwehr brechen zu können (vgl. Bundesministerium des Innern, für Bau und Heimat 2021a, 101). Das BMI fügt hinzu, dass man die Verschlüsselung zwar nutzen wolle, um Straftaten zu ermitteln, aber auch um präventive Maßnahmen zu ergreifen sowie um Nachrichtendiensten den Zugang zu diesen Informationen zu gestatten (vgl. Bundesministerium des Innern, für Bau und Heimat 2021a, 102). In einem offenen Brief aus dem Juni 2021 reagierten unterschiedlichste Vertreter aus Zivilgesellschaft und Wirtschaft mit Empörung auf den Entwurf der Strategie. Universitätsprofessoren, Forschungsinstitute und Interessenverbände, darunter bekannte Initiatoren wie Lilith Wittmann, die Deutsche Vereinigung für Datenschutz, die Stiftung Neue Verantwortung und der CCC, forderten, „alle Maßnahmen, die den Ausbau von Überwachungsbefugnissen statt der Stärkung der IT-Sicherheit zum Ziel haben ersatzlos zu streichen“ (Forum InformatikerInnen für

Frieden und gesellschaftliche Verantwortung e. V., 2021b). Die Forderungen des Briefes blieben unbeachtet, sodass die Vorschläge des Entwurfes ihren Weg nahezu unverändert in die finale Fassung der Strategie fanden. Dennoch offenbart sich auch hier der Securitization-Prozess, indem wesentliche Akteure verhandeln, was als Gefahrenursache gilt; mehr noch, von wem die Gefahr ausgeht. Denn während das BMI Kryptografie als Sicherheitsbedrohung deutet, da diese die Ermittlungen der Behörden erschwere, sehen der CCC und andere im Brechen von Verschlüsselung eine bedenkliche Bemächtigung des Staates. Mit 8.3.10 arbeite das Ministerium an einer „behördenübergreifenden Strategie für den Umgang mit Schwachstellen für die Strafverfolgungs- und Sicherheitsbehörden“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 103). Fortlaufend heißt es, man treffe eine

Risikoabwägung zwischen dem Gefährdungspotential von (Zero-Day-)Schwachstellen bei temporärer Ausnutzung durch die Sicherheits- und Strafverfolgungsbehörden und dem prognostizierten Nutzen für die nachrichtendienstliche Aufklärung, Gefahrenabwehr und Strafverfolgung (Bundesministerium des Innern, für Bau und Heimat 2021a, 103f).

Daraus ergibt sich, dass das Innenministerium seinen Sicherheitsbehörden erlauben möchte, Schwachstellen zu sammeln und für ihre Zwecke auszunutzen, um die daraus gewonnen Erkenntnisse gleich organisationsübergreifend miteinander auszutauschen. In der Strategie ist in diesem Zusammenhang die Rede von einem „verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits“, womit jedoch nicht kaschiert werden kann, dass für die Umsetzung Grund- und Persönlichkeitsrechte eingeschränkt werden müssten. Damit geht unter anderem das Vorhaben einher, Kompetenzen im BSI zu bündeln. So entwickeln die Entscheider das BSI neben dem Verfassungsschutz und dem Bundeskriminalamt zu einem elementaren Bestandteil der digitalen Sicherheitslandschaft in Deutschland; im Umkehrschluss also bauen sie die Privilegien des BSI weiter aus (vgl. Bundesministerium des Innern, für Bau und Heimat 2021a, 89). Der übliche Streit zwischen Freiheit und Sicherheit – wie er auch hier schon zur Sprache kam – wird in der Cybersicherheitsstrategie unausgewogen vereinfacht: „Der geschilderte Konflikt zwischen IT-Sicherheit und nachrichtendienstlicher Aufklärung, Gefahrenabwehr sowie Strafverfolgung“ diene dem „größtmögliche[n] Schutz der Bevölkerung“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 103). Die Verfasser des offenen Briefs bilden das oppositäre Lager und äußern sich für persönliche und unternehmerische Freiheit, wenn sie etwa die Installation von möglichen Überwachungsmechanismen anprangern und Kontrollmechanismen gegen

Sicherheitsorgane einfordern (vgl. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V., 2021b). Im Kern kritisieren sie eine Leugnung des demokratischen Prozesses durch Bundesregierung und Bundesinnenministerium, insbesondere weil vorherige Briefe ungeachtet blieben. Tatsächlich musste sich das BMI kurz darauf erneut der Kritik stellen: Zwar lud man die Öffentlichkeit ein, den Strategieentwurf zu sichten, räumte für die Prüfung der 128 Seiten aber nur eine Woche ein (vgl. Bundesministerium des Innern, für Bau und Heimat 2021c). Zusätzlich fällt auf, dass das Kabinett die Ziele der Strategie lediglich 18 Tage vor der Bundestagswahl 2021 beschloss und die enthaltenen Aufgaben somit der Folgeregierung auferlegte. Eine hinreichende, öffentliche Debatte der vielschichtigen Causa unter Einbeziehung der breiten Bevölkerung war auf diese Weise kaum möglich. Die Bundesregierung sendete ihren Adressaten – also den Bürgerinnen und Bürgern, den Unternehmen oder den Ländern – damit differierende Botschaften. Einerseits suggeriert schon das Verfassen einer Cybersicherheitsstrategie selbst, dass das Thema hohe Priorität genießt. Viele der deklarierten Ziele tragen zudem das Potenzial in sich, das deutsche Digitalisierungsvorhaben sicherer zu gestalten als bislang: Anwender sollen kompetenter, Technik soll sicherer konstruiert und Zukunftstechnologien noch intensiver erforscht werden; und das alles in enger Zusammenarbeit mit europäischen Partnern. Dazu im Widerspruch steht allerdings, dass das Bundesinnenministerium mit der Strategie plant, „sowohl die technischen als auch die fachlichen Fähigkeiten der Nachrichtendienste des Bundes zu stärken“ respektive „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung [zu] gewährleisten“ – und das unter weitgehendem Ausschluss partizipativer Instanzen (Bundesministerium des Innern, für Bau und Heimat 2021a, 101/107).

Zuvor wurde schon bemerkt, dass eine nennenswerte Anzahl der Messkriterien unspezifisch bleibt; aber auch die Wege zu den gesteckten Zielen bleiben konturlos. Das BMI schildert zum Beispiel, dass bei Cyberangriffen „die notwendigen Informationen [...] den betroffenen Organisationen nicht immer zeitnah und vollumfassend zur Verfügung“ stehen (Bundesministerium des Innern, für Bau und Heimat 2021a, 59). Wenn es dann als angeschlossenes Ziel ausgibt, eine Kommunikationsplattform zu schaffen, mittels derer demnächst „allgemeine Informationen und insbesondere technische Merkmale für die Detektion zwischen den betroffenen und auswertenden Organisationen (zum Beispiel BSI, Sicherheitsbehörden, IT-Sicherheitsdienstleistern

und große Unternehmen) [...] effizient ausgetauscht“ werden, so bleibt der Weg zu diesem Vorhaben weitestgehend im Dunkeln (Bundesministerium des Innern, für Bau und Heimat 2021a, 59). Wer initiiert und betreut diese Plattform? In welcher Form erreichen welche Informationen die Betroffenen? Wer soll Zugriff haben? Damit geben die Verfasser teils hochgesteckte Zielvorstellungen aus, ohne die Operationalisierung darzulegen. Sie machen verständlich, dass sie die Erfordernisse erkennen und die Absicht verfolgen, die vorhandenen Probleme anzugehen beziehungsweise einen Sollwert zu erreichen. Dabei ist die Strategie regelmäßig unverbindlich und inexakt, sodass sie vorrangig dazu dient, ein Zukunftsbild zu setzen. Das verdeutlicht sich unter anderem mit 8.2.4. Hier fasst das Innenministerium den Vorsatz, „Unternehmen in Deutschland schützen“ zu wollen und stellt in diesem Zuge fest, dass „KMU [...] den Herausforderungen aufgrund von Mängeln an Ressourcen und Wissen nicht ausreichend gewachsen“ sind (Bundesministerium des Innern, für Bau und Heimat 2021a, 61). Aus diesem Grund sind vier Zielvorstellungen zu erreichen:

1. „Die Zusammenarbeit zwischen Staat und Wirtschaft wurde weiter ausgebaut“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 61).
2. „Die Interaktion der Unternehmen mit den zuständigen Stellen in den Teilbereichen Prävention, Detektion und Reaktion der Cybersicherheit ist gestärkt“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 61).
3. „Maßnahmen zum Schutz von Unternehmen (insbesondere KMU), Rüstungsindustrie und Unternehmen mit deutscher Schlüsseltechnologie werden in Abstimmung mit und im Zusammenwirken von Bund und Ländern durchgeführt“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 61).
4. „Die Unternehmen und insbesondere KMU sind für IT-Sicherheit sensibilisiert, sie besitzen ein erhöhtes Problembewusstsein für Cyberrisiken und verfügen über entsprechende Beurteilungs- sowie Lösungskompetenzen“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 62).

Weder diese Wunschzustände noch die Beschreibung der Ausgangslage enthalten dabei Informationen über mögliche Maßnahmen, die Aufschluss über Instrumente oder Methoden geben könnten. Die Prüfkriterien bestehen aus stärker frequentierten Förder- oder Informationsprogrammen der Bundesregierung, erhöhten Mitgliederzahlen in Wirtschaftsverbänden oder aber einer geringeren Betroffenheit von Unternehmen

(vgl. Bundesministerium des Innern, für Bau und Heimat 2021a, 62). Obwohl das BMI auch in diesem Fall große Ambitionen formuliert und den Wirtschaftsschutz nachhaltig potenzieren möchte, finden sich in der Strategie nur generische und prozedurale Floskeln, die keine Informationen über die operative Umsetzung enthalten und vor allem keine fundamentalen Richtungswechsel anzeigen. Das Ministerium arbeitet Gegenwartszustände aus, die es mit Ideen einer optimierten Sicherheitszukunft verwebt. Es inszeniert sich als sorgende Behörde, die sich 44 Ziele steckt, die es wiederum innerhalb weniger Jahre zu erfüllen gilt. Die betont ehrgeizige Planung schafft es vor allem, das Ministerium als umtriebige Institution zu positionieren und dokumentiert nebenher, wie diffizil die digitalen Erfordernisse der Zeit sind.

Die Cybersicherheitsstrategie gibt vor, dass die Themen alle auf der Sicherheitsagenda der Bundesrepublik sind; alle gleichzeitig, alle gleichrangig und alle lösbar. Das BMI schafft es insbesondere über den Aufbau, über die Erzählstruktur des Papiers, diese Gleichordnung glaubhaft zu machen. Indem jedes Handlungsfeld eine Kurzgeschichte bildet, läuft es nicht Gefahr, anderen Feldern subordiniert zu werden. Die Geschichten beginnen mit der Frage, *Wo stehen wir?*, dem Ausgangspunkt der Erzählung, gar einer Heldenreise. Denn wenngleich jedes Handlungsfeld unterschiedliche Akteure benennt, ist das BMI selbst die konstante Größe, die in der Pflicht ist, sich der Herausforderung zu stellen. Mit der Frage, *Was wollen wir erreichen?*, definiert das BMI den Zielpunkt der Reise, an deren Ende steht, dass das Hindernis überwunden und das Idealgefüge hergestellt wurde. *Welche Wirkung erwarten wir?* entpuppt sich als ein narrativer Kunstgriff, da sich an dieser Stelle die zu erwartende Bilanz ausschmücken lässt, bevor sie überhaupt eintreten kann. Die Erfolgsgeschichte wird vorweggenommen und ihr Gelingen vorab attestiert. Exemplarisch kann das Ziel herangezogen werden, Verschlüsselung als Voraussetzung eines souveränen und selbstbestimmten Handelns flächendeckend einzusetzen:

Die konsequente Verschlüsselung digitaler Kommunikation und Speicherung erschwert den unerlaubten Zugriff und die Ausnutzung erheblich. Staat, Wirtschaft und Gesellschaft werden besser vor Cyberrisiken geschützt. Des Weiteren schaffen sichere Kommunikationsmöglichkeiten Vertrauen und Verlässlichkeit in einer digitalisierten Umgebung. Dies eröffnet Chancen für die Digitalisierung weiterer Lebensbereiche, für neue Geschäftsmodelle und weitere technische Innovationen (Bundesministerium des Innern, für Bau und Heimat 2021a, 49).

Mit qualitativen Beschreibungen der vermeintlich nahenden Zukunft durch Adjektive wie *sicher, besser, konsequent* oder *digitalisiert* zeichnet das Ministerium eine einseitige Imagination; in dem Fall eine Vision technologischen Fortschritts, die eine unumstößlich positive kollektive Zukunftsvariante aufzeigt. Der Absatz endet gar mit dem Versprechen einer erfolgreichen Digitalisierung und der Aussicht auf wirtschaftlichen Aufstieg. Aus dieser Warte, die unter anderem inhärente Risiken oder schadhafte externe Koeffizienten missachtet, gestaltet das BMI sein Zielbild nicht als einfach notwendig oder vielleicht mühsam, sondern als schmackhaft und erstrebenswert. Derart absolute Formulierungen finden sich immer wieder unter der Überschrift, *Welche Wirkung erwarten wir?*, zum Beispiel auch, wenn von sicherer Quantentechnologie die Rede ist: „Durch die Nutzung der Potenziale und die Minimierung der Risiken [...] wird ein nachhaltig hohes IT-Sicherheitsniveau zum Schutz von Staat, Wirtschaft und Gesellschaft gewährleistet“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 74). An anderer Stelle verspricht die Strategie europaweit homogene Sicherheitslösungen. Man erwarte in der Folge, dass „Verbraucherinnen und Verbraucher [...] durch die Nutzung gekennzeichnete Produkte geschützt“ seien (Bundesministerium des Innern, für Bau und Heimat 2021a, 37). Ferner sei bis zum Ende des Planungszeitraum 2025 oder 2026 das Vertrauen der Anwender in sichere Technik untermauert, „das Cybersicherheitsniveau im europäischen Binnenmarkt insgesamt erhöht“, „das Sicherheitsbewusstsein in Unternehmen und Wissenschaft gestärkt“ und „die Wettbewerbsfähigkeit europäischer Unternehmen“ belebt (Bundesministerium des Innern, für Bau und Heimat 2021a, 37). Es zeigt sich also auch hier, dass die Ziele mit Erwartungen angereichert werden, sodass sie zu Trägern zahlreicher, vornehmlich technophiler, Zukunftsvisionen werden. Diese Imagination kommt daher wie ein Ideal, seine Realisierung wird somit zum Bedürfnis: Die Strategie sät die Idee einer renommierten Informationstechnik Made in Germany. Sie suggeriert, dass mit dem Erreichen der Ziele Endanwender sicher und IT-Bedrohungen unter Kontrolle seien – aus dem stetig mahnenden Gefahrendiskurs soll hier schließlich ein Kontrolldiskurs werden. Mit den neuen Messkriterien schafft man ein potenzielles Instrument, um die Zielerreichung nachvollziehbar zu gestalten respektive um mehr Transparenz und demokratische Partizipation zu erlauben. Aber obwohl das Innenministerium die eingeführten Messkriterien als eminenten Fortschritt der Strategie identifiziert, fehlt der entscheidende Schritt zu tatsächlich einheitlich quantifizierbaren Erfolgsvorgaben. Denn zur „Umsetzung werden durch die Strategie

keine verbindlichen Vorgaben gemacht“ (Bundesministerium des Innern, für Bau und Heimat 2021a, 129). Stattdessen generieren die untergeordneten Institutionen ihre Zielsetzungen selbst. Insofern sind die strategischen Handlungsziele weniger spezifisch oder messbar und somit weniger SMART als vorgegeben.

Die substanzielle Leistung der deutschen Cybersicherheitsstrategie liegt vielmehr in ihrer Anlage als Bestandsaufnahme mit anschließender Absichtserklärung. Der Plan figuriert eine Vorstellung einer deutschen IT-Sicherheitslandschaft, wie sie dem Innenministerium zufolge ist und wie sie in wenigen Jahren sein sollte. Damit visualisiert das Ministerium auf der Informationsebene die Diskrepanz zwischen Ausgangspunkt und Destination. In der dramaturgischen Dimension erstellt es derweil eine befangene Wirklichkeitsvorstellung mit einer entsprechenden Imagination des künftigen Ideals; und präsentiert stets das Ministerium als Wegbereiter zu diesem Zustand. Denn die Beispiele demonstrieren, es handelt sich bei der Cybersicherheitsstrategie nicht um das wertfreie Abwägen objektiver Nutzeffekte und ihrer Kehrseiten, sondern um die Positionierung des Staates respektive des zuständigen Ministeriums als handelnder Protagonist, als technologischer Vorreiter. Die Strategie ist ein politisches Instrument, mit dem Zielvorstellungen transparent gemacht und bereits als Erfolge gefeiert werden können, schon bevor eine reale Konsequenz feststellbar ist. Deshalb darf die Cybersicherheitsstrategie unpräzise sein und Perspektiven ausgeben; sie sollte aber auch nur unter dieser Annahme gelesen werden.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	O	O			O	O		O			O

Vor allem diese 44 strategischen Ziele, die vielmals auf unvalidierten Hypothesen ruhen, geben den Anstoß, die Cybersicherheitsstrategie als überwiegend subjektiv zu kategorisieren. Wie schon festgestellt, sind Teile dieser Ziele bereits bei Vorlage der Strategie erreicht oder sie sind nicht selten so gefasst, dass sie unausweichlich erreicht werden. Damit orientiert sich die Zielformulierung nicht ausschließlich an einer bestehenden Bedrohungslage, sondern an politischen Vorzügen. Folglich ist dieses Papier aber auch – obschon einige Ziele mutlos gefasst sind – ein Ausdruck von Progression. Denn der Zweck der Strategie liegt darin, die deutsche Sicherheitslandschaft zu justieren, um den veränderten systemischen Grundwahrheiten gerecht werden zu können. Dazu handelt es sich um ein in mehrerlei Hinsicht innen

gerichtetes Dokument. Die Verfasser des Ministeriums richten ihre Botschaften an die deutsche Bevölkerung, an die deutsche Wirtschaft und an Landes- oder Kommunalpolitik, um einen Fahrplan vorzulegen; ausländische Adressaten gibt es kaum. Die Handlungsfelder und Absichtsformulierungen enthalten nur wenige außenpolitisch wirksame Vorsätze. Trotz deutlicher Intentionen, etwa die Kompetenz der Verbraucher zu fördern oder die Anwenderfreundlichkeit von IT-Produkten in den Blick zu nehmen, sind die formulierten Absichten technikzentriert; selbst innerhalb von Handlungsfeldern mit anwenderbezogenem Titel (vgl. Bundesministerium des Innern, für Bau und Heimat 2021a, 30ff). Das Ministerium gibt damit vor, auch weiterhin mehr auf die Absicherung von Infrastruktur, auf Verschlüsselung und Security-by-Design zu setzen als auf die Stärkung von Medienkompetenzen und mehr Handlungsempfehlungen oder Aufklärungskampagnen. Zwar zeichnen die Autoren der Strategie ein durchaus positives, ambitioniertes Bild von einer Zukunft mit maximierter Sicherheit im Digitalraum bei gleichzeitigem Ausbau der deutschen IT-Wirtschaft. Dennoch nimmt die Cybersicherheitsstrategie dafür zuvorderst stets die Vermeidung von Risiken in den Blick, statt die darin liegenden Potenziale zu unterstreichen. Die Autoren widmen gleich zu Beginn mehrere Seiten der Beschreibung aktueller und bevorstehender Gefahren und räumen so der Imagination von Unsicherheit als Hebel ihrer Programmatik großen Raum ein.

2.3.6 IT-Investitionen des Bundes

Dieses Kapitel führt vorneweg eine Prämisse ein: Das Kapital, das ein Staat für gewisse Zwecke anlegt, reflektiert die Priorität, die der Staat diesen Zwecken beimisst. Mit der Budgetierung, die zur Bewältigung oder mindestens zur Eindämmung einer Problemstellung aufgewendet wird, ordnen sich die Dinge anhand ihrer manchmal auch nur scheinbaren Dringlichkeit. In seiner Diagnose über *Das Geld und die Medientheorie* hält Jens Schröter fest, dass die Zentralität des Geldes im Kapitalismus „eine tiefgreifende Semiotisierung und Medialisierung“ desselben einschließt, man folgerichtig eine „primordiale Medienökonomie“ identifizieren kann (Schröter 2018, 67). So „sind im Rahmen der Dominanz des Geldes doch alle Dinge, sofern sie Waren sind, auch medial“ und „[...] speichern und übertragen als Waren Informationen über ihren <Wert>“ (Schröter 2018, 68). Aufgrund der Endlichkeit der Ressource Geld und des daraus folgenden Drucks, haushalten zu müssen, entsteht bei jeglicher Finanzplanung eine Hierarchie der Notwendigkeiten. Diese meist

unausgesprochene Klassifizierung ist ein wichtiger Indikator für die Gewichtung einer Aufgabe durch Staat und Gesellschaft und stellt zugleich ein Werkzeug der politischen Akzentuierung dar. Die Staatsausgaben können somit als Gradmesser verstanden werden – einerseits für ebenjenen Wert der Ware Informationssicherheit, andererseits für das Engagement auf diesem Feld.

Solche Investitionen unter anderem in Cybersicherheit sind selbstverständlich Bestandteil des Bundeshaushalts, der jedes Jahr aufs Neue vom Bundesfinanzministerium vorgelegt und vom Bundestag bestätigt wird. In dieser Haushaltsplanung sind für das Jahr 2021 Gesamtausgaben in Höhe von 498,62 Milliarden Euro bei einem Finanzierungsdefizit, also einem benötigten Kreditvolumen von circa 180 Mrd. Euro für alle Beschaffungen, Förderungen, Sozialausgaben oder Investitionen der Einrichtungen des Bundes, vorgesehen (vgl. Bundestag 2021a, 34). Von diesen 498,62 Mrd. Euro entfallen dann zum Beispiel 1,68 Mrd. Euro auf Maßnahmen des Umweltschutzes, während 1,49 Mrd. Euro für den Bergbau angedacht sind (vgl. Bundestag 2021a, 41f). Ganze 9,8 Mrd. Euro investiert der Bund in Straßen; in Eisenbahnen und den öffentlichen Personennahverkehr sogar 16,32 Mrd. Euro (vgl. Bundestag 2021a, 43). „Der Verteidigungsetat liegt im Haushaltsjahr 2021 bei 46,93 Milliarden Euro. Gegenüber dem Haushalt 2020 ist er um 2,8 Prozent gestiegen“ (Bundesministerium der Verteidigung 2021c). Damit zählt der Verteidigungshaushalt zu den größten jährlichen Posten des Bundes. Schon die Verwaltung der Bundeswehr verbraucht 6,06 Mrd. Euro. Die gesamte zivile, öffentliche Sicherheit hat dagegen einen Etat von 8,13 Mrd. Euro (Bundestag 2021a, 39). Die aber mit Abstand größten Aufwendungen der Bundesrepublik entstehen durch sozialstaatliche Leistungen, 2021 insgesamt 253,24 Mrd. Euro, von denen zum Beispiel das Arbeitslosengeld II auf 23,7 Mrd. Euro beziffert wird (Bundestag 2021a, 40f). Selbstverständlich bilden diese Zahlen nur einen Querschnitt des mehrere tausend Seiten fassenden Bundeshaushalts 2021 ab, jedoch geben sie einen Eindruck von den Größenordnungen der Ausgaben.

In diese Relationen lassen sich nun die Aufwendungen zur Förderung der IT-Sicherheit in Deutschland durch den Bund einsortieren. Dazu lohnt an dieser Stelle der Blick zurück auf diejenigen Einrichtungen des Bundes, die sich auf staatlicher Seite in der Hauptsache mit IT-Sicherheit befassen. Gleichzeitig muss erwähnt werden, dass genaue Zahlen stellenweise schwer zu bemessen sind, da Investitionen in Cybersicherheit einerseits nicht zentral vorgenommen und andererseits nicht zwingend als Einzahlung in

Sicherheit verbucht werden, sondern in die Beschaffung neuer Geräte oder in die Fortbildung von Mitarbeitern fließen kann. Gleichwohl geben die nachstehenden Summen einen Eindruck des finanziellen Aufwands auf diesem Gebiet. So mobilisiert das Bundesinnenministerium von seinem Gesamtvolumen, das bei 18,46 Mrd. Euro liegt, etwa 2,43 Mrd. Euro in „IT und Netzpolitik, Digitalfunk und Moderne Verwaltung“ (Bundestag 2021a, 547/573). Diese Summe finanziert unter anderem die IT-Konsolidierung des Bundes oder aber den Digitalfunk. Den mit Cybersicherheit betrauten Institutionen steht jedoch nur ein Bruchteil dessen zur Verfügung. Demnach kann das Bundesamt für Sicherheit in der Informationstechnik 2021 über 197,2 Mio. Euro verfügen, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich hat sogar nur 64,6 Mio. Euro zur Verfügung (vgl. Bundestag 2021a, 721/726). Die Agentur für Innovation in der Cybersicherheit befindet sich noch im Aufbau und kann zu diesem Zweck auf drei Jahre verteilt insgesamt 350 Mio. Euro ausgeben (vgl. Bundesministerium des Innern, für Bau und Heimat 2021b). Hinzu kommen weitere Behörden, die hier zuvor als wichtige Akteure für die IT-Sicherheit in Deutschland benannt wurden, aber auch andere Aufgabenfelder zu bestellen haben. Das Bundeskriminalamt zum Beispiel gibt etwa 193,9 seiner 791,6 Mio. Euro für „Aufträge und Dienstleistungen im Bereich Informationstechnik“ aus (Bundestag 2021a, 739). Für den gleichen Posten zahlt das gesamte Ressort des Bundeskanzleramts lediglich 46,7 Millionen seiner 3,6 Mrd. Euro, obwohl dort bekanntermaßen die Staatsministerin für Digitalisierung angesiedelt war (vgl. Bundestag 2021a, 237). Zum nachgeordneten Bundesnachrichtendienst sowie dem Verfassungsschutz werden keine detaillierten Einzelhaushalte veröffentlicht, sodass spezifische Ausgaben für Informationstechnik und sichere Infrastruktur nicht zu beziffern sind. Für einen der größten Auftraggeber des Bundes liegt ein solcher Plan dagegen vor. So ist nachzulesen, dass die Bundeswehr für „Aufträge und Dienstleistungen im Bereich Informationstechnik“ allein in 2021 Zahlungen in Höhe von rund 1,08 Mrd. Euro vornimmt (Bundestag 2021a, 2299).

Die folgende Tabelle fasst die genannten Zahlen anschaulich zusammen und rahmt sie mit kontextualisierenden Daten. Sie zeigt, wie hoch die Ausgaben der Bundesrepublik Deutschland für Informationstechnik und -sicherheit in Relation zu den Gesamtausgaben des Staates, aber auch einzelner Institutionen, ist. Um die Vergleichbarkeit gewährleisten zu können, wurden die gerundeten Summen in Millionen Euro angegeben. Dazu wurden die Positionen „Aufträge und

Dienstleistungen im Bereich Informationstechnik“ und „Erwerb von Anlagen, Geräten, Ausstattungs- und Ausrüstungsgegenständen sowie Software im Bereich Informationstechnik“ sowie gegebenenfalls ressortbedingte IT-Investitionen aus den Einzelplänen des Bundeshaushaltes 2021 ermittelt und addiert:

Einrichtung	Gesamtetat für das Jahr 2021 (in Mio. €)
Bundesrepublik Deutschland	498 620
sozialstaatliche Leistungen	253 240
Deutscher Bundestag	1 060
Bundesministerium der Verteidigung	46 930
davon für Informationstechnik	1 572
Bundesministerium des Innern, für Bau und Heimat	18 458
davon für Informationstechnik	2 429
Bundesministerium für Verkehr und digitale Infrastruktur	41 354
davon für Informationstechnik	1 404,6
Bundesministerium für Bildung und Forschung	20 799
davon für Informationstechnik	350,2
Sonderfall „Digitalpakt Schule“	4 194
Bundesministerium für Wirtschaft und Energie	10 434
davon für Informationstechnik	113,6
Sonderfall „Innovation, Technologie und Neue Mobilität“	416,4
Bundesministerium der Finanzen	8 742
davon für Informationstechnik	1 528,5
Statistisches Bundesamt	268,5
davon für Informationstechnik	90,8
Bundeskriminalamt	791,6

davon für Informationstechnik	193,9
Auswärtiges Amt	6 302
davon für Informationstechnik	227,2
Bundespolizei	4 729
davon für Informationstechnik	253,5
Bundeskanzleramt	3 652
davon für Informationstechnik	46,7
Informationstechnikzentrum Bund	849,2
Bundesnetzagentur	262,7
Agentur für Innovation in der Cybersicherheit	350 ²¹
Zentrale Stelle für Informationstechnik im Sicherheitsbereich	64,6
Bundesamt für Sicherheit in der Informationstechnik	197,2

Quelle: Haushaltsgesetz 2021 (Bundestag 2021a)/(Bundeshaushalt 2021)

Die Aufstellung demonstriert, dass Behörden, die nicht vorwiegend der Cybersicherheit verschrieben sind, Informationstechnik finanziell zumeist nur gering berücksichtigen. Das verdeutlicht sich etwa darin, dass die Einzelhaushalte der Bundesämter und Ministerium nur selten große monetäre Töpfe für die Digitalisierung und Absicherung der Administration vorsehen. So plant beispielsweise das Bundeskanzleramt lediglich 1,28 % seines Jahresetats 2021 für IT ein, das Bundesministerium für Bildung und Forschung nur 1,68 %²². Für das Auswärtige Amt nimmt Informationstechnik einen etwas höheren Stellenwert ein, da es bereit ist, 3,6 % des Einzelhaushalts hierfür zu reservieren. Das Bundesministerium für Verkehr und digitale Infrastruktur mobilisiert dagegen 17,48 % des Jahresbudgets 2021 für IT, das Bundeskriminalamt sogar 24,5 %. Daneben haben Schlüsselinstitutionen für die deutsche Cybersicherheit wie BSI oder

²¹ Finanziert sich bis 2023 aus den Haushalten des BMVg und des BMI.

²² Ohne Berücksichtigung des Digitalpakt Schule.

ZITiS nur vergleichsweise geringe Budgets – gemeinsam etwa so viel wie das Statistische Bundesamt. Die 197,2 Millionen Euro, die dem BSI 2021 zur Verfügung stehen, entsprechen 0,04 % des Bundeshaushaltes.

Bei den in der Tabelle ermittelten, teils addierten Summen handelt es sich um Zahlungen für Technologie und zugehörige Dienstleistungen; vereinzelt fallen beispielsweise zusätzlich flexibilisierte Ausgaben an. Die Daten geben also nur bedingt Auskunft darüber, wie hoch der Anteil für unmittelbare Investitionen in die Sicherheit der Netze, Infrastrukturen oder in Schulungen für die Bedienenden der Technik ist. Zudem bilden die Beispiele eine Auswahl des staatlichen Einsatzes für Informationstechnik ab. Diese exemplarische Selektion der Institutionen dieses Kapitels führt explizit nicht zu einer definiten Messgröße, zeigt aber durch die schlichte Addition der obigen Ausgaben die Bedeutsamkeit von Informationstechnik in direkter Konkurrenz zu den übrigen Aufwendungen. Insbesondere wenn man berücksichtigt, dass diese Posten wiederum nur zu einem nicht näher bestimmbar Anteil in die Sicherheit von Informationstechnik fließen, offenbart sich, wie gering die anzunehmenden Kosten für diesen Sektor ausfallen. Demgegenüber steht allerdings eine Zahl des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien, Bitkom: Im Jahr 2019 hat Cyberkriminalität in Deutschland demnach „102,9 Mrd. Euro Schaden“ an der deutschen Wirtschaft angerichtet (Bitkom 2020, 23). Damit übertrafen die Schäden durch Internetkriminalität jene durch Umweltkatastrophen in Deutschland um etwas das Achtfache, trotz des Ahrtal-Hochwassers (vgl. Gesamtverband der Versicherer 2022). 2020 und 2021 wuchs diese Schadenssumme bereits auf deutlich über 200 Milliarden Euro an – und damit nahezu auf die Hälfte des jährlichen Bundeshaushaltes (vgl. Bitkom 2022, 9). Obwohl also die Bedrohung durch Cyberangriffe derart eindrücklich belegbar ist, genießt die digitale Sicherheit zumindest monetär für Bundesregierung und -verwaltung keine entsprechende Priorität. Denn die Ware Informationssicherheit erhält mit der Budgetierung des Bundes einen Wert, der wiederum eine mediale Nachricht vor sich herträgt: Die Höhe der oben genannten Aufwendungen bestimmt, dass Cybersicherheit weniger diskutiert wird als es der Fall wäre, wenn die Ausgaben beispielsweise denen für die physische Sicherheit ähneln würden. Das determiniert unter anderem, dass die Öffentlichkeit nicht mit Interesse anknüpft und schließlich auch, dass Kabinett und Parlament die Cybersicherheit auch zukünftig im finanziellen Wettbewerb mit den zahlreichen weiteren Herausforderungen

des Bundes nachordnet. Die Priorisierung oder Nichtpriorisierung gibt nicht zuletzt preis, wie die Risikoabwägung der Entscheider ausgefallen ist; in diesem Fall werden die Kosten der erwartbaren Schäden in Kauf genommen und den Kosten für die Absicherung vorgezogen.

2.4 Querschnitt: Niederlande zwischen 1910 und 2022

Wie schon zuvor zur Bundesrepublik Deutschland erfolgt in diesem Absatz vor allem eine Einordnung der Niederlande unter Betrachtung historischer, politischer, sozialer und kultureller Gesichtspunkte.

Das Königreich der Niederlande im heutigen Verständnis ist eine parlamentarische Monarchie, wie es sie dort erst seit 1954 gibt (vgl. Overheid 1954). Es besteht aus vier Ländern mit je eigener Autonomie, namentlich die Niederlande, Aruba, Curaçao und Sint Maarten. Dabei blickt das Königreich auf ein Vorgängerreich mit einer bis ins 15. Jahrhundert reichenden Geschichte zurück, das während der darauffolgenden Epochen Kolonien überall auf dem Globus anhäufte, die bis zum Dekolonialisierungsprozess nach dem Zweiten Weltkrieg andauerten (vgl. Lademacher 1993, 15f/284ff). Das Königtum in seiner aktuellen Ausformung dient vornehmlich als Bezugsrahmen für die Bürger der vier Länder und als einender Identifikationsanker mit dem König als repräsentatives Oberhaupt. Die Regierungsverantwortung der Niederlande liegt derweil in Händen zweier Kammern, die gemeinsam das Parlament bilden. Diese Volksvertretung beschließt Gesetze über zwölf zwar integrierte, aber ökonomisch selbst verwaltende Provinzen (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2019, 26).

Im Gegensatz zu Deutschland setzt die relevante historische Erzählung bereits kurz vor dem Zweiten, sogar vor dem Ersten, Weltkrieg ein, nämlich zu Beginn der 1910er-Jahre. Zu dieser Zeit erlangten die Niederlande Renommee in juristischen Belangen, indem sie erreichten, dass internationale Verträge über das Zivil- und Familienrecht geschlossen wurden. Hierdurch erhielt schließlich 1911 der Amsterdamer Tobias Asser den Friedensnobelpreis (vgl. Kennedy 2017, 297). Diese Position der Niederlande als Verfechter multinationaler Rechtssprechung und als Gastgeber mehrerer Friedenskonferenzen legte vermeintlich den Grundstein für die Einrichtung des Ständigen Internationalen Gerichtshofs 1922 in Den Haag und dem im Jahr 1946 darauffolgenden Internationalen Gerichtshof. Die Niederlande behaupteten sich in ihrer

Neutralität, die sie auch im Verlauf des Ersten Weltkriegs beibehielt (vgl. Lademacher 1993, 520f). Dabei ist anzunehmen, dass diese Nichteinmischung weniger aus politischer Überzeugung erfolgte, sondern vielmehr aus der „Furcht vor außenpolitischer Abhängigkeit von den europäischen Mächten“ sowie globaler Handelsverwebungen (Lademacher 1993, 522). Diesem Pragmatismus, hervorgerufen durch ein militärisches Prekariat bei gleichzeitiger Bedrohung durch Deutschland und Großbritannien, entwuchs eine niederländische Politikkultur, die erst mit dem Beitritt zur NATO 1949 abebbte: „die Niederlande als der Prototyp der geruhsamen Existenz“ (Lademacher 1993, 521). James Kennedy sieht in obiger Gefährdungslage, der einheitlichen Sprache, dem Dienst unter einem König und der Neutralitätsposition wesentliche Züge der niederländischen Identität der 10er- und 20er-Jahre (vgl. Kennedy 2017, 293).

Seit jeher gibt es aber einen weiteren Identifikationsimpuls, der einen maßgeblichen Anteil am wirtschaftlichen wie auch sozialen Geschehen hat. Denn bedingt durch ihre niedrige geografische Lage war und ist das Meer zugleich Motor für Handel, Expansion sowie rasantes ökonomisches Wachstum, stellte jedoch zugleich eine der größten ständigen Bedrohungen dar. So liegt etwa ein Drittel der gesamten Landfläche derzeit unter dem Meeresspiegel – Tendenz steigend – und kann nur aufgrund menschengemachter Strukturen vor der Überschwemmung geschützt werden. Wiederkehrende Sturmfluten, beispielsweise von 1916 oder 1953 töteten tausende Menschen und richteten verheerende Schäden an (vgl. Kennedy 2017, 308/334). Die Angst vor dem nächsten Hochwasser veranlasste die zuständigen Behörden dazu, mehr als 3700 Kilometer Küstenschutzanlagen zu erbauen und modernste Frühwarnsysteme zu installieren (vgl. Rijkswaterstaat 2020). Die Niederlande waren somit schon immer zu stetigen Innovationen im Dammbau und der Anpassung ihrer Infrastruktur an neue Gegebenheiten gezwungen, um die existenzielle Bedrohung abzuwenden, die heute durch den voranschreitenden Klimawandel immer drängender wird. In der Folge bildet das Verhältnis zur See und die möglichst effektive Verwendung ihrer Vorzüge einen wesentlichen Bestandteil für das Zusammenleben in den Niederlanden, aber auch für den wirtschaftlichen Erfolg.

Nach der passiv-neutralen Kriegserfahrung von 1914 bis 1918 war die Gesellschaft geprägt von der Verzuiling²³, dem wirkungsmächtigsten niederländischen Sozialkonstrukt des 20. Jahrhunderts. Bereits 1918 übernahmen konfessionelle Parteien in Koalitionen aus Katholiken und Protestanten die Regierungsverantwortung. Sie förderten jene Organisationen und Interessenverbände, die ihrer religiösen und politischen Überzeugung nahestanden und schufen auf diese Weise eine sich selbst verstärkende Struktur des institutionalisierten Pluralismus, die Säulen (vgl. Kennedy 2017, 304f). Diese Säulen sozialer, politischer oder religiöser Art erzeugten parallel existierende Lebensräume, die sich jedoch alle als Niederländisch verstanden. „Deze verdeeldheid was diep en duurzaam, omdat ze gebaseerd was op serieuze verschillen van inzicht over de inrichting van de Nederlandse samenleving“²⁴ (Kennedy 2017, 292). Das Phänomen der Versäulung setzte sich sogar nach 1945 fort und hielt noch bis in die 80er-Jahre des letzten Jahrhunderts an. Für die Menschen im Land bedeutete das, dass ein Kind aus einem katholischen Haus eine katholische Schule besuchte, einem katholischen Freizeitverein beitrug und später wiederum eine katholische Familie begründete (vgl. Wielenga 2007). Alle Bezugsparameter des zivilen Lebens verliefen in einem vorwiegend konfessionell determinierten Umfeld. Die vertikalen Säulen ließen nur bedingt horizontalen Austausch zu, sodass sich weltanschauliche Blöcke bildeten, die einzig gemein hatten, sich als Niederländer und Bürger unter dem Koninkrijk der Nederlanden zu verstehen.

Obgleich aufgrund der gläubigen Strömungen anzunehmen wäre, dass die Niederlande nach dem Ersten Weltkrieg in eine Zeit des Reaktionismus verfielen, hielten auch hier wie in anderen Ländern Europas die bemerkenswerten Fortschritte in Mobilität, Industrie oder Ingenieurwissenschaften Einzug. Die grundverschiedenen Säulen aus Katholiken, Protestanten, Sozialdemokraten und Liberalen teilten das Bedürfnis nach technologischer Progression und Partizipation an den Vorzügen der Moderne, sodass die Jahre bis zur Weltwirtschaftskrise als in vielerlei Hinsicht progressiv zu bezeichnen sind (vgl. Kennedy 2017, 306ff). Trotz der abgeschotteten Verschiedenheit der Säulenangehörigen bestand Einigkeit darin, handlungsfähig bleiben zu wollen. So bildete sich eine „pragmatische Toleranz“ heraus: Die Andersartigkeit der jeweils sonstigen Säulen wurde hingenommen, um das Ziel der Befriedung zwischen den

²³ Deutsch: Versäulung

²⁴ Deutsch: Diese Uneinigkeit war tiefgreifend und nachhaltig, da sie auf gravierenden Meinungsverschiedenheiten über die Struktur der niederländischen Gesellschaft beruhte

isolierten Gebilden erreichen zu können (Wielenga 2007). „Aufgrund der treuen und gehorsamen Haltung der innerhalb der Säulen organisierten Masse verfügten die jeweiligen Säuleneliten über den notwendigen Spielraum für ihre überdachende Zusammenarbeit“ (Wielenga 2007).

Die trotz der Versäulung weiterhin kollektive Verbundenheit im Land voller religiöser und ethnischer Minderheiten, vor allem aus den zahlreichen Kolonialgebieten, verstärkte sich durch die gemeinsamen traumatischen Ereignisse des Zweiten Weltkriegs noch. Die plötzliche aber lange währende Besatzung durch das Dritte Reich zwischen 1940 und 1945 drängte die Niederlande in eine widerstrebende Opferrolle, sodass sich das Kollektiv gegen den Aggressor, das unausweichliche Feindbild, formieren konnte. „Die Besatzungsmacht stand da, bis an die Zähne bewaffnet und rassenideologisch fanatisiert, als eine unüberwindliche Realität“ (Lademacher 1993, 599). Die ab 1942 vermehrt aufkommenden Deportationen in Arbeitslager und Konzentrationslager festigten die Bitterkeit gegen das Deutsche Reich (vgl. Lademacher 1993, 580). Aus dieser tiefen Einigkeit im Widerstand gegen die deutschen Besatzer speiste sich zugleich die Verachtung für die Vielzahl an Kollaborateuren, die Hitlers Machtapparat bei Verwaltung und öffentlicher Ordnung stützten, aber auch bei Völkermord und Kriegsverbrechen gegen die eigenen Mitmenschen. Ganz nach dem Ausspruch *goed of fout*²⁵ galt für lange Zeit ein Schwarzweiß-Prinzip in der niederländischen Vergangenheitsbewältigung, demzufolge jede Form nicht aktiven Widerstands bereits als Zusammenarbeit mit dem Feind verstanden wurde (vgl. Lademacher 1993, 595).

Nach dem Kriegsende trafen in den Niederlanden Zukunftswünsche auf Gegenwartsrealität. Nach der Niederlage Japans entstand ein aus kolonialistischer Sicht vielversprechendes Machtvakuum in Südostasien. Gleichzeitig strebte man im Inland eine politische Erneuerung an (vgl. Kennedy 2007, 327ff). Tatsächlich aber stand in Indonesien der nächste militärische Konflikt bevor, den die Niederlande schließlich verloren und auch innenpolitisch vollzog sich eher eine Restauration statt einer Modernisierung. In den Nachkriegsparlamenten weilten weitestgehend Abbilder der Vorkriegskoalitionen. Die Niederländer fanden Halt in der währenden Treue zu ihren politisch-sozialen Säulen, dem Blick in die Zukunft und dem Wiederaufbau.

²⁵ Deutsch: richtig oder falsch

„Gemeinschaftszin, zelfdiscipline en noeste arbeid leken kenmerkend voor de Nederlanders in den jaren vijftig“²⁶ (Kennedy 2007, 336). Erneut war diese Zeit von einer über den Säulen stehenden nationalen Solidarität geprägt, die das Land zusammenhielt. Und wieder waren die Bürger beseelt von der Aussicht auf Fortschritt und Wohlstand: Man adaptierte schnellstmöglich originell Technologien, während Wahrzeichen der Progression wie die großen Häfen weiter anwuchsen. Die neuen, damals futuristisch anmutenden Hochwasserschutzsysteme taten ihr Übriges bei der Rekonstruktion eines zukunftsweisenden Paradigmas (vgl. Kennedy 2007, 341). Die Niederlande wurden zu dem, was man eine *selffulfilling prophecy* nennt: Man war geeint in dem Gefühl, modern zu sein, also wurde das Land im Zuge des Wiederaufbaus modernisiert.

Wie vielerorts auf der Welt führten die 60er- und 70er-Jahre auch in den Niederlanden zu zahlreichen gesellschaftlichen und politischen Umwälzungen. In Amsterdam bildeten sich dynamische Jugendkulturen, bedeutsame Künstlerkollektive, starke feministische Aktionsgruppen und Freiräume für Unterdrückte wie Homosexuelle, die allesamt das liberale Bild der Niederlande weitertrugen (vgl. Kennedy 2007, 352f). Diese Veränderungen gingen einher mit einer Auflösung des Säulensystems, dessen Auswirkungen dennoch viele weitere Jahre spürbar waren:

Veel Nederlanders worstelden zich los uit oude verbanden, die zij steeds meer begonnen te ervaren als knellend of niet meer relevant. Zij voelden zich vrij om hun eigen levensstijl te ontwikkelen in de nieuwe consumentenmaatschappij en verzorgingsstaat²⁷ (Kennedy 2007, 350).

Das Land trieb zu dieser Zeit eine Vielzahl sozialer Unruhen um, darunter auch die Entsäulung. Die fortschreitende Modernisierung der Gesellschaft hatte die in gleichem Maß abnehmende Bedeutung der Konfession zur Folge. Die religiös bestimmten Säulen verloren ihre Legitimierung und so waren auch die politischen Repräsentanten der Gemeinschaften ohne Unterstützung. Vor dem Hintergrund des aufblühenden Liberalismus entstanden neue Parteien, wie die überkonfessionelle CDA, während Individualisierung und Säkularisierung voranschritten (vgl. Lademacher 1993, 668). Die vielen sozialen Bewegungen in den 1970er-Jahren ließen in der Breite den Eindruck

²⁶ Deutsch: Gemeinschaftssinn, Selbstdisziplin und unermüdliche Arbeit schienen für die Niederländer in den 1950er Jahren bezeichnend zu sein.

²⁷ Deutsch: Viele Niederländer machten sich frei von alten Abhängigkeiten, die sie zunehmend als restriktiv oder nicht mehr relevant empfanden. Sie spürten die Freiheit, in der neuen Konsumgesellschaft und im Sozialstaat ihren eigenen Lebensstil zu entwickeln.

aufkommen, dass das Land als internationales Beispiel für Progression dienen könnte (vgl. Kennedy 2007, 363). Diese Tendenz schrieb sich fort, wenngleich durchsetzt von einer Reihe nicht unwesentlicher Unterbrechungen, beispielsweise durch das erkennbare Erstarken rechtsextremer Parteien. Aber auch in den folgenden Jahren schritt das Land aufgeschlossen voran und ermöglichte als einer der weltweit ersten Staaten 2000 die gleichgeschlechtliche Ehe, legalisierte Bordelle, oder gestattete die Sterbehilfe. „Soms kwam libertaire wetgeving voort uit de wens om illegale praktijken niet te gedogen, maar te reguleren“²⁸ (Kennedy 2007, 373). James Kennedy schreibt den Niederlanden die Strategie zu, mit der Entkriminalisierung einer Handlung nicht gleich eine uneingeschränkte Erlaubnis zu erteilen – man denke zum Beispiel an den Cannabis-Vertrieb – sondern den Staat stattdessen als teilhabendes Korrektiv einzusetzen. Ein legislatives Verständnis, das sich in einigen der genannten sozialen Reibungspunkte bis heute von dem vieler Nachbarstaaten unterscheidet.

Seit 1945 hielt sich das Königreich weitestgehend aus kriegesischen Handlungen heraus. Während des Korea-Krieges in den 50er-Jahren und während der Balkan-Kriege in den 90er-Jahren entsendeten die Niederlande Truppen zu verschiedenen UNO-Friedensmissionen. Insbesondere der Einsatz in Kroatien hat bis heute Folgen, denen sich die Niederlande stellen muss: Die Rolle der niederländischen Militärs beim Massaker von Srebrenica, in dem mehr als 8000 Muslime durch die Truppen des Kriegsverbrechers Ratko Mladic ermordet wurden, war lange ungeklärt und sorgte regelmäßig für Skandale. So fand man rassistische und erniedrigende Zeichnungen der Soldaten. Umstritten ist bis heute auch das Handeln des niederländischen Kommandanten Thom Karremans, der entschied, Srebrenica kampflos aufzugeben und anschließend mit Mladic über das Schicksal der gefangengenommenen Soldaten und der Zivilisten verhandelte. Schließlich kooperierten die Niederländer und halfen bei der Deportation von 320 Männern, die in der Folge umgebracht wurden (NPO Kennis 2017). Seit 2007 zogen Hinterbliebene, zusammengeslossen in der Opferorganisation *Mütter von Srebrenica*, unermüdlich immer wieder gegen den niederländischen Staat und die Vereinten Nationen vor Gericht, um die Niederlande mitverantwortlich für den Tod ihrer Familienmitglieder zu machen und eine Anerkennung des Schadens zu erwirken (vgl. Verbeek 2016, 18). Dieser Fall

²⁸ Deutsch: Mitunter entstand die liberale Gesetzgebung aus dem Wunsch heraus, illegale Praktiken nicht zu erlauben, sondern zu regulieren.

konfrontierte die Niederlande erstmalig seit dem Zweiten Weltkrieg mit der Frage nach Schuld und Kollaboration, sodass die Aufarbeitung nur zögerlich angegangen wurde und sich die gesellschaftliche Besprechung in der Regel auf punktuelle Ereignisse beschränkte, beispielsweise wenn die Mütter von Srebrenica einen Erfolg vor dem Europäischen Gerichtshof erstritten hatten. Ab 2002 waren niederländische Soldaten im Rahmen der ISAF-Mission der NATO auch in Afghanistan stationiert und leisteten dort einen internationalen Beitrag zur Friedenssicherung (vgl. Defensie.nl 2009). Sie beteiligen sich seitdem an weiteren multinationalen Militäroperationen, beispielsweise vor der Küste Somalias oder im Irak. Somit wirken die Niederlande militärisch zwar an NATO- oder UNO-Einsätzen mit, fallen aber nicht dadurch auf, Konflikte proaktiv voranzutreiben oder militärische Interventionen einzufordern.

Um die Zeit des Fortschritts, aber insbesondere der steten Unruhe, zu beenden, entwickelten die Niederländer Anfang der 80er-Jahre eine Konsensarchitektur, das sogenannte Poldermodell. Die vergangenen Jahrzehnte führten zu großer Arbeitslosigkeit und nur mäßigem Wirtschaftswachstum, weshalb die konkurrierenden Parteien des Arbeitskampfes den Versuch unternahmen, sich einander anzunähern. Gleichzeitig begab sich die gemäßigte Regierung dieser Zeit auf Augenhöhe mit einer Vielzahl gesellschaftlicher Akteure und bot unter anderem Steuersenkungen an, um die konkurrierenden Seiten ebenfalls zu Kompromissen zu bewegen (vgl. Kennedy 2007, 366). Auf diese Weise entstanden neue Dialoge zwischen Gewerkschaften und Arbeitgebern, die schnellere Einigungen und stärkere Prosperität ermöglichten. In diesen Jahren waren die Niederlande weitestgehend gesellschaftlich befriedet und genossen internationales Ansehen für ihr Sozialexperiment (vgl. Wielenga 2020, 263). Das Poldermodell war auch eine Metapher von historisch-nationaler Bedeutung: „Bereits seit dem Mittelalter hätten die Bewohner der Niederen Lande durch das Anlegen von Poldern pragmatisch kooperieren müssen, damit ihnen das Wasser nicht wortwörtlich zum Hals reiche“ (van Dam 2012). Damit distanzierte sich das Poldermodell auch von versäulten Strukturen. Es war ein Lösungsversuch, der die Vielfalt der niederländischen Subkulturen in Synergien gießen sollte und die gesellschaftliche Pluralität in politische Spielregeln überführte. Dieses bildhafte, konsensorientierte Regierungsleitbild wirkte der Neigung zu Immobilität, die Arend Lijphart fragmentierten Gesellschaften zuschreibt, entgegen (vgl. Lijphart 1969, 218). Jene Kompromissbereitschaft ist bis heute eine gar niederländische Grundüberzeugung,

da das diverse Parteiensystem ideologische Alleingänge unterbindet und die Annäherung noch so gegensätzlicher Protagonisten einfordert (vgl. van Dam 2012). Trotzdem bröckelte seit Beginn der 2000er-Jahre das gesellschaftliche und politische Gebilde aus Konsens und Billigung. Denn wie in nahezu allen übrigen Nationen Europas erstarkten rechtspopulistische und nationalistische Kräfte auch in den Niederlanden. Geert Wilders, Pim Fortuyn und andere bauten auf Polemik, um Narrative über Antagonisten und Feindbilder zu weben (vgl. Wielenga 2020, 268/270f).

Seit den frühen 2000er-Jahren digitalisierten die Niederlande ihre Infrastruktur konsequent, indem sie zunächst den Ausbau der DSL- und Kabeltechnologie vorantrieben. Während schließlich andere Staaten, darunter auch Deutschland, noch lange auf bewährte Kupferleitungen setzten und die teure Umrüstung auf Glasfaserleitungen scheuten, wurde 2004 in Nuenen das erste FTTH-Glasfasernetz des Landes installiert (vgl. Coöperatie OnsNet Nuenen 2012). Seitdem wächst das Netz stetig und steuert zum Technologiemix bei, der sich im Wesentlichen aus 4G/5G-, Glasfaser- und Kabel-Anschlüssen zusammenstellt und so den geografischen Gegebenheiten der Niederlande Rechnung trägt (vgl. oecd.org 2021b). Dass sich das Land vergleichsweise frühzeitig zu einer Diversifizierung seiner Kommunikationsinfrastruktur entschieden und sich breit aufgestellt hat, führt dazu, dass die Niederlande Rang Vier im Digital Economy and Society Index (DESI) 2021 der Europäischen Kommission belegen – sogar Rang Zwei im Bereich Konnektivität (vgl. European Commission 2021a, 7). Mit dem Ausbau moderner Internetverbindungen haben die Niederlande nicht nur ein zuverlässiges, redundantes Netz aufgebaut, das das gesamte Land mit schnellem Internet versorgt, sondern sie haben die frühen 2010er-Jahre genutzt, um die Rolle eines der am fortschrittlichsten digitalisierten Nationen Europas einzunehmen.

Im vergangenen Jahrzehnt hat jedoch kaum ein Vorfall das Sicherheitssentiment und die damit verbundene Außenpolitik der Niederlande so eklatant beeinflusst wie der Abschuss des Malaysia Airlines-Flugs MH17. Am 17. Juli 2014 wurde der Flug von Amsterdam nach Kuala Lumpur während Kampfhandlungen über der Ostukraine abgeschossen (vgl. De Hoon 2019, 247). An Bord befanden sich 298 Menschen, unter ihnen 192 Niederländer, die allesamt ums Leben kamen. Die Rakete selbst war russischen Ursprungs, der Abschuss fand von russisch kontrolliertem Gebiet statt und die Schützen waren prorussische Separatisten (vgl. De Hoon 2019, 248). Der Vorfall

löste in den Niederlanden Trauer und Schock aus. Landesweit fanden Gedenkveranstaltungen statt, am 23. Juli 2014 ein nationaler Staatstrauertag ausgerufen. 2017 öffnete in Vijfhuizen das Nationaal Monument MH17, eine Gedenkstätte für die niederländischen Opfer des Abschusses. Allem voran aber zeigte das Ereignis den Niederländern erstmalig seit dem Zweiten Weltkrieg, dass sie angreifbar waren und bedroht wurden.

Het neerschieten van vlucht mh17 boven Oekraïens grondgebied [...] en terroristische dreigingen maken duidelijk dat veel brandhaarden in de wereld directe of indirecte impact hebben op Nederland. Conflicten in het buitenland werken in eigen land door²⁹ (Wetenschappelijke Raad voor het Regeringsbeleid 2017, 18).

Infolge dieses Angriffs auf ein ziviles Flugzeug richtete sich die Aufmerksamkeit der niederländischen Öffentlichkeit verstärkt auf Russland. Insbesondere die Ermittlungsbehörden und Nachrichtendienste des Landes konzentrierten sich seit 2014 darauf, Russland den Abschuss nachzuweisen und weitere russische Interventionen im Westen zu belegen. Daraus erwuchs schließlich ein verhohlener Konflikt, von dem einzelne Eskalationsstufen publik wurden. So konnte die Joint Sigint Cyber Unit (JSCU), bestehend aus den Nachrichtendiensten AIVD und MIVD, nachweisen, dass die russische Hackergruppe *Cozy Bear* unter anderem in die Netze des Weißen Hauses eindringen und die US-Wahlen 2016 beeinflusste (vgl. NOS 2018c). 2018 war es der MIVD, der öffentlich machte, einen ebenfalls russischen Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OPCW) in Den Haag verhindert zu haben (vgl. YouTube: NOS Live 2018). Demnach erfolgte der Angriff im gleichen Zeitraum wie die Untersuchungen gegen Russland wegen der Giftanschläge auf Sergej Skripal und seine Tochter (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019b, 24). Auf einem Laptop der russischen Agenten seien unter anderem Daten gefunden worden, die darauf hindeuteten, dass die Täter darüber hinaus versucht hatten, Informationen zu den Ermittlungen über den Malaysia-Airlines-Flug 17 zu stehlen. Schließlich wurde 2021 bekannt, dass der AIVD schon 2017 russische Hacker in Netzwerken der niederländischen Polizei entdeckte – ebenfalls während der Untersuchungen zu MH17 (vgl. De Volkskrant 2021b).

²⁹ Deutsch: Der Abschuss des Fluges MH17 über ukrainischem Territorium [...] und terroristische Bedrohungen machen deutlich, dass viele Brandherde auf der Welt direkte oder indirekte Auswirkungen auf die Niederlande haben. Konflikte im Ausland haben Konsequenzen im eigenen Land.

Ank Bijleveld, die damalige Verteidigungsministerin der Niederlande, gab in der Fernsehsendung *WNL Op Zondag* im Oktober 2018 an, dass man sich im Cyberkrieg mit Russland befände. Wenngleich sie nicht selbst von einem Krieg mit Russland sprach, wie ihr populistische Medien im Inland damals zuschrieben, bestätigte sie die Aussage ihres Gegenübers „Maar we kunnen constateren dat er een cyberoorlog gaande is“³⁰ (TC 0.07-0.30) mit einem Ja und führte aus, wie sich die russischen Aggressionen in den Digitalraum verlagert hätten (YouTube: WNL Op Zondag 2018). Auf Nachfragen des Moderators, ob Bijleveld die aktuelle Situation auch als Cyberkrieg beschreiben würde, antwortete sie ebenfalls bejahend. Da diese Aussage, insbesondere vor dem Hintergrund der Auseinandersetzungen mit Russland wegen des Abschusses des Malaysia-Airlines-Flugs 17, in den Niederlanden für eine intensive Berichterstattung und für Verunsicherung sorgte, ließ die Ministerin wenige Tage später gegenüber dem Sender NOS vermelden, dass ihre Bemerkungen nur bildhaft und nicht wörtlich zu verstehen gewesen seien (vgl. NOS 2018a). Dieser Zwischenfall demonstriert einerseits, dass Begriffe wie Krieg oder Angriff in der digitalen Lebenswelt bislang nicht determiniert sind, indem sie auf nahezu keiner Vorerfahrung fußen. Andererseits belegt die Aussage der Ministerin das schwellende Bedrohungssentiment in den Niederlanden zu dieser Zeit. „Cyberonveiligheid, de bedreiging van vitale infrastructuur en de inzet van desinformatie (zoals vanuit Rusland rond het onderzoek naar de mh17 is gecreëerd) zetten in toenemende mate de toon“³¹ (Wetenschappelijke Raad voor het Regeringsbeleid 2017, 17). Hybride Bedrohungen, Cyberunsicherheit oder Desinformation – innerhalb weniger Jahre sieht sich die Öffentlichkeit unmittelbar mit neuen Begriffen und Gefahrenkategorien konfrontiert.

Kennedy und Lademacher kommen trotz der zeitlichen Differenz ihrer Publikationen zu einem bemerkenswert ähnlichen Urteil über die vergangenen Jahrzehnte der Niederlande und geben damit auch eine Prognose für kommende Jahre ab. So hebt James Kennedy vor allem die spezifischen Fähigkeiten des Landes hervor:

Vanuit dit perspectief is de rode lijn in de ontwikkeling van Nederland het vermogen om zowel snel te reageren op veranderende omstandigheden als kansen te zien en te grijpen om te innoveren. [...] Het laaggelegen land stimuleerde de opkomst van een gespecialiseerde economie, die sensitief reageerde op

³⁰ Deutsch: Aber wir können konstatieren, dass es einen Cyberkrieg gibt

³¹ Deutsch: Cyberunsicherheit, die Bedrohung lebenswichtiger Infrastrukturen und der Einsatz von Desinformation (wie sie Russland im Zusammenhang mit den Ermittlungen zu MH17 erschuf) geben zunehmend den Ton an.

ontwikkelingen in de internationale handel, waardoor Nederlanders werden opgestuwd in een cyclus van innovatie³² (Kennedy 2007, 383f).

Horst Lademacher stützt diese Feststellung, wenn er attestiert, „daß die Niederlande rascher und liberaler, vielleicht auch drastischer und bedingungsloser als anderswo Lösungen ausarbeiten“ (Lademacher 1993, 668). Das spiegelt sich beispielsweise im European Innovation Scoreboard der Europäischen Kommission, in dem die Niederlande regelmäßig Spitzenplätze belegen (vgl. European Commission 2021b, 16). Sowohl Lademacher als auch Kennedy sehen deshalb in den Niederlanden einen Staat, der versucht war und ist, die vorliegenden Gegebenheiten in Gelegenheiten zu verwandeln und mittels Flexibilität sowie Geschwindigkeit an fruchtbaren Innovationen teilhaben zu können. Obgleich die Ursachen hierfür in Pragmatismus und den Lehren vergangener Dekaden zu liegen scheinen, wird an dieser Stelle ein Fahrplan für bevorstehende Herausforderungen sichtbar. Besonders die Unwägbarkeiten der sich beschleunigenden Digitalisierung verlangen, was Kennedy einen Innovationszyklus und Lademacher einen „auffälligen Synkretismus“ nennt, nämlich eine nie anhaltende Selbstkorrektur und die Bereitschaft zur Neuordnung (vgl. Lademacher 1993, 669).

2.5 Niederlande heute

Ein US-amerikanisches Nachrichtenmagazin versuchte sich 2021 an einem knappen Abriss über die Niederlande:

Situated along the fringes of Western Europe, the Netherlands is a coastal lowland freckled with windmills characteristic of its development around the water. [...] More than 1,000 bridges and 20,000 miles of bike paths connect the densely populated nation, with most citizens concentrated in a grouping of cities along the coast, known as the Randstad. Much of the country is underwater, and the 60 million people that touch down in capital city Amsterdam's Schiphol Airport each year land more than a dozen feet below sea level (usnews.com 2021).

Mit diesen selektiven Angaben schaffen die Autoren ein klischeebeladenes Bild der Niederländer als vom Klimawandel besonders bedrohte Fahrradfahrer in einem Land voller Windmühlen. Das mag die vereinfachte Draufsicht mancher Amerikaner sein, gibt jedoch die Vielschichtigkeit der niederländischen Gesellschaft nicht wieder. Denn

³² Deutsch: Aus dieser Perspektive ist die rote Linie in der Entwicklung der Niederlande die Fähigkeit, sowohl schnell auf sich ändernde Umstände zu reagieren als auch Innovationsmöglichkeiten zu erkennen und zu nutzen. [...] Das tief liegende Land förderte die Entstehung einer spezialisierten Wirtschaft, die sensibel auf die Entwicklungen im internationalen Handel reagierte und die Niederländer in einen Innovationszyklus trieb.

heute sind die Niederlande ein Staat, in dem sich viele Menschen neben der Sprache vor allem durch Traditionen, wie dem Koningsdag oder dem Elfstedentocht, verbunden fühlen. Laut einer Untersuchung des Niederländischen Instituts für Sozialforschung spielen für die Menschen auch bedeutungstragende Ikonen – darunter das Tagebuch der Anne Frank oder De Nachtwacht von Rembrandt – eine wichtige Säule der niederländischen Identität aus. „Behalve deze elementen worden ook landschappelijke of omgevingskenmerken (zoals water) als karakteristiek gezien“³³ (Sociaal en Cultureel Planbureau 2019, 11). Gegenwärtig diskutiert das Land intensiv ebendiese Identität aufgrund des beschleunigenden Alltags und der Migration der vergangenen Jahre. Wie die Mehrzahl seiner Nachbarn in Europa sieht sich das Königreich mit Islamfeindlichkeit, Antisemitismus und erstarkenden Populisten konfrontiert. Die Finanzkrise von 2008 und diverse neoliberale Sozialreformen verlagerten viele staatliche Aufgaben, wie zum Beispiel die Altersvorsorge, vermehrt in die Verantwortung eines jeden Einzelnen. Dies ergab auch politische Fragmentierungen, die traditionelle Volksparteien schwanken lassen (vgl. Wielenga 2020, 273). Zusätzlich führten Terroranschläge auf europäischem Boden und insbesondere der besagte Abschuss des Malaysia Airlines-Flugs mit 193 niederländischen Opfern zu einem wachsenden Unsicherheitsgefühl der Bevölkerung in den vergangenen Jahren (vgl. Kennedy 2017, 378ff). Dennoch zeichnet sich das Land immer noch durch eine enorme gesellschaftliche Diversität aus, die indes häufig ihre Ursachen in dunklen Kapiteln der Geschichte hat, wie dem Kolonialismus oder der, wenn auch argwöhnischen und zögerlichen, Aufnahme jüdischer Flüchtlinge um 1938/39 (vgl. Lademacher 1993, 563). „De vermeende tolerantie van de Nederlanders is een terugkerend thema in de geschiedenis, en wordt verbonden aan dit pluralistische karakter van de samenleving“³⁴ (Kennedy 2017, 386). Gleichzeitig legen derzeitige Herausforderungen offen, dass längst nicht alle Hürden des Zusammenlebens genommen werden konnten: Die etwa 17 Millionen Einwohner stehen vor erstarkenden extremen Rechten wie Geert Wilders oder Thierry Baudet aus PVV³⁵ und FVD³⁶ (vgl. NOS 2019). Die fortschreitende Vergreisung, der Fachkräftemangel und die

³³ Deutsch: Jenseits dieser Elemente werden auch landschaftliche oder Umgebungsmerkmale (beispielsweise Wasser) als charakteristisch gesehen.

³⁴ Deutsch: Die vermeintliche Toleranz der Niederländer ist ein wiederkehrendes Thema in der Geschichte und hängt mit diesem pluralistischen Charakter der Gesellschaft zusammen.

³⁵ Partij voor de Vrijheid, deutsch: Partei für die Freiheit

³⁶ Forum voor Democratie, deutsch: Forum für Demokratie

Nachwehen des Brexits stellen große Hemmnisse für Wohlstand und gesellschaftliche Ruhe dar. Nicht zuletzt müssen auch die Niederländer die sozialen und wirtschaftlichen Schäden der COVID-19-Pandemie bewältigen.

Trotzdem besitzen die Niederlande vielerlei Eigenschaften, die vielversprechende Voraussetzungen für eine erfolgreiche und sichere Digitalisierung darstellen können. Denn wie die historische Zusammenfassung anhand der Schriften von Kennedy und Lademacher gezeigt hat, gelten die Niederlande nicht zu Unrecht als wandelbar und dynamisch – Eigenheiten, die in Zeiten rasanter Beschleunigung hilfreich sind. Dabei hilft dem Land seine geringe Größe und Einwohnerzahl, die ihm in der Geschichte häufig zum Nachteil wurde. Die Zentralregierung muss in einem überschaubaren Staat auf weniger regionale Besonderheiten eingehen als etwa französische Autoritäten. Zudem sind die vorhandenen Infrastrukturen übersichtlicher und können mit weniger Aufwand angepasst werden als im etwa neunmal so großen Deutschland. Die schon auf Dienstleistungen spezialisierte Ökonomie – 82,8 % der Erwerbstätigen arbeiten im Dienstleistungssektor – ist prädestiniert für eine aussichtsreiche digitale Wertschöpfung. Wohingegen Staaten, die ihren Wohlstand bislang auf Industriegüter oder den Gewinn fossiler Energieträger gebaut haben, nur schwerfällig reagieren können und gegebenenfalls Chancen verstreichen lassen müssen (vgl. Statistisches Bundesamt 2021a, 7). Marijn Fraanje, Leiter Informationstechnik der Gemeinde Den Haag, stellte bei der One Conference 2019 ein Beispiel für eine regionale Maßnahme vor, die skalierbar ist und als Vorbild für weitere Gebiete dienen soll: Als Teil der Cybersicherheitsstrategie Den Haags rief die Kommunalregierung Hacker auf, in einem koordinierten Wettstreit, die Strukturen und Organisationen der Stadt straffrei anzugreifen. Basierend auf diesem Wettbewerb entstand eine digitale Plattform, bei der entdeckte Sicherheitslücken veröffentlicht werden und auf diese Weise Druck auf die Verantwortlichen ausgeübt wird. Der Sicherheitsmangel einer Institution oder eines Unternehmens innerhalb der Stadt wird publik gemacht und kann so potenziell dazu führen, dass zum Beispiel Geschäftspartner oder Kunden ihre Dienste und Waren nicht mehr mit dieser Firma handeln möchten. In seinem Vortrag betonte Fraanje den Ausspruch: „Get people aware and show consequences“ (One Conference 2019a). Dieser Ansatz wirkt zwar harsch, führte aber laut Fraanje zu einer Art vorausseilendem Gehorsam und einer Verstärkung der Sicherheitsmechanismen. Tatsächlich verstand er die Maßnahme als aktiven Verbraucherschutz, da die Ergebnisse über neue und alte

Lücken so veröffentlicht werden, dass sie Bürgern zugänglich und entsprechend verständlich sind. Fraanjes explizites Ziel sei es, die wirkungsvolle Plattform anderen Städten in den Niederlanden anzubieten und auf diese Weise eine landesweite Präventionsinfrastruktur zu schaffen. Diese wiederum ist nur mittels zentralistischer Organisation und übersichtlicher Strukturen zügig in die Breite zu tragen.

Zu guter Letzt bleibt nicht unerwähnt, dass der Klimawandel vor allem in den Niederlanden zugleich Bedrohung als auch ein Katalysator für Innovation ist. Das Meer drängt die Küstenbewohner fortlaufend zu kreativen technischen Lösungen, die repliziert, übernommen und schließlich auch verkauft werden können. Niederländische Technologien für Deichsysteme werden mittlerweile weltweit eingesetzt, zum Beispiel in England, Vietnam und China, wodurch sich die „Exporte in diesem Bereich auf knapp acht Milliarden Euro“ in den letzten 20 Jahren verdoppelt haben (Handelsblatt 2017). Die gegenwärtigen Aufgaben des Landes werden erst gänzlich greifbar, wenn man feststellt, dass sie unmittelbar miteinander verknüpft sind. Perry van der Weyden, CIO der für die Wasser- und Straßeninfrastruktur verantwortlichen Rijkswaterstaat³⁷, stellte ebenfalls bei der One Conference 2019 in Den Haag den Zusammenhang zwischen Überschwemmungsschutz und Cybersicherheit her. In seiner Keynote exponierte er, dass die digitale Sicherheit mit der physischen unmittelbar verknüpft ist, weil besonders die modernen Wasserschutzstrukturen wirkungsvoll nur vernetzt reguliert werden können. Daher identifizierte er zunehmende digitale Angriffsszenarien als lebensbedrohliche Bedrohungen. Falls Cyberkriminelle die Deichsysteme manipulierten oder Schleusen öffneten, seien Menschen akut gefährdet. Der zentrale Appell seiner Ansprache bestand deshalb darin, Gefahren zu beobachten und ständige Adaptionen der Herangehensweise vorzunehmen (vgl. One Conference 2019b). Van der Weyden resümierte, dass zeitgerechter Hochwasserschutz nur durch die Echtzeitvernetzung von Frühwarn- und Schutzsystemen gewährleistet werden kann. Dafür müsse aber zeitgleich sichergestellt sein, dass Manipulationen oder Beschädigungen durch entfernte Angreifer ausgeschlossen werden können. Der Deich und die Deltawerke haben in den Niederlanden allegorische Funktion, sodass sie häufig als Metaphern herangezogen werden. 2016 betitelte das Verteidigungsministerium sein hauseigenes Magazin mit der

³⁷ Deutsch: Reichswasserverwaltung

Frage „Zijn onze digitale dijken hoog genoeg?“³⁸ (Defensie.nl 2016). Einen Bericht über die Investitionen von Rijkswaterstaat in dessen Abwehrfähigkeiten überschrieb die Kontrollinstitution Algemene Rekenkamer³⁹ „Digitale dijkverzwaring: cybersecurity en vitale waterwerken“⁴⁰ (Algemene Rekenkamer 2019). Ergänzend fordert die Unternehmenberatung PWC die „realisatie van een serieus digitaal deltaplan om onze digitale dijken te verhogen en versterken“⁴¹ (van Tiel 2021). Der Cyber Security Raad skizziert die tiefe Verwurzelung dieser Infrastruktur in den Niederlanden: „Van de stormvloedkeringen in het westen tot de sluizen en dijken in het oosten, het is een groot aaneengeschakeld netwerk van objecten waar verschillende partners verantwoordelijkheid hebben“⁴² (Cyber Security Raad 2022b). Und das Magazin iBestuur hält es für unabdingbar, die typisch niederländische Anpassungsfähigkeit in die Cybersicherheitsarchitektur zu überführen: „Als Nederland door aanvallen dreigt te overstroom, moeten digitale sluizen verdere instroom beperken“⁴³ (iBestuur 2019). Diese Metaphern scheinen so sehr in der niederländischen Sprache und Kultur verankert zu sein, dass auch hypermoderne Phänomene wie Cyberangriffe, KI oder Quantencomputing mit dieser Figuration aufgeladen werden. Diese Formel erlaubt es den Menschen, komplexe und neuartige Erscheinungen umreißen und sie in bestehende Kategorien einordnen zu können. Insofern sind die Deiche, Dämme und das Meer auch ein passendes Sinnbild für die Niederlande heute: Das Land hat sich durch seine gesellschaftliche Anpassungsfähigkeit, einen wachsenden Dienstleistungssektor und einer vergleichsweise fortgeschrittenen Digitalisierung eine vielversprechende Ausgangsposition für die bevorstehenden Herausforderungen erarbeitet, die es nun bedroht sieht und gegen äußere Unwägbarkeiten zu schützen versucht. Sowohl aus ihrer Historie als auch aus den gegenwärtigen lässt sich ein niederländischer Trotz ableiten, den Politik und Gesellschaft in den kommenden Jahren unter Beweis stellen müssen.

³⁸ Deutsch: Sind unsere digitalen Deiche hoch genug?

³⁹ Deutsch: Allgemeine Rechnungsprüfungsstelle

⁴⁰ Deutsch: Digitale Deichverstärkung: Cybersicherheit und kritische Wasserwerke

⁴¹ Deutsch: Realisierung eines ernstzunehmenden Deltaplans, um unsere digitalen Deiche zu erhöhen und zu verstärken.

⁴² Deutsch: Von den Sturmflutwehren im Westen bis zu den Schleusen und Deichen im Osten handelt es sich um ein großes, miteinander verbundenes Netzwerk von Objekten, in dem unterschiedliche Partner die Verantwortung haben.

⁴³ Deutsch: Wenn die Niederlande durch Angriffe überzulaufen drohen, müssen digitale Schleusen weiteren Zustrom verhindern.

2.5.1 Staatsprinzip: Dezentraler Einheitsstaat

Auf den ersten Blick lassen sich die Niederlande als Komponente des Königreichs der Niederlande vermeintlich einfach als Einheits- oder Zentralstaat klassifizieren. Das ist zwar nicht falsch, denn die Niederlande verfügen weder über Bundesländer noch existiert eine verfassungsrechtliche Subsidiarität, dennoch greift diese Sichtweise zu kurz. Das Land geht – anders als die sich auf eine gemeinsame Sprache berufende frühe deutsche Nation – aus einem Schutzbündnis hervor. Die *Republiek der Zeven Verenigde Nederlanden*⁴⁴ begründete sich Ende des 16. Jahrhunderts gegen das Feindbild der spanischen Katholiken, sodass man sich verbunden sah in Religion und Widerstand (vgl. Lademacher 1993, 109). In dieser Zeit noch eine lose Föderation eigenständiger Provinzen führte die französische Besatzung des späten 18. Jahrhunderts zu „Zentralisierung und Vereinheitlichung“, die sich auch über den Wiener Kongress hinweg fortsetzte (Lademacher 1993, 402). Über die *Bataafsche Republiek*⁴⁵ als Protektorat Frankreichs bis zur Proklamation der oranischen Monarchie als souveräne Nation wurde der Ruf nach Einheit und weniger Partikularismus lauter (vgl. Lademacher 1993, 420f). Das Königtum „ersetzte damals den Staatenbund der sieben niederländischen Provinzen“ (Bappert et al. 2006a). Selbst definieren sich die Niederländer heute als Bürger in einem „gedecentraliseerde eenheidsstaat“⁴⁶ (Kenniscentrum voor beleid en regelgeving 2019). Das meint, dass die Befugnisse innerhalb der mittlerweile parlamentarischen Monarchie in Den Haag zusammenlaufen, die zwölf Provinzen sowie die drei „bijzondere gemeenten“⁴⁷ aber eigene Kompetenzen besitzen und im Rahmen des geltenden Rechts selbstbestimmt entscheiden können. Es gilt der Leitsatz: „decentraal wat kan, centraal wat moet“⁴⁸ (Kenniscentrum voor beleid en regelgeving 2019).

Im Gegensatz zu Deutschland findet sich der Dezentralisierungsmechanismus der Subsidiarität nicht in der nationalen Verfassung, dem Grondwet, wieder. Dennoch verteilen die verschiedenen Ebenen der öffentlichen Verwaltung Befugnisse und Verantwortlichkeiten stets an die kleinstmögliche Einheit. In den sogenannten

⁴⁴ Deutsch: Die Republik der Sieben Vereinigten Niederlande

⁴⁵ Deutsch: Batavische Republik

⁴⁶ Deutsch: dezentraler Einheitsstaat

⁴⁷ Deutsch: besondere Gemeinden

⁴⁸ Deutsch: dezentral was möglich ist, zentralisiert was muss

*Aanwijzingen voor de regelgeving*⁴⁹, einem Begleitwerk für die Legislative, ist das Prinzip konkretisiert:

Als uitgangspunt geldt dat, indien taken op doelmatige en doeltreffende wijze kunnen worden verricht door besturen van provincies, gemeenten, waterschappen of de openbare lichamen Bonaire, Sint Eustatius en Saba, zij niet behoren te worden opgedragen aan het Rijk. Evenmin behoren taken die op doelmatige en doeltreffende wijze door besturen van gemeenten of waterschappen kunnen worden verricht, te worden opgedragen aan de besturen van provincies⁵⁰ (Overheid 1992a).

Damit können Provinzen oder kleinere Verwaltungen das geradezu föderale Prinzip der Subsidiarität nicht über die Verfassung der Niederlande einfordern, sondern insistieren auf die *Aanwijzingen* sowie auf Artikel 116 des Gemeindegesetzes und Artikel 114 des Provinzengesetzes (vgl. Overheid 1992b).

Das versieht die Gemeinden und Provinzen zunächst mit direkter demokratischer Legitimierung, einer Haushaltsführung, gewissen Entscheidungsbefugnissen und eigenen Steuergebieten (vgl. Overheid 1992a). Gleichzeitig sieht Artikel 123 des Grondwet vor, dass Provinzen und Gemeinden aufgehoben und neue installiert werden können (vgl. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2019, 30). Ebenso ist es möglich, Entscheide per königlichem Beschluss außer Kraft zu setzen, wenn sie beispielsweise mit dem öffentlichen Interesse kollidieren (vgl. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2019, 31). Wenngleich solch rigide Maßnahmen zumeist ausbleiben, sieht sich eine Einheitsregierung wie die der Niederlande nicht derart an die Subsidiarität gebunden wie der Bund in Deutschland (vgl. Broschek 2016, 336). Genauer konstruierte man die Rechte der Provinzen nicht als Pflicht für die Nationalregierung, sondern vielmehr als Vorgabe, die etwa den Minister für Inneres und Königsbeziehungen anweist, die politische Freiheit der kleineren Verwaltungsinstanzen zu begünstigen (vgl. Overheid 1992a). Trotz alledem sind diese territorialen Verwaltungen keinesfalls mit ähnlichen Rechten wie etwa deutsche Bundesländer ausgestattet.

⁴⁹ Deutsch: Hinweise zur Gesetzgebung

⁵⁰ Deutsch: Wenn Aufgaben von den Provinzen, Gemeinden, Wasserschaften oder den öffentlichen Körperschaften Bonaire, Sint Eustatius und Saba effizient und effektiv wahrgenommen werden können, gilt als Ausgangspunkt, dass diese nicht der Zentralregierung übertragen werden sollten. Auch sollten Aufgaben, die von den Gemeindeverbänden oder Wasserschaften effizient und effektiv wahrgenommen werden können, nicht den Landesräten übertragen werden.

Das wichtigste Merkmal des dezentralisierten Einheitsstaates ist die Tatsache, dass die Staatsaufgaben, die der Zentralstaat erlassen hat, zum Teil an dezentrale Organe der Selbstverwaltung abgegeben worden und diese Organe die Aufgaben unter der Rechts- und Fachaufsicht des Staates erledigen (Bappert et al. 2006a).

Das bedeutet, dass die Provinzen und Gemeinden der Niederlande bestimmte Aufgaben autonom verwalten dürfen, sie aber stets im Sinne und im Auftrag des Einheitsstaates zu agieren haben. Anders als in föderalen Systemen besitzen die untergeordneten Verwaltungseinheiten und Regierungsgebiete keine Verfassungen und auch keine Gesetzgebungskompetenzen (vgl. Bappert et al. 2006a/2006b). Hinzukommt, dass die Provinzen und Gemeinden der Niederlande eine eigene Fiskalpolitik betreiben, ihre Finanzierung aber zu 90 % und mehr aus Zuwendungen der Staatskasse stammt – hier besteht also eine unmittelbare Unmündigkeit (vgl. Bappert et al. 2006c).

Aus den benannten Eigenschaften des dezentralen Einheitsstaates ergeben sich Konditionen, die sich von denen föderaler, republikanischer Systeme abheben. Während also die Provinzen in den Niederlanden kaum über eigene Einnahmequellen verfügen, erheben die Bundesländer beispielsweise Erbschafts- oder Grunderwerbssteuer und teilen gewisse Abgaben wie die Einkommensteuer mit dem Bund (vgl. Destatis 2021b). Das bedeutet, dass die Provinzen und Gemeinden der Niederlande auf die Legitimierung und Finanzierung angestrebter Projekte durch die Einheitsregierung angewiesen ist. Das wiederum ermöglicht der Regierung in Den Haag, landesweit einheitliche Standards festzuschreiben, die allgemeingültig sind und nicht durch Landespolitik unterminiert werden. Durch die vergleichsweise schwache Position von Provinzparlament und Provinzregierung können Beschlüsse in kurzer Zeit über das ganze Land ausgerollt werden. Das schließt eine regionale Ungleichbehandlung auf Grundlage teilstaatlicher Souveränität in den Niederlanden weitestgehend aus. Damit geht jedoch einher, dass weniger partizipative Gremien eingesetzt sind, die den Willen der Bevölkerung oder Partikularinteressen vertreten. Dies bemerkte die Regierung und führte schließlich im Jahr 2003 auf Initiative der Partei D66 eigens einen Minister voor Bestuurlijke vernieuwing en Koninkrijksrelaties⁵¹ ein (vgl. Eerste Kamer der Staten-Generaal 2007). Hiermit wollte man sich unter anderem des Problems annehmen, dass Bürgermeister und Kommissare in den Niederlanden durch die Krone berufen statt durch das Volk gewählt werden. Wenngleich dieses Ministeramt nur kurze Zeit Bestand hatte, war es Ausdruck einer teils mangelnden demokratischen Legitimität und eines Reformbedarfs,

⁵¹ Deutsch: Minister für Verwaltungserneuerung und Königsbeziehungen

den bis heute regelmäßig insbesondere der Europarat beklagt (vgl. De Volkskrant 2021a).

Jenseits dessen kann die einheitsstaatliche Organisation und das Weniger an möglicherweise missbilligenden Instanzen landesweite Projekte begünstigen, zum Beispiel in den Bereichen Bau, Klimaschutz oder Digitalisierung. Der Ausbau nationaler Glasfasernetze ist exemplarisch: Während in den Niederlanden im Dezember 2020 21,3 % aller Festnetzanschlüsse mit dem Gigabit-Netz verbunden waren, konnten in Deutschland nur 5,4 % diesen Vorzug nutzen (vgl. oecd.org 2021a). Denn in der Bundesrepublik existiert zwar ein „Graue-Flecken-Förderprogramm“, die Beantragung, Umsetzung und Finanzierungsverantwortung wird jedoch „von Kommunen, Landkreisen, kommunalen Zweckverbänden“ übernommen (Bundesministerium für Verkehr und digitale Infrastruktur 2021). Das bedeutet im föderalen System, dass unter anderem sogenannte Markterkundungsverfahren durchgeführt, Haushaltsmittel des Bundes blockiert, Ausschreibungen eingeleitet und Endverwendungsnachweise erbracht werden müssen – für die kommunalen Verwaltungen entsteht also ein immenser Aufwand (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2021). In den zentral regierten Niederlanden verläuft dieser Prozess anders: Die Behörden verzichten weitestgehend auf komplexe Verwaltungsmechaniken und haben den Ausbau des Glasfasernetzes stattdessen liberalisiert. Das bedeutet, für den städtischen Raum schafft die niederländische Regierung einfache Marktzugänge und Investitionsanreize, sodass privatwirtschaftliche Investoren angezogen werden. Beispielsweise beschloss sie für die gesamten Niederlande, dass öffentliche Einrichtungen und Infrastrukturbetreiber verpflichtet sind, ihre Anlagen und Gebäude für den Glasfaserausbau zur Verfügung zu stellen, wenn Bedarf besteht (vgl. Ministerie van Economische Zaken en Klimaat 2018, 29). Auf diese Weise versucht die Regierung, den freien Markt zu lenken, staatliche Investitionen gering zu halten und so die Kosten des Ausbaus wesentlich zu reduzieren. Auf dem Land, wo der Breitbandanschluss nicht rentabel gelingen kann, substituieren die Niederlande mit Mobilfunk. So wird der Prozess insgesamt zwar beschleunigt, gleichzeitig führt dieses Vorgehen dazu, dass die Regierung noch auf der Suche nach solidarischen Finanzierungskonzepten für die Lebensräume ist, die nicht einmal mit mobilem Internet lohnend abzudecken sind (vgl. Ministerie van Economische Zaken en Klimaat 2018, 31).

Im Gegensatz zur deutschen Verfassung findet sich in dem niederländischen Grundwet kein Hinweis auf Informationstechnik. Jedoch steht dort, dass Gesetze jeglicher Art ausschließlich von der Regierung und dem Zwei-Kammern-Parlament, den *Generalstaaten*, beschlossen und vom König ratifiziert werden (vgl. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2019, 17/19). Das bedeutet, dass Regulierungen im Bereich der IT-Sicherheit nicht wie in Deutschland zwischen Bund und weiteren souveränen Einheiten verhandelt, sondern für das gesamte Land bestimmt werden. Das *Wet beveiliging netwerk- en informatiesystemen (Wbni)*⁵² regelt komplementär zum deutschen IT-Sicherheitsgesetz Zuständigkeiten, Meldepflichten sowie die Aufsicht über Kritische Infrastrukturen. Hieraus geht unter anderem hervor, dass der Minister van Justitie en Veiligheid⁵³ für Belange der Informationssicherheit als zentraler Kontaktpunkt für die gesamten Niederlande fungiert (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 2).

2.5.2 Internationale Rolle in Europa und der Welt

Die Position der Niederlande in Europa ist deutlich weniger einfach zu fassen als die Deutschlands. Die Gründe liegen zum einen in dem weniger prädominanten Status und zum anderen in der politischen Volatilität der letzten Jahrzehnte: Während das Land zu Beginn des jungen Jahrtausends die Liberalisierung wiederentdeckte und den Cannabiskonsum wie auch die aktive Sterbehilfe legalisierte, fiel es in den vergangenen Jahren vermehrt durch Rechtspopulisten wie Geert Wilders und Wellen des Euroskeptizismus auf. Dabei ist „The country as small as a city“, wie sich die Niederlande selbst vermarkten, nicht nur Gründungsmitglied der Europäischen Union, sondern gehört auch zu den größten Profiteuren des Binnenmarktes (Holland.com 2021). Innerhalb der europäischen Staatengemeinschaft besetzen die Niederlande eine dichotome Nische: Sie sind abhängig vom europäischen Markt wie vom außenpolitischen Schutzschirm; zugleich sind sie einflussreiche Kritiker der Finanz- und Steuerpolitik der EU. Dabei koppelten die Niederlande in den vergangenen Jahrzehnten ihr Wohl an Europa:

⁵² Deutsch: Das Gesetz über die Sicherheit von Netzwerk- und Informationssystemen

⁵³ Deutsch: Minister für Justiz und Sicherheit

Nederland maakt deel uit van Europa: geografisch, historisch, cultureel en economisch. Europa is essentieel voor onze welvaart, vrijheid en veiligheid. Blijvende betrokkenheid bij het Europese proces is daarom in het directe belang van Nederlandse burgers en bedrijven⁵⁴ (VVD-CDA 2010).

Trotzdem ist das Königreich kein geräuschloses Mitglied der EU, sondern gehören innerhalb der Union zu den sogenannten *Frugalen Vier*, einer losen Interessenverbindung der fiskalkonservativen Länder Dänemark, Schweden, Österreich und die Niederlande. In der größeren *Allianz der Verantwortung* fordern die Niederländer mit sieben weiteren Staaten der EU zu strikterer Austerität und zur Reduzierung von Staatsschulden auf (vgl. Andersson et al. 2021, 1). Mit dieser Erwartung beschnitten die Niederlande die Souveränität von illiquiden Nachbarn wie Portugal, Italien oder Griechenland und traten so wenig nachsichtig innerhalb der europäischen Solidargemeinschaft auf. Dieser pragmatisch-calvinistische Arbeits- und Kapitalethos setzt die „innerweltliche protestantische Askese“ des 17. und 18. Jahrhunderts fort, wie sie bereits Max Weber beschrieb (Weber 2016, 163). Im Englischen hat sich für die niederländische Sparsamkeit sogar der Ausspruch „Go Dutch“ verbreitet: Jeder in einer Gruppe – egal ob bei einem Restaurantbesuch oder in einem Staatenbund zahlt seine Ausgaben selbst, statt sie solidarisch auf alle Schultern zu verteilen (vgl. Collins Dictionary 2021).

2016 erregten die Niederlande zudem Aufsehen, indem sie durch ein Referendum das Assoziierungsabkommen der EU mit der Ukraine zwischenzeitlich kippten, obwohl die damals übrigen 27 Mitgliedsstaaten dem Abkommen bereits zugestimmt hatten (vgl. Reuters 2016). Und schon 2005 beriefen sich die Niederländer auf eine Volksabstimmung, als sie mit Frankreich eine gemeinsame europäische Verfassung verhinderten (vgl. Deutsche Welle 2005). Es scheint sich wie ein roter Faden durch die jüngste niederländische Vergangenheit zu ziehen, die politische Neutralität wahren und eine gewisse Distanz aufrechterhalten zu wollen. Hieraus spricht unter anderem eine tief sitzende Angst vor Assimilation durch große Nachbarn oder transnationale Staatenbünde. Den Niederländern waren Eigenständigkeit und Flexibilität seit der Loslösung von Spanien und später von Deutschland elementar wichtig, sodass diese Schlagworte bis heute regelmäßig im Mittelpunkt von Debatten, zum Beispiel mit

⁵⁴ Deutsch: Die Niederlande gehören zu Europa: geografisch, historisch, kulturell und wirtschaftlich. Europa ist für unseren Wohlstand, unsere Freiheit und Sicherheit von wesentlicher Bedeutung. Die weitere Beteiligung am europäischen Prozess liegt daher im unmittelbaren Interesse der niederländischen Bürger und Unternehmen.

Brüssel, stehen. Die Niederlande sehen sich folglich innerhalb Europas der Herausforderung gegenüber, sich gegen große Nachbarstaaten behaupten und Zweckkoalitionen eingehen zu müssen (vgl. accountant.nl 2021).

Mit dem Brexit und dem Verlust des britischen Partners schien dieser Druck zuzunehmen und in den Niederlanden war die Sorge zu verspüren, „künftig nicht länger gehört zu werden“ (Euronews 2021). Daher bat die niederländische Zweite Kammer der Generalstaaten den Adviesraad Internationale Vraagstukken⁵⁵ – ein unabhängiger Rat, der Regierung und Parlament in Belangen der Außenpolitik zur Seite steht – um Empfehlungen, wie nach dem Austritt Großbritanniens zukünftig Bündnisse mit EU-Mitgliedsstaaten zu schließen sind; insbesondere in europäischen Angelegenheiten und Fragen der Sicherheit (vgl. adviesraadinternationalevraagstukken.nl 2021). Aus der Antwort des Adviesraad lässt sich ableiten, dass die Niederländer eine Machtverschiebung in Europa feststellten: Einerseits verlor man ein gleich gesinntes Schwergewicht, andererseits sahen sie eine Gelegenheit, die internationale Bedeutung des Landes zu untermauern, indem die Niederlande als Ombud zwischen den Briten und den Festlandeuropäern auftraten: „Nu het VK de EU gaat verlaten, kan Nederland als wellicht bevoorrechte Britse gesprekspartner op het continent, binnen de EU, aan belang winnen“⁵⁶ (Adviesraad Internationale Vraagstukken 2018, 56). Der Adviesraad regte an, der EU zuvorzukommen und proaktiv Themen einzubringen und die Agenda der Europäischen Union selbst zu bestimmen, bevor Debatten durch andere Parteien eingefärbt sind. Für diese Intention sollten die Niederlande neue Koalitionen inmitten der EU eingehen, die ungeachtet vergangener Differenzen oder heutiger Uneinigkeiten zweckgebunden sein und keine Bündnisoption ausschließen sollten (vgl. Adviesraad Internationale Vraagstukken 2018, 57). Diese flexible bis opportunistische Diplomatie ist aus Sicht der Niederländer notwendig, um die Positionen des kleinen Landes gegen die großen Mitgliedsstaaten durchsetzen zu können. Zusätzlich intensivieren sie die freundschaftlichen Beziehungen zu Frankreich, „om invloed uit te oefenen op de richting van mogelijke Frans-Duitse initiatieven“⁵⁷ (Adviesraad Internationale Vraagstukken 2018, 61). Aufgrund ihrer geringen geografischen Größe bemessen die Niederlande ihre europapolitische Bedeutung

⁵⁵ Deutsch: Beirat für Internationale Angelegenheiten

⁵⁶ Deutsch: Jetzt da Großbritannien die EU verlässt können die Niederlande als möglicherweise privilegierter britischer Gesprächspartner auf dem Kontinent, innerhalb der EU, an Bedeutung gewinnen.

⁵⁷ Deutsch: um Einfluss auf die Richtung von möglichen Französisch-Deutschen Initiativen zu nehmen.

gelegentlich gering und suchen demgemäß ein Gegengewicht zur deutsch-französischen Verbindung. Dabei täuscht der Eindruck, der Küstenstaat sei ein Zwerg in Europa: Er stellt die fünftgrößte Ökonomie des Kontinents und weist sogar das zweithöchste Bruttoinlandsprodukt pro Kopf auf (vgl. Destatis 2021a). In Konsequenz sind die Niederlande nicht nur Teil der Frugalen Vier oder der Allianz der Verantwortung, sondern gehören seit 2018 zur sogenannten Hanze-coalitie⁵⁸ oder Hanzeliga, zu der unter anderem Finnland, Irland und die drei baltischen Staaten zählen (vgl. Clingendael Spectator 2018). Die Länder, die damit an die mittelalterliche Hanse erinnern wollen, plädieren unter der Führung der Niederlande für nationale Autonomie der EU-Ökonomien ohne europäische Haushalte oder Wirtschaftsminister, stattdessen mit verbindlichen Handelsabkommen (vgl. Clingendael Spectator 2018). Mit diesem Zusammenschluss versuchen die Beteiligten, auf die europäische Fiskalpolitik im eignen Sinn einzuwirken und das Machtgefälle in der Union auszugleichen. Auch das zeigt: Die Niederlande sind sich ihrer gegenwärtigen Rolle sowie ihrer Handlungsoptionen bewusst und positionieren sich als Begründer von strategischen Zweckbündnissen wie auch als Sprachrohr weiterer kleiner Staaten Europas.

Auf dem außereuropäischen Parkett sind die Niederlande neben Nationen wie Frankreich, den USA, China oder auch Deutschland ein kleiner Akteur. Das Land hat nur in wenigen Ausnahmen eine führende Funktion und ist aus militärischer oder diplomatischer Sicht gar unbedeutend. Daraus resultierend grundlegend eine eher eingeschränkte internationale Strahlkraft. In gewissen Belangen dagegen sind die Niederlande von elementarer Relevanz, zum Beispiel bei der multilateralen Verurteilung von Verbrechen gegen die Menschlichkeit durch den Internationalen Strafgerichtshof in Den Haag, der das oberste Rechtsprechungsorgan der Vereinten Nationen darstellt. Zudem sind die Niederlande auf einigen Gebieten führend und erfahren dafür auch über den Kontinent hinaus Anerkennung. Das Land gilt beispielsweise als äußerst lebenswert: Im OECD Better Life Index liegen die Niederlande in den meisten Messkategorien sichtlich über dem Durchschnitt und bilden vor allem in den Kategorien Zufriedenheit, Sicherheit und Beschäftigung den Gipfel (vgl. oecdbetterlifeindex.org 2020). In weiteren Untersuchungen, etwa von Transparency International oder Reporter ohne Grenzen, belegen die Niederlande regelmäßig Spitzenplätze bei Themen wie Menschenrechten, Freiheit oder Integrität –

⁵⁸ Deutsch: Hansekoalition

teils deutlich vor Deutschland (vgl. Transparency.org 2020/Reporters without borders 2021). Politisch ist das Land hingegen zerrissener als viele seiner Nachbarn: Die Spaltung in einen national-autoritären und einen progressiv-libertären Pol zeigt sich nicht nur im niederländischen pluralistischen Parteiensystem, sondern schlägt sich gar in der geografisch-demografischen Verteilung nieder:

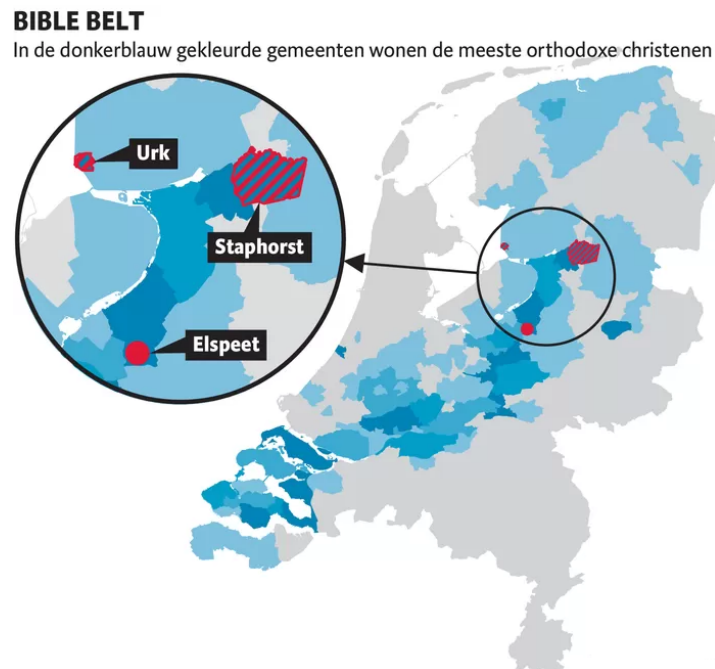


Abbildung 11: Bible Belt (De Stentor 2021)

Während die dicht besiedelte Randstad im Westen der Niederlande die ökonomische wie politische Zentrale des Landes ausmacht und ebenso für Progression wie für Modernismus steht, ist der angrenzende, ländliche Bible Belt Abbild des Konservativismus. Der unmittelbar neben der Randstad liegende Gürtel ist geprägt von der Frömmigkeit der reformierten Kirchen, Traditionalismus und teils von der Ablehnung staatlicher Institutionen. Der im historischen Rückblick identifizierte Wandel begleitet die Niederlande demnach bis heute und scheint eine Kernkompetenz des Landes zu sein. Bis heute haftet den Niederländern ihre pertinente Anpassungsfähigkeit an, ihr Pragmatismus, aber auch der Nachgeschmack jahrzehntelanger Verzuiling. Derweil haben es die Niederlande stets vollbracht, Identitätsverlust abzuwenden, indem sie ihr Selbstverständnis über Königtum sowie ihren nach Fortschritt eifernden Opportunismus konservieren. Ein Paradigma, das insbesondere mit Blick auf IT-Sicherheit nützlich sein kann.

2.6 Wie ordnet sich Cybersicherheit in den Niederlanden?

Wie schon Kapitel 2.3 dienen die folgenden Absätze dazu, bedeutende Akteure und Institutionen der nationalen Cybersicherheitsinfrastruktur aufzuzeigen, um letztlich Aussagen über IT-Strategien und die Priorisierung digitaler Sicherheitspolitik treffen zu können. Dabei sei erneut betont, dass diese Methode nur eine Momentaufnahme präsentieren kann. Noch in einer Studie der Universität Groningen von 2012 unter niederländischen Staatsanwälten etwa gab einer der Befragten die Parole „Blood comes before bytes“ aus, wonach digitale Straftaten seinerzeit vermeintlich nachrangig behandelt wurden (Bulanova-Hristova et al. 2016, 20). Seit dieser Aussage war im abgelaufenen Jahrzehnt jedoch ein eklatanter Wandel zu beobachten. So gründete sich im darauffolgenden Jahr das Security Delta, eine gemeinnützige Kooperation privatwirtschaftlicher und öffentlicher Akteure. Mehr als 275 niederländische Organisationen haben sich zum Ziel gemacht, präventive IT-Sicherheitsmaßnahmen zu ergreifen, indem sie etwa Talente fördern oder Unternehmen bei der Absicherung ihrer Systeme beraten. „De focus ligt hierbij op Cybersecurity & -weerbaarheid, Data & AI/Intel en Slimme Veilige Samenlevingen“⁵⁹ (Security Delta 2022). Ebenfalls im Jahr 2013 richtete die niederländische Regierung erstmalig die One Conference aus, um den internationalen Austausch von Cybersicherheitsexperten zu unterstützen und in Den Haag zu etablieren. Heute rekrutiert die Strafverfolgung in den Niederlanden junge IT-Straftäter über das Präventionsprogramm Hack_Right, sodass diese ihr Talent nach einem mehrstufigen Sozialisierungsprogramm für ethisches Hacking einsetzen können (vgl. Openbaar Ministerie 2018). Solche Kurswechsel haben sich in den vergangenen Jahren vielerorts in niederländischen Institutionen ereignet und sind der rapiden Digitalisierung geschuldet. Zudem setzte sich verstärkt die Erkenntnis durch, dass die beste Infrastruktur – man denke an die gewaltigen Staudämme an den Küsten des Landes – fragil ist, wenn sie auf technischem Weg sabotiert wird. Der substanzielle Bedarf der Niederlande an resistenter, wehrfähiger Informationstechnik ist also evident und schlägt sich entsprechend in den Organisationen und Ordnungsgefügen nieder, die digitale Sicherheit garantieren sollen.

⁵⁹ Deutsch: Der Fokus liegt auf Cybersecurity und Resilienz, Daten und Künstlicher Intelligenz und auf sicher vernetzten Gesellschaften.

2.6.1 Staatliche Institutionen

Die Zuständigkeit für das Thema Informationssicherheit verteilt sich in den Niederlanden auf nur wenige Organisationen unter drei Ministerien: Im Ministerie van Justitie en Veiligheid⁶⁰ sind der Nationaal Coördinator Terrorismebestrijding en Veiligheid⁶¹ (NCTV) und das Nationaal Cyber Security Centrum (NCSC) angesiedelt. Der NCTV dient der Terrorismusabwehr und engagiert sich insbesondere für den Schutz Kritischer Infrastrukturen vor Cyberangriffen. Dafür hat das NCTV unter anderem die Nederlandse Cybersecurity Agenda abgesteckt. Das NCSC bildet das operative Gegenstück zum strategischen NCTV. „Het NCSC is het incident response-team voor de Rijksoverheid en de vitale sectoren in Nederland“⁶² (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021b). Der NCTV fungiert als koordinierender Auftraggeber, wohingegen das NCSC IT-Sicherheitsvorfälle bewältigt und die Sicherheit der Regierungsnetze gewährleistet. Ergänzt werden diese beiden Institutionen seit 2018 durch das Digital Trust Center des Ministerie van Economische Zaken en Klimaat⁶³, das wiederum den beratenden Kontaktpunkt explizit für niederländische Unternehmen darstellt.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties⁶⁴

Dem Innenministerium, dem Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), obliegen die öffentliche Verwaltung, Belange des Bauens und Wohnens, die Pflege der Beziehungen zu den karibischen Inseln des Königreichs, die Digitalisierung der Administration sowie der Schutz der Demokratie. Trotz der Fülle der Aufgaben ist augenfällig, dass Aspekte der inneren Sicherheit und des Polizeiwesens nicht, wie beispielsweise in Deutschland, Frankreich oder Österreich, im Innenministerium liegen, sondern im Ministerie van Justitie en Veiligheid. Das BZK beaufsichtigt dagegen den In- und Auslandsnachrichtendienst Algemene Inlichtingen- en Veiligheidsdienst⁶⁵ (AIVD). Der AIVD dient nach eigener Auskunft dazu, Kommunikation abzufangen, um Bedrohungen für die Niederlande frühzeitig zu erkennen. Dazu ist der AIVD Teil des Cyber Security Raad wie auch im NCSC engagiert und soll zu einem gemeinsamen und

⁶⁰ Deutsch: Minister für Justiz und Sicherheit

⁶¹ Deutsch: Nationaler Koordinator für Terrorismusbekämpfung und Sicherheit

⁶² Deutsch: Das NCSC ist das Incident Response Team für die Regierung und die Kritischen Infrastrukturen in den Niederlanden.

⁶³ Deutsch: Ministerium für Wirtschaft und Klima

⁶⁴ Deutsch: Ministerium für innere Angelegenheiten und Königsbeziehungen

⁶⁵ Deutsch: Allgemeiner Nachrichten- und Sicherheitsdienst

integralen Lagebild der Informationssicherheit beitragen (vgl. Algemene Inlichtingen- en Veiligheidsdienst 2011).

Ministerie van Justitie en Veiligheid⁶⁶

Schon dem Namen nach kümmert sich das niederländische Ministerie van Justitie en Veiligheid (JenV) nicht nur um die Justiz, sondern auch um die Sicherheit des Landes. Das Ministerium befasst sich mit der Aufrechterhaltung des Rechtsstaates, der Prüfung von Gesetzesvorlagen, der Strafverfolgung, Jugend- und Verbraucherschutz, Asyl- und Migrationsangelegenheiten, Antisemitismusbekämpfung und der Durchsetzung von Sanktionen. Auch die Terrorismusbekämpfung, Krisenkommunikation und Cybersicherheit gehören zum Spektrum des JenV. Dazu betreibt das Ministerium unter anderem Staatsanwaltschaft und Polizei der Niederlande und ist verantwortlich für den NCTV sowie das NCSC. Zum 14. Oktober 2010 verlegte das Kabinett Rutte-Verhagen die Dienste „directoraat-generaal Veiligheid, de Immigratie- en Naturalisatiedienst en de Inspectie Openbare Orde en Veiligheid“⁶⁷ vom Innen- in das Justizministerium (Nationaalarchief 2010). Diese Konsolidierung von Polizei, Staatsanwaltschaft und Gesetzgebung unter der Aufsicht eines einzelnen Ministeriums ist unüblich für demokratische Staaten mit Gewaltenteilung und versetzt das JenV in eine durchaus machtvolle Schlüsselrolle innerhalb der niederländischen Ressortlandschaft.

Nationaal Coördinator Terrorismedbestrijding en Veiligheid⁶⁸ (NCTV)

Der Nationaal Coördinator Terrorismedbestrijding en Veiligheid (NCTV) ist die staatliche Institution zur Abwehr und Vorbeugung terroristischer Gefährdungen und extremistischer Tendenzen. Infolge der Anschläge in New York, Madrid oder auch 2004 in Amsterdam wird der NCTV als Nationaal Coördinator Terrorismedbestrijding (NCTb) gegründet und 2011 mit anderen ehemaligen Sicherheitsorganen zum NCTV zusammengeschlossen (vgl. Nationaal Coördinator Terrorismedbestrijding en Veiligheid 2022a). Dort sind seither die Aufgaben „terrorismedbestrijding, cybersecurity, nationale veiligheid, crisisbeheersing en weerbaarheid tegen statelijke dreigingen“⁶⁹ gebündelt, die teils als Aufträge, wie im Fall von Cybersicherheit an das NCSC, an

⁶⁶ Deutsch: Ministerium der Justiz und Sicherheit

⁶⁷ Deutsch: Generaldirektion Sicherheit, Einwanderungs- und Einbürgerungsdienst und Aufsichtsbehörde für öffentliche Ordnung und Sicherheit

⁶⁸ Deutsch: Nationaler Koordinator für Terrorismusbekämpfung und Sicherheit

⁶⁹ Deutsch: Terrorismusbekämpfung, Cybersicherheit, nationale Sicherheit, Krisenmanagement und Abwehrfähigkeit gegen staatliche Bedrohungen

weitere Behörden delegiert werden (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2022b).

Der NCTV benennt auf der eigenen Webseite drei Hauptaufträge. Darunter befindet sich die Aufgabe, die Niederlande vor terroristischen Anschlägen zu schützen; ergänzt durch die Aufgabenstellung, insbesondere staatliche Akteure abzuwehren. Als ersten Auftrag aber führt der NCTV ins Feld, die Niederlande digital sicher zu machen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2022b). Diese Reihenfolge ist ein Indiz für die Bedeutung der IT-Sicherheit innerhalb der niederländischen Sicherheitsarchitektur und Terrorismusabwehr. Zumindest an dieser Stelle steht die virtuelle über der physischen Sicherheit oder wird mindestens gleichrangig betrachtet, denn die niederländische Gesellschaft und Wirtschaft sei laut NCTV besonders vulnerabel über den digitalen Angriffsvektor (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2022b). Im Rahmen der Veröffentlichung des Cybersecuritybeeld Nederland 2021 unterstrich der NCTV seine Priorisierung von Digitalthemen in einer Pressemitteilung: „De digitale en de fysieke wereld zijn niet meer van elkaar te onderscheiden en digitale processen vormen het zenuwstelsel van de maatschappij“⁷⁰ (Rijksoverheid 2021b). Damit erhält die Cybersicherheit nicht nur den gleichen Stellenwert wie die physische Absicherung, sondern kommt als inhärenter Baustein, gar als eine Bedingung, gegenwärtiger Lebensweisen daher.

Nationaal Cyber Security Centrum⁷¹ (NCSC)

Seit der Grundsteinlegung des Nationaal Cyber Security Centrum 2012 war der NCTV die Aufsichtsbehörde des NCSC und übergab das ausgegliederte NCSC 2019 als selbstständige Institution unter Leitung von Hans de Vries in das Ressort des Ministerie van Justitie en Veiligheid. Seitdem ist der NCTV koordinierender Auftraggeber des NCSC (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021b). Das NCSC ist somit eine zentrale Einrichtung für die Sicherheit von Informationstechnik in den Niederlanden und bildet ein Pendant zum deutschen BSI. Das NCSC ist nicht wie das BSI dem Innenministerium nachgeordnet, sondern untersteht dem Minister für Justiz und Sicherheit.

⁷⁰ Deutsch: Die digitale und die physische Welt sind nicht mehr voneinander zu unterscheiden und digitale Prozesse bilden das Nervensystem der Gesellschaft.

⁷¹ Deutsch: Nationales Cybersicherheitszentrum

Mit der Gründung des NCSC 2012 ist anzunehmen, dass die Niederlande den Handlungsbedarf erst spät erkannt haben; das BSI etwa nahm bereits 1991 seine Arbeit auf. Dem ist jedoch nicht so, denn erstens sind die Niederländer im internationalen Vergleich medioker: Das französische ANSSI gründete sich 2009, das britische NCSC 2016, die amerikanische CISA 2018 und das italienische Pendant ACN wurde erst 2021 ins Leben gerufen. Zweitens verfügten die Niederlande bereits 1993 über ein Gesetz zur Computerkriminalität, für das das Wetboek van Strafrecht⁷² angepasst wurde (vgl. Staatsblad van het Koninkrijk der Nederlanden 1993, 1ff). Dort wurde unter anderem erstmals juristisch festgeschrieben, was unter Daten und automatisierten Systemen zu verstehen und insbesondere wann in diesem Zusammenhang von einer Straftat zu sprechen ist. Eine legitimierte Institution zum Schutz digitaler Infrastruktur fehlte zu diesem Zeitpunkt genauso wie eine entsprechende Gesetzgebung, die der globalisierten Kriminalität Rechnung tragen und über die Grenzen der Niederlande Wirkung zeigen konnte (vgl. Bulanova-Hristova et al. 2016, 26).

Unter der Überschrift „Ontwikkelingen die om actie vragen“⁷³ in der nationalen Cybersicherheitsstrategie der Niederlande von 2011 lässt sich ein Hinweis darauf finden, warum die Geschichte des NCSC just 2012 begann – 21 Jahre nach der Gründung des BSI (Tweede Kamer der Staten-Generaal 2011, 2). Dort ist die Rede von erhöhter Verwundbarkeit der Kommunikationstechnik wie auch von immer fortgeschrittenerer Schadsoftware:

Zo is in de tweede helft van 2010 geavanceerde malware – Stuxnet – ontdekt, die zich specifiek richt op industriële procesautomatisering. [...] Het vermoeden bestaat dat deze aanval door een staat gefinancierd is, gericht tegen de vitale infrastructuur in een andere staat, met wereldwijde neveneffecten bij andere (vitale) organisaties⁷⁴ (Tweede Kamer der Staten-Generaal 2011, 2).

Insbesondere Stuxnet kann demnach als Initialzündung für das NCSC gesehen werden. Die Malware war 2010 auf Millionen Rechnern weltweit auffindbar und sollte Industrieanlagen sowie Kritische Infrastrukturen gezielt stören. Stuxnet war besonders aufwendig programmiert und wurde nach seiner Entdeckung vielfach erste oder „globale Cyberwaffe“ getauft (ZEIT ONLINE 2010). Und nicht nur in den

⁷² Deutsch: Strafgesetzbuch

⁷³ Deutsch: Entwicklungen, die ein Handeln erfordern.

⁷⁴ Deutsch: Beispielsweise wurde in der zweiten Hälfte 2010 die fortschrittliche Malware Stuxnet entdeckt, die speziell auf die industrielle Prozessautomatisierung abzielt. Es wird vermutet, dass dieser Angriff von einem Staat finanziert wurde, der sich gegen Kritische Infrastruktur in einem anderen Staat richtet, mit weltweiten Nebenwirkungen auf andere (lebenswichtige) Organisationen.

Niederlanden sorgte Stuxnet für Aufsehen sowie neue Sicherungsstrategien: In Deutschland gründete sich beispielsweise die Allianz für Cyber-Sicherheit aus dem BSI heraus – ein privat-öffentliches Netzwerk zum Schutz deutscher Unternehmen.

Auch darin begründet sich der Auftrag, den sich die niederländische Behörde in ihrem Web-Auftritt zuschreibt, nämlich digitale Gefahren abzuwehren, Krisen zu beherrschen, eine Kooperationsplattform für Cybersicherheit zu sein und stets Handlungswege oder Lösungen anzubieten (vgl. Nationaal Cyber Security Centrum 2018b). Vergleichbar mit dem BSI ist das NCSC prioritär für die Sicherheit staatlicher Netze, Ämter, Ministerien, des Parlaments und für den Schutz Kritischer Infrastrukturen verantwortlich:

De primaire doelgroep van het NCSC is de rijksoverheid en de vitale infrastructuur. De vitale sectoren zijn cruciaal voor het goed functioneren van de Nederlandse samenleving. Voorbeelden van vitale sectoren zijn energie, water en telecom⁷⁵ (Nationaal Cyber Security Centrum 2018b).

Das Wet beveiliging netwerk- en informatiesystemen (Wbni)⁷⁶ ist das niederländische Gesetz, welches unter anderem die Aufgaben des NCSC klar definiert und dabei aufzeigt, wo der Schwerpunkt der Behörde liegt. So hat das NCSC im Kern zwei Verpflichtungen:

1. Das NCSC übernimmt die Aufsicht, Beratung, Unterstützung und den Schutz Kritischer Infrastrukturen und Regierungsorganisationen hinsichtlich ihrer digitalen Immunität und hat dazu die Befugnisse, sogenannte Computer Security Incident Response Teams (CSIRT) zu organisieren und im Bedarfsfall zu entsenden (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 2f).
2. Ferner informiert das NCSC in definierten Fällen relevante Institutionen oder auch die Öffentlichkeit über einen Vorfall. Zum Beispiel dann, wenn Kritische Infrastruktur funktionsunfähig wird, ein Dienstbetreiber der Veröffentlichung freiwillig zustimmt oder dann, wenn eine akute Bedrohung für die Gesellschaft besteht, sofern eine Mitteilung unterbliebe (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 9).

In diesem Aspekt gleichen sich der niederländische und der deutsche Ansatz nahezu. Vorrang hat der Betrieb vitaler Strukturen, um das ungestörte Bestehen staatlicher

⁷⁵ Deutsch: Die primäre Zielgruppe des NCSC ist der Staat und die Kritische Infrastruktur. Die Kritische Infrastruktur ist grundlegend für das Funktionieren der niederländischen Gesellschaft. Beispiele für Kritische Infrastrukturen sind Energie, Wasser und Telekommunikation.

⁷⁶ Deutsch: Gesetz über die Sicherheit von Netzwerk- und Informationssystemen

Ordnung gewährleisten zu können. Erst danach folgt der Schutz sonstiger ökonomischer Entitäten und der IT der Zivilbevölkerung.

Nicht zuletzt wird dem Ministerie van Justitie en Veiligheid verordnet, als „centraal contactpunt“⁷⁷ für jegliche Fragen der Cybersicherheit bereitzustehen – national wie europäisch (Staatsblad van het Koninkrijk der Nederlanden 2018b, 1f): „Dit betekent dat wanneer het NCSC een melding ontvangt die ook voor andere landen relevant is, dat deze operationele informatie gedeeld wordt met het contactpunt in andere lidstaten“⁷⁸ (Nationaal Cyber Security Centrum 2022b). Das NCSC ist demnach der Knotenpunkt zur Koordinierung binnenländischer IT-Sicherheitsangelegenheiten wie auch die Schnittstelle zu grenzüberschreitenden Partnerorganisationen. Wenngleich diese und die zuvor benannten Aufgaben als Arbeitsaufträge für den Minister formuliert sind, hat dieser die Arbeitsaufträge und Funktionen an das NCSC delegiert, womit der wesentliche Anteil der staatlichen Cybersicherheitsanstrengungen in den Niederlanden hier zusammenläuft. Das NCSC agiert primär informierend und dementsprechend präventiv (vgl. Bulanova-Hristova et al. 2016, 22f). Dazu bringt die Behörde private und öffentliche Partner zusammen und fungiert als Scharnier zwischen anderen staatlichen Sicherheitsorganen wie dem Digital Trust Center, der National High Tech Crime Unit oder der Terrorismusabwehr des Landes.

Damit entspricht das Nationaal Cyber Security Centrum im engsten Sinn seinem Auftrag, Kritische Infrastruktur und Regierungsnetze zu beschützen. Den Schutz übriger privatwirtschaftlicher Informationstechnik spart das NCSC weitestgehend aus. Die digitale Sicherheit von Privatanwendern wird lediglich punktuell in Präventions- und Sensibilisierungsprodukten aufgegriffen, so etwa in der öffentlich-privaten Initiative veiliginternetten.nl. Videos und andere Medien der Behörde dienen dagegen der Aufmerksamkeitssteuerung und der Imagination, das NCSC sei die Lösung digitaler Sicherheitsprobleme.

Politie / National High Tech Crime Unit (NHTCU)

Während das NCSC eine koordinierende Funktion in der Krisenbewältigung einnimmt, ist die National High Tech Crime Unit als Baustein der niederländischen Polizei

⁷⁷ Deutsch: zentraler Knotenpunkt

⁷⁸ Deutsch: Das bedeutet, dass wenn das NCSC eine Meldung empfängt, die auch für andere Länder relevant ist, diese operativen Informationen mit der Kontaktstelle in anderen Mitgliedstaaten geteilt werden.

strafverfolgend tätig. In Fällen landesweiter Bedeutsamkeit kommen in dieser Einheit der nationalen Polizei IT-Experten zusammen (vgl. Bulanova-Hristova et al. 2016, 18). Da die Ressourcen der NHTCU jedoch begrenzt sind, zieht sie anlassbezogen die Unterstützung der zehn regionalen Polizeien des Landes heran. Dort bilden sich dann Ermittlerteams aus Informatikern und Kriminalisten, die Angriffe zurückverfolgen und Täter ausmachen (vgl. Odinet et al. 2017, 18). Weil es sich, wie eingangs herausgearbeitet, bei den Niederlanden um einen dezentralen Einheitsstaat handelt, sind die Kompetenzen der Polizei nicht derart segmentiert über die nationalen Einrichtungen verteilt wie etwa in einem föderalistischen Staat. Der Verantwortungsbereich der NHTCU liegt insbesondere bei Straftaten, die ein besonderes Maß an technischer Expertise erfordern und von landesweiter Bedeutung sind. Alle anderen Fälle, beispielsweise von Online-Betrug oder Datendiebstahl obliegen den regionalen Polizeieinheiten (vgl. Odinet et al. 2017, 19). Die NHTCU füllt somit den Raum zwischen der konventionellen Polizeiarbeit und dem NCSC. Die Einheit soll durch ihre Spezialisierung ebenjene Lücke zwischen dem Erkennen einer digitalen Straftat und der Ermittlung von verantwortlichen Personen schließen, um Cybercrime langfristig unattraktiver zu machen.

Ministerie van Economische Zaken en Klimaat⁷⁹

Das Wirtschafts- und Klimaministerium der Niederlande ist das dritte bedeutende Ressort für die Cybersicherheit im Königreich. Zuvorderst zeigt sich das Ministerie van Economische Zaken en Klimaat (EZK) verantwortlich für Wirtschaft und Innovation, Digitalisierung, Klimaschutz, Nachhaltigkeit und Energiesicherheit wie auch für internationale Zusammenarbeit. Um dieser breiten Aufgabenpalette gerecht werden zu können, gruppieren sich unterhalb des Ministeriums zahlreiche Behörden und Ämter, die mit einzelnen Facetten befasst sind. Allein für Digitalisierung und Informationssicherheit unterstehen dem EZK mindestens vier Behörden, die aus unterschiedlichen Ausgangspositionen beitragen. Die Rijksinspectie Digitale Infrastructuur⁸⁰ mit ihrer wiederum untergeordneten Behörde Agentschap Telecom⁸¹ überwacht die Einhaltung des Telekommunikationsgesetzes, den sicheren Betrieb der Kommunikationsnetze und unter anderem die Vergabe von Mobilfunkfrequenzen. Der

⁷⁹ Deutsch: Ministerium für Wirtschaft und Klima

⁸⁰ Deutsch: Reichsinspektion für digitale Infrastruktur

⁸¹ Deutsch: Telekommunikationsagentur

Dienst ICT Uitvoering⁸² (DICTU) administriert und entwickelt digitale Dienste des Reiches wie beispielsweise Arbeitsumgebungen, Apps oder Webseiten. Die Autoriteit Consument en Markt⁸³ (ACM) ist die niederländische Behörde, die die Interessen der Endverbraucher vertritt und somit auf unter anderem das Ministerium, aber auch auf Hersteller und Dienstleister einwirkt, um Produkte und Dienste im Sinne der Konsumenten zu verbessern. Dabei handelt es sich um eine Behörde, die sich als unabhängig bezeichnet, jedoch vom niederländischen Wirtschaftsministerium beaufsichtigt ist – eine Information, die auf der Webseite der ACM nicht zu finden ist (vgl. Rijksoverheid 2023b). Nicht zuletzt untersteht dem EZK das Digital Trust Center, ein Schnittstellenamt, das Unternehmen unterstützt, Netzwerke schafft und sie in Fragen der Informationssicherheit berät.

Digital Trust Center Nederland

Das Digital Trust Center hält für alle Unternehmen Rat und Hilfe bereit, die nicht zu den Kritischen Infrastrukturen gehören, also nicht vom NCSC unterstützt werden. Das bedeutet, das DTC stellt sowohl präventive Informationen als auch Risikowarnungen für die Wirtschaft zur Verfügung und teilt zusätzlich unternehmensspezifische Bedrohungshinweise aus dem NCSC mit betroffenen Firmen (vgl. Digital Trust Center 2022a). Dabei macht sich das Digital Trust Center Netzwerkeffekte zunutze, indem es landesweite öffentlich-private Netzwerke erstellt, innerhalb derer Informationen zwischen Betroffenen, Mitwirkenden und öffentlichen Einrichtungen ausgetauscht werden (vgl. Ministerie van Economische Zaken en Klimaat 2021, 8). Das DTC setzt zu diesem Zweck auf niedrighschwellige Angebote, um möglichst vielen Unternehmen und Firmen den Einstieg in ebendiese Netzwerke zu erleichtern. Mit dem Basisscan Cyberweerbaarheid⁸⁴ etwa können auch Unternehmen, die sich bislang wenig um ihre IT-Sicherheit bemüht haben, Hilfe finden und Handlungsbedarfe identifizieren (vgl. Digital Trust Center 2022b). Mit dem Programm Landelijk Dekkend Stelsel⁸⁵ beabsichtigen das DTC und das NCSC, ein Kooperationssystem zu etablieren, in dem Regierungsorganisationen, Betriebe und Provider zusammengeschlossen sind und Informationen über digitale Bedrohungen schnell und präzise miteinander teilen. „Het doel van deze kennisuitwisseling is digitale ontwrichting te voorkomen en

⁸² Deutsch: Dienst für IKT-Umsetzung

⁸³ Deutsch: Behörde für Verbraucher & Markt

⁸⁴ Deutsch: Cyberabwehrkräfte

⁸⁵ Deutsch: Landesweites Deckungssystem

Nederland cyberweerbaarder te maken“⁸⁶ (Nationaal Cyber Security Centrum 2022c). Aus verschiedenen Quellen laufen Informationen zusammen, darunter Polizeien, NCSC, AIVD, private Meldungen und Anzeigen der Kritischen Infrastruktur. Diese Gemengelage wird analysiert, sodass die Zulieferer der Rohdaten sowie Kommunikationsanbieter und Reichsregierung ein möglichst vollständiges Bild der gegenwärtigen Lage erhalten und bestmöglich reagieren können. Das DTC und das NCSC nehmen hierin die Funktion von Supervisoren ein, die die Informationen sortieren, auswerten und an die erforderlichen Institutionen ausgeben. Dem DTC kommt zudem die Aufgabe zu, betroffene Branchen und Unternehmen zu kontaktieren und zu warnen. Die Informationen laufen in einem solchen Fall beispielsweise über das NCSC ein, werden evaluiert und wenn notwendig an die entsprechenden Betriebe weitergegeben, damit diese Updates einspielen oder Systeme wiederherstellen können, bevor der Vorfall großflächig und nachhaltig Schaden anrichten kann (vgl. Digital Trust Center 2021). Damit ist das Digital Trust Center nicht nur Netzwerkpartner und Informationsanbieter für niederländische Unternehmen, sondern ein wesentlicher Teil einer Sicherheitskette, die die ökonomische Handlungsfähigkeit des Landes sicherstellen soll und von grundlegender Bedeutung für die Reaktionsgeschwindigkeit von Wirtschaft und Regierung ist.

Cyber Security Raad⁸⁷

Der Cyber Security Raad berät das niederländische Kabinett bei Problemstellungen, die die Informationssicherheit betreffen. Der Rat hat die Funktion, die Kompetenzen der Ministerriege so zu erweitern, dass die Entscheidungsträger dort zu fundierten Beschlüssen kommen können. Um dieser Aufgabe nachkommen zu können, setzt sich der CSR aus Vertreterinnen und Vertretern der Wirtschaft, also Geschäftsführern oder CIOs bedeutender Unternehmen, wie aus Beauftragten der öffentlichen Hand, darunter Mitarbeiterinnen und Mitarbeiter der Polizei, des Militärs oder des Wirtschaftsministeriums zusammen. Und schließlich komplettiert sich das Gremium durch Wissenschaftler, die einen multiperspektivischen Austausch gewährleisten sollen (vgl. Cyber Security Raad 2020, 27). Der Rat ist aufgefordert, die Regierung – auch ungebeten – zu beraten, zur nationalen Cybersicherheitsstrategie beizutragen und

⁸⁶ Deutsch: Ziel dieses Wissensaustauschs ist es, digitalen Störfällen zuvorzukommen und die Niederlande gegenüber Cyberangriffen widerstandsfähiger zu machen.

⁸⁷ Deutsch: Cybersicherheitsrat

während schwerwiegender Zwischenfälle mit seinen Fähigkeiten zu unterstützen (vgl. Cyber Security Raad 2022a).

Defensie Cyber Commando⁸⁸

Das Defensie Cyber Commando (DCC) ist Bestandteil der Armee und schon dem Namen nach verantwortlich für die Landesverteidigung gegen militärische Angreifer. Das ist zum Beispiel dann der Fall, wenn ein Staat versucht, die niederländische Energieversorgung mit informationstechnischen Mitteln zu sabotieren. Dazu passt, dass das DCC geheimdienstliche Aufgaben wahrnimmt, um Bedrohungen und Spionage aus dem Cyberraum zu antizipieren. Dagegen ist es weniger selbstverständlich, dass das DCC darüber hinaus Angriffsbefugnis besitzt. Das bedeutet, es darf sowohl in fremde Systeme eindringen, um Informationen zu sammeln als auch „digitale systemen van tegenstanders aanvallen, manipuleren of uitschakelen“⁸⁹ (Defensie.nl 2022). Das Defensie Cyber Commando nimmt eine bemerkenswerte Position ein, da sich seine Berechtigungen in dieser Form und Deutlichkeit weder in den Niederlanden noch in Deutschland erneut finden lassen – insbesondere nicht in einem militärischen Kontext.

CERT Watermanagement⁹⁰

Das CERT Watermanagement (CERT-WM) ist eines von zahlreichen Cyber Emergency Response Teams, wie es sie in nahezu jedem Sektor des Landes gibt. Allerdings stellt das CERT-WM eine Besonderheit dar, die so in Deutschland und vielen weiteren europäischen Staaten nicht besteht. Im CERT-WM kommen die 21 Wasserbehörden der Niederlande sowie Rijkswaterstaat, die oberste Wasserschutzbehörde, zusammen, um die Informationen über Cyberangriffe auf die Wasserinfrastruktur des Landes zu bündeln. Zur naturgegebenen Bedrohungslage gibt Rijkswaterstaat heraus: „Bescherming tegen hoogwater is en blijft daarom van levensbelang: voor miljoenen Nederlanders en onze economie. [...] We onderhouden 2500 km aan dijken, dammen, stuwen en stormvloedkeringen en beschermen de kust“⁹¹ (Rijkswaterstaat 2022). Wenn beispielsweise die Steuerung dieser Schutzanlagen in die Hände von Angreifern gerieten, könnten sich die Niederlande existenziellen Bedrohungen konfrontiert sehen.

⁸⁸ Deutsch: Verteidigungs-Cyber-Kommando

⁸⁹ Deutsch: digitale Systeme von Gegenspielern angreifen, manipulieren oder deaktivieren

⁹⁰ Deutsch: Wassermanagement

⁹¹ Deutsch: Der Schutz vor Hochwasser ist und bleibt daher von lebenswichtiger Bedeutung: für Millionen Niederländer und unsere Wirtschaft. [...] Wir unterhalten 2500 km Deiche, Dämme, Sperren und Sturmflutwehre und schützen die Küste.

Daher legen die Wasserverwaltungen großen Wert auf die digitale Sicherheit der Infrastruktur wie auch auf die Integrität der Mitarbeiter. Mehrjährige Sicherungsprojekte sowie die Vereinigung in einem CERT sollen sicherstellen, dass Schwachstellen frühzeitig beseitigt, Angriffe abgewehrt werden können und die Niederlande ein insgesamt hohes Schutzniveau erreicht. Zu diesem Zweck wurde im sogenannten Security Operations Centre der Rijkswaterstaat das CERT Watermanagement eingerichtet, das relevante Systeme überwacht, im Notfall die Rettungsketten aktiviert, Meldungen verfasst und Störfälle einordnet (vgl. CERT-WM 2022).

Wie schon im Passus zu den deutschen Bundesinstitutionen geschildert, ist den Sicherheitsorganen des Staates systeminhärent, dass sie im Wortsinne konservativ agieren, um den Sicherheitszustand zu bewahren und Risiken zu adressieren. Sie richten sich zudem an übrige staatliche Akteure, gesetzgebende Institutionen oder an das Gros der Bevölkerung und üben damit mittelbar Einfluss auf die einzelnen Anwender. Obwohl mit der Autoriteit Consument en Markt in den Niederlanden eine relevante Verbraucherschutzorganisation besteht, liegt insgesamt auch hier der Schwerpunkt auf der technischen Prävention von Angriffsvektoren. NCSC, NCTV oder das DCC wenden viele Ressourcen auf, um materielle Abwehrmechanismen einzurichten und zu betreiben. Keine der Amtsstellen wartet stattdessen mit einer wirksamen Kampagne zur Genese von Digitalkompetenz und Resilienz auf, um jeden Einzelnen und damit das Gesamtgefüge besser sichern zu können. Jedoch kann der niederländische Staat seine Mittel in wenigen Behörden bündeln, die auf nur drei Ministerien aufgeteilt sind. Das bedeutet, dass in Fällen von Amtshilfe eine überschaubare Zahl von Institutionen zu beteiligen ist. Zudem lassen sich die Behördenhaushalte einfacher aufstellen und es bilden sich weniger Parallelstrukturen aus. Vor allem heißt das aber auch, dass die Cybersicherheitsstrukturen für Außenstehende plausibel gegliedert sind. Indem die IT-Sicherheitseinrichtungen übersichtlich und begreiflich bleiben, fällt es schließlich leichter, ihre Sinnhaftigkeit zu belegen.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	X	X		X		X		X			X

Gleichsam ist feststellbar, dass die niederländische IT-Politik teils sichtbar von Angstmotiven beeinflusst ist. Es ist kaum von der Hand zu weisen, dass etwa die Gründung des NCSC 2012 eine direkte Reaktion auf die weltweit gefürchtete Malware

Stuxnet war. Zudem betreibt das Land ganze Behörden wie Rijkswaterstaat beziehungsweise das übergeordnete CERT, um einer Angst vor (digitalen) Anschlägen auf Hochwasserstrukturen zu begegnen. Die Kombination aus vagem Unbehagen aufgrund weniger greifbarer Bedrohungen und der für Laien kaum durchdringbaren Komplexität von Informationssicherheit erleichtern die Produktion von Imaginationen, Szenarien und Erzählungen der Furcht.

2.6.2 Institutionen der Gesellschaft

Abseits der staatlichen existieren selbstverständlich auch in den Niederlanden alle nur erdenklichen Ausprägungen von Organisationen, Institutionen und Akteuren, die sich auf dem Feld der Informationssicherheit engagieren. Darunter befinden sich Nichtregierungsorganisationen, Ausgründungen ehemaliger Regierungsprojekte, Lobbyverbände, Interessengemeinschaften oder öffentlich-private Partnerschaften. Bei der Suche nach relevanten Einrichtungen realisiert man unweigerlich, dass eine beachtliche Menge entweder staatlich betrieben werden oder mindestens einen Auftrag durch die Reichsregierung innehaben, obwohl sie keine Behörde sind. Die Plattform veiliginternetten.nl ist hierfür ein Musterfall: Die Initiative entstand als Kooperationsprojekt des Ministerie van Economische Zaken en Klimaat, des Ministerie van Justitie en Veiligheid und der Platform voor de InformatieSamenleving⁹² (ECP). Im Rahmen der ECP beteiligen sich zudem zahlreiche Technologieunternehmen und Interessenvertretungen, sodass Veilig Internetten von einem Netzwerk öffentlich-privater Partnerschaften getragen wird. Mit diesem Webportal bieten die Akteure Tipps und Hilfestellungen zu verschiedensten Herausforderungen des digitalen Alltags an. „Ze vinden er tips hoe ze veilig omgaan met hun online privacy, hoe ze veilig gebruik maken van wifi, wat ze kunt doen en laten op sociale media, en ze vinden er uitleg over hoe zij kinderen helpen veilig online te zijn“⁹³ (Veilig Internetten 2015). Diesen Vorsatz nehmen die Betreiber ernst, sodass neben Hilfestellungen zur Datensicherheit auch Hinweise zum Datenschutz und sogar zu tangierenden Themen wie Cybermobbing zu finden sind. Die Tipps beschränken sich nicht auf Prävention, sondern auch Opfern von Cyberkriminalität oder Hilfesuchenden bei technischen Problemen stehen Hilfestellungen zur Verfügung. Obendrein suggerieren der Comicstil der Illustrationen

⁹² Deutsch: Plattform für die Informationsgesellschaft

⁹³ Deutsch: Sie finden Tipps zum sicheren Umgang mit ihrer Online-Privatsphäre, zur sicheren Nutzung von WLAN, was sie in sozialen Medien tun und lassen können, und sie finden Erklärungen, wie sie Kindern helfen, online sicher zu sein.

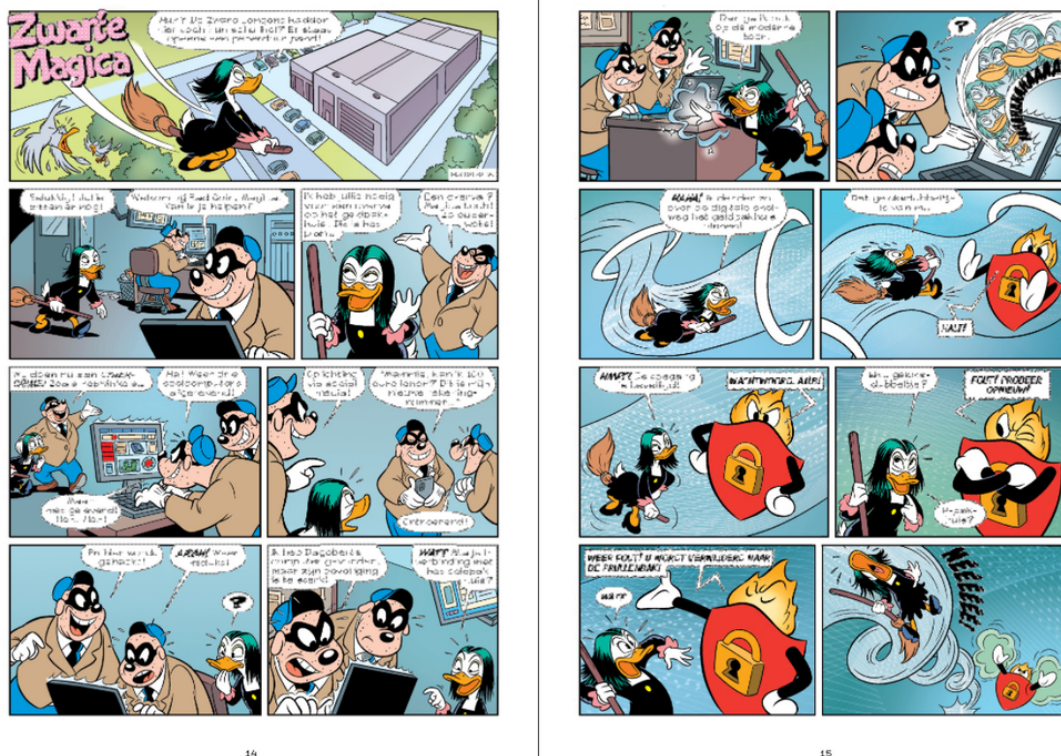
wie auch die zahlreichen Animationen zwar, dass Endanwender mit einem eher geringen technischen Wissensstand angesprochen werden, die für das Thema noch gewonnen werden müssen; allerdings finden sich genauso Fragen und Antworten, die sich zielgerichtet an Arbeitnehmer, Unternehmer oder Lehrer und Eltern wenden.



Abbildung 12: Antwoord op vragen en hulp bij problemen. Voor iedereen⁹⁴ (Veilig Internetten 2021)

Veilig Internetten richtet sich an alle, die Fragen zum sicheren Gebrauch des Internets haben (vgl. Veilig Internetten 2021). Damit geht aber auch einher, dass das Portal nicht alle Kompetenzniveaus adressieren und somit nur ausgewählten Anwenderbedürfnissen Rechnung tragen kann. Altersbedingt variierenden Ansprüchen, die beispielsweise zwischen Schülern und Senioren nicht von der Hand zu weisen sind, berücksichtigt Veilig Internetten nur rudimentär. Zum Safer Internet Day 2022, einem jährlichen, internationalen Aktionstag gab Veilig Internetten bekannt, dass sie eine Donald Duck-Ausgabe mit angepassten Botschaften für Kinder gestaltet haben, um auch schon Kinder ohne Umwege anzusprechen.

⁹⁴ Deutsch: Antworten auf Fragen und Hilfe bei Problemen. Für alle.



Außerhalb solcher Leuchtturmprojekte jedoch beschränkt sich die Plattform auf Inhalte für Erwachsene, die digitale Kompetenzen lehren oder in ihr persönliches Umfeld tragen und so die Informationen der Webseite multiplizieren. Veilig Internetten ist nicht gewinnorientiert oder werbefinanziert. Stattdessen dient die Initiative unter anderem dazu, das Engagement der Kooperationspartner sichtbar zu machen und einen übergreifenden Konsens über Schutzmaßnahmen darzustellen. Das Angebot ist nicht dialogisch und geht damit nicht auf individuelle Anforderungen ein. Nicht zuletzt ist Veilig Internetten weitestgehend auf dieses Onlineangebot beschränkt und außerhalb dessen kaum medial präsent.

⁹⁵ Deutsch: Heute ist Safer Internet Day

InformatieSamenleving 2021). Heute gibt die Organisation an, unabhängig und neutral zu sein und spricht statt von *Absprachen* von Zusammenarbeit, Wissensaustausch und einer verantwortungsvollen Gestaltung der Digitalisierung:

ECP | Platform voor de InformatieSamenleving is een onafhankelijk en neutraal platform waar overheid, wetenschap, bedrijfsleven, onderwijs en maatschappelijke organisaties publiek-privaat samenwerken aan en kennis uitwisselen over een verantwoorde vormgeving van onze digitaliserende samenleving⁹⁷ (ECP | Platform voor de InformatieSamenleving 2021).

Wenngleich die Organisation hier erklärt, digitale Interessen aller Gruppen innerhalb der Niederlande zu vertreten, liegt das Augenmerk der ECP auf Akteuren der Wirtschaft. Sowohl die Eigenbeschreibung als auch die Liste der umgesetzten Projekte und der Teilnehmer zeigen deutlich, dass ECP als Bindeglied zwischen der niederländischen Ökonomie und dem Staat agiert. Dafür ruft ECP regelmäßig zu zahlreichen Dialogplattformen und Gesprächsanlässen auf, zu denen Wirtschaft, Politik und Gesellschaft zusammenkommen und über Themen der Informationstechnologie verhandeln. Die Nederlandse AI Coalitie⁹⁸, Platform Gezondheid, zorg & ICT⁹⁹, Anti-DdoS-Coalitie¹⁰⁰ oder das NL Internet Governance Forum sind solche Gelegenheiten für Begegnung, um Unternehmen, Interessenverbände und Politik zusammenzubringen. Gegen den Vorwurf des Lobbyismus wehrt sich die Organisation, indem die ECP explizit betont, dass sie kein Lobbyverband sei (vgl. ECP | Platform voor de InformatieSamenleving 2021). Zudem untermauert die Breite der Teilnehmer wenigstens ein Mindestmaß an Neutralität. Neben mehreren Ministerien beteiligen sich die Gemeinden Amsterdam und Den Haag, die Zuyd University of Applied Sciences, die niederländische Polizei sowie zahlreiche Tech-Konzerne wie IBM, Google oder Microsoft. Sogar öffentlich mit dem Vorwurf der staatlichen Einflussnahme bis hin zur Spionage konfrontierte chinesische Unternehmen wie Tencent und Huawei gehören ECP an. Auch deshalb beschreibt man sich wie folgt: „Ze [ECP] fungeert als intelligente, neutrale tafel/spreekbuis voor onderwerpen die van belang zijn voor de ontwikkeling van de informatiesamenleving en waarbij behoefte is om publiek-privaat

⁹⁷ Deutsch: ECP | Plattform für die Informationsgesellschaft ist eine unabhängige und neutrale Plattform, auf der Regierung, Wissenschaft, Wirtschaft, Bildung und soziale Organisationen öffentlich-privat zusammenarbeiten und Wissen über eine verantwortungsvolle Gestaltung unserer digitalisierten Gesellschaft austauschen.

⁹⁸ Deutsch: Niederländische KI-Koalition

⁹⁹ Deutsch: Plattform Gesundheit, Pflege und Informationstechnik

¹⁰⁰ Deutsch: Anti-DdoS-Koalition

op te trekken“¹⁰¹ (ECP | Platform voor de InformatieSamenleving 2021). Damit pflegt ECP das Image des unabhängigen Wegbereiters, statt einer Interessenunion.

In die Kategorie der gesellschaftlichen Organisationen mit staatlichem Ursprung fällt auch die Vereniging van Nederlandse Gemeenten¹⁰² (VNG). Die VNG wurde initiiert, damit die niederländischen Kommunen enger zusammenarbeiten und insbesondere damit sie eine stärkere Position gegen die Reichsregierung in Den Haag einnehmen können (vgl. VNG.nl 2020). Heute ist die VNG nach wie vor die Interessengemeinschaft der Gemeinden, befasst sich mittlerweile aber mit einem deutlich diversifizierten Aufgabenfeld; dazu gehört die digitale Sicherheit der sensiblen Informationen, die die Bürger bei der Kommune hinterlegen müssen. Mit der *Agenda Digitale Veiligheid 2020 – 2024* legte die VNG Anfang 2020 ein Papier vor, das zwar wenige Maßgaben oder Forderungen enthält, aber einige Positionen der Vereinigung zum Ausdruck bringt. Man betont darin etwa, dass die Gemeinden ihre Informationssicherheit weitestgehend eigenverantwortlich gestalten, hier also eine gewisse Souveränität besitzen (vgl. VNG 2020, 11). Neben der oppositionellen Funktion unterstreicht die VNG, die Zusammenarbeit und den Wissensaustausch mit weiteren, ähnlichen Organisationen zu arrangieren, um Synergieeffekte nutzen zu können (vgl. VNG 2020, 17). Dies gibt weniger Auskunft über konkrete Sicherungsmaßnahmen der kommunalen Informationstechnik als über die grundsätzliche Rolle der Institution als Bindeglied zur Reichsregierung wie zu gleichrangigen Akteuren. Die Vereniging van Nederlandse Gemeenten ist ein Instrument und Sprachrohr der Basisdemokratie, das für realpolitische Belange einsteht, um die Kommunalposition innerhalb der vertikalen Regierungsorganisation des dezentralen Einheitsstaates zu vertreten.

Während die bis hierher aufgeführten Institutionen unter staatlicher Beteiligung entstanden oder teils noch staatlich gefördert werden, haben sich in der Domäne Cybersicherheit zivile Organisationen gegründet, die zur Absicht haben, auf Gesetzgebung und Politik in ihrem Sinn zu wirken. In Cyberveilg Nederland¹⁰³ gruppieren sich die relevanten Unternehmen der Informationssicherheit in den

¹⁰¹ Deutsch: Sie [ECP] fungiert als intelligenter/s, neutraler/s Tisch/Sprachrohr für Themen, die für die Entwicklung der Informationsgesellschaft wichtig sind und bei denen Bedarf an öffentlich-privater Zusammenarbeit besteht.

¹⁰² Deutsch: Vereinigung niederländischer Kommunen

¹⁰³ Deutsch: Cybersicher Niederlande

Niederlanden, wie zum Beispiel KPN Security, AntSec, TÜV-Nederland oder ESET. Cyberveilig Nederland bezeichnet sich selbst als Interessenvertretung dieser Firmen und macht kein Geheimnis aus den Handlungsmotiven: „Dé belangenorganisatie voor een optimaal ondernemingsklimaat voor cybersecuritybedrijven“¹⁰⁴ (Cyberveilig Nederland 2021). Der Zusammenschluss zahlreicher nationaler und internationaler IT-Konzerne versucht, die ökonomischen Umstände so zu gestalten, dass sie den Mitgliedern ein möglichst profitables Wirtschaften erlauben. Cyberveilig Nederland hat die kommerziellen Chancen der Digitalisierung ausgemacht und gelangt zu der Feststellung, dass es notwendig ist, mehr Vertrauen in Informationstechnik zu schaffen und deshalb mehr Aufmerksamkeit auf dieses Anliegen zu lenken (vgl. Cyberveilig Nederland 2023). Diese Bemühungen tragen sichtbar Früchte, da die Organisation seit Ende 2020 durch das NCSC und den NCTV zur Schnittstellenorganisation erklärt wurde, um die Zusammenarbeit zwischen den Sicherheitsbehörden und den Cybersicherheitsunternehmen zu verbessern. Damit kommt dem Interessenverband eine bemerkenswerte Funktion innerhalb des Landelijk Dekkend Stelsel und damit innerhalb der niederländischen Sicherheitsarchitektur zu.

Eine weitere gewichtige Interessenvertretung innerhalb der niederländischen IT-Sicherheit stellt die MKB-Nederland (midden- en kleinbedrijven¹⁰⁵) dar. Der Zusammenschluss der kleinen und mittleren Unternehmen ist ein unverhüllter Lobbyverband, der sich wiederum durch Lokalorganisationen strukturiert und sich für die Belange seiner Mitgliedsunternehmen einsetzt.

Ook in uw directe omgeving komt MKB-Nederland op voor uw ondernemersbelang. We hebben veel contact met gemeenten, provincies en andere belanghebbende partijen, bovendien helpen we uw lokale ondernemersvereniging met de lobby¹⁰⁶ (MKB-Nederland 2018).

Von der kommunalen Kleinvertretung, über die Provinzen bis zur Reichsebene besitzt MKB-Nederland skalierte Pendants oder kooperiert bei Bedarf mit weiteren Interessenverbänden, um die Ersuchen der Betriebe an den wirkungsvollsten Schnittstellen zu platzieren. Selbst in Brüssel betreibt der Lobbyverband ein Büro, das

¹⁰⁴ Deutsch: Die Interessenvereinigung für ein optimales Geschäftsklima von Cybersicherheitsunternehmen.

¹⁰⁵ Deutsch: mittlere und kleine Betriebe

¹⁰⁶ Deutsch: Auch in Ihrer unmittelbaren Umgebung setzt sich MKB-Nederland für Ihre Unternehmensinteressen ein. Wir haben viele Kontakte zu Kommunen, Provinzen und anderen interessierten Parteien. Obendrein helfen wir auch Ihrem lokalen Wirtschaftsverband bei der Lobbyarbeit.

die „belangen van het Nederlandse bedrijfsleven in de Europese Unie“¹⁰⁷ vertritt (MKB-Nederland 2018). Als oberstes Motiv der Einflussnahme auf die Tweede Kamer und die Ministerien, allen voran auf das Ministerie van Economische Zaken en Klimaat, ruft MKB-Nederland die ökonomisch-liberale Grundsatzforderung aus, das Wirtschaften zu erleichtern und Regeln auf ein notwendiges Maß zu beschränken (vgl. MKB-Nederland 2018). Mit Blick auf die Cybersicherheit ihrer Mitglieder hat die MKB eine spezifische Agenda, die in verschiedenen offenen Briefen und Kolumnen deutlich wird. Zuoberst appelliert MKB, ebenso wie die Regierung, an die Eigenverantwortung eines jeden Bürgers und Unternehmens für den individuellen Schutz, insistiert zugleich aber auf eine noch intensivere öffentlich-private Zusammenarbeit (vgl. MKB-Nederland 2019). Ferner fordert MKB größere staatliche Investitionen in die digitale Unternehmenssicherheit, um Schäden zu begrenzen und das Wirtschaften zu erleichtern; Regulationen thematisiert MKB im Zusammenhang mit Digitalisierung und IT-Sicherheit dagegen nicht. Stattdessen verlangt die Interessengruppe beispielsweise die Zentralisierung der Polizeikompetenzen in Cyberangelegenheiten, um die Reaktionsfähigkeit zu beschleunigen und den Informationsaustausch zu begünstigen (vgl. MKB-Nederland 2021).

Unter den zivilgesellschaftlichen Akteuren befinden sich neben solchen in staatlicher Hand oder mit nachweislicher Nähe zum Staat auch solche, die sich zur Aufgabe gemacht haben, die Interessen der Endanwender zu vertreten oder Kritik explizit an der Administration auszuüben. Eine der bedeutendsten Institutionen dieser Kategorie ist sicherlich Consumentenbond¹⁰⁸, mit über 430.000 Mitgliedern die größte Verbraucherschutzorganisation der Niederlande. Der Consumentenbond zeichnet sich dadurch aus, dass er sich unabhängig von Wirtschaft und Staat aufstellt, ergo aus keiner dieser Quellen Zuwendungen erhält. Diese Unabhängigkeit finanziert die Organisation größtenteils über Mitgliedsbeiträge und den Verkauf von Publikationen, teils durch die Lizenzierung von Produktzertifikaten für Unternehmen. Der Verband bedient eine breite Palette von Themen, die Verbrauchern Hilfe bieten können; Informationssicherheit stellt nur eines hiervon dar. Im Wesentlichen erfüllt der Consumentenbond in diesem Segment zwei Funktionen für die Verbraucher. Erstens veröffentlicht Consumentenbond regelmäßig aktuelle Anwenderhinweise, zum Beispiel zum Erstellen starker Passwörter,

¹⁰⁷ Deutsch: Interessen der niederländischen Unternehmensschaft in der Europäischen Union

¹⁰⁸ Deutsch: Verbraucherbund

zur Einrichtung eines VPN oder warnt etwa vor Betrug in Messengern. Der Consumentenbond sensibilisiert dann vor Gefahren und gibt präventive Hinweise dazu, wie die Anwender ihren digitalen Alltag schadenfrei bewältigen können. Zweitens geht der Verband aktiv gegen Missstände vor und vertritt die Interessen von Konsumenten gegenüber dem Gesetzgeber, vor Gericht oder auch gegenüber der Wirtschaft. Dazu geht der Consumentenbond entweder unmittelbare Verstöße an; etwa gegen Facebook, da das Unternehmen mutmaßlich gegen Datenschutzrecht verstoße und die Nutzer einen Anspruch auf Entschädigung hätten (vgl. Consumentenbond 2023a). Oder der Verband betreibt Aktivismus, um die Umstände zugunsten der Verbraucher zu verändern. Seit 2018 demonstriert der Consumentenbond beispielsweise gegen Google, weil das Unternehmen unrechtmäßig und ohne das Wissen der Nutzer Standortdaten erhebe sowie Entscheidungen und Handlungen von Anwendern aktiv beeinflusse. Um dies zu unterbinden, organisierte der Verband Demonstrationen, führte Petitionen durch und setzte sich für eine Verschärfung bestehender Datenschutzgesetze ein (vgl. Consumentenbond 2023b). Resultierend daraus ist der Consumentenbond, auch stellvertretend für weitere Verbraucherschutzorganisationen, ein marktwirtschaftliches wie politisches Korrektiv, das den Bedürfnissen der Kunden, Anwender wie Individuen ein Sprachrohr ist.

Organisierte Korrektive, also Anstalten, die sich zum Ziel gemacht haben, den Staat in Digitalangelegenheiten zu beraten und wo nötig zu kritisieren, sind in den Niederlanden darüber hinaus rar gesät. Zwar existieren regelmäßige Treffen oder Konferenzen wichtiger Hacker und IT-Experten, nennenswerte Vereine mit einer Satzung und einer gemeinsamen Stimme gibt es in dieser Form jedoch nur wenige. Zu einem Ableger der Quadrennial Dutch hacker convention kommen alle vier Jahre mehrere tausend niederländische Hacker und Interessierte zusammen, die mit jedem Mal unter neuem Namen stattfindet – zuletzt als *May Contain Hackers* oder *Hacking Anyway*. Das Event organisieren Freiwillige, ohne dass ein monetäres oder politisches Interesse besteht. Stattdessen zielte man bei der Erstaufgabe darauf ab, das Image der kriminellen Hoodyträger auszuräumen und sich europaweit unter White Hats zu vernetzen. Bemerkenswerterweise zählte der deutsche Chaos Computer Club zu den Initiatoren der Veranstaltung im Jahr 1989 (vgl. Wired 2001). Auf zum Beispiel [hackflag.org](https://www.hackflag.org) vernetzen sich Hacker und angehende Hacker online. Das Forum verbindet Hobbytechniker mit erfahrenen Hackern und ermöglicht einen unkomplizierten Wissensaustausch „voor

educatieve doeleinden“¹⁰⁹ (HackFlag 2022). Die Plattform hält sogar Tutorials und Hacking-Anleitungen per Video bereit, um Einsteigern grundlegende Mechaniken zu vermitteln. Aber auch bei HackFlag handelt es sich nicht um einen Verein oder eine Organisation, die planvoll oder zielgerichtet vorgeht, um sich gegebenenfalls zu institutionalisieren.

Die Presselandschaft zeigt sich divers und kann neben Technologiemaagazinen, wie ID.nl, NOS.nl, ictmagazine.nl oder computable.nl, mit Informationen für Verbraucher unterschiedlicher Kompetenzniveaus, auch netzpolitische Medien aufweisen. Dazu gehört zum Beispiel die niederländische Stiftung Bits of Freedom, die sich die Netzneutralität und Informationsfreiheit auf die Fahnen geschrieben hat. Wenngleich Bits of Freedom eine Stiftung ist, befasst sich die Organisation Mitteln klassischer Medien- und Kampagnenarbeit, um die niederländische Netzpolitik mitzugestalten. Dazu gehört nach eigener Aussage, für „meer bewustwording over deze ontwikkelingen“¹¹⁰ zu sorgen, indem sie „mensen, bedrijven en organisaties, wetenschappers, ambtenaren, politici en de media“¹¹¹ informieren (Bits of Freedom 2022). Bits of Freedom veröffentlicht regelmäßig Dossiers zu übergeordneten Themenbereichen, beispielsweise zu Biometrie und Gesichtserkennung, und untermauert die dort geäußerten Meinungen mit Untersuchungen (vgl. Hooyman 2019, 3). Darauf baut Bits of Freedom dann mit Forderungspapieren auf, sodass sie eine kritische, fundierte Gesamtbetrachtung in eine Debatte eingeben können und regulativ auf die Digitalpolitik wirken (vgl. Houwing 2020).

Nicht zu vergessen sind jene Organisationen, die allem voran Sensibilisierung und Aufklärung der Anwender betreiben, um für mehr digitale Sicherheit zu sorgen. Diese Institutionen möchten nicht auf entsprechende Regulationen oder Verbraucherschutzinitiativen warten, sondern versuchen, die Menschen dazu zu befähigen, Risiken richtig einschätzen oder sich aus Problemsituationen bestenfalls selbst befreien zu können. Das Network Mediawijsheid¹¹², das unter anderem von der ECP und der Europäischen Kommission getragen wird, betreibt die Webseite Mediawijsheid.nl sowie den Jugendableger HoeZomediawijs.nl. Dort finden

¹⁰⁹ Deutsch: für Bildungszwecke

¹¹⁰ Deutsch: mehr Bewusstsein für diese Entwicklungen

¹¹¹ Deutsch: Menschen, Unternehmen und Organisationen, Wissenschaftler, Beamte, Politiker und die Medien

¹¹² Deutsch: Netzwerk Medienkompetenz

Interessierte Informationen über starke Passwörter, Fake News oder auch smartes Spielzeug. Insbesondere HoeZomediawijs.nl stellt zahlreiche Videos und Anleitungen bereit, die für die Zielgruppe verständlich aufbereitet sind. Jedoch handelt es sich in beiden Fällen um Angebote, die Erwachsene wie Kinder aktiv aufsuchen müssen, um ihre Informationen oder Hilfestellungen zu erhalten. Kampagnen, Medienkooperationen oder Multiplikatorengewinnung stehen nicht im Fokus des Netzwerkes. Das Alleinstellungsmerkmal von Netwerk Mediawijsheid liegt im umfangreichen Angebot von Lehrmaterialien für die frühe Ausbildung einer wachsenden Medienkompetenz (vgl. Mediawijsheid.nl 2017). Die Organisation bietet einen Überblick über bestehende Lehrmittel, verlinkt auf weitere Initiativen und stellt Inhalte für jedes Schulniveau zur Verfügung. Exemplarisch für übrige Engagements im Bereich altersgerechter Digitalbildung zeigt sich seniorweb.nl. Das Onlineangebot SeniorWeb ist ein landesweiter Verein mit mehr als 150000 Mitgliedern, der vorwiegend älteren Menschen die Teilhabe an einer digitalen Gesellschaft ermöglichen möchte. Zu diesem Zweck bietet SeniorWeb Onlinekurse, Schulungen vor Ort über die gesamten Niederlande verteilt, aber auch Hilfeangebote per Telefon, per E-Mail oder sogar als direkte Unterstützung für zuhause an (vgl. SeniorWeb 2020). Darüber hinaus stellt das Portal zahlreiche Informationsartikel mit konkreten Anleitungen bereit, die von der Erstellung von Screenshots unter Windows bis hin zur Absicherung von Cloudsystemen reichen. Das Netwerk Democratie bemüht sich ebenso um digitale Partizipation und den souveränen Umgang mit Technologie, verfolgt aber einen anderen, mehr politisch motivierten Ansatz. Zu diesem Zweck veranstaltet das Netzwerk jährlich eine Masterclass Netpolitiek, die gemeinsam mit weiteren Organisationen stattfindet. Mit unter anderem Amnesty International, Bits of Freedom, Openstate foundation oder Internet Society NL informiert das Netwerk Democratie Entscheidungsträger und angehende Entscheider über aktuelle Herausforderungen und Trends des Digitalraums, damit diese Botschaften im Sinne des Netzwerks verinnerlichen, diese als Multiplikatoren in die Breite tragen und qualifizierte Beschlüsse fassen können (vgl. Netwerk Democratie 2019).

Abseits dieser Strukturen haben sich aus der niederländischen Wissenschaftsgemeinschaft relevante Institutionen auf dem Feld der Informationssicherheit ausgebildet. Die NWO, die Nederlandse Organisatie voor Wetenschappelijk Onderzoek¹¹³, dient dazu, wissenschaftliche Projekte und Vorhaben

¹¹³ Deutsch: Niederländische Organisation für wissenschaftliche Forschung

finanziell wie qualitativ zu unterstützen. Dabei ist die Organisation nicht an spezifische Themen oder Forschungsfelder gebunden, sondern lediglich ihren eigens formulierten Werten untergeordnet. Das Cyber Security-Programm der NWO ist etwa eine Konsequenz der National Cyber Security Strategy und subventioniert langfristig angelegte Forschungsprojekte, die der Cyber Security Agenda Rechnung tragen (vgl. NWO 2015). Darüber hinaus besteht seit 2013 ein nationales Cyber Security Cluster, das Security Delta (HSD). Dieses Cluster begründet sich in einer Initiative verschiedener Einrichtungen aus Politik und Wissenschaft, die zum Ziel haben, durch Förderung, Austausch und Synergien, Sicherheitsinnovationen zu befördern (vgl. Security Delta 2022). Das Hague Security Delta, seit 2019 Security Delta, erwirtschaftet keine Gewinne, untersteht keiner weiteren Einrichtung und vertritt keine singulären Interessen (vgl. Security Delta 2022). Im Security Delta sind Institutionen organisiert, die gemeinsam an „Cybersecurity & weerbaarheid, Data & AI/Intel en Slimme Veilige Samenlevingen“¹¹⁴ arbeiten (Security Delta 2022). Physisch kommen die Teilnehmenden zumeist in Den Haag zusammen – am HSD Campus. Hierbei handelt es sich um einen Ort für Tagungen, Forschung, Austausch und Kreativität, der als Treffpunkt für Unternehmen, Regierung und Wissenschaft dient. Der Campus liegt im sogenannten Central Innovation District. Dort befinden sich die regionalen Niederlassungen bedeutender Techkonzerne, Universitäten und Start-ups, um das Campusangebot niedrigschwellig und attraktiv zu zentralisieren (vgl. HSD Campus 2021). Unter anderem geht aus der HSD-Partnerschaft das Projekt Hack The Hague hervor, das von einem organisierenden Unternehmen, der Stadt Den Haag, dem NCSC sowie zwei Ministerien 2017 auf die Beine gestellt wurde. Ziel dieser jährlichen Aktion ist es, sogenannte ethische Hacker darum zu bitten, die digitale Infrastruktur der Stadt Den Haag anzugreifen, gefundene Einfallstore zu dokumentieren und auf diese Weise zur kollektiven Informationssicherheit beizutragen (vgl. Cybersprint 2022). Schon im Laufe des Events 2019 entdeckten 79 Experten 102 Sicherheitslücken, die in der Folge geschlossen werden konnten (vgl. Security Delta 2019). Doch Hack The Hague ist mehr als ein gewöhnlicher Hackathon. Die Organisatoren begleiten den Hack der Stadt medial: In sozialen Medien wie Twitter¹¹⁵ oder Facebook, in Blogs und Foren, in der Presse, im Fernsehen, in Podcasts und im Radio kommunizieren die Stadt und der

¹¹⁴ Deutsch: Cybersicherheit und -abwehrkraft, Data & KI/Intel und smarte, sichere Gesellschaften

¹¹⁵ Der Dienst wird in dieser Arbeit, trotz des neuen Namens X, weiter Twitter genannt, da die Namensänderung erst nach dem Ende des Untersuchungszeitraums eingeführt wurde.

Veranstalter über den organisierten Cyberangriff auf Den Haag (vgl. Cybersprint 2021). Das hat gleich mehrere Effekte für die Stadt und die Hacker: Die Aktion gewinnt die nötige Akzeptanz der Haager Bevölkerung, sodass in diesem Zuge gleich Befürchtungen abgebaut werden. Nebenbei machen die Organisatoren neugierig auf das Arbeitsfeld; sie werben in der Community, damit insbesondere fähige Hacker teilnehmen. Durch die Veröffentlichung der Ergebnisse spricht die Stadt den Teilnehmenden Anerkennung aus und generiert dadurch Interesse unter weiteren Hackern sowie gegebenenfalls den Antrieb, beim nächsten Umlauf selbst Sicherheitslücken entdecken zu wollen. Dafür erdachte man sich passende Auszeichnungen, zum Beispiel den „most sophisticated hack“ oder den „most surprising hack“, die die Gewinner öffentlich teilen können und die motivierend sowie wertschätzend formuliert sind (Security Delta 2019). Den Haag kreiert so aus einer über Jahrzehnte negativ konnotierten Fähigkeit, dem Hacken, ein mediales Ereignis, holt es in ein organisiertes Hellfeld und bereitet der Aktion eine Bühne.

Obwohl sich die Niederländer der zunehmenden Bedeutung digitaler Fähigkeiten bewusst zu sein scheinen und dies als Erfolgsfaktor für die Ökonomie des Landes identifiziert haben, schlägt sich das bisher nicht vollumfänglich in der schulischen und universitären Ausbildung nieder. An niederländischen Schulen erhalten nicht alle Schüler Informatikunterricht. Zwar ist das Fach recht verbreitet und wird teils bereits an Grundschulen gelehrt; es ist aber nicht verpflichtend in den entsprechenden Curricula festgeschrieben (vgl. European Education and Culture Executive Agency 2022, 10). Erst in höheren Sekundarstufen wird Informatik ein eigenes Pflichtfach (vgl. European Education and Culture Executive Agency 2022, 78). Damit ist die schulische Grundlagenausbildung in Informatik respektive auch in IT-Sicherheit in den Niederlanden ähnlich unpräzise ausgestaltet wie in Deutschland. In den Niederlanden ist man sich sogar gewahr, dass eine flächendeckende Versorgung mit Informatikunterricht zurzeit nicht möglich wäre, da Informatik bereits heute das Fach mit dem größten Lehrermangel ist – 2021 waren 24,3 % des Stellenbedarfs unbesetzt. Für 2026 geht das Ministerie van Onderwijs, Cultuur en Wetenschap¹¹⁶ sogar von knapp 50 % unbesetzten Stellen aus (vgl. Ministerie van Onderwijs, Cultuur en Wetenschap 2021, 90). Der Lehrkräftebedarf für Informatik hebt sich so stark von dem anderer Fächer ab, dass das Ministerium in seinem Untersuchungsbericht darauf verzichtet, die Daten zu Informatik

¹¹⁶ Deutsch: Ministerium für Bildung, Kultur und Wissenschaft

in ein visualisierendes Diagramm der Lehrkräftevakanz aufzunehmen, da diese derart exorbitant seien, dass die übrigen Werte nicht mehr zu entziffern wären (vgl. Ministerie van Onderwijs, Cultuur en Wetenschap 2021, 91). Dementsprechend ist es an den Schulen, Informatik in den Lehrplan aufzunehmen oder nicht. Das führt dazu, dass jenseits von Leuchtturmprojekten, wie etwa dem Emmauscollege in Rotterdam, an dem Gamedesign oder Robotik unterrichtet werden, keine ganzheitliche IT-Ausbildung vorgehalten wird. Trotz vergleichsweise vieler hochgebildeter Menschen ist der Beruf des Lehrers aber, insbesondere für Informatik, unattraktiv. Dabei waren zum Wintersemester 2021/2022 knapp 43860 der insgesamt etwa 1,3 Mio. Studierenden für Informatik eingeschrieben, 7330 davon waren internationale Studenten (vgl. Centraal Bureau voor de Statistiek (CBS) 2022). Dem eklatanten Lehrkräftemangel steht zudem gegenüber, dass 56,4 % der 25-34-jährigen in den Niederlanden einen Abschluss im tertiären Bildungssektor erreicht haben; in Deutschland sind es 37,3 % (vgl. OECD 2022, 46). Jedoch sind Einstiegsgehälter für Lehrkräfte bis 2022 vergleichsweise niedrig und teils unter dem Medianverdienst der Niederlande. Darüber hinaus werden Grundschullehrer entschieden weniger entlohnt als ihre Kollegen der weiterführenden Bildungseinrichtungen – in Summe macht das den Beruf des Lehrers für Informatikstudenten tendenziell unattraktiv (vgl. Ministerie van Onderwijs, Cultuur en Wetenschap 2022, 2). Das ist unter anderem deshalb bemerkenswert, weil Deutschland und die Niederlande mit je etwa 14.700 \$ nahezu identische Ausgaben für Bildungseinrichtungen pro Teilnehmer aufweisen und sich mit vergleichbaren Defiziten in der Digitalausbildung konfrontiert sehen (vgl. OECD 2022, 321).

Ähnlich wie in der schulischen Bildung ist das universitäre Angebot im Themenfeld der Cybersecurity uneinheitlich. Einige Universitäten und Hochschulen haben sich auf Informationssicherheit spezialisiert: An der Technischen Universität Eindhoven besteht ein Forschungscluster Sicherheit, das sich in der Lehre in Studiengängen wie *Computer Science and Engineering* oder *Information Security Technology* widerspiegelt. Seit 2019 unternimmt die Hochschule mit dem Eindhoven Artificial Intelligence Systems Institute (EAISI) außerdem den Versuch, den noch jungen Technologiebereich mit intensiver Grundlagenforschung aber auch durch die Entwicklung neuer Anwendungen anzutreiben (vgl. Eindhoven University of Technology 2020). Die TU Delft unterhält

eine Fakultät *Elektrotechniek, Wiskunde en Informatica*¹¹⁷, an der Bachelor- sowie Masterstudiengänge und weitere Spezialisierungsprogramme in Cybersecurity belegt werden können (vgl. Technische Universiteit Delft 2020). Verschiedene niederländische Hochschulen, darunter die Haagse Hogeschool mit einer Professur *Cyber Security in het mkb*¹¹⁸ und einer Professur *Cyber Security and Safety*, konzentrieren sich neben der Lehre vor allem auf die Forschung und das Schaffen neuen Wissens im Bereich der IT-Sicherheit (vgl. De Haagse Hogeschool 2022). Um der Wissenschaft eine Richtmarke vorzugeben und die wissenschaftlichen Bemühungen zu fokussieren, erstellt das NCSC mehrjährige Untersuchungsagenden. Diese Programme setzen Schwerpunkte, nach denen sich die wissenschaftlichen Institutionen ihre Forschungsbemühungen ausrichten können. Von 2019 bis 2022 gab das NCSC den Impuls, vor allem Krisenmanagement, Risikomanagement, strategische und soziale Aspekte von Cybersicherheit sowie Technologie und Cybersicherheit zu betrachten und legte so das Augenmerk darauf, den Faktor Mensch in Schadensketten näher zu untersuchen (vgl. Nationaal Cyber Security Centrum 2019, 3).

Neben alledem besteht in den Niederlanden schon seit den 80er-Jahren ein Kooperationsnetzwerk unterschiedlichster Bildungseinrichtungen, die Digitalinnovationen in Bildung und Forschung vorantreiben und für diese nutzbar gestalten wollen. SURF ist ein Zusammenschluss von Universitäten, Hochschulen, Forschungseinrichtungen und berufsbildenden Schulen des ganzen Landes mit dem Ziel, die Bildung mittels Informationstechnik zu optimieren (vgl. SURF 2021c). Für das Kabinett formulierte SURF 2021 einen Appell, der die Agenda des Netzwerkes zusammenfasst: SURF forderte den intensiven Gebrauch digitaler Lehrmittel, ausgiebige Investitionen in digitale Infrastruktur sowie den selbstverständlichen, sicheren Umgang mit Technologie, „om als Nederland de positie te behouden die het op dit moment heeft als innovatieve kenniseconomie en digitale mainport“¹¹⁹ (SURF 2021a). Man wolle bestehende Hürden ausräumen, indem Informationen mittels Digitaltechnik zugänglicher werden (vgl. SURF 2021a). Damit arbeitet SURF aus zwei Richtungen an einer sicheren und vor allem performanten Digitalisierung. Einmal fördert das Bildungsnetzwerk die selbstbestimmte Interaktion mit Technologie, also eine

¹¹⁷ Deutsch: Elektrotechnik, Mathematik und Informatik

¹¹⁸ Deutsch: Cybersicherheit in mittleren und kleinen Betrieben

¹¹⁹ Deutsch: damit die Niederlande ihre derzeitige Position als innovative Wissensökonomie und digitaler Mainport erhalten können.

ausgeprägte digitale Medienkompetenz, die breite Teilhabe und wiederum Fortschritt begünstigt. Auf der anderen Seite beabsichtigt SURF, die Forschung an digitalen Innovationen stets zu forcieren, damit die Niederlande eine führende internationale Rolle einnehmen können und einen zukünftigen Wettbewerbsvorteil innehaben. Dafür entwickeln die Netzwerkmitglieder gemeinsam Lehr- und Informationsmaterialien; SURF organisiert Webinare, Trainings und Netzwerktreffen, bietet für Bildungseinrichtungen hilfreiche IT-Dienstleistungen an und betreibt ein eigenes CERT, bei dem betroffene Einrichtungen im Notfall Hilfe finden können. Mehr noch stellt SURF selbst digitale Infrastruktur bereit, beispielsweise den Supercomputer Snellius, den Forschungsinstitutionen für ihre Zwecke verwenden können (vgl. SURF 2021b). Mit dem Netzwerk können die verbundenen Organisationen zusätzlich geschlossen gegenüber IT-Diensteanbietern auftreten, um ihre Kundenposition zu stärken. Genauso können sie ihre Interessen gegenüber Staat und Politik wirkungsvoller vertreten, sodass SURF unmittelbar über beispielsweise Fördermittel für Bildung und Forschung mitentscheidet (vgl. Rijksoverheid 2020b).

Dieses Kapitel hat gezeigt, dass rein zivilgesellschaftlich organisierte Akteure ohne staatlichen Gründungshintergrund oder direkte staatliche Beteiligung außerhalb lobbyistischer Verbände in den Niederlanden rar gesät sind. Dagegen existieren zahlreiche bedeutende Organisationen, die direkt aus öffentlich-privaten Partnerschaften stammen. Die gesellschaftlichen Institutionen sind auch deshalb nicht a priori staatskritisch aufgestellt, sondern vielmehr darauf bedacht, Einflüsse in Parlament oder Provinzregierung geltend zu machen. Regierungen und zivilgesellschaftliche Akteure stehen sich nur selten oppositionell gegenüber, sondern befinden sich in einer tendenziell koalierenden Architektur. Niederländische Äquivalente ethischer Hackerkollektive ähnlich dem deutschen Chaos Computer Club treten nicht in vergleichbarer Größe und Bedeutsamkeit auf. An ihrer Stelle findet man diverse Konferenzen, Meetups und Securitytalks bestehend aus Individuen und IT-Security-Unternehmen in allen erdenklichen Konstellationen. So existieren nur wenige organisierte Akteure, die sich für Security by Design, Update-Pflicht oder Anwenderschutz einsetzen und nicht zugleich wenigstens anteilig von der Rijksoverheid unterstützt werden. Selbst große Verbraucherschutzorganisationen sind in den Niederlanden zum Teil von Regierungsstellen getragen oder selbst Regierungsorgane, wie die Autoriteit Consument en Markt. Eine starke Position haben dagegen

Forschungsorganisationen wie NWO oder SURF. Während die NWO ihre Finanzierungen vor allem entlang der NCSA vergibt, arbeitet SURF unmittelbar daran, die Niederlande als Wissensökonomie zu erhalten und auszubauen. SURF möchte Bildung mittels und in Digitaltechnik verbessern und begreift IT-Kompetenz als Ressource. Das Security Cluster bildet mit dem HSD Campus in Den Haag auch physisch einen Forschungs- und Interessenverbund aus, in dem Institutionen zusammen an Sicherheit arbeiten – eine Art niederländisches Silicon Valley der IT-Sicherheit, in dem die Aggregation von Wissen, auch über Technologie, im Mittelpunkt steht.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bediener- fokus	Innen	Außen	Chance	Risiko
	X	X			X		X	X		X	

Dagegen zielen das Network Mediawijsheid, Bits of Freedom, der Consumentenbond oder auch Veilig Internetten insbesondere darauf ab, Menschen zu einem souveränen Umgang mit Digitaltechnik zu befähigen und ihnen Entscheidungsfreiheit auf Grundlage eines adäquaten Risikobewusstseins zu ermöglichen. Insgesamt stößt man bei der Untersuchung niederländischer Organisationen der Zivilgesellschaft zu einem überwiegenden Maß auf Einrichtungen, die in ihrer Agenda, ihren Veröffentlichungen und ihrem Handeln auf Chancen bauen und Risiken zumeist als überwindbare Hürden darstellen. Auch die starke Position niederländischer Forschungszusammenschlüsse spiegelt die progressive und chancenorientierte Attitüde niederländischer Verbände wider – bei gleichzeitig überwiegend subjektiver Sicherheitsnarrative. Wenngleich selbst große Institutionen wie Cyberveilig Nederland für ihre Arbeit beispielsweise auf das CSBN verweisen, wirken alle hier aufgeführten Interessenverbände, Organisationen und Lobbyvereine in ihrem Sinne respektive im Sinne ihrer Mitglieder auf die staatliche Digitalpolitik ein, bestimmen durch ihre Kommunikation das Bild von Informationssicherheit und Digitalisierung und sind in unterschiedlichem Maße bedeutsam für einen ausgewogenen Diskurs (vgl. MKB-Nederland 2019). Dabei verfallen sie nur in seltenen Fällen in Gefahrendiskurse oder stellen Angstmotive in den Vordergrund. Allerdings lässt sich gleichfalls festhalten, dass sich in den Niederlanden neben den starken Forschungsbündnissen vor allem einige wenige interessengeleitete Organisationen, wie ECP, hervortun. So begründen sich etliche unterschiedlich bedeutsame Initiativen aus der Platform voor de InformatieSamenleving, darunter Veilig Internetten oder Alert Online. Gleichzeitig ist ECP ein gewichtiges Sprachrohr zur Politik mit eigenen Positionspapieren und Zielvorstellungen. Nicht zuletzt dient ECP als

exemplarischer Vertreter für die augenfällig vielzähligen gesellschaftlichen Akteure, die aufgrund ministerieller Förderungen oder ihres staatlichen Gründungshintergrunds ihre äußerst enge Verwebung mit dem Staat nicht leugnen können – eine signifikante Charakteristik niederländischer Cybersicherheitsorganisationen.

2.6.3 Wet beveiliging netwerk- en informatiesystemen¹²⁰ (Wbni) & Computercriminaliteit III

2016 trat die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) ((EU) 2016/1148) in Kraft, die von den Mitgliedsstaaten in nationales Recht zu überführen war. Während einige Länder, darunter Deutschland, dies wesentlich über Änderungen bestehender Gesetze implementiert haben, haben die Niederlande juristische Pflöcke neu eingeschlagen und die NIS-Richtlinie zum Fundament ihrer Cybersecurity-Tätigkeiten gemacht. Das Wet beveiliging netwerk- en informatiesystemen gilt seit dem 09. November 2018 und überführt ausdrücklich europäisches in nationales Recht der Niederlande (vgl. Amtsblatt der Europäischen Union 2016). Die grundlegende Intention des Gesetzes ist die Sicherung der niederländischen Informationstechnik, wobei trotzdem auftretende Schäden durch Cyberangriffe möglichst gering zu halten sind (vgl. Nationaal Cyber Security Centrum 2018a). Das Wbni verpflichtet dafür Betreiber Kritischer Infrastrukturen und digitale Dienstleister, gewisse Sicherheitsvorkehrungen zu treffen und Vorfälle mit IT-Bezug an das Computer Security Incident Response Team (CSIRT) zu melden. Das CSIRT steht innerhalb des Gesetzestextes synonym für das NCSC, ist jedoch vergleichbar mit CERT-Bund eine Suborganisation innerhalb der Behörde, deren Fokus auf der akuten Krisenbewältigung liegt (vgl. Nationaal Cyber Security Centrum 2018a). Die Relevanz des NCSC äußert sich auch in seiner Netzwerkposition als zentrale Kontaktstelle für ausländische Sicherheitsbehörden und Vorfälle innerhalb der Niederlande mit potenziellen Auswirkungen auf EU-Mitgliedsstaaten (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 7). Das NCSC wurde so als Verbindungsstelle zu entsprechenden Stellen anderer Nationen, wie dem deutschen BSI oder dem französischen *autorité nationale en matière de sécurité et de défense des systèmes d'information*¹²¹ (ANSSI), positioniert.

¹²⁰ Deutsch: Gesetz über die Sicherheit von Netzwerk- und Informationssystemen

¹²¹ Deutsch: Nationale Behörde für die Sicherheit und Verteidigung von Informationssystemen

Zuvorderst regelt das Wbni die Kompetenzen des CSIRT beziehungsweise des NCSC sowie des Ministeriums und legt schließlich den Umgang der Institutionen mit den in der Vorfallbearbeitung angefallenen sensiblen Informationen fest. Eine Perspektive auf weitere Anspruchsberechtigte oder Bevölkerungsgruppen bleibt an dieser Stelle gänzlich aus. So beginnt der Gesetzestext mit den Pflichten des NCSC, die sich in drei Kernaufgaben gliedern: Erstens muss das CSIRT die definierten Gruppen, bestehend aus Unternehmen der Kritischen Infrastruktur, Regierungseinrichtungen, digitalen Diensteanbietern oder anderen für die öffentliche Ordnung relevante Institutionen, so unterstützen, dass diese ihre Dienstfähigkeiten aufrechterhalten oder notfalls wiederherstellen können. Ferner soll das NCSC diese Gruppe über Bedrohungen informieren und präventiv dazu beraten. Und schließlich wird dem NCSC auferlegt, Analysen und Untersuchungen durchzuführen – ausdrücklich ohne dabei gegen Personen zu ermitteln – damit sich Bedrohungen und Vorfälle künftig reduzieren (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 2).

Artikel 7 des Wet beveiliging netwerk- en informatiesystemen legt deshalb jene Kriterien fest, die einen angemessenen Sicherheitsstandard herstellen sollen. Dazu gehören die Sicherheit von Systemen und Anlagen, eine adäquate Vorfallbehandlung, die Gewährleistung von Betriebsabläufen, Überwachung, Kontrolle und Tests von Einrichtungen und Strukturen sowie die Beachtung internationaler Normen (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 4). Während das Gesetz diese fünf Parameter nicht weiter spezifiziert, werden Vorfälle einprägsam nach nur zwei Attributen bewertet. Ob ein Sachverhalt tatsächlich meldewürdig ist und damit Relevanz für Staat, Wirtschaft oder Gesellschaft aufweist, zeigt sich entweder, wenn ein vitale aanbieder¹²² feststellt, dass ein Störfall unmittelbar gravierende Konsequenzen für den Betrieb hat. Oder er registriert eine Kompromittierung seiner IT-Systeme, die potenziell Wirkungen auf die Integrität und Verfügbarkeit seiner Dienste haben könnte (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 4). Wird ein solcher Vorfall durch den Anbieter oder Hersteller festgestellt, ist dieser dazu verpflichtet, den Sachverhalt unverzüglich dem CSIRT zu melden. Das niederländische Informationssicherheitsgesetz schreibt präzise fest, welchen Nachrichteninhalt eine solche Meldung enthalten soll. Daraus folgt eine Bewertung der Schwere des Vorfalls

¹²² Deutsch: entspricht einem Betreiber Kritischer Infrastruktur, ist jedoch weiter gefasst als seine deutsche Entsprechung.

und eine Einordnung für die weitere Bearbeitung. So wird etwa vorgegeben, dass Art und Umfang eines Vorfalls zu beschreiben sind, dass das erste Auftreten des Ereignisses gemeldet wird und dass der Zeitpunkt geschätzt werden muss, zu dem die Störung voraussichtlich behoben sein wird (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 5). Darüber hinaus sieht Artikel 11 vor, dass mögliche Folgen innerhalb und außerhalb der Niederlande evaluiert werden und dass der meldende Betreiber die Aufsichtsbehörden über bereits getroffene oder eingeleitete Maßnahmen zur Fehlerbehebung informiert. Auf diese Weise erreichen das CSIRT respektive das NCSC und das Justizministerium standardisierte erste Lagebewertungen, auf welchen die weitere Bearbeitung aufbauen kann. Betreiber Kritischer Infrastrukturen und digitaler Dienstleistungen, wie Telekommunikationsunternehmen, sind zusätzlich verpflichtet, die Anzahl betroffener Nutzerinnen und Nutzer anzugeben und das geografische Gebiet einzugrenzen, in dem der Vorfall auftritt (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 5).

Während das deutsche Informationssicherheitsgesetz den Schutz personenbezogener Daten als hohes Gut versteht und der genauen Definition behördlicher Sicherungspflichten viel Raum zugesteht, formuliert das Wbni Schutzmechanismen allem voran für unternehmensbezogene Informationen (vgl. Bundesgesetzblatt 2009, 2823):

Ter uitvoering van de in artikel 3 genoemde taken verstrekt Onze Minister geen vertrouwelijke gegevens met betrekking tot een aanbieder als:

- a. de geheimhouding van die gegevens onvoldoende is gewaarborgd, of
- b. onvoldoende is gewaarborgd dat zij uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt¹²³ (Staatsblad van het Koninkrijk der Nederlanden 2018b, 7).

Nur falls die Anbieterdaten unerlässlich zur Auflösung oder Prävention eines Störfalls sind, kann der Justizminister den Schutz der Informationen aufheben und diese an CSIRT, weitere IT-Notfalleinheiten sowie Auskunfts- und Sicherheitsdienste weiterleiten. Nur in besonders schwerwiegenden Fällen ist der Justizminister befugt, Daten an zusätzliche Institutionen und sogar an die Öffentlichkeit weiterzugeben (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018b, 7). Artikel 23 Wbni weist

¹²³ Deutsch: Zur Ausführung der in Artikel 3 genannten Obliegenheiten stellt unser Minister keine vertraulichen Daten mit Bezug zu einem Anbieter aus, wenn: a. die Geheimhaltung dieser Daten nur mangelhaft gewährleistet werden kann, oder b. unzureichend sichergestellt ist, dass diese ausschließlich zu jenem Nutzen verwendet werden, für den Sie ausgestellt wurden.

an, dass das CSIRT dann eine Ausnahme von diesem Datenschutz machen kann, wenn nach Beratschlagung mit dem Anbieter der Dienstleistung oder Hardware das Gemeinwesen über den Vorfall informiert sein muss, um „een incident te voorkomen of een lopend incident te beheersen“¹²⁴ (Staatsblad van het Koninkrijk der Nederlanden 2018b, 9). Das Wbni steckt damit die Kompetenzen des NCSC ab und ordnet der Behörde zwar eine zentrale, aber eine zugleich limitierte Aufgabe zu, die vor allem den Schutz von Staat und Kritischer Infrastruktur umfasst. Die Prävention von Kriminalität, die Sensibilisierung der Anwender oder auch die Verfolgung von Tätergruppen obliegen dagegen weiteren Einrichtungen wie den Polizeien und sind in einem weiteren essenziellen Gesetz für die niederländische Cybersicherheit geregelt, Computercriminaliteit III.

Dieses Gesetz sorgte im Gegensatz zum Wbni 2018 und 2019 für Aufsehen, weil es die Kompetenzen der Polizeien und Staatsanwaltschaften zur Verfolgung von Straftaten im Cyberraum erheblich ausweitete. Im Kern umfasst das Gesetz Änderungen im Wetboek van Strafrecht¹²⁵ sowie im Wetboek van Strafvordering¹²⁶ und hält drei bemerkenswerte Befugniserweiterungen für Ermittler bereit: So können die Ermittlungsbehörden seit dem 01. März 2019 im Falle schwerer Straftaten oder im Verdacht auf diese Straftaten in Geräte eindringen und dort Daten nach Belieben untersuchen. Zudem können sie gefundene Daten unzugänglich machen, Kommunikation abhören oder auch Informationen kopieren, um Ermittlungen voranzutreiben. Schließlich gestattet das Gesetz, nun auch unter anderem Datendiebstahl als Straftat zu verfolgen – das schließt ausdrücklich den Besitz gestohlener Informationen ein, ohne den Diebstahl selbst nachweisen zu müssen (vgl. Rijksoverheid 2019). Als wesentliche Voraussetzung nennt Computercriminaliteit III das Vorhandensein eines Straftatverdachts nach Artikel 67, Absatz 1 des Wetboek van Strafvordering. Dazu gehören jegliche Straftaten, die mit einer Haftstrafe von mindestens vier Jahren zu ahnden sind, aber beispielsweise auch Vergehen wie Aufruf zu Gewalt, Diebstahl, Veruntreuung, illegaler Handel mit Pornografie oder Verrat von Verschlusssachen (vgl. Overheid 2021).

Die Ermittler erhalten das Recht, direkt an Telekommunikationsdienstbetreiber heranzutreten und sie zu verpflichten, „bepaalde gegevens die worden opgeslagen of

¹²⁴ Deutsch: einem Vorfall vorzubeugen oder um einen laufenden Vorfall zu beherrschen

¹²⁵ Deutsch: Strafgesetzbuch

¹²⁶ Deutsch: Strafprozessordnung

doorgegeven, ontoegankelijk te maken“¹²⁷ (Staatsblad van het Koninkrijk der Nederlanden 2018a, 4). Diese Ausübung staatlicher Gewalt ist aber nicht nur bei einem Nachweis eines Deliktes gestattet, sondern nach Artikel 125p und 126nba des Wet Computercriminaliteit auch schon bei „verdenking van een misdrijf“¹²⁸ möglich, oder wenn die angelastete Tat mit weiteren Straftaten des Verdächtigen zusammenhängen könnte (Staatsblad van het Koninkrijk der Nederlanden 2018a, 5). Das Gesetz legt hier großes Augenmerk auf die Dokumentation dieser Ermittlungsmethoden. So sollen Zeitpunkt, Hilfsmittel zur technischen Ermittlung, erhobene Daten oder die umgesetzten Maßnahmen schriftlich vermerkt werden und bedürfen einer Anordnung der Staatsanwaltschaft (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018a, 5). Dennoch kann das nicht darüber hinwegtäuschen, dass nicht näher geregelt ist, wann der Schutz individueller, sensibler Informationen höher einzuschätzen ist als der zu erwartende Ermittlungserfolg durch das Beschneiden persönlicher Freiheiten. Diese Entscheidung, ob und mit welchen Instrumenten in ein Computersystem eingedrungen wird, liegt bei den niederländischen Strafverfolgern und stellt insofern einen potenziell erheblichen Eingriff in die bürgerlichen Grundrechte dar.

Ferner räumt das Computercriminaliteit III der Justiz ein, darüber zu verfügen, dass Sicherheitslücken in Soft- oder Hardware, die noch nicht öffentlich bekannt sind, unter Verschluss gehalten werden, um sie als Ermittlungswerkzeug einsetzen zu können, beispielsweise um Verdächtige technisch zu observieren (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018a, 10). Der officier van justitie¹²⁹ kann so zwar einen Ermittlungsvorteil aufseiten der Polizeien erzielen, nimmt aber die Cybersicherheit aller User dieses Produkts durch das Offenhalten der entsprechenden Schwachstelle in Kauf. Zusätzlich hebt dieser Mechanismus den international anerkannten Coordinated Vulnerability Disclosure-Prozess der IT-Vorfallbearbeitung aus, indem Informationen nicht mehr verantwortungsvoll zwischen dem Betreiber des IT-Dienstes und etwa dem NCSC geteilt und schließlich publiziert werden, um die Sicherheitslücke bestmöglich auszuräumen. Das öffentlich-rechtliche Nachrichtenportal NOS.nl fasst das Ausmaß der kontroversen Gesetzesänderung zusammen: „De politie mag straks zowel bekende als onbekende lekken gebruiken om digitaal in te breken op iemands computer. Het gaat

¹²⁷ Deutsch: bestimmte Daten, die gespeichert oder übermittelt werden, unzugänglich machen

¹²⁸ Deutsch: Verdacht auf ein Verbrechen

¹²⁹ Deutsch: Staatsanwalt

daarbij niet alleen om pc's of laptops, maar ook om smartphones of servers“¹³⁰ (NOS 2018b). Auch wenn das Gesetz, schon seinem Namen nach, Kriminalität mit und durch Computer unterbinden soll, betreffen die Hackbefugnisse ebenso Smartphones, Server, Autos, Medizintechnik oder das Internet of Things. Insofern lässt sich die Gesetzesnovelle Computercriminaliteit III von 2018 durchaus als eklatante Stärkung polizeilicher Ermittlungsbefugnisse und somit auch als Expansion des staatlichen Mandats bezeichnen. Dazu entstand eine intensive politische Debatte. So hatten Mitglieder der D66-Fraktion zahlreiche Fragen an das Parlament gestellt und im Mai 2018 eine Antwort der Eerste Kamer¹³¹ erhalten. Darin beschreibt die Kammer, dass der Einsatz von Hackbefugnissen nicht nur, wie im Gesetz beschrieben, durch einen rechter-commissaris¹³², sondern immer auch durch die sogenannte Centrale Toetsingscommissie¹³³ geprüft wird (vgl. Officielebekendmakingen 2018). Mit dieser zusätzlichen Hürde versuchten die Vertreter der Eerste Kamer, die Kritiker der Opposition davon zu überzeugen, dass sich die teils erheblichen Beschneidungen des Datenschutzes stets einer Prüfung der Verhältnismäßigkeit unterziehen, weil diese Maßnahmen mehrfach geprüft werden. Jedoch sind diese Prüfinstanzen, bis auf die Untersuchungsrichter, stets Teil der Staatsanwaltschaft, die wiederum teil des Justizministeriums ist, und damit nicht unabhängig. Vor allem aber sieht der Gesetzestext selbst keine Prüfungskommission vor:

Het bevel [...] kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. De machtiging vermeldt de onderdelen van het bevel en de periode waarvoor de machtiging van kracht is¹³⁴ (Staatsblad van het Koninkrijk der Nederlanden 2018a, 5).

Das bedeutet, dass Computercriminaliteit III die neuen Befugnisse der Polizei zwar mit richterlicher Kontrolle und präziser Dokumentationspflicht verkettet, gleichzeitig aber diesem Grundrechtseinschnitt nur wenige juristische Hürden entgegenstellt. Allerdings ist der Versuch von D66 letztlich gescheitert, Computercriminaliteit III im

¹³⁰ Deutsch: Die Polizei wird bald sowohl bekannte als auch unbekannte Lecks nutzen, um digital in den Computer einer Person einzubrechen. Dabei geht es nicht nur um PCs oder Laptops, sondern auch um Smartphones oder Server.

¹³¹ Deutsch: Erste Kammer (Das niederländische Oberhaus, das sich aus gewählten Vertretern der Provinzen zusammensetzt)

¹³² Deutsch: Untersuchungsrichter

¹³³ Deutsch: zentraler Überprüfungsausschuss

¹³⁴ Deutsch: Die Anordnung kann nur nach schriftlicher Genehmigung des Untersuchungsrichters auf Antrag des Staatsanwalts erlassen werden. In der Vollmacht sind die Auftragsbestandteile und der Geltungszeitraum der Vollmacht aufzuführen.

Gesetzgebungsverfahren in ihrem Sinne zu formen. Ebenso erfolglos war der Anlauf von GroenLinks, eine unabhängige Prüfkommision einzurichten (vgl. Eerste Kamer der Staten-Generaal 2018). Insofern ist die Prüfung durch die Toetsingscommissie kein Bestandteil des Gesetzes und somit keinesfalls obligatorisch, sondern vielmehr eine interne Vorgabe der Staatsanwaltschaft – gewissermaßen ein Compliance-Gremium zwischen dem beantragenden Staatsanwalt und dem prüfenden Richter.

Während Computercriminaliteit III die Ermittlungsarbeit berührt, verleiht das Wbni dem CSIRT weitreichende Aufgaben für die Sicherung Kritischer Infrastruktur und eine besonders hervorgehobene Rolle im Institutionengefüge. Gerade deshalb sticht ins Auge, dass das NCSC oder der NCTV im gesamten Wbni nicht namentlich vorkommen. Dass das CSIRT mit dem NCSC gleichzusetzen respektive ein Teil des NCSC ist, findet im Gesetzestext somit keinerlei Erwähnung. Damit ist dies zwar eine faktische, aber keine nominelle Bemächtigung des NCSC. Das hat vor allem zwei Konsequenzen: Es stellt heraus, dass die Niederlande über ein Computer Security Incident Response Team verfügen und suggeriert so, dass man schnell und professionell auf Vorfälle reagieren kann. Zusätzlich sieht das Wbni vor, dass im CSIRT, also im NCSC, Incident-Meldungen europäischer Partner einlaufen und koordiniert werden. Das bedeutet auch, dass, wenn erforderlich, das CSIRT Informationen und Aufgaben an weitere Behörden, öffentliche Stellen oder Unternehmen in den Niederlanden weitergeben muss. Eine augenscheinliche Differenzierung zwischen NCSC und CSIRT führt gegebenenfalls zu einer besseren Akzeptanz von Weisungen oder Forderungen insbesondere unter gleichrangigen Behörden. Bei der Untersuchung des Wet beveiliging netwerk- en informatiesystemen fällt darüber hinaus auf, dass das Wbni ohne nennenswerte Debatte verabschiedet wurde und auf keinen öffentlichen Widerstand gestoßen ist. Das mag daran liegen, dass in erster Linie Großunternehmen und die Regierung in die Pflicht genommen wurden sowie daran, dass das Gesetz zunächst keine Verpflichtungen für Anwender einschließt. Das Gesetz enthält im Wesentlichen Botschaften, die der niederländischen Bevölkerung zumutbar sind beziehungsweise sie nur mittelbar tangieren. Noch dazu ist das Wbni thematisch nicht sonderlich attraktiv für eine breite Öffentlichkeit, da es sich überwiegend um eine Implementierung europäischen Rechts in niederländisches Gesetz handelt.

Erwähnenswert ist aber allemal, dass NCSC und NCTV selbst das Gesetz aufgreifen und es als ihre juristische Arbeitsgrundlage benennen (vgl. Nationaal Cyber Security

Centrum 2022b). Erstens setzt die Regierung damit das Signal, dass das Wbni die Sicherheit des Landes anhebt, ohne dabei Freiheiten der Bevölkerung einzuschränken. Zweitens betont der Gesetzgeber mit dem Wbni, dass vordringlich Unternehmen Kritischer Infrastruktur unter besonderem Schutz stehen, sie aber damit auch Verpflichtungen unterliegen und kontrolliert werden. Zu guter Letzt, und das ist auch die Tatsache, die von NCSC und NCTV hervorgehoben wird, konstituiert das Wbni das NCSC als die nationale Stelle für Cybersicherheit, in der alles zusammenläuft. Das NCSC selbst entwirft daraus sogar eine rhetorische Logik, indem es die Relevanz des Gesetzes unterstreicht: „De Wbni is erop gericht de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen“¹³⁵ (Nationaal Cyber Security Centrum 2022b). Denn wenn das Wbni, die Gesetzesgrundlage des NCSC, tatsächlich die gesamte Gesellschaft schützt, förderlich für die Sicherheit ist und verhindert, dass IT-Vorfälle größeren Schaden anrichten, dann muss auch das NCSC von eminenter Bedeutung für die Niederlande sein, so die Schlussfolgerung der Behörde selbst.

Das Gesetz Computercriminaliteit III wurde nicht derart lautlos verabschiedet. Es sorgte für Aufsehen und wurde unter anderem als „Hackwet“¹³⁶ bezeichnet, weil es streitbare Punkte beinhaltet und deutlich größere Bevölkerungsgruppen potenziell direkt berühren kann (rtlNieuws 2016). Insbesondere die neue Befugnis der Polizei, in Systeme einzubrechen, trat eine Kontroverse los. So hatte die Regierung mit Computercriminaliteit III neben der politischen auch eine mediale Herausforderung zu bewältigen, die multifaktorielle Schwierigkeiten bereithielt. Denn das Gesetz betrifft im Grundsatz jede Person, die in den Niederlanden lebt. Die riesige Betroffenheit ist verknüpft mit einem potenziellen tiefen Eingriff in die individuelle Privatheit. Diese Möglichkeit zur Störung der bürgerlichen Intimität verleiht dem Gesetz eine zutiefst moralische Komponente und setzt deshalb großes Vertrauen in den Staat und seine Kontrollgremien voraus. Dementsprechend befeuerten die Gegner des Gesetzes die Debatte mit Fragen: „Kunnen we er zomaar vanuit gaan dat de politie zijn krachten niet misbruikt“¹³⁷ (rtlNieuws 2016)? Das Advocatenblad fragte, wie man hackende Polizisten kontrollieren könne (vgl. Advocatenblad.nl 2017). Die Boulevard-Zeitung AD ging

¹³⁵ Deutsch: Das Wbni ist darauf aus, die digitale Widerstandsfähigkeit der Niederlande zu erhöhen, die Folgen von Cybervorfällen zu begrenzen und so gesellschaftlichen Unruhen zuvorzukommen.

¹³⁶ Deutsch: Hackergesetz

¹³⁷ Deutsch: Können wir einfach davon ausgehen, dass die Polizei ihre Macht nicht missbraucht?

noch weiter und fragte unter Bezug auf die Polizei: „Moeten we onze smartphonecamera afplakken tegen hackers“¹³⁸ (AD.nl 2017)? Bits of Freedom schloss sich dieser Rhetorik an, stellte allerdings keine Frage, sondern baute die Kampagne „Stop het hackvoorstel“¹³⁹ gegen das Gesetz auf: „De politie wil kunnen inbreken op elke computer en telefoon in Nederland en laat daarmee onze achterdeuren wagenwijd openstaan voor criminelen“¹⁴⁰ (Bits of Freedom 2016). Zwar spitzen die Verantwortlichen dieser Kommunikation den Sachverhalt zu, jedoch konzentrieren sie den Diskurs auf das zentrale Dilemma. Denn während die Polizei für dieses Gesetz argumentiert, weil es erst ermögliche, kriminelle Strukturen im Internet zu bekämpfen, sieht die Gegenseite die persönliche Freiheit eines jeden Niederländers gefährdet. Bart Jacobs, Professor für Digital Security an der Radboud Universiteit Nijmegen, verdichtet die Gegenposition in einem Fernsehinterview darauf, „dat de politie belang krijgt in de aanwezigheid van fouten in software en eigenlijk de politie is da om ons de beschermen en niet de zwakheden uit te buiten die we hebben“¹⁴¹ (NOS 2018b). Auch deshalb erschien im Herbst 2022 eine vom Ministerium beauftragte, umfangreiche Evaluation des Gesetzes in der polizeilichen Praxis mit zahlreichen Problemstellen und Verbesserungsvorschlägen. In der Debatte rund um das Gesetz trafen also gegenüberstehende Narrative aufeinander, deren Kernargumente zudem unbestreitbar korrekt sind und sich dennoch gegenseitig ausschließen.

Letztlich traten beide Gesetze in Kraft und tragen seitdem mehrere Botschaften mit sich:

1. *Dem CSIRT beziehungsweise dem NCSC kommt eine Schlüsselposition der Cybersicherheit in den Niederlanden zu.*

Indem durch das Wbni Meldungen über Cybersicherheitsvorfälle an das NCSC übermittelt werden müssen, das wiederum die Koordination auf nationaler Ebene und mit internationalen Partnern übernimmt, legitimiert das Gesetz das NCSC schlussendlich als die Cybersicherheitsbehörde für Zwischenfälle landesweiter Signifikanz.

¹³⁸ Deutsch: Müssen wir nun unsere Smartphone-Kameras gegen Hacker abkleben?

¹³⁹ Deutsch: Stoppt den Hack-Vorschlag

¹⁴⁰ Deutsch: Die Polizei möchte in jeden Computer und jedes Telefon in den Niederlanden einbrechen können und lässt somit unsere Hintertüren für Kriminelle offenstehen.

¹⁴¹ Deutsch: dass die Polizei ein Interesse am Vorhandensein von Fehlern in der Software hat und dass die Polizei eigentlich da ist, um uns zu schützen und nicht, um die Schwächen auszunutzen, die wir haben.

2. Die Niederlande haben, in dieser Form in westlichen Demokratien seltene, Instrumente zur Bekämpfung von Cyberangriffen und zur Rückverfolgung von Tätern.

In Deutschland kann mit § 100a StPO zwar auch die Telekommunikation von Verdächtigen überwacht, Daten abgefangen und Personen digital beschattet werden, allerdings geht die niederländische Gesetzgebung weiter: Die Niederlande können nicht nur Informationen abpassen, sondern sie können Daten unzugänglich machen und Sperrungen sowie Take Downs anordnen (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018a, 1). Dass dieses Werkzeug funktioniert, betonen die Ermittlungsbehörden gerne öffentlich. In einem Schreiben des Justizministers an das Parlament bestätigt dieser gar, dass „de bevoegdheid ook in internationaal onderzoek ingezet“¹⁴² wird (Officielebekendmakingen 2021).

3. Die Analyse von personenbezogenen Daten durch die Polizeien ist eine Notwendigkeit, die ausschließlich digitale Sicherheit Unbeteiligter gewährleisten soll.

Hier umspannt das Gesetz ein Beruhigungsnarrativ, dessen unilaterale Betrachtung, ohne eventuelle Nachteile offensiv zu diskutieren und gegebenenfalls zu entkräften, insbesondere relativiert, dass in den Niederlanden schon wenige Indizien genügen, um eine Telekommunikationsüberwachung anzuweisen. Dazu gehören eine Beschreibung der organisierten, kriminellen Vereinigung und „indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon ten aanzien van wie uit feiten en omstandigheden een redelijk vermoeden voortvloeit“¹⁴³ (Staatsblad van het Koninkrijk der Nederlanden 2018a, 7). Dass also nur wenige Anhaltspunkte und nicht bestimmbare Merkmale genügen, aus denen ein Verdacht entworfen werden kann, wird von zahlreichen Paragrafen und Gesetzesverweisen eingerahmt, die suggerieren, dass dieses Ermittlungswerkzeug nur bedacht einsetzbar und damit für das Gros der Bevölkerung unverfänglich sei. Dabei zeigt schon das Vorwort der rechtlichen Bestimmung die Diskussion rund um Computercriminaliteit III auf:

Alzo Wij in overweging genomen hebben, dat het wenselijk is om geautomatiseerde werken op afstand heimelijk binnen te kunnen dringen met het oog op de opsporing van ernstige misdrijven, gegevens op doeltreffende wijze ontoegankelijk te kunnen doen maken ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten [...]; Zo is het, dat Wij, de Afdeling

¹⁴² Deutsch: die Befugnis auch in internationalen Untersuchungen eingesetzt

¹⁴³ Deutsch: sofern bekannt, der Name oder eine sonst möglichst genaue Angabe der Person, bei der aufgrund von Tatsachen und Umständen ein begründeter Verdacht besteht

advisering van Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan¹⁴⁴ (Staatsblad van het Koninkrijk der Nederlanden 2018a, 1).

Die Präambel zählt gekonnt die Vorteile des Gesetzes auf und erwähnt, dass diese mit weiteren Kriterien abgewogen wurden – jene werden aber nicht benannt oder gar gegenübergestellt. Das Parlament diffundiert hier stattdessen die Verantwortung für den Beschluss, indem es darauf hinweist, lediglich der Empfehlung des Raad van State gefolgt zu sein.

4. Digitale Straftaten sind ebenso als schwere Verbrechen zu verstehen; darunter beispielsweise Datenhehlerei.

Hierin liegt der entscheidende Unterschied zu Gesetzen anderer europäischer Länder wie Deutschland: Mit Computercriminaliteit III können seit März 2019 zahlreiche digitale Straftaten, etwa Datenhehlerei, Sammlung von Daten aus kriminellen Aktivitäten oder die virtuelle Belästigung von Minderjährigen als eigene Kategorie strafbarer Handlungen benannt und kriminalisiert werden, ohne sie lediglich als Pendants physischer respektive konventioneller Straftaten zu begreifen (vgl. Staatsblad van het Koninkrijk der Nederlanden 2018a, 2f). Dadurch dass diese Akte als digitale Delikte in einem dedizierten Gesetz markiert sind, stehen sie zwar nicht mehr unter Strafe als in manch anderen Ländern, aber sie erhalten eine gewichtige Qualität, sodass diese Form der Kriminalität adäquate Wahrnehmung erfahren kann. Zugleich gibt es kaum Anhaltspunkte dafür, dass die Gesetze aus einem Angstdiskurs erwachsen sind. Der Wunsch, vor allem von staatlicher Seite, die Sicherheitsmaßnahmen zu erhöhen und zunehmende Kontrolle über individuelle Nutzer zu erlangen, ist zwar polarisierend, aber nachvollziehbar. Das Hauptaugenmerk des Wbni liegt auf der Sicherung staatlicher und Kritischer Infrastruktur; angesichts der täglichen Cyberangriffe auf europäische Staaten ein einleuchtender Schritt, der auf objektiven Tatsachen ruht. Computercriminaliteit III stärkt ebenfalls die Sicherheitsbehörden und bezieht seine Legitimierung aus der seit Jahren zunehmenden Bedrohung. Dennoch könnte diesem Gesetz nachgesagt werden, dass es auf Grundlage objektiv bestehender Sicherheitsdefizite ein Kontrollmittel etabliert, das sich vornehmlich gegen Menschen in den Niederlanden richtet, obwohl

¹⁴⁴ Deutsch: Da wir berücksichtigt haben, dass es wünschenswert ist, aus der Ferne heimlich in automatisierte Prozesse einzudringen, um schwere Straftaten aufzudecken, Daten wirksam unzugänglich machen zu können, um eine Straftat zu beenden oder um neuen Straftaten zuvorzukommen [...]; daher haben wir nach Anhörung der Beratungsabteilung des Raad van State und in Absprache mit den Staten-Generaal folgendes gebilligt und verstanden.

Cyberkriminalität vorrangig nachweislich aus Drittstaaten heraus begangen wird. Diese Debatte wurde wie oben beschrieben emotionalisiert und auf der Basis subjektiver Ansichten geführt. Die Staatsanwaltschaft selbst vermischte Tatsachen, sodass der Eindruck entstand, die Überwachung niederländischer Computer schütze die niederländische IT-Infrastruktur nachhaltig:

Nederland staat in de top 10 van landen ter wereld met de meeste cyberaanvallen. De uitstekende infrastructuur van snel, goedkoop en stabiel internet in Nederland trekt wereldwijd cybercriminelen aan, die de servers in ons land gebruiken voor hun illegale praktijken¹⁴⁵ (Openbaar Ministerie 2016).

Mit dergleichen Argumentationssträngen entsteht der Eindruck, dass ein maßgeblicher Sicherheitsgewinn möglich wäre, wenn Ermittler in Computer aller Art eindringen dürften – ein Zusammenhang, den vorliegende Erkenntnisse nicht stützen. Es offenbart sich dennoch, dass die Regierung mit Wbni und Computercriminaliteit III der immer deutlicheren Gefährdungslage Rechnung zu tragen versucht. Zugleich werden solche Risiken, die direkt an die rechtlichen Bestimmungen geknüpft sind, wie die Einschränkung individueller Persönlichkeitsrechte, von staatlicher Seite nur selten erwähnt oder im Diskurs relativiert, indem der scheinende Sicherheitsgewinn hervorgehoben wird. Die Legitimierung der Gesetze gründet insbesondere auf der Größe der Bedrohungen, auf die sie reagieren, sowie in ihrer Abwendung. Chancen für unter anderem die Ökonomie oder die Zivilgesellschaft werden weder im Gesetzestext noch in der umgebenden Debatte merklich aufgegriffen. Stattdessen entfaltet sich eine Kulisse, in der Bürgerrechtler gegen Computercriminaliteit III vorzugehen versuchen, während die Polizeien nun die aus dem Gesetz resultierenden Erfolge gegen die organisierte Kriminalität im Internet unterstreichen; und so Risiken unterschiedlicher Prävention adressieren.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	X	X			X	X		X			X

Auch die Niederlande streben mit ihren IT-Sicherheitsgesetzen nach dem Erhalt eines bestehenden oder vergangenen, vermeintlich sicheren, Zustandes. Das zeigt sich unter anderem darin, dass weder ein Zielzustand ausgemalt noch Maßnahmen eingeleitet

¹⁴⁵ Deutsch: Die Niederlande gehören zu den zehn Ländern weltweit mit den meisten Cyberangriffen. Die hervorragende Infrastruktur aus schnellem, günstigem und stabilem Internet in den Niederlanden lockt Cyberkriminelle aus aller Welt an, die die Server in unserem Land für ihre illegalen Aktivitäten nutzen.

werden, die einen wesentlichen Fortgang der Gesellschaft herstellen sollen. Stattdessen erhalten NCSC und Polizei erweiterte Befugnisse, um Sicherheit herbeizuführen und eine Raison im Digitalraum zu bewirken. Innerhalb dieser Bemühung, ein sicherheitspolitisches pre-digitales Zeitalter zurückzugewinnen, verschieben die Niederländer allerdings die juristischen Grenzen weiter als manch andere. So kann die ausführliche Telekommunikationsüberwachung von Individuen aufgrund einzelner Verdachtsmomente ebenso Schablone für weitere Demokratien sein wie die ausdrückliche Benennung illegaler, digitaler Handlungen als ebensolche. Die Niederlande drehen die Schraube staatlicher Bemächtigung zur Absicherung der eigenen Bevölkerung weiter und haben mit Computercriminaliteit III ein Gesetz verabschiedet, das nicht nur symbolische Wirkkraft hat, sondern reale Folgen für die Menschen in den Niederlanden nach sich ziehen und als repressives Hilfsmittel missbraucht werden könnte. So lassen die Niederländer ein Stück jener Liberalität hinter sich, die ihnen in der Vergangenheit als anhaftendes Handlungsmotiv nachgesagt wurde. Damit sind sie insofern auch, innerhalb des per se reaktionären Sicherheitsumfeldes, ein progressiver Akteur auf dem Feld der Cybersicherheit, der sowohl mit typischen vergangenen Beweggründen bricht als auch die bislang im Parlamentarismus noch unausgetretenen Pfade der Bevölkerungsüberwachung beschreitet. Erneut richten sich die hier beschriebenen Lenkungsinstrumente auf technische beziehungsweise legislative Maßnahmen, die jedoch den Anwender als Sicherheitsleck oder -gewinn weitestgehend außer Acht lassen. Bildungsoffensiven oder Präventionsprogramme gegen IT-Kriminalität sind in diesen Gesetzen nicht zu entdecken. Dennoch handelt es sich sowohl beim Wbni als auch bei Computercriminaliteit III um Vorschriften, die der eigenen Bevölkerung dienen sollen, sich im Fall von Computercriminaliteit III jedoch sogar gegen die Niederländer richten können. Eine sichtbare außenpolitische Wirkung oder gar Regularien, die grenzüberschreitende Ermittlungen wesentlich erleichtern, lassen sich nicht ausmachen.

2.6.4 Cybersecuritybeeld Nederland 2019–2021

Das Cybersecuritybeeld Nederland¹⁴⁶ (CSBN) ist ein jährlicher Report des niederländischen NCTV und NCSC in Abstimmung mit dem Ministerie van Justitie en Veiligheid¹⁴⁷. Das Dokument geht auf mehr als 60 Seiten auf die aktuelle Gefahrenlage für die Informationstechnik der Niederlande ein. Dabei untermauert das NCSC seine Ausführungen und Bedrohungsskizzen mit Zahlen über Cyberangriffe, neue Malware oder finanzielle Aufwendungen zur Schadenbeseitigung. Durch die annuelle Distribution in Reportform scheinen Veränderungen und Verläufe über die jeweils betrachteten Zeitfenster hinaus durch. Diese Praxis eines solchen Berichts ist vergleichbar mit der Vorgehensweise vieler anderer nationaler IT-Sicherheitsbehörden, darunter das NCSC UK, das französische ANSSI¹⁴⁸ oder auch das deutsche BSI mit seinem ebenfalls jährlich erscheinenden Lagebericht.

Während noch das Cybersecuritybeeld 2019 und 2020 mit der Vorstellung eines Dreieckmodells begannen, welches visualisierte, wie NCSC und NCTV die Sicherheitslage des Landes kategorisieren und in Relation setzen, leitet das Cybersecuritybeeld 2021 prompt mit einem Bedrohungsszenario ein. Denn bereits die erste Überschrift des Berichts lautet „Cyberaanvallen tasten zenuwstelsel maatschappij aan“¹⁴⁹ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 7). Die Autoren vergleichen Angriffe auf die IT-Infrastruktur mit Verletzungen des Nervensystems und konstatieren, dass Cyberattacken Lähmungen auslösen können (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 7). Diese dramatische Analogie führt der NCTV auf vier akute wie grundlegende Risiken für die nationale Sicherheit zurück: So warnt er vor Informationsdiebstahl, zum Beispiel durch Spionage; vor der Sabotage von Diensten, etwa durch Ransomware; vor der Kappung globaler Lieferketten und schließlich warnt der NCTV vor großen Ausfällen aufgrund von Naturkatastrophen, menschlichem Versagen oder technischer Unzulänglichkeiten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 7). Seit 2019 nimmt die Beschreibung solch möglicher Worst Cases innerhalb des Vorwortes mehr und mehr Raum ein bis es dann 2021 das gesamte Vorwort ausfüllt. Bis 2019 erklärten die Autoren zu Beginn mittels eines Dreieckmodells, wie NCTV und NCSC zur

¹⁴⁶ Deutsch: Cybersicherheitsbild Niederlande

¹⁴⁷ Deutsch: Ministerium für Justiz und Sicherheit

¹⁴⁸ Ausgeschrieben: Agence nationale de la sécurité des systèmes d'information

¹⁴⁹ Deutsch: Cyberangriffe greifen das Nervensystem der Gesellschaft an

Einschätzung der Bedrohungssituation gelangten. Dieses Modell besteht aus den Aspekten „dreiging, belang en weerbaarheid“¹⁵⁰, dessen Dreiteilung die Berichte 2019 und noch 2020 je folgten und als Struktur für die Erläuterungen zugrunde legten (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 8). Das CSBN 2021 verwirft dieses Vorgehen teilweise und greift das bewährte Gerüst nicht mehr explizit in der Inhaltsübersicht auf. Im Übrigen beansprucht der Teil *Bedrohungen* 2021 erheblich mehr Raum des Berichts als in den Vorjahren, sodass die dreigeteilte Struktur aufweicht. Unter dem Motiv *dreiging*¹⁵¹ listen NCTV und NCSC in der 2019er-Fassung ihres Rapports die größten Bedrohungsquellen auf und legen hierbei unterschiedliche Maßstäbe der Konkretisierung an. So spricht die Cybersicherheitsbehörde vage von Risiken, die von einer steigenden Abhängigkeit von ausländischen Unternehmen ausgingen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 11). Nur wenige Seiten zuvor ist die Rede von Attacken, die direkt oder durch beauftragte Dritte von Staaten durchgeführt werden und die niederländische Souveränität angreifen. Hier werden China, Iran sowie Russland explizit mit unmittelbaren Vorwürfen konfrontiert (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 7). Insbesondere Russland wird 2019 mehrfach angeklagt – hier stellen die Niederländer einen direkten Bezug zwischen ihrer digitalen Vulnerabilität und den Untersuchungen von Flug MH17 her (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 16). Durch die namentliche Nennung der Staaten äußert das NCSC unverhüllte Kritik; und exponiert die Niederlande damit bewusst der Aufmerksamkeit und gegebenenfalls der Aggression staatlicher Nachrichtendienste, APT-Gruppen oder Desinformationskampagnen. Beispiele für Abhängigkeitsverhältnisse mit transnationalen Konzernen werden dagegen nicht präzisiert. Zudem identifizieren die Jahresberichte 2018 und 2019 staatliche Akteure gar als relevantester Bedrohungsursprung für die niederländische Sicherheit und ökonomische Handlungsfähigkeit (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018a, 27). Begründet wird diese These mit der weiterhin stark wachsenden digitalen Infrastruktur. Der Angriff auf diese oder auf Teile nationaler, Kritischer Infrastruktur aus dem Ausland kann als Druckmittel zur Durchsetzung diplomatischer Interessen ausgenutzt und gegen die Niederlande oder ihre europäischen Partner gerichtet werden. Darüber hinaus sei eine Triebfeder, vor allem chinesischer Akteure,

¹⁵⁰ Deutsch: Bedrohung, Bedeutung und Resistenz

¹⁵¹ Deutsch: Gefahr

die Spionage (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 15f). Auch in diesem Fall wird mit China ein Staat als kriminell handelnder Antagonist angeklagt. 2020 und 2021 lässt sich dagegen keine ähnlich deutliche Attribuierung finden. Zwar identifizieren die Behörden sogenannte staatliche Akteure in beiden Folgeberichten als eine der schwerwiegendsten Problemstellungen für die Informationssicherheit, jedoch werden die Akteure nur noch selten benannt und noch seltener mit Vorhaltungen versehen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 39ff).

Der Bericht 2020 spricht, wie schon 2019, von Spionage, Erpressung durch Ransomware sowie dem Ausfall Kritischer Infrastrukturen als größte Risiken für die nationale Sicherheit der Niederlande (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 29f). 2020 aber identifizieren die Behörden mit sogenannten Hack&Leak-Operationen eine weitere hybride Angriffsvariante: Zunächst stehlen die Täter Informationen von Staat oder Unternehmen, um sie anschließend zu dekontextualisieren und mit einem neuen Framing ausgestattet zu veröffentlichen. Diese Form der Desinformation wird von den Niederländern hervorgehoben, weil sie Fakten mit Falschbehauptungen vermengt und so ein besonderes Potenzial hat, Gesellschaften zu destabilisieren und Gruppen gegeneinander aufzubringen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 29). Derartige Bedrohungen werden nach CSBN erneut und gezielt durch staatliche Akteure geschaffen, wohingegen die Gefahr, die von nichtstaatlichen Akteuren ausgeht, 2020 als rückläufig eingestuft wird (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 30). Das CSBN 2021 legt dar, dass die im Jahr 2020 und teils schon in vorausgegangenen Berichten geschilderten Gefahren weiter zugenommen haben. So fügt das CSBN 2021 unmittelbar nach der angstbesetzten Gemengelage aus dem Vorwort noch die Implikationen der Corona-Pandemie hinzu. Denn die Autoren stellen fest, dass die Pandemie die Digitalisierung beschleunigt und sogar neue Bedrohungen beziehungsweise neue Tathergänge begünstigt hat. Man sei während der Kontaktbeschränkungen sehr auf Remote-Prozesse angewiesen gewesen, das Homeoffice beispielsweise wurde zur Normalität. Gleichzeitig griffen Cyberkriminelle vermehrt Gesundheitseinrichtungen an, da diese an Relevanz gewannen und man sich hohe Lösegelder versprach. Schließlich beobachtete das NCSC zielgerichtete Phishing-Angriffe, in denen mit den Ängsten und Hoffnungen der Bevölkerung gespielt wurde (vgl. Nationaal Coördinator

Terrorismebestrijding en Veiligheid 2021a, 24). Noch im Bericht 2020 wurde bemerkt, dass die Pandemie auch digital eine neue Bedrohungsdimension darstellen könnte, mehr als eine kurze Erwähnung fand COVID-19 dort aber nicht (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 18). 2021 dann blickt der NCTV auf eine pandemiegeprägte Risikobetrachtung: Er identifiziert Ransomware als realistische Gefahr für komplexe Organisationsnetzwerke, sieht vermehrt Desinformationskampagnen statt medizinischer Aufklärung oder entdeckt gefälschte Anti-COVID-Apps, die Schadsoftware verbreiten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 17ff). Wenngleich diese Methoden real sind und die Cyberkriminalität im Windschatten der Pandemie weitere Facetten ausgebildet hat, emotionalisieren NCTV und NCSC ihren Jahresbericht zunehmend, indem sie dieses Bedrohungsbild – frei von der Nennung von Daten – voranstellen. Das CSBN lässt dem Risikoszenario und zugehörigen Spekulationen zunehmend Raum. Auf diese Weise wird der Bericht von Beginn an subjektiviert und mit Unbehagen angereichert.

Zusätzlich zu den verantwortlichen Beteiligten versuchen NCTV und NCSC, die Ursachen für die niederländische Angreifbarkeit im digitalen Raum zu benennen. Die Behörden sehen veraltete Technologie genauso als Risikofaktor wie die bisher unverändert hohe Wahrscheinlichkeit für Angreifer, niemals als solche entdeckt zu werden. Im Umkehrschluss heißt das, dass sowohl der Zugriff auf Informationen als auch die Verschleierung der Tat vergleichsweise simpel sind (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 12). „Door de verdergaande digitalisering verandert de afhankelijkheid van onderliggende systemen en infrastructures“¹⁵² (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 19). Die voranschreitende Digitalisierung ist laut CSBN ein Katalysator für dieses Missverhältnis, da immer mehr Geräte installiert, vernetzt und ungesichert betrieben werden. Beispielhaft veranschaulicht das NCSC diese Entwicklung an den synchronen Technologien Cloud und IoT. Diese seien die Grundlage für die Digitalisierung bislang völlig manueller Prozesse und führten gleichzeitig zu einem immensen Anstieg personengebundener Daten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 19). Abhängigkeit auf mehreren Ebenen, von Technologien, von Servern in Drittstaaten oder von geopolitischen Konflikten, zieht sich entsprechend

¹⁵² Deutsch: Durch die fortschreitende Digitalisierung verändert sich die Abhängigkeit von zugrundeliegenden Systemen und Infrastrukturen.

durch alle drei Berichtsjahre. Unterdessen beobachtet das NCSC in den vergangenen Jahren sogenanntes Cybercrime-as-a-Service, also das Angebot von Cyberattacken durch Kriminelle auf verschiedensten Onlinemarktplätzen. Sobald Privatkunden in der Lage seien, digitale Straftaten im Internet zu bestellen wie jede andere Dienstleistung, steige die Zahl der Angriffe deutlich an, so die Vermutung des Berichts (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 27). Schon das CSBN 2018 illustrierte das Dilemma an einem Exempel: Demnach sei es einem 18-jährigen Niederländer im Januar 2018 gelungen, vielzählige digitale Regierungsangebote zu überlasten, indem er für 40 € die entsprechende Anwendung beschafft und ausgeführt hatte (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018a, 17). Mit dieser Art der Auslagerung von Expertise ist potenziell jeder Internetnutzer befähigt, eine Cyberattacke als Ware zu bestellen und etwa eine DDoS-Attacke durchzuführen. Hierum baut sich laut CSBN ein Markt auf, der den komplexen Vorgang eines Hacks demokratisiert und von den Fähigkeiten der eigentlichen Täter entkoppelt (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 28). Aufgrund der teils geringen Kosten können auch Ziele ins Visier geraten, die anzugreifen sich bisher aus wirtschaftlichen oder strukturellen Gründen nicht rentiert hätte. Diese Zunahme der Verfügbarkeit von Malware trägt dem folgend das Potenzial für eine weitere Skalierung der Bedrohungslage in sich.

Unter *belang*¹⁵³ erhält der Leser einen Eindruck von der Relevanz verschiedenster Bedrohungen für die Sicherheit der Niederlande. Der NCTV und das NCSC nehmen hier eine Einordnung möglicher Angriffe sowie potenzieller Ursachen und Nachwirkungen vor. Das CSBN stellt dar, dass Cyberangriffe unter anderem Ketteneffekte auslösen können. Das bedeutet, dass die Beeinträchtigung eines Systems, beispielsweise der Stromversorgung, nachfolgende Systeme, etwa Krankenhäuser oder Lieferketten in der Lebensmittelversorgung, ebenso schädigen kann (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 34). Dies führen die Autoren auf ein Monopol der Digitaltechnologie sowie auf einen Mangel an analogen Rückfallsystemen zurück (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 22). Aufgrund der Diffusion von Digitalem und Analogem versuchen sich NCTV und NCSC 2021 deshalb in ihrem Bericht an einer Definition des Begriffs Digitalraum: „De digitale ruimte is de complexe omgeving die het resultaat is van

¹⁵³ Deutsch: Bedeutung

onderling verweven digitale processen, ondersteund door wereldwijd gedistribueerde fysieke ICT en verbonden netwerken“¹⁵⁴ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 33). Demzufolge macht den digitalen Raum aus, dass in ihm digitale und physische Vorgänge und Strukturen zusammenkommen und er keinesfalls ausschließlich als System ohne Außenwirkung zu verstehen ist. Entsprechend stellen NCTV und NCSC unter *belang* in allen drei Berichtsjahren vor allem Abhängigkeitsrelationen der Niederlande fest. Hier geht es aber nicht nur um die Abhängigkeit von der Technologie als solcher, sondern mindestens ebenso um die (auch technologiebedingte) unabwendbare Bindung an andere Staaten und Großkonzerne. NCSC und NCTV weisen darauf hin, dass Facebook, Amazon, Apple, Google und Microsoft gewaltige Marktmacht zukommt. „Deze bedrijven hebben een gezamenlijke waarde die gelijk staat aan het bruto nationaal product van Frankrijk“¹⁵⁵ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 22). Das CSBN setzt folglich die ökonomische Signifikanz dieser Unternehmen mit Einfluss und politischer Macht gleich. Es wird in diesem Zusammenhang gar von einer Bedrohung für die Souveränität und die Autonomie des niederländischen Staates und der Europäischen Union gesprochen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 22). Großkonzerne werden in diesem Papier als ernst zu nehmende Partizipatoren am geopolitischen Geschehen beschrieben wie es sonst nur Staaten zugeschrieben wird. Ob es für diese Annahme weitere Kennzahlen gibt, die die These untermauern oder wie sich das Land aus dem Relativgefüge emanzipieren möchte, lässt das CSBN offen. Die Niederländer werden dagegen äußerst konkret, wenn sie vom Ausbau ihres 5G-Mobilfunknetzes sprechen und benennen ausdrücklich das chinesische Unternehmen Huawei als Risiko für die sichere Implementierung der Technologie. Mit diesen grundlegenden Vorbehalten geht die Annahme einher, die dichtere Konzentration von Informationen führe zu größeren Schäden, sodass Spionage und Datendiebstahl auch zukünftig attraktive Mittel für gewisse Regime sein werden (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 23). Genauso offensiv verkündet das NCSC, dass man den russischen Anbieter für IT-Sicherheitslösungen, Kaspersky, aus sämtlichen Regierungssystemen ausgeschlossen und eine Zusammenarbeit beendet habe

¹⁵⁴ Deutsch: Der digitale Raum ist die komplexe Umgebung, die das Ergebnis miteinander verflochtener digitaler Prozesse ist, unterstützt durch weltweit verteilte physische IT und verbundene Netzwerke.

¹⁵⁵ Deutsch: Diese Unternehmen haben einen gemeinsamen Wert, der dem Bruttosozialprodukt Frankreichs entspricht.

(vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 27). Die Bedenken gegen Großunternehmen werden laut Cybersecuritybeeld damit begründet, dass staatliche Angriffe zunehmend auf Dritte, darunter Unternehmen, ausgelagert werden. Dieses Vorgehen verschleierte den eigentlichen Hintergrund der Tat und erschwere die Nachvollziehbarkeit für die Ermittlungsbehörden (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 27). Weiter spekulieren die Berichtsverfasser über mögliche Cyberangriffe von Drittstaaten auf die Niederlande, die ihre Angriffsfähigkeiten und -aktivitäten immens ausgebaut hätten. Die Behörden benennen keine einzelnen Vorgänge oder gehen auf Vorfälle mit unmittelbaren Konsequenzen ein, aber man habe „concrete manifestaties van dreigingen waargenomen“¹⁵⁶ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 39). Deshalb sei man sicher, dass die Verletzlichkeit der Niederlande direkt mit offensiven Interessen anderer Staaten zusammenhänge (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 40f). Aus dem CSBN 2021 lässt sich deutlich herauslesen, dass die Niederlande digitale Kapazitäten als bedeutsame Ressource der Verteidigung verstehen. Wenn das CSBN also vermerkt, dass Staaten wie Indien, China, Vietnam oder der Libanon diese Ressource intensiv anhäufen, befürchten sie indirekt eine Verschiebung geopolitischer Verhältnisse, bei der die Niederlande ins Hintertreffen geraten könnten.

Der eigentliche Bericht, das *Jaarbeeld*¹⁵⁷ oder der *Terugblik*¹⁵⁸, reicht von 6 Seiten im Jahr 2021 bis hin zu 10 Seiten 2020 – damit füllen NCSC und NCTV also nur einen Bruchteil des Gesamtdokuments mit diesen Informationen. Dabei setzen sie in jedem Jahr auf Leuchttürme, also prominente Vorfälle, die das gegenwärtige Vorgehen von Tätergruppen anschaulich machen. 2019 stellt der Bericht beispielsweise dar, dass Phishing weiterhin höchst erfolgreich gewesen sei und die Kriminellen den Schaden in den Niederlanden innerhalb eines Jahres mehr als verdreifacht hätten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 28). Diesen Seiten zufolge war die Hackergruppe Dragonfly besonders auffällig, indem sie Unternehmen der Energieerzeugung unter anderem mit Spear-Phishing angriffen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 25). Diese Beschreibungen krimineller Angriffsmechaniken und das Exempel Dragonfly wirken bedrohlich; ihre

¹⁵⁶ Deutsch: konkrete Manifestationen von Bedrohungen wahrgenommen

¹⁵⁷ Deutsch: Jahresbild

¹⁵⁸ Deutsch: Rückblick

Konsequenzen, insbesondere für die niederländische Bevölkerung werden in diesem Zuge jedoch weder eingeordnet noch relativiert. 2020 dann führt das CSBN an gleicher Stelle aus, dass Ransomware die dominierende Methode gewesen sei und vor allem staatliche Akteure sichtbar auftraten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 15f). Exemplarisch umschreibt der Bericht die öffentlich bekannten Umstände des Ransomware-Angriffs Ende 2019 auf die Universität Maastricht und verbleibt damit ohne Neuigkeit oder ergänzende Auskunft (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 17). Schließlich nehmen die Autoren 2021 die Auswirkungen der Corona-Pandemie auf die IT-Sicherheit in den Blick und stellen fest, dass Phänomene wie Desinformation oder Phishing zugenommen haben; machen dazu aber keine quantifizierbaren Angaben. Als Beispiel für einen schwerwiegenden IT-Vorfall führt das CSBN 2021 die Kompromittierung von Software-Produkten der Firma SolarWinds an, die unter anderem Regierungseinrichtungen weltweit verwenden (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 20). Auf Details zum Vorfall verzichtet der Bericht; auch einen Zusammenhang zur Pandemie oder dem zuvor beschriebenen Bedrohungsszenario stellen NCSC und NCTV hier nicht her.

AIVD en MIVD: digitale sabotage een van de grootste cyberdreigingen

De AIVD en MIVD beschouwen de mogelijke digitale verstoring en sabotage van de vitale infrastructuur als een van de grootste cyberdreigingen voor Nederland en zijn bondgenoten.⁷ Meerdere staten hebben bewezen de capaciteiten en de bereidheid te hebben om digitale sabotage in te zetten om hun geopolitieke doelstellingen te bereiken. De AIVD constateert al langere tijd dat sommige van deze staten voorbereidingen treffen om digitale sabotage voor toekomstig gebruik mogelijk te maken. Deze voorbereidingen bestaan uit het zich innestelen in ICT-systemen van onder meer vitale infrastructuur. Ook de MIVD onderkende in 2019 diverse voorbereidende sabotageactiviteiten gericht tegen westerse landen en bondgenootschappelijke belangen.⁸ Momenteel ontbreekt het staten aan de intentie om digitale sabotage tegen Nederland in te zetten. Deze intentie is echter veranderlijk van geopolitieke ontwikkelingen.⁹

Informatie-operaties door statelijke actoren

Enkele landen gebruiken informatie-operaties als instrument in hybride conflicten. Via die operaties proberen ze verdeeldheid te zaaien over onderwerpen die bij de verschillende doellanden of bondgenootschappelijke organisaties gevoelig liggen. Maatschappelijke polarisatie en de versplintering van het politieke landschap in een groot aantal landen vormen een voedingsbodem daarvoor. Onderzoek van de MIVD bracht in 2019 informatie-operaties gericht tegen Nederland, andere westerse landen en bondgenootschappelijke belangen aan het licht.¹⁰

Cyberaanvallen vormen aantrekkelijk verdienmodel voor criminelen

Cyberaanvallen zijn het afgelopen jaar veelvuldig (succesvol) ingezet door cybercriminelen voor afpersing, informatiediefstal en CEO-fraude¹¹. Het is voor hen een aantrekkelijk verdienmodel.¹² Afpersing blijkt succesvol te zijn door de inzet van ransomware (zie Inzet van ransomware als middel voor afpersing).

Mogelijke nieuwe vormen van samenwerking topsegment cybercriminelen

De politie ziet een mogelijke nieuwe vorm van interactie tussen verschillende groepen binnen het topsegment van cybercriminelen. Voorheen opereerden deze groepen redelijk autonoom en voerden ze vele processtappen eigenstandig uit. Nu lijkt er sprake te zijn van samenwerking tussen specifieke groepen. Zowel de politie als een aantal beveiligingsbedrijven vinden het aannemelijk dat sommige criminele actoren binnen het topsegment toegang tot bedrijfsnetwerken onderling verhandelen, nadat ze deze hebben gecompromitteerd en beoordeeld op de waarde.¹³

Statelijke actor combineert spionage en cybercrime

In 2019 bleek een staatsgelieerde hackersgroep zich bezig te houden met zowel spionage als financieel gemotiveerde operaties.¹⁴ Criminelen gebruiken vaak dezelfde (openbare) middelen als statelijke actoren en vice versa. In het verleden hebben staatsgelieerde actoren uit een ander land zich ook met financieel gemotiveerde aanvallen bezig gehouden.

Modi operandi en ingezette middelen grotendeels gelijk gebleven

Inzet van ransomware als middel voor afpersing

Steeds vaker wordt waargenomen dat criminele actoren ransomware zodanig inzetten dat zij het slachtoffer onder druk kunnen zetten om tot betaling van losgeld over te gaan. Het gaat de actoren vooral om organisaties die de mogelijkheid hebben om grotere geldbedragen te betalen¹⁵ en/of waarvoor bedrijfscontinuïteit en waardevolle unieke data een belangrijke rol spelen. Kenmerkend voor de werkwijze is de uitgebreide verkenning van het bedrijfsnetwerk. Dit stelt de actor in staat om de waarde van de data en de schade voor het slachtoffer in te schatten en om de ransomware op de meest effectieve wijze te plaatsen. Op basis van dat inzicht varieert het gevraagde losgeld van enkele tienduizenden tot miljoenen euro's.¹⁶ Er lijkt een toename te zijn van ransomware-aanvallen waarbij data niet alleen versleuteld wordt, maar ook gekopieerd. Wanneer een organisatie het losgeld niet wilde betalen, dan publiceerden criminelen in sommige gevallen de data.¹⁷

Begin februari 2020 publiceerden cybersecurity experts over nieuwe ransomware, genaamd EKANS, die zich richt op industriële controlesystemen (ICS) en zou zijn ontwikkeld door criminelen. Deze systemen worden gebruikt voor bijvoorbeeld de drinkwater- en energievoorziening. De aanvalsmethode is relatief eenvoudig, maar de ransomware lijkt speciaal ontwikkeld om ICS aan te vallen. Tot de slachtoffers van EKANS behoren waarschijnlijk de staatsoliemaatschappij van Bahrein en bedrijven in de maakindustrie. EKANS is mogelijk de eerste ICS-gerichte ransomware die het werk is van een criminele actor.¹⁷

III CEO-fraude is een vorm van Business Email Compromise (BEC)-fraude, waarbij getracht wordt een medewerker te misleiden om geld over te maken naar een rekening van een crimineel.

Abbildung 14: Exemplarischer Auszug aus dem CSBN 2020 (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 16)

Es zeigt sich, dass im eigentlichen Report-Bereich des CSBN kaum bis gar keine Statistiken über landesweite Betroffenheit, Schadenssummen oder Daten über erfolgreich abgewehrte Angriffe zu finden sind. Wie die Abbildung einer beispielhaften Seite aus dieser Rubrik offenlegt, reihen die Überschriften Aussagen aneinander. Die

Wahrheit dieser Äußerungen liegt dem Bericht als Prämisse zugrunde, kann aber nicht durch die Leserschaft anhand von Daten und Informationen überprüft werden. Zugleich nehmen diese Titelzeilen bereits Deutungen vor, die über die reine Berichtsform hinausgehen. Nicht die einzelnen Aufmacher, sondern die Menge und Qualität der Überschriften montieren ein Situationsbild, das weniger auf Statistik als auf kuratierten Botschaften ruht: „AIVD en MIVD: digitale sabotage een van de grootste cyberdreigingen“¹⁵⁹, „Informatie-operaties door statelijke actoren“¹⁶⁰, „Cyberaanvallen vormen aantrekkelijk verdienmodel voor criminelen“¹⁶¹, „Mogelijke nieuwe vormen van samenwerking topsegment cybercriminelen“¹⁶², „Staatelijke actor combineert spionage en cybercrime“¹⁶³, „Modi operandi en ingezette middelen grotendeels gelijk gebleven“¹⁶⁴ und „Inzet van ransomware als middel voor afpersing“¹⁶⁵ sind nur die Überschriften, die auf dieser einen Seite hervorgehoben sind und das Leserauge einfangen (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 16). Diese Zeilen über Geheimdienste, staatliche Angriffe, Spionage und Ransomware können mindestens als tendenziös bezeichnet werden und hinterlassen einen beunruhigenden Eindruck – sie adressieren die Emotio statt der Ratio. Ohne nun bewerten zu können, ob diese Meldungen korrekt oder angemessen sind, lässt sich festhalten, dass jede einzelne einen boulevardesquen Charakter aufweist und die Schlagzeile der Information vorzieht.

Mit *weerbaarheid* bezeichnet das CSBN die Fähigkeit der Niederlande, einer Bedrohungslage im Digitalraum entgegenzutreten und sie abzuwehren. Dieses Kapitel dient demnach einer Einschätzung der Robustheit der aktuellen Sicherheitsinfrastruktur. Das Papier leitet 2019 selbstkritisch mit der Bemerkung ein, dass lediglich zwei von elf niederländischen Ministerien 2018 mit angemessen modernen und einsatzbereiten Sicherheitsmaßnahmen und -technologien ausgestattet gewesen seien (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 33). Eine Ursache dafür sieht das NCSC im ICV-Bericht¹⁶⁶, einer Art Wasserstandsmeldung über die Informationssicherheit der Ministerien. In diesem seien demzufolge keine klaren Kennziffern definiert, die ein aussagekräftiges Monitoring zuließen (vgl. Nationaal

¹⁵⁹ Deutsch: AIVD und MIVD: Digitale Sabotage eine der größten Bedrohungen

¹⁶⁰ Deutsch: Informations-Operationen durch staatliche Akteure

¹⁶¹ Deutsch: Cyberangriffe bilden attraktives Verdienstmödel für Kriminelle

¹⁶² Deutsch: Mögliche neue Formen der Zusammenarbeit im Topsegment der Cyberkriminellen

¹⁶³ Deutsch: Staatlicher Akteur kombiniert Spionage und Cyberkriminalität

¹⁶⁴ Deutsch: Modi Operandi und eingesetzte Mittel sind größtenteils gleich geblieben

¹⁶⁵ Deutsch: Einsatz von Ransomware als Mittel für Erpressung

¹⁶⁶ ICV: In Control Verklaring – Kontrollmeldung

Coördinator Terrorismebestrijding en Veiligheid 2019a, 33). Demzufolge ist eine einheitliche Ausstattung mit Ressourcen, Wissen und Technologie kaum möglich. Zusätzlich werde Software häufig innerhalb einer Institution eingerichtet und genutzt, aber extern betrieben und gewartet. Unweigerlich erhöht dies die Zahl beteiligter Dienstleister und Schnittstellen deutlich. Das NCSC führt auch darauf den mangelnden Überblick und zeitgleich eine Zunahme der Angriffsflächen zurück (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 35). Das CSBN 2019 zählt erneut diverse Risiken für die Abwehrkräfte der Niederlande auf, darunter die rasante Entwicklung von 5G und Künstlicher Intelligenz wie auch die zunehmende Konnektivität (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 37). NCSC und NCTV sehen die Integrität von Information unter anderem durch Deepfakes bedroht und fürchten sogar mögliche Segmentierungen des Internets durch Russland und China (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 38f). Daraus leitet die niederländische Regierung ab, die Abwehrstärke von Bürgern und Organisationen verbessern zu müssen. Wie das geschehen soll, bleibt an dieser Stelle diffus (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 40). Dagegen schlagen die Autoren vor, das Nationaal Detectie Netwerk¹⁶⁷ (NDN) auszubauen, da dies in der Lage sei, Gefahren schneller erkennbar machen. In diesem Netzwerk werden sogenannte indicators of compromise, IoC, geteilt – also Informationen, mit denen die übrigen Netzwerkpartner Bedrohungen oder mögliche Kompromittierungen identifizieren können (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 45). Dies stärkt nachvollziehbar die digitale Resilienz der Niederlande; bemerkenswert ist jedoch, dass das NDN in den Berichten der Folgejahre keine Erwähnung mehr findet. 2020 entfällt dann die Benennung möglicher Verbesserungen der gegenwärtigen Abwehrstärke gänzlich. Stattdessen konstatiert das Kapitel über die weerbaarheid, dass die Niederlande essenzielle Basisschutzregeln nur unzureichend beachten – ein Attest, das der Bericht sowohl Unternehmen als auch der Reichsregierung ausstellt (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 37). So hätten neun von 16 untersuchten Regierungsorganisationen ihre Schutzmaßnahmen nicht ausreichend implementiert und bildeten einen Schwachpunkt in der nationalen Cyberabwehr. Hinzu komme, dass das Lagebild mangelhaft sei: Es bestand im Berichtszeitraum oft kein Wissen darüber,

¹⁶⁷ Deutsch: Nationales Detektionsnetzwerk

welche IT-Systeme in den Organisationen genutzt wurden oder welche Ausgaben für die Technik vorgesehen waren (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020a, 39f). Auch 2021 bleibt die Frage nach potenziellen Optimierungen oder nach drängenden Handlungsfeldern größtenteils unbeantwortet. Stattdessen verweist der Bericht erneut darauf, dass Unternehmen und Staat einfache Basisschutzmaßnahmen vernachlässigen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 43).

Op nationaal niveau gaat het onder andere om structurele problemen zoals de groeiende afhankelijkheid van buitenlandse software en hardware producenten en dienstverleners. Ook problemen zoals de afnemende diversiteit in technologische oplossingen en toeleveranciers kunnen een systeemrisico vormen¹⁶⁸ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 46).

Abhängigkeit von ausländischen Unternehmen bei gleichzeitiger Abnahme inländischer Produktions- und Innovationskraft tue ihr übriges, um die niederländische Widerstandsfähigkeit gegen digitale Risiken zu unterminieren. Deshalb, so fährt der Bericht fort, sei es alternativlos, in die Menschen zu investieren – in jene Spezialisten, die Neuschöpfungen vorantreiben und in die Weiterbildung der Bedienenden – damit sie besser gerüstet sind (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 46). Damit macht das Cybersecuritybeeld Nederland über alle drei beobachteten Reportjahre keine konkrete Angabe über die tatsächlichen Abwehrkräfte niederländischer Netze, Infrastrukturen oder Unternehmen. Es fehlt an einer Art Maßstab oder einem Wert, anhand dessen eine Verbesserung feststellbar oder verifizierbar sein könnte. In der Folge ist es schwer bis unmöglich, herauszufinden, ob die Niederlande den Risiken und Angriffsvektoren bereit gegenübersteht oder ob die Infrastrukturen und Kompetenzen des Landes heillos unterlegen sind. Gleichzeitig verhärtet sich mit jedem Jahr die Tonalität des CSBN, das eine immer bedrohungsorientiertere Sprache und Justierung an den Tag legt, um ein prosperierendes Risikoszenario zu erzeugen. Während das CSBN 2021 Gefahren und Risiken auf 27 Seiten elaboriert, teilen sich die Kapitel über die Bedeutsamkeit und die Abwehrfähigkeiten dagegen nur neun der 54 Seiten des Berichts. 2020 erstreckte sich die Risikobeschreibung auf 12 Seiten, 2019 lediglich auf 10. Bei aller Verschiebungen

¹⁶⁸ Deutsch: Auf nationaler Ebene geht es unter anderem um strukturelle Probleme wie die zunehmende Abhängigkeit von ausländischen Soft- und Hardwareherstellern und -Dienstleistern. Auch Probleme wie die abnehmende Vielfalt technologischer Lösungen und Zulieferer können ein systemisches Risiko darstellen.

in der digitalen Sicherheitssphäre, die der Report zwischen 2019 und 2021 beschreibt, bezeugt das CSBN nur wenige faktenbasierte Steigerungen der Gefahrenintensität. Stattdessen zeigt sich eine deutliche Veränderung der Berichtsform, mit der NCSC und NCTV suggerieren, dass sie alles ihnen Mögliche unternehmen, aber weitere große Investitionen und Anstrengungen in die Cyberabwehr nötig sind, um mit dem anscheinend rasant wachsenden Bedrohungsszenario schritthalten zu können. Die Gefahrensituation wächst demzufolge unentwegt weiter, sodass das NCSC und andere Organisationen ihre Anstrengungen ebenfalls anschieben müssten. Hier lässt sich ein gewisser Bias annehmen, da Sicherheitsinstitution wie NCTV und NCSC ihre Legitimierung aus den Unsicherheitsverhältnissen beziehen. NCSC und NCTV sind im Grunde der Versuch, der Gefahr durch regelhafte Institutionen beizukommen und die Ursache eines Unbehagens zu bekämpfen, ohne sie vollends zu beheben. Denn gleichzeitig kann die Institution kein intrinsisches Interesse daran haben, dieses Gefühl gänzlich abzustellen, da sie andernfalls ihre eigene Existenz erodieren ließe.

Zusammenfassend lässt sich festhalten, dass der Schwerpunkt des Cybersecuritybeeld Nederland über die untersuchten Jahre hinweg unzweifelhaft auf der Darstellung von akuter Unsicherheit und drohendem Unheil liegt. Dass hieraus auch Opportunitäten, beispielsweise für die niederländische Wirtschaft erwachsen könnten, belassen die Berichte überwiegend im Hintergrund. Bei der Untersuchung der CSBN fiel auf, dass die Berichte nur äußerst selten mit prüfbaren Fakten aufwarten und damit möglicherweise plausibel, ihre Resultate und Schlussfolgerungen aber kaum reproduzierbar sind. Die wenigen Zahlen, die die Argumentation tragen könnten sowie die teils populistische Verschlagwortung stützen die Annahme, dass die Dokumente tendenziell emotionalisierte Dramaturgie anbieten statt datenbasierte Empirie.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	X	X		X		X			X		X

Das bedeutet explizit nicht, dass Zweifel an der Wahrheit der herangezogenen Vorfallbeschreibungen bestehen müssen. Allerdings handelt es sich um singuläre Geschehnisse, die zwar gewisse Muster erkennen, aber ohne die Einbettung in eine statistische Gesamtheit keine grundsätzliche Ausrichtung der Sicherheitspolitik rechtfertigen lassen. In Summe ergibt sich somit die Einschätzung, dass innerhalb des CSBN das subjektive Unsicherheitsempfinden die objektive Unsicherheitslage

überblendet. Dieser Eindruck verstärkt sich, da in zahlreichen Passagen direkte Anklage gegen einzelne Staaten aufgrund prominenter Vorkommnisse erhoben wird, vor allem in Richtung Russlands und Chinas. Wiederholt heben die Verfasser hervor, dass man Angriffe von staatlicher Seite antizipiert. Darin steckt nebenbei die Botschaft, dass Aggressoren klar benannt und von der gesamten Öffentlichkeit beäugt werden statt den Ursprung der Täter aus diplomatischer Höflichkeit oder aus politischem Kalkül diskret zu anonymisieren. Einschneidende physische wie digitale Erfahrungen mit den genannten und anderen Ländern beziehungsweise Regierungen führen dazu, dass die Niederlande hier zu verstehen geben, Angriffe jeglicher Art nicht hinzunehmen – sie wenden sich durch den Bericht deutlich an außenpolitische Adressaten. Zusätzlich sind die Niederlande dem Bericht folgend von Drittstaaten, ausländischen Unternehmen und Lieferketten existenziell abhängig. Das lässt nahezu vergessen, dass das Dokument vordergründig die eigene Bevölkerung zur Leserschaft hat. Indem das Papier immer wieder festhält, wie gravierend die herangetragene Bedrohungslage und damit wie wichtig die Arbeit der Sicherheitsorgane ist, nutzen die Autoren äußere Unsicherheitsfaktoren zur Zementierung innerer Sicherheitssentimente. In der Konsequenz kann das Cybersecuritybeeld Nederland zwar als Bericht, aber auch dem Namen nach als Bild gelesen werden: Wenn Bedrohung, Gefahr und Risiko die Bedingungen für die, wie in den Ausführungen über Institutionen aufgezeigt, kollektive Billigung einer Institution sind, offenbart sich erneut die Securitization, wie Balzacq sie beschrieb – ein gesprochener Akt, durch den systeminhärente Akteure subjektives Sicherheitsempfinden herstellen können, das wiederum der eigenen Agenda dienlich ist.

2.6.5 Nederlandse Cybersecurity Agenda & Nationale Cybersecurity Strategie

Am 21. April 2018 legte der Minister für Justiz und Sicherheit vorgelegt der Zweiten Kammer des Parlaments die *Nederlandse Cybersecurity Agenda* vor (vgl. Rijksoverheid 2018). Die Agenda ist unterschrieben mit *Nederland digitaal veilig*¹⁶⁹ und untermauert den Anspruch der Niederlande, IT-Sicherheit proaktiv zu gestalten. Das Vorwort, das Minister Ferd Grapperhaus verfasst hat, leitet deshalb mit dem Hinweis ein, dass Cybersicherheit oberste Priorität für das niederländische Kabinett habe (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 5). Der Minister betont dabei die Bedeutung internationaler Zusammenarbeit und sieht geteilte Verantwortungen, sowohl zwischen Staat, Wirtschaft

¹⁶⁹ Deutsch: Niederlande digital sicher

und Gesellschaft, als auch innerhalb der NATO und der EU. Zudem plädiert Grapperhaus dafür, trotz aller Strategien und Strukturen stets Flexibilität zu bewahren und sich auch zukünftig hochmodern aufzustellen. Nur so könne man „nieuwe digitale kwetsbaarheden en dreigingen“¹⁷⁰ begegnen (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 5). Bereits sieben Jahre zuvor schlug das Kabinett, vertreten durch den damaligen Minister van Veiligheid en Justitie¹⁷¹, Ivo Opstelten, dem Parlament die *Nationale Cyber Security Strategie* vor. Im Gegensatz zur NCSA ist die Nationale Cyber Security Strategie (NCSS) von 2011 ein knappes, mittlerweile in die Jahre gekommenes Papier, in dem die Grundpfeiler der niederländischen Cybersicherheitsarchitektur begründet liegen. Wenngleich beide Dokumente dieselben Herausforderungen behandeln und teils einander bedingen, weisen sie doch sichtliche Verschiedenheiten auf.

Die Cybersicherheitsagenda der Niederlande umfasst 46 Seiten, lässt sich aber auf eine einzelne Zielformulierung herunterbrechen, die in der Agenda mehrfach aufgeführt ist:

Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 7).¹⁷²

Um dieses vorrangige Ziel möglich zu machen, wurden dem sieben Aufgabenfelder untergeordnet, die durch konkrete Maßnahmen zu erreichen sein sollen. Diese Absichten sind unscharf formuliert, nicht um inexakt zu bleiben, sondern vielmehr um Impulse für zuträgliche Imaginationen herzustellen:

1. Die Niederlande haben ihre digitale Schlagkraft aufgestellt.
2. Die Niederlande tragen zu internationalem Frieden und Sicherheit im digitalen Raum bei.
3. Die Niederlande sind Vorreiter in der Förderung von sicherer Hard- und Software.
4. Die Niederlande verfügen über wehrhafte digitale Prozesse und eine robuste Infrastruktur.

¹⁷⁰ Deutsch: neuen digitalen Verwundbarkeiten und Bedrohungen

¹⁷¹ Deutsch: Minister für Sicherheit und Justiz

¹⁷² Deutsch: Die Niederlande sind in der Lage, die ökonomischen und gesellschaftlichen Gelegenheiten der Digitalisierung zu versilbern und die nationale Sicherheit in der digitalen Domäne zu beschützen.

5. Die Niederlande bauen mit Cybersecurity-Maßnahmen wirksame Barrieren gegen Cyberkriminalität auf.

6. Die Niederlande sind Pionier bei der Wissensentwicklung im Bereich der Cybersecurity.

7. Die Niederlande verfügen über einen integralen, öffentlich-privaten Ansatz der Cybersecurity (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 7).¹⁷³

Realität sollen diese Zielbilder durch eine Cybersecurity-Allianz werden, die sich aus staatlichen Stellen und Wirtschaftsunternehmen gemeinschaftlich zusammensetzen soll (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 7). Die Verantwortung für die Zielerreichung wird so auf mehrere Schultern verteilt und nicht ausschließlich von Staat oder Regierung getragen. Neben vagen Vorgaben, wie den Punkten 1 und 5, die eine allgemeine Verstärkung der IT-Sicherheitsbestrebungen ins Auge fassen, lassen sich Ambitionen und Absichten entdecken, die Aussagen über die strategische Ausrichtung der Niederlande zulassen. So ist der Wunsch nach einer Vorreiterrolle in Bezug auf sicherheitstechnologische Innovationen und Wissensentwicklung unter 3. ein Hinweis auf die ausgeprägte Wahrnehmung der sich bietenden ökonomischen Chancen. In aufkeimenden und stark wachsenden Branche werden Nischen erst noch besetzt, wodurch eine frühzeitig optimistische Positionierung in diesem global vernetzten Gefüge möglich ist. Aber nicht nur auf technischer Ebene wünschen sich die Niederlande eine Vorreiterrolle. Denn die Agenda sieht ebenfalls vor, dass das Land wesentliche Bedeutung in der Durchsetzung der globalen Rechtsordnung im Digitalraum gewinnt. Indem sie auf Rechte und Normen der internationalen Gemeinschaft einwirken und sich als Vermittler zwischen Staaten wie auch zwischen nichtstaatlichen Akteuren einbringen, möchten die Niederlande unter anderem Menschenrechte auch in bislang juristischen Zwischenräumen des Internets gewährleisten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 23). Bemerkenswert ist zudem eine Darstellung unter Absicht zwei:

Nederland is in staat, al dan niet in coalitieverband, onverwijd en adequaat te reageren bij digitale aanvallen door statelijke actoren en beschikt over offensieve

¹⁷³ Übersetzung des Autors aus dem Niederländischen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 7)

capaciteiten die een bijdrage leveren aan het vermogen tot afschrikking¹⁷⁴ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 23).

Hier setzen die Autoren auf einen konfrontativen Duktus, indem sie von *Angriffen*, *offensiven Kapazitäten* und *Abschreckung* sprechen. Damit offenbart das Königreich militärische Ambitionen, die über eine reaktive Verteidigungspolitik innerhalb der NATO oder der EU hinausgehen und alleinige Handlungsfähigkeit sicherstellen sollen. Eine derart offensive Richtlinie setzt voraus, dass die Niederlande über fortgeschrittene Technologie und ausgeprägte Expertise verfügen sowie Grundvertrauen in diese Fähigkeiten wie auch in die Rechtmäßigkeit des eigenen Tuns haben.

Um solche Grundüberzeugungen international vertreten zu können, müssen die Niederlande befähigt sein, einer antizipierten Gefährdungslage auch präventiv zu begegnen, so eine Prämisse in der NCSA. Dafür beabsichtigt die Regierung, Verantwortung auf die Beteiligten aus Wirtschaft und Gesellschaft zu verteilen und proklamiert mit Absicht 7 eine partnerschaftliche Herangehensweise, um die Stärken des öffentlichen sowie des privaten Sektors miteinander zu verbinden. Die Niederlande sollen von den resultierenden Synergien profitieren können – das nennt die Agenda den „integrale Nederlandse cybersecurity aanpak“¹⁷⁵ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 43). In diesem partizipativen Vorgehen sieht sich die Regierung in der Rolle des Regisseurs, also des tonangebenden Koordinators, nicht in der Funktion eines apodiktischen Regulativs (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 43). Die Agenda adressiert deutlich Unternehmen wie Bürger und weist auf ihre Eigenverantwortlichkeit, aber auch auf ihre Gestaltungsmöglichkeiten hin:

Voor de overheid betekent dat vooral: een krachtige regierol, stimuleren en voorwaarden scheppen. Zodat bedrijfsleven en burgers hun eigen digitale veiligheid en weerbaarheid kunnen vormgeven. Want daar blijven ze uiteraard zelf verantwoordelijk voor¹⁷⁶ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 5).

Das heißt für die Regierung, dass sie zuvorderst auf Selbstregulierung setzt, ergo davon ausgeht, dass sich individuelle Anwender wie auch ganze Organisationen im Digitalen

¹⁷⁴ Deutsch: Die Niederlande sind in der Lage, ob im Koalitionsverband oder nicht, sofort und angemessen auf digitale Angriffe staatlicher Akteure zu reagieren und verfügen über offensive Fähigkeiten, die zu ihrem Abschreckungsvermögen beitragen.

¹⁷⁵ Deutsch: integraler niederländischer Cybersicherheitsansatz

¹⁷⁶ Deutsch: Für die Regierung bedeutet dies vor allem: eine starke Regierolle, Anregungen und Rahmenbedingungen schaffen. Damit Wirtschaft und Bürger ihre eigene digitale Sicherheit und Abwehrkraft gestalten können. Denn dafür bleiben sie natürlich selbst verantwortlich.

so verhalten, wie es für ihr eigenes und das Wohl der übrigen verträglich ist. Erst wenn diese Selbstregulierung scheitert, greift die Legislative mit Vorgaben ein. Schon die Untersuchung des Wet beveiliging netwerk- en informatiesystemen veranschaulichte, dass nur unvermeidliche Regulierungen formuliert wurden, die lediglich für den unmittelbar betroffenen Kreis der Diensteanbieter und Kritischen Infrastrukturen gelten, damit stets Spielräume für alle Akteure in den Niederlanden erhalten bleiben können. Diese liberale Agenda versucht zu verhindern, dass der ökonomische Wettbewerb unnötig eingeschränkt wird und zugleich unterstreicht sie die Attraktivität des Wirtschaftsstandortes (vgl. Tweede Kamer der Staten-Generaal 2011, 4). Diese Smith'sche Annahme, dass der Egoismus eines Jeden zu einer kollektiven Nutzenmaximierung führt, ist eine zutiefst kapitalistische Prämisse, die der Agenda vielfach zugrunde liegt. Unter anderem sollen Bürger und Unternehmen fähiger werden, um Cyberkriminalität zu erschweren. Ferner zielt die Agenda darauf ab, Anreize zur Verwendung sicherer Hard- und Software zu schaffen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 36). „Het mainstreamen van cybersecurity is het doel: de digitale veiligheid moet in iedere organisatie onderdeel zijn van de dagelijkse processen“¹⁷⁷ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 7). Demzufolge impliziert die Agenda, dass die Macht des Marktes und die Eigenverantwortlichkeit eines jeden dazu führen, die Sicherheitstransformation zu vollziehen.

Damit diese Zukunftsimaginationen bei gleichzeitig minimalinvasiver Einmischung des Staates möglich werden, versieht der NCTV die sieben Absichten der Cybersecurity Agenda mit Doelstellingen¹⁷⁸ und Maatregelen¹⁷⁹. Jede der Intentionen besteht damit aus zahlreichen Zielsetzungen und Maßnahmen, die die Schritte hin zum jeweiligen Vorsatz aufzeigen und nebenbei eine spätere Überprüfung und Messbarkeit erlauben sollen. Allerdings variieren die Doelstellingen wie auch die Maatregelen in ihrer Granularität, in ihrer Konkretisierung und auch in ihrer Verbindlichkeit. Absicht fünf, also der Schaffung von Barrieren gegen IT-Kriminalität, wird etwa die Zielsetzung zugeordnet, dass diese Hindernisse existieren und effektiv Cyberkriminelle abwehren (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 35). Das

¹⁷⁷ Deutsch: Das Mainstreamen von Cybersecurity ist das Ziel: Die digitale Sicherheit muss in jeder Organisation Grundsatz der täglichen Prozesse sein.

¹⁷⁸ Deutsch: Zielsetzungen

¹⁷⁹ Deutsch: Maßnahmen

wiederum soll unter anderem durch folgende Maßnahme Gestalt annehmen: „Er worden voorstellen ontwikkeld om burgers en bedrijven digitaal meer vaardig te maken zodat cybercriminelen minder kans maken“¹⁸⁰ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 36). Außerdem soll die Verwendung von sicherer Hard- und Software gefördert sowie das Gesetz Computercriminaliteit III umgesetzt werden (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 35f). Von diesen drei Maßnahmen stellt lediglich die Gesetzeseinführung eine Verbindlichkeit her, wenngleich die eigentliche Konkretion die Inhalte des Gesetzestextes sind, die in der Agenda jedoch keine Erwähnung finden. Im Übrigen entwickelt der NCTV mit diesen Maatregelen alleinig Vorschläge für Mechanismen, die Bürger und Unternehmen zu mehr Resilienz verhelfen könnten, damit Cyberkriminelle daraufhin geringere Erfolgchancen hätten. An dieser exemplarischen Stelle hat die NCSA überwiegend Empfehlungscharakter ohne fixierte Zielgrößen; die Gefahr, dass mit diesen Doelstellingen später ein Scheitern der Agenda sichtbar werden könnte, ist entsprechend gering.

Mit Absicht drei möchten die Niederlande eine Vorreiterrolle in der Förderung sicherer Hard- und Software einnehmen. Dafür formuliert der Nationaal Coördinator Terrorismebestrijding en Veiligheid verschiedenste Ambitionen wie zum Beispiel, dass sie sich dafür engagieren, digitale Gefährdungen zu identifizieren, indem entsprechende Produkte auf ihre Sicherheitseigenschaften hin getestet werden. Diese Sicherheitsrisiken sollen minimiert werden, indem auf Seiten der Anwender das Bewusstsein für solche Gefahren geschärft und parallel die Haftung von Herstellern und Anbietern reformiert wird (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 27). Das ist aus Sicht niederländischer Verbraucher erstrebenswert und ein anschaulich formuliertes Ziel. Allerdings enthalten die angeschlossenen Maßnahmen unscharfe Toleranzen und sind vielmehr Beschreibungen intendierter Handlungsoptionen als präzise, schrittweise Skizzen zur Zielrealisierung. So möchte man mit Herstellern und Wissenschaftlern ins Gespräch kommen, um über „verbeterpunten en oplossingen“¹⁸¹ in Fragen der Haftung fehlerhafter, digitaler Produkte zu diskutieren (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 28). Diese Absichtserklärung ist an keinerlei Ergebnis oder Zusicherung geknüpft, sondern verbleibt zunächst als Verheißung.

¹⁸⁰ Deutsch: Es werden Vorschläge entwickelt, um Bürger und Unternehmen digital zu befähigen, damit Cyberkriminelle weniger Chancen haben

¹⁸¹ Deutsch: Verbesserungen und Lösungen

Darüber hinaus wolle man sich in europäischen Expertengremien für verpflichtende Sicherheitsupdates einbringen oder beispielsweise prüfen, welche Kriterien für den Einkauf von Hard- und Software innerhalb der Reichsregierung gelten sollten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 28). „Als onderdeel van de cybersecurity bewustwordingscampagnes van veiliginternetten.nl lanceert de overheid een of meer beleidsondersteunende publiekscampagnes voor digitaal veilige hard- en software“¹⁸² (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 29). Die Regierung sieht die Sensibilisierung der Bevölkerung demnach als ein Instrument, um Hard- und Software sicherer zu betreiben. Jedoch zeigt sich in dieser Maßnahme aus Absicht drei die Richtungslosigkeit, die innerhalb der gesamten Agenda zu finden ist. Statt einer Beschreibung von Inhalt, Zielgruppe, Kosten und Laufzeit der genannten Kampagne, findet sich nur eine unpräzise Angabe darüber, dass es eine, vielleicht auch mehrere, Kampagnen geben soll.

In Absicht sechs, also die *Niederlande sind führend im Bereich Cybersicherheit-Wissensentwicklung*, steht das Ziel, dass Bürger und Unternehmen die Bedeutung digitaler Bedrohungen erkennen und sie befähigt sind, diesen entgegentreten (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 40). Um dies in die Wege zu leiten, möchte die Regierung die grundlegende wie auch die weiterführende Bildung entsprechend ausbauen.

Digitale vaardigheden, waaronder mediawijsheid en cybersecurity, zijn nadrukkelijk aandachtspunten in de integrale curriculumherziening in het primair en voortgezet onderwijs. In 2018 zullen hiervoor voorstellen worden ontwikkeld, die vanaf 2019 in wet- en regelgeving uitgewerkt zullen worden¹⁸³ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 40).

Das schließt ein, in die Cybersicherheitsforschung zu investieren sowie die bestehenden Informationskampagnen effektiver miteinander zu verknüpfen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 40). Bis heute jedoch sind diese Digitalkompetenzen nicht Teil der offiziellen Lehrpläne in den Niederlanden (vgl. VO-Raad 2022).

¹⁸² Deutsch: Im Rahmen der Sensibilisierungskampagnen für Cybersicherheit von veiliginternetten.nl startet die Regierung eine oder mehrere politikunterstützende, öffentliche Kampagnen für digital sichere Hard- und Software.

¹⁸³ Deutsch: Digitale Kompetenzen, unter anderem Medienkompetenz und Cybersicherheit, sind besondere Schwerpunkte der integralen Lehrplanüberprüfung in der Grund- und Sekundarbildung. Dazu werden 2018 Vorschläge entwickelt, die ab 2019 in Gesetze und Verordnungen überführt werden.

Hier zeigt sich zwar, dass die Agenda Instrumente enthält, die sie differenziert ausführt und die konkreter sind als andere. Daneben aber stellt der NCTV Konzeptskizzen und vage Perspektiven einer sichereren Technologiesellschaft vor, deren Realitätswirkung in Zweifel gezogen werden kann. Ihre Ideen konstituieren die Autoren mitunter über die performative Kraft der Sprache: Mit Wendungen wie „Nederland heeft zijn digitale slagkracht op orde“ oder „Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling“ erzeugt der NCTV eine Erfüllungsfantasie schon im Moment des Lesens (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 7). Die sieben Absichten der Agenda stehen im futuristischen Präsens, das prospektiv Entschlossenheit sowie die Annahme einer hohen Erfolgswahrscheinlichkeit in sich trägt. Das verbindet der NCTV mit einem in Optimismus verpackten Passus über die Ursachen und Konsequenzen der Agenda. Schon in der Überschrift stellen die Autoren klar, dass Cybersicherheit ökonomische Werte produziert; um dann zu deklarieren, dass die Niederlande dafür bereits sehr gute Vorbedingungen aufweisen:

Nederland is een van de meest gedigitaliseerde landen ter wereld. We beschikken daarmee over uitstekende voorwaarden om internationaal koploper te zijn, in het veilig en in vrijheid snel nieuwe technologieën uitrollen en gebruiken¹⁸⁴ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 9).

Damit positionieren sich die Niederlande nicht nur als schon jetzt führende Nation in der Digitalisierung, sondern mit der Formulierung des *Wir* beziehen sie die Leser als Protagonisten dieser Erfolgsimagination unmittelbar ein. Im Gegenzug ist die Rede von „de overheid“¹⁸⁵ oder von „overheidspartijen“¹⁸⁶ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 13). Obwohl das Papier unter der Verantwortung eines Regierungsministeriums verfasst ist, liest sich die Agenda auf diese Weise wie eine Schrift über Politik, nicht wie eine politische Schrift. Leser könnten den Eindruck gewinnen, dass ein Bürger in der Agenda seine Vorstellungen einer wirksamen Strategie niedergeschrieben hat und diese nun der Regierung vorlegt – eine rhetorische Technik, die Subjekt und Staat gleichstellt.

Darauf folgt die Beurteilung, dass digitale Bedrohungen stark zugenommen hätten und dieses gesteigerte Risiko die Mitwirkung aller Gesellschaftsteile erfordere

¹⁸⁴ Deutsch: Die Niederlande sind eines der meist digitalisierten Länder der Welt. Damit verfügen wir über hervorragende Voraussetzungen, international führend bei der schnellen, sicheren und freien Einführung sowie Nutzung neuer Technologien zu sein.

¹⁸⁵ Deutsch: die Regierung

¹⁸⁶ Deutsch: Regierungsparteien

(vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 9). Dieses Eingeständnis wird wiederum eingeklammert durch eine weitere Umschreibung möglicher Nutzeffekte für die Niederlande:

[E]en sterke Nederlandse cybersecurity sector stimuleert kennisontwikkeling, de arbeidsmarkt en werkgelegenheid, en draagt bij aan het internationale profiel van Nederland op economisch, militair en veiligheidsgebied¹⁸⁷ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 9).

Die NCSA wird so mit gleichermaßen notwendigen wie vorteilhaften Maßnahmen in Szene gesetzt. Dass dabei Kosten aufkommen, neue Vorschriften nötig werden oder Wettbewerbsnachteile entstehen könnten, findet dagegen keine Erwähnung. Zumal sowohl die Skalierung als auch der Grad der Quantifizierung, insbesondere innerhalb der Maatregelen, die die Zielerreichung verwirklichen sollen, variieren. Der Weg zum Ziel bleibt zumeist unklar und ist nicht näher definiert. Messgrößen fehlen gänzlich und auch Termine oder Fristen sind nicht vorgesehen. Die Agenda enthält nahezu keine Kriterien, die Rechenschaft oder eine Aussage über die Verwirklichung der ausgesprochenen Absichten zuließen und kommt als Patentrezept daher, das alles leisten soll. Mal heißt es, „Standaarden en certificering leveren een belangrijke bijdrage aan de digitale veiligheid van hard- en software“¹⁸⁸, womit entsprechend das Ziel sicherer IT-Produkte erreicht werden soll (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 28). Diese Maßnahme aber enthält keine Sollwerte, keinen Zielzeitraum, keine Kennzahlen – es handelt sich vielmehr um einen generalisierenden Kommentar ohne weitere Handlungsverpflichtung. An anderer Stelle heißt es, die Regierung Sorge dafür, IT-Hersteller und -Dienstleister, auch international, zur Verwendung moderner Kommunikationsprotokolle zu bewegen, sodass schließlich die digitalen Infrastrukturen resilienter betrieben werden (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 33). Hier ist aber weder benannt, was unter modern zu verstehen ist, ob es sich um eine einmalige oder eine zyklische Bemühung handelt, bis wann die Maßnahme umgesetzt sein soll, noch ob diese Protokolle und Standards verpflichtend sein und für wen sie gelten werden. Derlei Beispiele für unbestimmte Umsetzungsinstrumente lassen sich in der Nederlandse Cybersecurity Agenda zahlreich finden und sind Belege für die pauschalisierende und undifferenzierte

¹⁸⁷ Deutsch: Ein starker niederländischer Cybersicherheitssektor stimuliert die Wissensentwicklung, den Arbeitsmarkt und die Beschäftigung und trägt zum internationalen Profil der Niederlande in den Bereichen Ökonomie, Militär und Sicherheit bei.

¹⁸⁸ Deutsch: Standards und Zertifizierungen liefern einen wichtigen Beitrag für die digitale Sicherheit von Hard- und Software.

Verfasstheit der Agenda, die in weiten Teilen Verbindlichkeit missen lässt. Stattdessen stellen die sieben Ambitionen einen Rundumschlag der Cybersicherheit dar, dessen Erfüllung geradezu eine technologische Utopie wäre; allerdings hier nicht als solche gekennzeichnet ist.

Die *Nationale Cyber Security Strategie* (NCSS) von 2011 liegt ebenso im Verantwortungsbereich des niederländischen Ministeriums für Justiz und Sicherheit, hatte in ihrem Beschlussjahr hingegen vorrangig einen konstituierenden Zweck. Neben weiteren, im Grunde zur Agenda identischen, Absichtsformulierungen enthält die NCSS insbesondere den Entscheid, den Cyber Security Raad und das Nationaal Cyber Security Centrum ins Leben zu rufen (vgl. Tweede Kamer der Staten-Generaal 2011, 5). Weiterhin schlägt die Strategie bereits früh die Eckpfeiler der heutigen Agenda ein. Dazu gehört der stetige Blick auf die internationale Zusammenarbeit, die Förderung von Forschung und Bildung im Bereich der Informationstechnik genauso wie „Zelfregulering als het kan, wet- en regelgeving als het moet“¹⁸⁹, die sich in der NCSA und in weiteren Regierungspapieren wiederfinden (Tweede Kamer der Staten-Generaal 2011, 4f). 2011 sah die niederländische Regierung demnach vor, die Eigenverantwortung von Bürgern, Unternehmen, aber auch etwa von Kommunalregierungen zu maximieren und ihnen somit Handlungsfreiheiten zu lassen, sie damit aber in die Pflicht zu nehmen. An dieser Stelle kommt fast beiläufig das Selbstverständnis des niederländischen Staates zum Vorschein: Die Regierung stimuliert, setzt Anreize und reguliert nur dort, wo es notwendig ist, um grundlegende Vorgaben zu machen. Entlang dieser geschaffenen Rahmenbedingungen bleibt dann individuelle Souveränität für die Akteure aus Wirtschaft und Gesellschaft. Diese Ungezwungenheit lässt mehr Raum für Unsicherheitsfaktoren, die in der Strategie aber nur selten als Risiken beschrieben werden. Stattdessen sind die Autoren davon überzeugt, dass durch die umrissenen Vorgaben „de economie gestimuleerd en welvaart en welzijn verhoogd“¹⁹⁰ werden (Tweede Kamer der Staten-Generaal 2011, 4f). Trotz dessen benennen die Verfasser die Gefahr als eine wesentliche Motivation hinter der NCSS von 2011; zahlreiche Vorfälle, besonders die Malware Stuxnet, seien entdeckt und als Bedrohung für wichtige Infrastrukturen identifiziert worden (vgl. Tweede Kamer der Staten-Generaal 2011, 2). Gleichsam schließt die Regierung daraus, dass der

¹⁸⁹ Deutsch: Selbstregulierung wenn möglich, Gesetze und Verordnungen wenn nötig.

¹⁹⁰ Deutsch: die Ökonomie gestärkt und Wohlstand und Wohlbefinden erhöht

Digitalraum ein globaler Raum ist, der jedwede Form von Grenze überschreitet oder durchdringt (vgl. Tweede Kamer der Staten-Generaal 2011, 3). Resultierend aus diesen Folgerungen setzt die NCSS auf einen technologischen Ansatz, indem man etwa Kritische Infrastrukturen absichern und IT-Lieferanten zu Security-by-Design bewegen will (vgl. Tweede Kamer der Staten-Generaal 2011, 6f). Aber schon aufgrund ihres überschaubaren Umfangs von lediglich acht Inhaltsseiten ist die Nationale Cyber Security Strategie nur als Unterbau oder Impuls zu verstehen, auf dem wiederum die Nederlandse Cybersecurity Agenda gründet¹⁹¹.

Die Bedeutung der Nationale Cyber Security Strategie liegt in ihrer Funktion als Ursprungspapier gleich mehrerer Cybersicherheitsinstitutionen. Die Nederlandse Cybersecurity Agenda hingegen breitet das Bild einer zukünftigen Digitalgesellschaft aus und formuliert optimale Rahmenbedingungen. Gemein haben beide Dokumente, dass sie kaum auf spezifische Bedrohungen eingehen, die für die beschriebenen Maßnahmen ursächlich sein könnten. Stattdessen betonen die Verfasser immer wieder, dass Digitalisierung und Cybersicherheit ökonomische Chancen ermöglichen, die den Niederlanden neue Wirtschaftszweige eröffnen könnten. Es klingt stets die Hoffnung an, dass die Niederlande auf diesem Gebiet eine namhafte Stellung einnehmen könnten: „Investeren in cyber security betekent investeren in onze toekomst“¹⁹² (Tweede Kamer der Staten-Generaal 2011, 3). Das bedeutet nicht nur, dass der Blick an dieser Stelle deutlich mehr auf Opportunitäten statt Widrigkeiten liegt, sondern zeigt auch, dass die Papiere vornehmlich ein Sentiment bedienen statt tatsächlichen Realbedrohungen zu begegnen.

Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienerfokus	Innen	Außen	Chance	Risiko
	X	X			X	X		X		X	

Mehrfach betonen die Verfasser beider Schriften, dass die Niederlande auf Selbstregulierung der Unternehmen wie der Bürger setzen und demzufolge nur dort Maßgaben veranlassen, wo Leitlinien unausweichlich sind. Der sozialpolitische Ausdruck *Fördern statt Fordern* ließe sich übertragen: Man räumt der Wirtschaft Freiheiten ein, indem man sie nicht über die Maße reglementiert, und schenkt dem

¹⁹¹ Im Herbst 2022 präsentierte die amtierende Ministerin für Justiz und Sicherheit, Dilan Yeşilgöz-Zegerius, die aktualisierte Nederlandse Cybersecuritystrategie 2022–2028 sowie den dazugehörigen Aktionsplan.

¹⁹² Deutsch: In Cybersicherheit zu investieren, heißt in unsere Zukunft zu investieren.

Einzelnen sein Zutrauen. So soll der Standort Niederlande im direkten Vergleich mit stark durch Sicherheitsvorgaben regulierten Ländern attraktiver wirken. NCSS und NCSA betonen diese Eigenverantwortlichkeit und setzen auf die Macht des freien Marktes. Dabei beinhaltet dieses liberale Versprechen auch die hier unausgesprochene Verpflichtung, verantwortungsvoll und im Sinne der übrigen Mitglieder der Gesellschaft zu handeln.

Ein weiteres signifikantes Merkmal niederländischer IT-Sicherheitsstrategie liegt in der Verfolgung einer internationalen Vorreiterrolle, wie es etwa die Ambitionen drei und sechs der NCSA wiedergeben. Hierin verbirgt sich die außenpolitische Proklamation eines bemerkenswerten Eigenwerts, die Partnern wie auch Konkurrenten aufzeigen soll, dass die Niederlande – auch wenn sie ein kleiner Staat sind – auf dem Gebiet der Cybersicherheit eine gewichtige Lenkungsfunktion am Tisch der globalen Mächte einnehmen. Die Verfasser akzentuieren die nationale Expertise, attestieren den Niederlanden aber zusätzlich immer wieder, sich in einer zwischenstaatlichen Konkurrenzsituation um eine Art Digitalhegemonie zu befinden.

Door de investeringen in omringende landen in cybersecurity onderzoek, is het wenselijk dat er in Nederland een (meerjarige) impuls komt voor cybersecurity onderzoek om zo talent, en daarmee onze cybersecurity kennispositie, te behouden¹⁹³ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 39).

Abseits der Frage, ob die Niederlande diese Position bereits innehaben oder in naher Zukunft ausfüllen könnten, reproduzieren sie doch immer wieder diese Imagination und tragen auf diese Weise selbst zu ihrer Fremdwahrnehmung als ebensolche Cybersecurity-Nation bei. Zugleich senden beide Dokumente innen gerichtete Botschaften an die Niederländer aus. Auf diese Weise erhält der Leser einen Eindruck von einer imaginierten Zukunft mit einer weitestgehend sicheren Informationstechnik, in der Bedrohungen entweder nicht mehr nennenswert oder wenigstens kontrollierbar sind. Es entsteht insgesamt der Eindruck, dass die Niederlande in der Lage wären, Umweltfaktoren auszuklammern und selbst über ihr künftiges Sicherheitsniveau zu entscheiden. Durch die Beschreibung einer positiven Ausgangssituation sowie einer noch optimistischeren Entwicklungsperspektive fördern NCSS und NCSA eine

¹⁹³ Deutsch: Durch Investitionen umgebender Länder in Cybersicherheitsforschung ist es wünschenswert, dass es in den Niederlanden einen (mehrjährigen) Impuls für die Cybersicherheitsforschung gibt, um Talent und damit unseren Cybersicherheitswissensstand zu erhalten.

bejahende Blickweise auf die Chancen des digitalen Lebens. Die Benennung von Unsicherheiten nimmt auch deshalb eine verschwindend geringe Rolle ein. Dazu trägt neben alldem die gewählte Sprache bei, die vor Selbstgewissheit strotzt: Die Verfasser setzen Zukunftsbilder in ein selbsterfüllendes Präsenz (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 23). Die Niederlande bezeichnen sich dazu als *tonangebend* und sie formulieren deutlich ihren europäischen Gestaltungswillen (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 38/vgl. Tweede Kamer der Staten-Generaal 2011, 7).

2.6.6 IT-Investitionen

Beim Blick auf die Ausgaben der Niederlande für Informationssicherheit ist die Miljoenennota, also der nationale Haushaltsplan, nur bedingt hilfreich. Dieses Dokument ist deutlich weniger umfangreich als sein deutsches Pendant und führt keine Posten mit einem vergleichbaren Detailgrad. Das bedeutet natürlich nicht, dass der Haushalt weniger genau geführt wird oder an dieser Stelle zu wenige Vergleichsgrößen zur Verfügung stehen. Stattdessen erstellen die Ressorts eigene Haushalte, die in jährlich beschlossenen Gesetzen festgeschrieben werden. Die Positionen dieser Haushalte sind dabei weder für alle Ressorts festgeschrieben und identisch noch sind sie gleichartig skaliert oder komparabel; eine Untersuchung ist dadurch erheblich erschwert. Während die nun folgenden Gesamtausgaben der Häuser und Ressorts aus der Miljoenennota und den Haushalten der Ministerien stammen, wurden die Angaben über die spezifischen Investitionen in Informationstechnik dem Rjks ICT-Dashboard¹⁹⁴ entnommen. Hier kann die niederländische Öffentlichkeit einsehen, welche Ministerien die höchsten Ausgaben für Informations- und Kommunikationstechnik vornehmen oder wie sich die ICT-Ausgaben in den vergangenen Jahren dynamisiert haben. Dort ist beispielsweise abzulesen, dass die Niederlande 2021 über alle Ressorts 4,55 Mrd. Euro für Projekte vorsehen, die unmittelbar der Digitalisierung oder der digitalen Sicherheit im Land zugutekommen sollen (vgl. Rijksoverheid 2023a).

In einem Schreiben an das Kabinett aus dem Oktober 2021 forderte die ständige Commissie voor Digitale Zaken¹⁹⁵ des Parlaments, dass Ausgaben für Informationstechnik sowie Investitionen in digitale Technologien und Infrastruktur in den Haushalten und Berichten transparenter dokumentiert werden sollten. Die

¹⁹⁴ Deutsch: Reichs-Dashboard für Informations- und Kommunikationstechnik

¹⁹⁵ Deutsch: Kommission für digitale Angelegenheiten

Kommission kritisierte, dass es kaum gangbar sei, tatsächliche Ausgaben für diese Bereiche exakt zu ermitteln, da diese Aufwendungen entweder in größeren Positionen inkludiert seien oder sie nicht als solche benannt werden (vgl. Tweede Kamer der Staten-Generaal 2021, 3). Das Innenministerium, das diese Kritik für das Kabinett in einem Brief beantwortet hat, stimmte zu und befand ebenfalls, dass es oft nicht möglich sei, Maßnahmen der Digitalpolitik eindeutig von den übrigen Positionen zu trennen (vgl. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2021, 2). Das bedeutet für die nachfolgende Aufstellung, dass es sich bei den verfügbaren Haushaltsmitteln – wie im Kapitel zu deutschen IT-Investitionen – einzig um Annäherungswerte handeln kann. Für den hier beabsichtigten Erkenntnisgewinn ist dieser Umstand jedoch zu vernachlässigen, da die Relationen, man könnte sagen aufgrund ihrer analogen Ungenauigkeiten, ablesbar sind und somit einen Vergleich der niederländischen und deutschen Datensätze zulassen. Es ist anzunehmen, dass die Größenordnungen und Verhältnismäßigkeiten von einer beidseitigen Unschärfe nicht verwässert werden, sodass die folgenden Aussagen auch bei präziseren Daten unverändert blieben.

Bei der Betrachtung der Daten ist zunächst augenfällig, dass in den Niederlanden nahezu der identische Anteil des Gesamtjahreshaushaltes in Höhe von 336 Mrd. Euro wie in Deutschland für sozialstaatliche Leistungen verbucht wird; etwa 50 % aller verfügbaren Gelder fließen in die öffentliche Fürsorge. Von den übrigen Milliarden erhalten das Ministerium für Soziales und Arbeit mit 52,4 Mrd. Euro sowie das Ministerium für Bildung, Kultur und Wissenschaft mit etwa 43,6 Mrd. Euro die größten Haushalte. Wohingegen Ressorts, die in vielen anderen Staaten besonders kostenintensiv ausgelegt sind, wie Verteidigung oder Wirtschaft, in den Niederlanden mit 11,6 und 7,8 Mrd. Euro vergleichsweise überschaubar ausgestattet werden (vgl. Ministerie van Financiën 2020, 46). Dagegen fließen 5 Mrd. Euro in die internationale Zusammenarbeit (vgl. Ministerie van Financiën 2020, 49). 4,8 Mrd. Euro verbucht allein das Innenministerium 2021 als *huurtoeslag*¹⁹⁶ in den Wohnungsmarkt (vgl. Ministerie van Financiën 2020, 188). Und nicht weniger als 722 Millionen Euro sehen die Niederländer für das Projekt *Een veilig Groningen met perspectief*¹⁹⁷ vor, um Groningen und das Umland gegen weitere Erdbeben aufgrund der intensiven Gasförderung zu wappnen (vgl. Ministerie van Financiën 2020, 205). Die Sicherheit des

¹⁹⁶ Deutsch: Mietzuschuss

¹⁹⁷ Deutsch: Ein sicheres Groningen mit Perspektive

Deltas wie der Wasserwege lösen 1,2 Mrd. Euro, während die Zinsaufwendungen und Rückzahlungen der erwarteten Staatsverschuldung von fast 502 Mrd. Euro ganze 22,4 Mrd. Euro per annum verlangen (vgl. Ministerie van Financiën 2020, 107/194).

Die extrahierten Daten der untenstehenden Tabelle verhalten sich gleichermaßen zueinander wie zuvor die Zahlen in der deutschen Erhebung: Die Aufstellung enthält Informationen über relevante Institutionen in der Informationstechnik und -sicherheit wie auch über fachferne Ministerien und Behörden, um einen Bezugsrahmen herzustellen. Damit die Relationen sichtbar sind, wurden auch hier die gerundeten Summen in Millionen Euro angegeben. Zu diesem Zweck wurden die Ausgaben aus den ICT-Dashboards der jeweiligen Organisationen addiert. In der Quelle werden die Daten unterschieden in *Beheer en onderhoud*¹⁹⁸ und *Vernieuwing*¹⁹⁹, die wiederum gegliedert sind in *internes Personal*, *externes Personal* und *Material*. Aus der Addition ergeben sich dann die Gesamtausgaben der Ministerien für Informationstechnologie. Auch das ist analog zu den deutschen Statistiken: Die Trennschärfe zwischen informationstechnischen oder gar IT-Sicherheitsausgaben und nur verwandten Investitionen ist nicht gegeben beziehungsweise von der niederländischen Regierung festgesetzt. Dennoch bietet die Aufstellung eine probate Annäherung, welche die Dimensionen und finanzpolitischen Priorisierungen beleuchtet.

¹⁹⁸ Deutsch: Verwaltung und Unterhalt

¹⁹⁹ Deutsch: Erneuerung

Einrichtung	Gesamtetat für das Jahr 2021 (in Mio. €)
Königreich der Niederlande	336 600
sozialstaatliche Leistungen	166 200
Staten-Generaal ²⁰⁰	191
Königtum	46
Ministerie van Defensie ²⁰¹	11 629
davon für Informationstechnik	900,6
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties ²⁰²	6 643
davon für Informationstechnik	648,4
Sonderfall ‚Doorontwikkeling en innovatie digitale overheid‘ ²⁰³	14,38
Ministerie van Justitie en Veiligheid ²⁰⁴	14 211
davon für Informationstechnik	590,6
Ministerie van Volksgezondheid, Welzijn en Sport ²⁰⁵	25 879
davon für Informationstechnik	87,2
Ministerie van Sociale Zaken en Werkgelegenheid ²⁰⁶	52 493
davon für Informationstechnik	58,6
Ministerie van Onderwijs, Cultuur en Wetenschap ²⁰⁷	43 684
davon für Informationstechnik	169,8
Ministerie van Infrastructuur en Waterstaat ²⁰⁸	16 476

²⁰⁰ Deutsch: ‚Generalstaaten‘ – Name des niederländischen Parlaments

²⁰¹ Deutsch: Verteidigung

²⁰² Deutsch: Innere Angelegenheiten und Königreichsbeziehungen

²⁰³ Deutsch: Weiterentwicklung und Innovation Digital Government

²⁰⁴ Deutsch: Volksgesundheit, Wohlbefinden und Sport

²⁰⁵ Deutsch: Soziales und Arbeit

²⁰⁶ Deutsch: Justiz und Sicherheit

²⁰⁷ Deutsch: Bildung, Kultur und Wissenschaft

²⁰⁸ Deutsch: Infrastruktur und Wasserwege

davon für Informationstechnik	440,2
Ministerie van Financiën ²⁰⁹	9 265
davon für Informationstechnik	1 047,7
Ministerie van Buitenlandse Zaken ²¹⁰	11 393
davon für Informationstechnik	147,2
Ministerie van Economische Zaken en Klimaat ²¹¹	7 837
davon für Informationstechnik	332,8
Beperking van de Klimaatverandering ²¹²	3 371
Diergezondheidsfonds ²¹³	34
Defensiematerieelbegrotingsfonds ²¹⁴	4 610
Shared Service Centrum-ICT ²¹⁵	232,6
Logius ²¹⁶	235,5
Algemene Inlichtingen- en Veiligheidsdienst ²¹⁷	300,7
Nationale Politie	6 094
Digital Trust Center	2,53
NCSC	8,3

Quelle: Miljoenennota 2021 (Ministerie van Financiën 2020)/Rijks ICT-dashboard (Rijksoverheid 2023a)/Einzelpläne der Ministerien (Tweede Kamer der Staten-Generaal 2020a, b, c)

Erneut bietet sich ein Blick auf die Ausreißer der Liste an, also auf jene Institutionen, die besonders wenig und die besonders viel ihres Jahresetats auf Informationstechnik

²⁰⁹ Deutsch: Finanzen

²¹⁰ Deutsch: Auswärtige Angelegenheiten

²¹¹ Deutsch: Auswärtige Angelegenheiten

²¹² Deutsch: Eindämmung des Klimawandels

²¹³ Deutsch: Tiergesundheitsfonds

²¹⁴ Deutsch: Verteidigungsausrüstungsfonds

²¹⁵ Behörde des Innenministeriums, die digitale Produkte und Dienste für die Verwaltung bereithält

²¹⁶ Behörde des Innenministeriums, die digitale Schnittstellen für Bürger und Unternehmen zur Regierung unterhält

²¹⁷ Deutsch: Allgemeiner Nachrichten- und Sicherheitsdienst

verwenden. Denn hier lassen sich eklatante Unterschiede ausmachen: Das für Bildung zuständige Ministerie van Onderwijs, Cultuur en Wetenschap gibt mit 169,8 Millionen Euro nur 0,39 % seiner fast 44 Mrd. Euro für Informationstechnik aus. Das Finanzministerium investiert in seinem Ressort dagegen 11,3 % seiner Gelder 2021 in IT. Tatsächlich liegen aber die Häuser, in denen die Zuständigkeit für Informationssicherheit und Digitalisierung verankert ist, in relativen Zahlen zwischen diesen zwei Extremen. Das niederländische Wirtschaftsministerium, in dem das Digital Trust Center angesiedelt ist, entnimmt 4,25 % seiner 7,8 Mrd. Euro, das Ministerium für Inneres und Königreichsbeziehungen, dem der AIVD unterstellt ist, 9,76 % und das Verteidigungsministerium ganze 7,74 % für Kapitalaufwände rund um Informationstechnik oder -sicherheit. Das Ministerie van Justitie en Veiligheid, in dem sowohl die wesentlichen Sicherheitsbehörden als auch das NCSC aufgehängt sind, investiert mit 590,6 Millionen Euro 4,16 % in Informationstechnik. Vergleichbar zu Deutschland liegt es an den Ressorts selbst, in welcher Höhe sie in Informationssicherheit investieren, sodass sie dies zumeist entsprechend ihrer Zuständigkeit für das Thema, nicht unbedingt entsprechend ihrem Schutzbedarf, tun. Bei einem Blick auf die etwa 8,7 Millionen Euro, die dem NCSC für 2021 zur Verfügung stehen, fällt in der Gegenüberstellung auf, dass die Mittel des Nationaal Cyber Security Centrum lediglich 0,0026 % der staatlichen, niederländischen Ausgaben für das gesamte Jahr ausmachen und damit deutlich hinter den Investitionen in Deutschland für das BSI zurückbleiben (vgl. Tweede Kamer der Staten-Generaal 2020a, 74). Im Vergleich beansprucht das Budget der Polizei 6,094 Mrd. Euro, also 1,81 % des Gesamthaushaltes pro Jahr (vgl. Tweede Kamer der Staten-Generaal 2020a, 88). Dieser Polizeietat schließt Ermittlungen gegen Cyberkriminelle oder Digitalstraftaten zwar ein, aber dennoch kommt man bedingt durch die erhebliche Diskrepanz nicht umhin zu bemerken, dass der physischen Sicherheit signifikant größere monetäre Ressourcen zugeteilt werden als der digitalen. Auch deshalb befindet der Cyber Security Raad, der das Kabinett in Fragen der Informationssicherheit berät, in seinem Bericht *Integrale aanpak cyberweerbaarheid*²¹⁸, dass in der Legislatur 2021–2025 weitere 833 Mio. Euro nötig seien, um den Minimalanforderungen gegenwärtiger Cybersicherheitsherausforderungen begegnen zu können (vgl. Cyber Security Raad 2021, 5). Unabhängig davon, welche Zahlen und Ausgaben noch herangezogen

²¹⁸ Deutsch: Integraler Ansatz Cyberabwehrkräfte

werden, nehmen die Investitionen der Niederlande zur Absicherung des Digitallebens nie mehr als einen nur bruchstückhaften Charakter an. Umgekehrt signalisiert dieser relational geringe Wert auch, dass das Risiko trotz der messbaren und wachsenden Bedrohungslage als geringfügig betrachtet wird. Das wird besonders sichtbar, wenn man berücksichtigt, dass das Königshaus mit 46 Millionen Euro jährlich über etwa sechsmal so viel Geld verfügen kann wie das NCSC. Selbst der Diergezondheidsfonds, mit dem man Tierseuchen früh erkennen und sich auf mögliche Ausbrüche vorbereiten will, ist mit 34 Millionen Euro um ein Vielfaches größer als der Etat der niederländischen Cybersicherheitsbehörde. Diese Daten geben zwar Auskunft über die Investitionsbereitschaft beider Staaten respektive ihrer Behörden und damit über die Bedeutung, die der IT-Sicherheit in Etatabwägungen eingeräumt wird. Dennoch sagen diese Informationen nicht, ob diese Mehr- oder Minderinvestitionen zu einem Mehr oder Weniger an Sicherheit führen, da die Umgebungssysteme vielschichtig sind und Cybersicherheit mit zahlreichen Mitteln vorangetrieben werden kann: Denn auffällig ist auch, dass die Niederlande bei kleinerem Staatshaushalt mehr als doppelt so viel Geld für ihr Bildungs- und Forschungsministerium vorsehen wie die Bundesrepublik. Zusätzlich wurde bereits in vorausgegangenen Kapiteln erkennbar, dass Forschungsinstitutionen, -Verbände, und -Netzwerke wie SURF, NWO oder der HSD Campus bedeutende Ressourcen für die Dienstleistungs- und Wissensgesellschaft der Niederlande sind. Somit lässt sich annehmen, dass die Kompetenzaggregation ein probater Weg für die Niederlande ist, um ihre digitale Sicherheit langfristig voranzutreiben.

2.7 Zwischenbilanz – Systeme in den Niederlanden & Deutschland

In Deutschland sind schon auf Bundesebene zahlreiche Ressorts, Ministerien und Behörden an der Ausgestaltung der IT-Sicherheit beteiligt. Diese Kompetenzzerstreung ist teils dem historischen Aufwuchs der letzten Jahrzehnte geschuldet: Während das kommerzielle Internet, Digitaltechnologie und die globale Vernetzung rasant voranschritten, brauchte die Verwaltung stets einige Zeit, das Organisationsmanagement der je neuen Realität anzupassen. Statt Ressorts gänzlich umzuverteilen oder massenhaft Institutionen zu schaffen, dockte man Digitalisierung und Informationssicherheit an Bestehendes, beispielsweise das Verkehrsministerium oder das Ministerium des Innern, an. Teil der Wahrheit ist aber, dass das Digitale jeden Lebensbereich durchdringt, sodass nahezu jede Institution eine betreffende Aufgabe im eigenen Zuständigkeitsbereich

identifizieren konnte. Diese Komposition wird schließlich mit dem Föderalismus addiert, der der Administration von Cybersecurity eine komplexe Längsebene verleiht, in der die Autonomie der Bundesländer sowie ihre Widerspruchsrechte, eigene Verwaltungsstrukturen und ihre regional unterschiedlichen Interessen weitere Zeit und Ressourcen verlangen. Gleichzeitig befördert dieser Umstand aus der Sicht von Laien eine gewisse Verantwortungsdiffusion. Für Endanwender zum Beispiel, die ihre digitale Sicherheit bedroht sehen, ist gegebenenfalls nur mühsam erkennbar, wann sie etwa das BSI, wann den Bundesdatenschutzbeauftragten und wann die lokale Polizei für ihre spezifische Fragestellung ansprechen sollten. Und tatsächlich zeigten die bisherigen Kapitel, dass die Privilegien sehr verteilt sind: So darf der Bundesnachrichtendienst ausländische Kommunikation erfassen, das BSI darf nationale Lageinformationen zusammentragen und aktiv die Bevölkerung warnen, strafrechtlich ermitteln dürfen hingegen nur das Bundeskriminalamt und die Polizeien der Länder. Dieser Vielschichtigkeit versucht man mit dem Nationalen Cyber-Abwehrzentrum Rechnung zu tragen, in dem die bedeutsamen Akteure zusammenkommen. Diese Behelfslösung verbindet zwar die Institutionen miteinander, löst aber nicht die Undurchsichtigkeit des Systems für seine Umwelt.

Die Benennung relevanter, staatlicher Organisationen fällt in den Niederlanden leichter als in Deutschland, da sich die Cybersecurity-Landschaft übersichtlicher präsentiert. Der dezentrale Einheitsstaat organisiert die digitale Sicherheit des Landes aus Den Haag, ohne dabei weiteren föderalistischen Regionalregierungen Rechnung tragen zu müssen. Die Niederlande warten mit überschaubaren Strukturen auf, sodass die Themenfelder sowie die Trennungslinien zwischen den Organisationen selbst für Außenstehende erkennbar bleiben. Diese Einfachheit lässt die Cybersicherheitsinfrastruktur nachvollziehbar erscheinen; zugleich lassen sich Entscheidungen, etwa im Schulwesen, ohne Regionalregierungen schnell in die Breite tragen, da weniger Institutionen und weniger demokratische Gremien zu beteiligen sind. Den Haag kann somit den Ton setzen, die Teilhabe fällt allerdings geringer aus als im Föderalismus.

Seit 2013 spiegelt sich dieser Zentralismus auch im Polizeiwesen wider. Die regionalen Polizeien des europäischen Teils der Niederlande wurden zur Nationale Politie zusammengezogen und sind entsprechend gleichrangig mit NCSC, NCTV und Digital Trust Center Nederland, sodass sich diese Institutionen mit unterschiedlichen

Schwerpunkten um die innere digitale Sicherheit der Niederlande kümmern. In Deutschland entspannt sich ein diffiziles Netz administrativer Zuständigkeiten: Bundesnetzagentur, Bundeskanzleramt, ITZ-Bund, BSI, ZITiS, BKA, das Nationale Cyber-Abwehrzentrum, der BfDI, der Nationale Cyber-Sicherheitsrat, die Agentur für Innovation in der Cybersicherheit sowie diverse Einrichtungen der Bundesländer und beteiligte Ministerien nehmen Funktionen für die innere digitale Sicherheit in Deutschland ein. Die Polizei ist, im Gegensatz zu den Niederlanden, Sache der Bundesländer, sodass sich an genau dieser Stelle ein wesentliches Konfliktfeld der Informationssicherheit in Deutschland ausmachen lässt: Die Trennung der Kompetenzen zwischen Polizeien auf Landesebene und Cyberbehörden auf Bundesebene ist hinderlich, weil sie den Informationsaustausch erschwert und die nötige Geschwindigkeit hemmt. Das BSI etwa muss von Cybercrime betroffene Personen an die Polizei vermitteln, ohne den Vorfall aufnehmen zu dürfen. Die Polizei wiederum kann nicht in jeder lokalen Dienststelle IT-Experten bereithalten, die den Bedarfen der Opfer gerecht werden könnten. Die Niederlande erhöhen ihre Schlagkraft gar auf Kosten der Gewaltenteilung. Seit 2010 bündelt das Justizministerium unter anderem NCSC und Polizei, aber auch die Staatsanwaltschaft, wodurch Strafverfolgung, Ermittlung, Schutz von Infrastrukturen, aber auch Cybersicherheit in einem Ministerium liegen. Damit ist das NCSC deutlich enger mit der Jurisdiktion verknüpft als das BSI.

Naturgemäß sind die untersuchten materiellen Institutionen beider Länder vorwiegend zweckgerichtete Organisationen mit dem Ziel der Verwaltung oder Gestaltung systemischer Komponenten. Sie verarbeiten Prozesse auf der Makro- beziehungsweise Mesoebene, beispielsweise wenn das BSI Cyberangriffe auf Bundesdienste verhindert oder wenn das NCSC Unternehmen Kritischer Infrastruktur mit neuen Mindeststandards belegt. Bei aller Ähnlichkeit offenbart der direkte Vergleich mithilfe der Added Values Unterschiede: Nicht nur, dass die Strukturen in Gänze in Deutschland komplexer sind, oder das BSI über ein Vielfaches an finanziellen Mitteln verfügt im Vergleich mit dem NCSC, sondern auch die Narrationen der staatlichen Institutionen weichen voneinander ab.

	Kapitel	Mikro	Makro	Subjek- tiv	Objektiv	Restaur- ativ	Progre- ssiv	Technik- fokus	Bedien- erfokus	Innen	Außen	Chance	Risiko
DE	Institutionen des Bundes		O		O	O		O		O			O
NL	Staatliche Institutionen		X	X		X		X		X			X

Während sowohl der laufende Betrieb als auch die Gründung von Organisationen in Deutschland von Sachlichkeit geprägt sind und Handeln stets von objektivierbaren Ursachen abgeleitet ist, zeigen sich die Niederländer sichtlich emotionalisierter. Die Schöpfung des NCSC ist eine direkte Reaktion auf einen globalen Zwischenfall. Die Kommunikation der Ämter vollzieht sich überwiegend in Gefahrenbeschreibungen, für die häufig kollektiv verankerte, gravierende Flutszenen auf die digitale Sicherheitslage projiziert werden. Ganze Infrastrukturen und Behörden begründen sich in dieser Furcht vor Wellenschlag und Überschwemmung. Woher kommt an dieser Stelle die Neigung zu Gefahrendiskursen? Der digitalen Vernetzung kommt innerhalb der niederländischen Wissens- und Dienstleistungsökonomie eine fundamentale Rolle zu, sodass die Integrität informationstechnischer Systeme zu einem besonders wertvollen Gut wird. In diese Gemengelage stoßen klimatische Risiken, denen die Niederlande ebenfalls mit digitaler Steuerung ihrer Dammsysteme Herr werden möchten, sowie geopolitische Gefährdungen, etwa durch Gewalt von Drittstaaten, Terrorismus oder aggressive Wirtschaftspolitik. Diesem Druck standzuhalten erfordert einen gesellschaftlichen Wachzustand, den die Niederländer durch Affektion statt durch rationale Erklärungen herzustellen versuchen. Auch in Deutschland unterstreichen BMI und BSI die hohe und entsprechend den Pressemitteilungen zumeist steigende Bedrohungslage, ohne dabei aber expressive Vergleiche oder eingebrannte Imaginaries zu bemühen, sodass eine Emotionalisierung zumeist ausbleibt.

Die gesellschaftlichen Institutionen ergeben ein ähnliches Bild: In beiden Ländern sind lobbyistische Organisationen wesentliche Einflussmöglichkeiten, sodass insbesondere große Wirtschaftsverbände mächtige Stellungen eingenommen und den unmittelbaren Austausch mit dem politischen System teils in Gremien institutionalisiert haben: So formt sich der Nationale Cyber-Sicherheitsrat auch aus Vertretern des Deutschen Industrie- und Handelskammertags (DIHK) oder des Branchenverbands Bitkom. In den Niederlanden hat der Interessenverein Cyberveilig Nederland sogar eine bedeutsame Verbindungsfunktion innerhalb der Sicherheitsarchitektur erhalten, das MKB-Nederland betreibt ein ständiges Büro in Brüssel. Beide politischen Systeme stützen sich auf eine

starke Lobbydurchsetzung zugunsten ökonomischer Institutionen. Weniger intensiv fällt je die Interessenvertretung für Verbraucher und Endanwender aus, die in beiden Ländern nicht aus finanziellen Motiven, sondern in der Regel von staatlicher Seite aufgrund politischer Verantwortung respektive gesetzlicher Aufgaben angeschoben wird.

Auffällig ist, dass vor allem die gesellschaftlichen Organisationen in Deutschland ihre unterschiedlichen Forderungen und Wünsche auf ungleiche Erzählungen von Grundwahrheiten bauen. Während der Bundesverband IT-Mittelstand feststellt, es sei „nicht akzeptabel“, dass „kein Digitalministerium kommt“ und ein solches Ministerium „an allen digitalpolitischen Projekten beteiligt sein und Richtlinienkompetenz besitzen“ sollte, zieht die Stiftung Neue Verantwortung gänzlich andere Schlüsse (Bundesverband IT-Mittelstand e. V. (BITMi) 2021b). Sie sieht in einem solchen Ministerium vielmehr „eine Scheinlösung [...], die uns nicht nur nicht weiterbringt, sondern von den wirklich wichtigen Fragen ablenkt“ (Heumann 2021, 2). Dabei berufen sich beide Redner vage auf strukturelle Herausforderungen, machen aber gegensätzliche Lösungsvorschläge. In einem Konsultationsverfahren des Bundesdatenschutzbeauftragten zu KI in der Strafverfolgung reichte unter anderem der Verein LOAD eine Stellungnahme ein, die eine nicht belegte Auffassung der sicherheitspolitischen Rahmenbedingungen als Tatsachenschilderung vermittelt: „Sie [die Sicherheitsbehörden] tapen nicht im Dunkeln, sondern leben in einem goldenen Zeitalter der Überwachung und abnehmender Kriminalität. Es ist Zeit durch ein Moratorium ein Stoppschild zu setzen“ (LOAD e. V. 2021b). Der Chaos Computer Club ging ähnlich vor als er Mutmaßungen über zukünftig mögliche Szenarien anstellte und diese in einen wahrscheinlich daherkommenden Bedrohungskontext setzte:

Diese Kamera-Systeme [zur Überwachung innerstädtischer Plätze] sollen zwar *noch* keine Gesichtserkennung durchführen, jedoch bieten sie die Grundlage für eine nachträgliche Gesichtserkennung auf dem gesammelten Bildmaterial. [...] Und was die Geheimdienste biometrisch treiben, weiß der Fuchs und werden wir erst irgendwann in der Zukunft in der Zeitung lesen (Chaos Computer Club 2020).

Allein die unscheinbare Ergänzung des Wortes „noch“ impliziert, dass eine Nutzung von Gesichtserkennungssystemen in Zukunft zu erwarten ist und hier ein Orwell'sches Risiko vom Staat ausgehen könnte. Das wiederum trägt das populistische Potenzial in sich, grundsätzliches Misstrauen gegenüber staatlichen Einrichtungen zu wecken und

die Argumente der Gegenseite durch konstruierte Dystopien zu unterminieren, statt sie de facto zu entkräften.

	Kapitel	Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienfokus	Innen	Außen	Chance	Risiko
DE	Institutionen der Gesellschaft		O	O			O		O	O		O	
NL	Institutionen der Gesellschaft		X	X			X		X	X		X	

Unter den gesellschaftlichen Institutionen in Deutschland zeichnet sich eine Tendenz zu emotionalisierender Sprache, teils ohne Benennung einer Faktengrundlage, ab. Ihre niederländischen Entsprechungen kommen in ihrer Kommunikation erkennbar zurückhaltender daher, legen jedoch ebenso unterschiedliche Maßstäbe an Umstände der Cybersicherheit, um subjektive Narrative erzeugen zu können. Die Institutionen nehmen seltener oppositionelle Positionen ein und agieren dem Staat gegenüber weniger offensiv und kritisch. Das liegt unter anderem darin begründet, dass Unternehmen, Staat und Wissenschaft in Forschungszusammenschlüssen kooperieren. Zugleich ist oder war der Staat selbst an vielen Institutionen der Gesellschaft beteiligt und fördert privat-öffentliche Partnerschaften, die – ähnlich dem historischen Poldermodell – für Koalition statt Konflikt sorgen.

Die immateriellen Einrichtungen der Cybersicherheit, also die Gesetze, Strategien und wiederkehrenden Berichte, offenbarten die bislang größten Differenzen beider Länder in der Betrachtungsweise digitaler Sicherheits Herausforderungen. Während die Niederlande tendenziell auf Chancen setzen, versucht die Bundesrepublik einen Sicherheitszustand zu restaurieren, der in dieser Form nie existiert hat. Dabei ist das Vorgehen dem Anschein nach zunächst gleich. Denn egal, ob es sich um das Wet beveiliging netwerk- en informatiesystemen oder das IT-Sicherheitsgesetz handelt: Beide Gesetze legen die Funktion sowie die Aufgaben und Zuständigkeiten der jeweiligen nationalen Cybersecurity-Behörde sowie Kooperationsmechanismen zu Kritischen Infrastrukturen fest, obwohl die Gesetzestitel mehr vermuten lassen. Wbni oder IT-SiG erfassen Cybersicherheit dabei keinesfalls in ihrer juristischen Gänze, sondern überhöhen vielmehr die Relevanz der exekutiven Institutionen. Periodische Novellen des IT-Sicherheitsgesetzes bauen die Schlüsselposition der Behörde seit Jahren stets aus, indem Zuständigkeiten und Handlungsmacht im BSI zentralisiert

werden: Aus dem Kerngeschäft, der Sicherung der Netze des Bundes, erwachsen weitere Kompetenzen, wie zum Beispiel die Absicherung Kritischer Infrastrukturen, der digitale Verbraucherschutz oder die Zertifizierung von Technologien. Eine bemerkenswerte, abrupte Machtzentralisierung fand in den Niederlanden Anfang 2019 mit der Einführung von Computercriminaliteit III statt. Plötzlich können Strafverfolger aufgrund von Verdachtspunkten Sicherheitslücken für Ermittlungszwecke offenhalten, Daten und Geräte beschlagnahmen, in Systeme eindringen und Personen virtuell observieren. Das Gesetz stellt hohe Gefängnisstrafen in Aussicht, wenn insbesondere Minderjährige online belästigt, illegale Daten vervielfältigt oder Personen digital betrogen werden. Die Eerste Kamer des Parlaments fasste den Gesetzesentwurf folgendermaßen zusammen:

Dit wetsvoorstel versterkt [...] de opsporing en vervolging van computercriminaliteit. Hiermee wordt de wetgeving aangepast aan de technologische ontwikkelingen op internet en het gebruik van computers voor communicatie en de verwerking en opslag van gegevens. Ook worden burgers beter beschermd tegen bijvoorbeeld het verleiden van een minderjarige tot ontucht (grooming) of de verspreiding van kinderpornografie en ernstige computercriminaliteit²¹⁹ (Eerste Kamer der Staten-Generaal 2017).

Computercriminaliteit III trage demnach der fortschreitenden Vernetzung und Geschwindigkeit des Internets Rechnung und schütze Bürger, allen voran Jugendliche und Kinder, vor schwerer Cyberkriminalität. Während die erste Intention außer Frage steht und das Gesetz dieser auch nachkommt, geriet zweitens in die Kritik: Da die gesetzliche Regelung vor allem Tätergruppen betrifft, die in und aus den Niederlanden operieren, besteht mit Computercriminaliteit III kaum eine wirksamere Handhabe gegen digitale Straftaten, insbesondere bei jenen gegen Jugendliche und Kinder – solche Delikte werden gehäuft länderübergreifend und standortunabhängig begangen (vgl. Bundeskriminalamt 2022a, 36).

²¹⁹ Deutsch: Dieser Gesetzesentwurf stärkt die Ermittlung und Verfolgung von Computerkriminalität. Dadurch wird die Gesetzgebung an die technologischen Entwicklungen im Internet und die Nutzung von Computern zur Kommunikation sowie zur Verarbeitung und Speicherung von Daten angepasst. Außerdem werden Bürger besser geschützt, beispielsweise gegen den Missbrauch Minderjähriger zur Unzucht (Grooming) oder gegen die Verbreitung von Kinderpornografie wie auch gegen schwere Computerkriminalität.

	Kapitel	Mikro	Makro	Subjek- tiv	Objektiv	Restaur- ativ	Progre- ssiv	Technik- fokus	Bedien- erfokus	Innen	Außen	Chance	Risiko
DE	Cybersicher- heitsstrategie		O	O			O	O		O			O
	IT- Sicherheitsge- setz		O		O	O		O		O			O
NL	Nederlandse Cybersecurity Agenda & NCSS		X	X			X	X		X		X	
	Wet beveiliging netwerk- en informatiesyst emen (Wbni) & Computercrim inaliteit III		X	X			X	X		X			X

Die Niederlande drehen die Schraube staatlicher Bemächtigung zur Absicherung der eigenen Bevölkerung weiter und haben mit Computercriminaliteit III ein Gesetz verabschiedet, das nicht nur symbolische Wirkkraft hat, sondern reale Folgen für die Menschen nach sich ziehen und als repressives Hilfsmittel missbraucht werden könnte.

Jenseits dieses Eingriffes, so demonstriert die Nederlandse Cybersecurity Agenda, nimmt die Regierung eher eine anleitende, weniger eine regulierende Funktion ein. Mit der NCSA setzen die Niederlande liberale Impulse, indem sie an Eigenverantwortung appellieren und staatliche Zuständigkeit, beispielsweise für den Schutz der Endanwender, der Unternehmen ohne besonderes öffentliches Interesse, oder aber für die Zertifizierung von Produkten, ablehnen. Die Regierung sieht hierin die Gelegenheit, einen attraktiven Digitalmarkt zu schaffen und so Kompetenz, Kapital und Unternehmen in den Niederlanden nachhaltig anzusiedeln. In der Gegenüberstellung ist zu bemerken, dass im Rahmen der Added Values gleich mehrere Male die Einschätzung *subjektiv* statt *objektiv* getroffen wurde. Diese Urteile haben mehrere Ursachen. So werden weder in der NCSS noch in der NCSA Bedrohungen konkret benannt und ausformuliert, sondern sie sind in eher abstrakten Bedrohungschiffren dargelegt. Beide Papiere sind zudem zuvorderst Absichtsdokumente, die zwar eine real wirksame Handlungsrichtung erkennen lassen, aber vor allem als politische Resonanzkörper fungieren. Dass die Verhältnismäßigkeit von Computercriminaliteit III nicht uneingeschränkt gegeben ist, belegt ebenso die Entkopplung von messbarer Sachlage und Regierungshandeln. Die deutsche Cybersicherheitsstrategie ruht auf unvalidierten

Hypothesen, die nicht zur Ableitung von elementaren Zielen geeignet sind. Sie bleibt unscharf und überhöht die Möglichkeiten, die die Bundesregierung innerhalb einer Legislatur angehen kann. Lediglich das Wbni lässt auf niederländischer Seite Ableitungen erkennen, die vor allem Auswirkung auf Kritische Infrastrukturen haben und zielbewusste, erkennbare Sicherheitszugewinne realisieren können. Das IT-Sicherheitsgesetz, das seit 2021 in Deutschland wirkt, ist als Adaption an veränderte Aufgabenstellungen ebenfalls ein kohärentes, logisch ableitbares Gesetz, das Sicherheitsinteressen auf Grundlage tatsächlicher Risiken verfolgt – in manchen Augen ungenügend, in anderen zu vehement.

Der jährliche Bericht des BSI *Die Lage der IT-Sicherheit in Deutschland* kommt gerade im Verlauf der Jahre 2019 bis 2021 uneinheitlich daher; sowohl aufgrund der nur wenigen konsekutiven Messgrößen als auch aufgrund der sich fortwährend wandelnden Berichtsstruktur. Diese formale Inkonsistenz verursacht eine lediglich geringe Vergleichbarkeit der diversen Reportjahre, wodurch Hergänge, Besserungen oder Eskalationstendenzen oft unerkennbar bleiben. Gleichzeitig bieten die Berichte jeweils große Datenmengen und Einblicke in die Quantifizierung gewisser Cybersicherheitsbereiche. Das *Cybersecuritybeeld Nederland* wartet hingegen kaum mit Daten auf, sondern enthält Thesen und Äußerungen, die zumeist unbelegt bleiben.

	Kapitel	Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienfokus	Innen	Außen	Chance	Risiko
DE	Lagebericht		O		O		O	O		O			O
NL	CSBN		X	X		X		X			X		X

Dieser unterschiedliche Angang ergibt sich aus differierenden Zielgruppen der Berichte: Während der Lagebericht komplex formuliert, mit Statistiken angereichert und mit Fachtermini gespickt ist und sich somit an Experten, Organisationen und staatliche Institutionen richtet, ist das CSBN einfacher strukturiert, besteht aus leicht verständlichen Botschaften und adressiert mit diesen sowohl Laien als auch außenpolitische Akteure. Der deutsche Bericht nimmt die technische Analyse, wenn auch kuratiert und selektiert, in den Mittelpunkt. Die Niederländer dagegen zielen auf Gefühle ab, indem der Bericht Furcht einflößende Gegenwarts- und Zukunftsszenarien aufstellt, die es abzuwenden gilt. Messungen, Relationen oder Empirie sind merklich nebensächlich. Dazu passt, dass das CSBN restaurativ anmutet. Indem Befürchtungen vordergründig sind, induziert man bei den Lesern den Wunsch, frühere

Sicherheitszustände wiederherzustellen, statt sich eventuell neuen Gegebenheiten anzupassen. Der Lagebericht hat sich im Untersuchungszeitraum stetig angepasst, befindet sich im Wandel und stellt Sicherheitsherausforderungen je mit entsprechenden Reaktionsempfehlungen zusammen, sodass Veränderungen der Lebenswirklichkeit mit individuellen Handlungsrevisionen verbunden zu sein scheinen. Der Lagebericht versteht sich als zahlengebundener, möglichst objektiver Arbeitsnachweis wie auch als Sachstandermittlung. Das CSBN kommt daneben wie eine (außen)politische Kundgabe daher: Man klagt feindselige Staaten unumwunden an, veranschaulicht Gefahrenherde aus dem Ausland und macht deutlich, dass weiterhin große Bemühungen zur Herstellung von Sicherheit nötig seien.

Das Schaubild von Hergig und Rupp vor einigen Seiten bildet die Cybersicherheitsarchitektur Deutschlands auf Organisationenebene nahezu vollständig ab. Der Darstellung und dem Text lag der Anspruch zugrunde, eine möglichst lückenlose Übersicht aufzustellen. Wenngleich die Autoren diesem Ziel gerecht wurden, blieben durch die Methode der Aufzählung andere bedeutende Variablen ungeachtet. So zeigt gerade die eingehende Betrachtung der Zwischenräume, die bei Hergig und Rupp nicht sichtbar sind, charakterisierende Wesenszüge der Cybersicherheitsarchitekturen auf, die Rückschlüsse auf die kovariierenden Imaginationen und Kulturen ermöglichen. Die Analyseergebnisse schlüsseln die wesentlichen Unterschiede zwischen den deutschen und niederländischen Untersuchungsgegenständen innerhalb drei der sechs Binärpaarungen auf: Subjektiv/Objektiv, Restaurativ/Progressiv sowie Chance/Risiko. In Deutschland sortieren sich die Untersuchungsobjekte überwiegend als objektiv ein. IT-Sicherheitsgesetz, Lagebericht sowie die Institutionen des Bundes ruhen mehrheitlich auf einer objektiven Einschätzung der Sicherheitslage, indem sie aufgrund gewisser Parameter ins Leben gerufen wurden oder die Datenlage wiedergeben. Mindestens referenzieren sie auf reliable Kennziffern, sodass die Argumentationskette aus Ursache, Lösungskonzept und Lösungsumsetzung im Regelfall stringent ist. Obschon das Innenministerium auch die Cybersicherheitsstrategie damit einleitet, „auf Basis einer entsprechenden Risikoanalyse“ vorgehen zu wollen, zeigt sich das Papier durchweg als in die Zukunft gerichtetes Leitbild, das keinen Nachweis für diese empirische Grundlage erbringt (Bundesministerium des Innern 2016, 8). Insofern stellen die Cybersicherheitsstrategie und die Institutionen der Gesellschaft, die per se unterschiedliche Inzentive und Erklärungsmuster aufweisen, die subjektiv markierten

Vergleichsgegenstände – inmitten ansonsten zweckmäßig ausformulierter Staatsprodukte. In den Niederlanden zeigt sich ein deutlich anderes Bild, in dem alle beobachteten Dokumente, Einrichtungen und Gesetze eine subjektivierende Unterkonstruktion aufweisen. So lässt sich die Gründung des NCSC in eine direkte Linie mit der Malware Stuxnet stellen. Computercriminaliteit III erlegt den Niederländern ein Gesetz auf, das es Ermittlungsbehörden erlaubt, in den Niederlanden digitale Observationen durchzuführen – unter der Behauptung, die Bevölkerung vor Cyberkriminalität zu schützen. Die Cybersicherheitsagenda von 2018 formuliert zudem mit militärischen Kampfbegriffen wie *Abschreckung* und *offensive Kapazitäten* eine neue Dimension von Cybersicherheit in Europa. Kurz zuvor ereignete sich ein Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OPCW) in Den Haag, 2017 infiltrierten russische Hacker Netzwerke der niederländischen Polizei und 2014 entwickelte sich eine breite Russlandaversion infolge des Abschusses von Flug MH17 (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2018b, 23). Nur diese Beispiele verdeutlichen, dass die Cybersicherheitsarchitektur der Niederlande häufig von externen Parametern und punktuellen, angsterfüllenden Ereignissen restrukturiert wird, die im Rahmen politischer Diskurse die Institutionalisierung von Affekten befeuern. Subjektiv sind die Untersuchungsgegenstände auch, weil sie größtenteils nicht reliabel sind. Selbst das CSBN, also ein jährlich erscheinendes Lagebild, lässt den Tatsachennachweis und damit die leserseitige Nachvollziehbarkeit vermissen. Stattdessen zeigt sich, dass die geschilderten Produkte respektive Institutionen auf Angstnarrative sowie die Vermeidung eines konstruierten Unheils setzen statt IT-Bedrohungen, wie teilweise in Deutschland, über emotionsfreie, logische Handlungsketten zu entmystifizieren. Weil dieses Mittel über die Untersuchungsgegenstände hinweg immer wieder zu beobachten ist, kann angenommen werden, dass es sich um ein wissentlich eingesetztes Motiv, also um ein strategisches Werkzeug, handelt, das in den Niederlanden üblich Verwendung findet.

Blickt man nun auf die Frage, ob eines der beiden Länder eher progressive oder tendenziell restaurative Ansätze verfolgt, sind die Erwartungen, auch aufgrund der historisch erlernten Schablonen schnell verteilt: Die Niederlande sind vermutlich überwiegend vorwärts gewandt, wohingegen die Deutschen langsamer, bürokratischer und konservativer sind. In den betrachteten Added Values dagegen liegen beide Länder quantitativ gleich auf. Während sich in Deutschland Cybersicherheitsstrategie,

Lagebericht und gesellschaftliche Institutionen progressiv zeigen, sind es in den Niederlanden die Nederlandse Cybersecurity Agenda, Computercriminaliteit III wie auch die Institutionen der Gesellschaft. Das Cybersecuritybeeld Nederland sowie die staatlichen Einrichtungen präsentieren sich hingegen bewahrend, zeigen wenig bis keine innovativen Anstöße und versuchen, das analoge Paradigma von Sicherheitsinstitutionen, nämlich einen in der Vergangenheit als sicher wahrgenommenen Zustand wiederherstellen zu wollen, auf die digitale Lebenswelt zu projizieren. Progressiv ist hier erst einmal das konstruierte Imaginary einer voranschreitenden Cybernation, die eine internationale Vorreiterrolle einzunehmen versucht. Die reine Infrastruktur gibt diese Position bislang nicht her – das Mantra-artige Zukunftsbild soll aber tragen und Impulsgeber zur Realisierung dieses Bildes sein; eine Modernisierungspraktik, die den Niederländern beispielsweise aus den Fünfzigerjahren in Erinnerung sein könnte.

In Deutschland sind es das IT-Sicherheitsgesetz und die staatlichen Institutionen, die mehrheitlich als erhaltend und tendenziell reagierend statt gestaltend klassifiziert werden. Die Ursachen, insbesondere für die jeweils konservative Anlage der staatlichen Institutionen, können aufgrund der Untersuchung in unterschiedlichen Spezifika der Cybersicherheitskulturen vermutet werden. In Deutschland scheinen die Gründe auf der Hand zu liegen: Ein gewichtiger Behördenapparat mit vielen Beamten und großen finanziellen Aufwänden neigt dazu, sich selbst zu erhalten und die eigens auferlegte Bürokratie zu exerzieren. Die angesprochene Zuständigkeitskomplexität und der bundesrepublikanische Föderalismus tun ihr übriges, um Progression in einem extrem dynamischen Aufgabenfeld zu behindern. Die Niederlande hingegen verfügen über eine im Grunde gegenteilige Struktur. Das Land und seine Administration sind kompakt, anpassungsfähig und plausibel organisiert. Der Einheitsstaat umfasst nur wenige Behörden mit deutlichem IT-Bezug und gibt Sicherheitskompetenzen, beispielsweise an seine Provinzen, ab. So beweglich und agil dieses System klingt und sicherlich auch sein kann, so limitiert ist es durch diese Kompaktheit.

	Kapitel	Mikro	Makro	Subjektiv	Objektiv	Restaurativ	Progressiv	Technikfokus	Bedienfokus	Innen	Außen	Chance	Risiko
DE	Cybersicherheitsstrategie		O	O			O	O		O			O
	IT-Sicherheitsgesetz		O		O	O		O		O			O
	Lagebericht		O		O		O	O		O			O
	Institutionen des Bundes		O		O	O		O		O			O
	Institutionen der Gesellschaft		O	O			O		O	O		O	
NL	Niederländische Cybersecurity Agenda & NCSS		X	X			X	X		X		X	
	Wet beveiliging netwerk- en informatiesystemen (Wbni) & Computercriminaliteit III		X	X			X	X		X			X
	CSBN		X	X		X		X			X		X
	Staatliche Institutionen		X	X		X		X		X			X
	Institutionen der Gesellschaft		X	X			X		X	X		X	

Neben diesen beiden Added Values-Paarungen gibt es in einer Dritten beachtenswerte Parameter. Beachtenswert nicht, weil die Unterschiede zwischen Deutschland und den Niederlanden auf diesem Gebiet so eklatant wären, sondern weil die Differenzen geringer ausfallen, als eingangs angenommen wurde. In beiden Ländern zeigen sich die gesellschaftlichen Institutionen optimistisch und chancenorientiert, während Gesetze, Lageberichte und staatliche Institutionen zumeist die Bedrohungen in die Mitte ihrer Erzählungen rücken. Ein Unterschied ist zwischen den Cybersicherheitsstrategien beziehungsweise Agenden auszumachen: In der niederländischen Variante erhält der Leser einen Eindruck von einer lohnenswerten Zukunft mit einer weitestgehend sicheren Informationstechnik, in der Bedrohungen entweder nicht mehr nennenswert oder wenigstens kontrollierbar sind. Die niederländischen Papiere forcieren den Eindruck, dass die Niederlande in der Lage wären, Umweltfaktoren auszuklammern und

selbst über ihr künftiges Sicherheitsniveau zu entscheiden. Im deutschen Pendant ist der Ton ein anderer, da die Autoren die strategischen Absichten in einer Erörterung darstellen. Sie zeichnen ein mögliches Positiv der Zukunft, aber nicht ohne dabei stets zu mahnen und die Gefahren voranzustellen. Die Gefahr ist Träger der Erzählung und nicht nur eine notwendige Erwähnung.

Abschließend bietet es sich an, wieder an die primordiale Medienökonomie nach Schröter zu erinnern. Indem man Geld einen Wert zuschreibt, der wiederum die Werthaftigkeit von Waren beziffert, wird deutlich, wie der Wert der Informationssicherheit durch den Bund und die niederländische Regierung bemessen wird. In Deutschland erhielt die Cybersicherheitsbehörde 2021 einen Haushalt in Höhe von 197,2 Millionen Euro, also einen Anteil von 0,04 % des Staatshaushaltes. Das NCSC hingegen musste seine Aufgaben mit etwa 8,7 Millionen Euro meistern, was wiederum 0,0026 % der niederländischen Gesamtausgaben abbildete. Diese in der Gegenüberstellung auffallend ausgiebigere Finanzierung von IT-Sicherheit in Deutschland zeigt sich über alle Ressorts hinweg, beispielsweise in den Bundesministerien der Verteidigung, des Innern, für Bau und Heimat oder für Verkehr und digitale Infrastruktur. Die Niederlande investieren vergleichsweise wenig Geld in ihre oberste IT-Sicherheitsbehörde, setzen zudem mit 170 Menschen im Jahr 2022, wie lediglich einem Interview mit dem damaligen NCSC-directeur Hans de Vries zu entnehmen ist, kaum personelle Ressourcen ein und verfügen damit über eine unterdimensionierte digitale Sicherheitsarchitektur angesichts ihres wirtschaftlichen Gewichts und ihrer außenpolitischen Verwicklungen (vgl. iBestuur.nl 2022). Das wiederum macht es nötig, sich zu spezialisieren und priorisierte Aufgaben wie den Schutz Kritischer Infrastrukturen in den Fokus zu rücken. Das Ordinationsinstrument Geld ist hier nicht nur ein Ausdruck der Dringlichkeit einer staatlichen Aufgabe innerhalb einer politischen Kultur, sondern auch ein Indikator für die Risikoaffinität oder -aversion dieser Kultur. Die niederländische Cybersicherheitsarchitektur ist absolut wie relativ mit signifikant weniger finanziellen wie personellen Mitteln ausgestattet als die deutsche und, der vorausgegangenen Argumentation folgend, damit so konzipiert, mehr Unsicherheit hinzunehmen als ebendiese deutsche.

3 Cybersicherheitskultur in der Praxis

Nach der Aufschlüsselung der formalen Kriterien, der Administrationen und Regeln, die die Informationssicherheit beider Länder bestimmen, richtet sich der Blick nachfolgend auf Geschehnisse, denen sich diese Sicherheitsinstitutionen in der jüngeren Vergangenheit gegenübersehen.

Zuvor lohnt sich ein knapper Exkurs zum wohl ersten Schadprogramm, das weltweit für Aufsehen sorgte und bereits in früheren Kapiteln Erwähnung fand: der Wurm Stuxnet, der sich im Sommer 2010 gegen iranische Atomzentrifugen richtete. Die Schadsoftware wurde auf unzähligen Rechnern auf der ganzen Welt entdeckt, entfaltete seine schädliche Wirkung aber nur bei spezifischen Uranzentrifugen. So sabotierte Stuxnet, dessen Ursprung in den USA oder Israel vermutet wird, das iranische Atomprogramm. Signifikant für genau diesen Wurm ist seine Komplexität, die nahelegt, dass nicht einige wenige Personen hinter dem Angriff standen, sondern dass staatliche Ressourcen nötig waren, um eine derart umfangreiche Hochtechnologie entwickeln zu können (vgl. Hansel 2011, 570). Zudem gilt Stuxnet bis heute als „das erste Beispiel der Substitution konventioneller Waffen durch eine Computernetzwerkattacke“ (Hansel 2011, 565). Jedoch mischte sich der Diskurs rund um diesen Cyberangriff mit Hollywood-ähnlichen Agentennarrativen: Der britische Telegraph beispielsweise berichtete Anfang 2011 von einem möglichen iranischen Tschernobyl (vgl. Telegraph.co.uk 2011). Im selben Monat enthüllte die New York Times, dass Stuxnet in einer geheimen, israelischen Atomanlage ausprobiert worden sei – eine gemeinsame Aktion Israels und der USA, um die iranische Atombombenentwicklung zu sabotieren (vgl. New York Times 2011). Ebenfalls in diesem Zeitraum titelte das Handelsblatt „Die Angst vor dem digitalen Pearl Harbor“ und schrieb im Artikel, dass unter anderem der „scheinbar so glorreiche Sieg der US- und israelischen Experten beim Bau des Schädlingvirus Stuxnet [...] die Phantasie und die Angst“ anheize (Handelsblatt 2011). Die unsichtbare Bedrohung erteilte eine Magie-gleiche Faszination für die Wirkmacht digitaler Geisterbeschwörung. Ihr übriges taten die Adaptionen der Popkultur, zum Beispiel in *Ghost in the Shell: Arise* oder in *Tom Clancy's Splinter Cell: Blacklist*, um Stuxnet als historische, digitale Superwaffe zu bedichten. Die Dokumentation *Zero Days* inszenierte 2016 erneut die Vorgänge rund um den Wurm und fügte die hochkomplexen technischen wie diplomatischen Vorgänge zu einer verdaulichen Erzählung mit dem dramatischen Untertitel *World War 3.0* zusammen.

Augenfällig war in diesem Fall, dass dem Computerprogramm Stuxnet eine menschliche, bewusst handelnde Täterrolle zugeschrieben wurde. 2010 zitierte der Spiegel Wieland Simon, einen Sprecher von Siemens, deren Zentrifugen von Stuxnet betroffen waren. Um die Funktionsweise und die Ziele des Wurms zu erläutern, nutzte Simon Formulierungen, wie „Das Verhaltensmuster von Stuxnet deutet darauf hin [...]“ oder, dass „Stuxnet auf einen speziellen Prozess oder eine Anlage zielt“ (Spiegel.de 2010). Computable.nl sprach dem Wurm ähnlich lebendige Eigenschaften zu: Demnach sei das Programm „zeer geruisloos“²²⁰ und „onzichtbar“²²¹, aber vor allem wisse Stuxnet „wat het wil en waar het is“²²² (Computable 2010). Derartige Diskurse und insbesondere ihre inhärenten Anthropomorphisierungen lassen sich seither auch bei zeitgenössischen Schadprogrammen, Cyberangriffen und Digitaldebatten feststellen; sie sind Attribute ihrer Cybersicherheitskulturen.

Eines der ausgewählten nachfolgenden Phänomene ist eine Schadsoftware, die in der jüngeren Vergangenheit ebenso zu international bedeutsamen Cybervorfällen geführt hat – Emotet. Während dieser Blick die reaktiven Veranlagungen der Sicherheitsarchitekturen in den Mittelpunkt rückt, ergänzt Studie zwei die sich entfaltenden Bilder um präventive Dispositionen, indem sie offenlegt, wie die Niederlande und Deutschland dem neuen Mobilfunkstandard 5G begegnen. Die Betrachtung dieser beiden Fallstudien erlaubt es jeweils, den gegebenenfalls national divergierenden Umgang mit ein und derselben Herausforderung sichtbar zu machen. Fall drei hebt die mitunter verschiedenen Bedingungen hervor, mit denen die Länder je umzugehen haben; dieses Kapitel enthält ihre spezifischen Inszenierungen von Cybersicherheit sowie die Selbstdarstellungen von NCSC und BSI.

3.1 Fallstudie 1: Die Schadsoftware Emotet

In den Jahren 2017 bis 2021 hieß das große Schreckgespenst der Informationstechnik Emotet. Über E-Mail-Anhänge, Makros oder Links nutzt diese Schadsoftware bekannte Sicherheitslücken aus und nistet sich bevorzugt in Windows-Systemen ein. Indem Emotet Zugang zu Outlook und den dort hinterlegten E-Mail-Accounts erlangt, kann sich das Programm selbst per sogenanntem Outlook Harvesting in E-Mails an die Kontaktliste des Opfers versenden. Was Emotet obendrein wesentlich von anderen

²²⁰ Deutsch: sehr geräuschlos

²²¹ Deutsch: unsichtbar

²²² Deutsch: was es will und wo es ist

Schadprogrammen unterscheidet, sind die authentisch wirkenden Mail-Vorlagen, die das Schadprogramm verwendet, um angeschriebene Personen einer kompromittierten Kontaktliste zu täuschen. Da der Absender den Betroffenen bekannt ist und Emotet sich zudem auf vorherige E-Mails und bestehende Kontexte bezieht, ist für Laien kaum erkenntlich, ob sie tatsächlich von einer Kollegin oder von der Schadsoftware kontaktiert werden. Der Inhalt der Mail verleitet dann etwa dazu, den Anhang zu öffnen, weil sich dahinter ein angeblich wichtiges Dokument befindet. Auf diese Weise infiziert Emotet den nächsten Rechner und ganze Netzwerke von Unternehmen, Behörden, aber auch Verbrauchern. Zudem wurde Emotet so angelegt, dass es weitere Schadsoftware, unter anderem Trojaner – bekanntestes Beispiel hierfür ist TrickBot – und Ransomware, nachlädt, um sich Zugang zu Systemen zu verschaffen oder um die betroffenen Rechner nach erfolgtem Zugriff zu verschlüsseln und die Eigentümer zu erpressen. Durch seine Schleuserfunktion verschärft Emotet die Infektion beziehungsweise schneidet es sie auf die Absichten der Täter zu. Insofern vereint Emotet die schlimmsten Eigenschaften von Malware: Das Virus verbreitet sich äußerst schnell und unspezifisch, es ist selbstreplizierend und besitzt große Schadenswirkung. Obendrein handelt es sich bei Emotet um eine polymorphe Schadsoftware, also um ein Programm, das seinen Quelltext unter bestimmten Bedingungen selbsttätig verändert, um beispielsweise Virenskans zu entgehen. Gleichzeitig besitzt die Malware die Abilität, wie ein legales Software-Produkt Updates zu erhalten und sich zu optimieren. Mit diesem Konzept machte Emotet das sogenannte Spear-Phishing, also maßgeschneiderte Phishing-Attacken auf Individuen, massentauglich und wurde gar als Malware-as-a-Service (MaaS) vertrieben.

In den Niederlanden wurden überhaupt nur wenige Betroffene dieser speziellen Form von Cyberangriff öffentlich bekannt. Nicht vonseiten der Unternehmen und ebenso wenig von staatlicher Seite wurden Musterfälle kommuniziert. Diese Strategie liefert den Tätergruppen oder möglichen Nachahmern keinen Anreiz durch mediale Aufmerksamkeit und Unternehmen. Darüber hinaus stehen betroffene Kommunen und Betriebe nicht am Pranger. Das bedeutet zugleich auch, dass Emotet nur geringe Aufmerksamkeit erhält und sein Risikopotenzial weniger bekannt wird. Im Jahr 2019, in dem sich Emotet-Vorfälle massiv häuften, fiel jedoch die Universität Maastricht digitaler Erpressung zum Opfer und zahlte ein Lösegeld in Bitcoin, um den Lehr- und Forschungsbetrieb wiederherstellen zu können. Obwohl die Universität nie explizit

wurde, ist es aufgrund des Infektionsverlaufs und der Konsequenzen sehr wahrscheinlich, dass es sich um Emotet handelte. So schrieb Manuel Atug, Gründer der Arbeitsgruppe Kritische Infrastrukturen, bei Twitter gar von einer „#emotet Welt“, in der die Universität Maastricht „komplett lahmgelegt“ wurde (@Honkhase 2019e, Twitter 25.12.2019, 11:36 Uhr). Auch Matthias Bolte-Richter adressiert in einer Kleinen Anfrage an die Landesregierung NRW Emotet als Ursache für diesen Vorfall (vgl. Bolte-Richter 2020, 1). Eine Web-Publikation von Kaspersky.nl zeigt dagegen, dass gleichzeitig zahlreiche deutsche Geschädigte öffentlich waren, darunter das Klinikum Fürstfeldbruck oder die Stadtverwaltung Frankfurt (vgl. Kaspersky.nl 2020). Daraus lässt sich eine erste Prämisse herstellen: Die Tatsache, dass weniger Angriffsfälle in den Niederlanden publik wurden als in Deutschland, lässt darauf schließen, dass die Aufarbeitung diskreter abläuft als in Deutschland, aber auch dass die Information von mittelbar Betroffenen – beispielsweise von Firmenkunden – weniger häufig erfolgt. Man könnte dagegen konstatieren, die Niederlande seien weniger häufig betroffen, gegebenenfalls ein weniger attraktives oder ein besser geschütztes Angriffsziel. Das Cybersecuritybeeld Nederland 2019 bringt hier erstes Licht ins Dunkel. In diesem Jahr schätzte der Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) Ransomware als abebbende Gefahrenquelle ein. Das CSBN enthielt für den Beobachtungszeitraum März 2018 bis Februar 2019 Überschriften wie „Ransomware lijkt af te nemen“²²³ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2019a, 27). Im vergleichbaren Berichtszeitraum identifiziert der BSI-Lagebericht „eine erneute intensive Ransomware-Kampagne Ende des Jahres 2018 und Anfang 2019. [...] Ransomware stellt nach wie vor eine starke Gefährdung dar und verursacht große Schäden“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 7). Wenngleich Ransomware und Emotet nicht gleichzusetzen sind, ist Emotet doch ein bedeutsames Vehikel zur Verbreitung von Ransomware. Diese Indikation legt nahe, dass Deutschland tatsächlich schwerer betroffen zu sein scheint als die Niederlande, wenngleich exakte Daten hierzu nicht öffentlich sind. 2020 dann warnte die niederländische Regierung wieder vor Emotet, wenn auch unkonkret. Das NCSC ist in seiner Meldung um einen neutralen, beschreibenden Ton bemüht, indem es lediglich die Funktionsweise von Emotet sowie ausgewählte Ratschläge formuliert. „Vanwege de toename in aanvallen adviseert het

²²³ Deutsch: Ransomware scheint abzunehmen.

NCSC om verschillende best practices te volgen, zoals het blokkeren van bepaalde e-mailbijlagen met .dll, .exe, .zip en andere bestandsextensies“²²⁴ (Nationaal Cyber Security Centrum 2020a). Zwar spricht die Behörde von einer Zunahme der entsprechenden Angriffe, benennt aber nicht die tatsächliche Häufigkeit und macht auch keine Angaben darüber, in welchen Bereichen Emotet besonders erfolgreich ist. In den öffentlichen Dokumenten des BSI sind Betroffenenzahlen ebenfalls rar gesät. Das Bundesamt bezeichnet Emotet 2021 konkret als „eine der größten Bedrohungen durch Schadsoftware weltweit“ und schafft so nicht nur eine Kategorisierung der Malware, sondern eröffnet vor allem einen Deutungshorizont, der statt nutzbringender Informationen uferlosen Raum für Spekulationen lässt (Bundesamt für Sicherheit in der Informationstechnik 2021d).

Dagegen macht das deutsche Bundesamt Angaben zu betroffenen Gruppen, wenn es beispielsweise sagt, der „signifikante Anstieg dieser Zahlen im Vergleich zum Vorjahresbericht ist insbesondere auf die hohe Anzahl von Emotet-Wellen zurückzuführen“ (Bundesamt für Sicherheit in der Informationstechnik 2019a, 38). Neben diversen einzelnen Emotet-Fällen, die das BSI im Untersuchungszeitraum deklariert und öffentlich bespricht – etwa im Lagebericht – führt es nicht zuletzt vereinzelt sachbezogene Daten an: „Allein im Jahr 2020 wurden dem BSI aus der Beobachtung von Spam-Bots mehr als 40.000 in Deutschland betriebene E-Mail-Konten bekannt, die durch Emotet kompromittiert worden waren“ (Bundesamt für Sicherheit in der Informationstechnik 2021a, 21). Während die obige Meldung des NCSC als eine von wenigen Veröffentlichungen der Behörde zu Emotet nüchtern anmutet und nur wenige Informationen zur Sicherheitslage preisgibt, zeigt sich auch die niederländische Zweitverwertung bedingt interessiert. Nennenswert ist zu diesem Zeitpunkt bloß KPN, einer der bedeutendsten Mobilfunkbetreiber des Landes, der einen seiner Artikel mit „De beruchte malware Emotet is weer aan een opmars bezig“²²⁵ beginnt und so das wenig attraktive Narrativ einer anhaltenden Bedrohungslage ohne entscheidenden Neuigkeitswert repliziert (kpn 2020). Ebenfalls in dieser Zeit entwirft G DATA, der niederländische Ableger eines deutschen Cybersecurity-Dienstleisters, ein Bild von Emotet als Schweizer Taschenmesser der Internetkriminalität, das zudem „als

²²⁴ Deutsch: Aufgrund der Zunahme von Angriffen empfiehlt das NCSC, verschiedene Best Practices zu befolgen, beispielsweise das Blockieren bestimmter E-Mail-Anhänge mit .dll, .exe, .zip und anderen Dateierweiterungen.

²²⁵ Deutsch: Die berüchtigte Schadsoftware Emotet ist wieder auf dem Vormarsch.

een soort bruggenhoofd op de systemen van geïnfecteerde gebruikers“²²⁶ fungiere (G DATA 2019). Dieser Vergleich, der einige Monate später erneut aufgegriffen wird, gießt die hochkomplexe und instabile Technologie der Malware in die gleichermaßen fassbare wie wirklichkeitsnahe Form des bekannten Multifunktionswerkzeugs. Diese Mechanik simplifiziert Emotet selbstverständlich bis zur Unkenntlichkeit, gibt dem Programm zugleich aber eine Fassung, die die durch Emotet bereiteten Herausforderungen für eine breite Bevölkerung erst feststellbar macht.

Indes überschlagen sich im vergleichbaren Zeitraum die Nachrichten zu Emotet in Deutschland. Im Sommer 2019 gibt das Technikmagazin heise bekannt, dass es selbst Opfer einer Emotet-Angriffskampagne geworden ist. heise nimmt den Vorfall zum Anlass, die Infektion detailliert zu dokumentieren, Fehler im Sicherheitsmanagement einzuräumen und insbesondere die langwierigen und aufwändigen Konsequenzen für die IT-Infrastruktur darzustellen. Auffällig ist, wie heise die Mechaniken der Malware beschreibt. So beginnt Emotet „sofort, sein Unwesen im Heise-Netz zu treiben“ – das Computerprogramm begeht demnach eine verwerfliche Handlung und erhält schließlich eine Kategorie eines moralisch-ethischen Konzepts (heise online 2019b). heise schreibt ferner: „Zum Zeitpunkt X legt Emotet die IT des Opfers komplett lahm und präsentiert eine Lösegeldforderung“ (heise online 2019b). Die Malware, natürlich Werkzeug von Straftätern für kriminelle Handlungen, wird in diesem Erzähltypus selbst zum Antagonisten, der ein gewähltes Opfer malträtiiert und auf seinen Vorteil bedacht ist. heise hypostasiert die schadhaften Codezeilen, indem das Magazin dem Programm menschenähnliches Handeln und Bewusstsein zuschreibt. Der Verfasser des Artikels geht schlussendlich so weit, Emotet zweckbestimmtes, intentionales Verhalten zu attestieren: „Das Ziel von Emotet sind vor allem Firmen, Behörden und andere Institutionen, bei denen Geld zu holen ist. Das von Emotet erfundene Dynamit-Phishing knüpft an existierende Kommunikationsbeziehungen an“ (heise online 2019b). Ihm folgend hat die Malware die Fähigkeit, Mechaniken zu erfinden und in dieser Deutung eine Schwelle zum humanoiden zu überschreiten.

Am 23. August 2019 vermeldet das CERT-Bund, dass eine im Sommer zerschlagene Emotet-Serverinfrastruktur nun wieder aktiv sei (vgl. Twitter.com 2019a). Im November desselben Jahres gibt der Regierende Bürgermeister Berlins Hinweise zum Schutz vor

²²⁶ Deutsch: als eine Art Brückenkopf auf den Systemen infizierter Anwender

Emotet an die Bevölkerung heraus, nachdem das Berliner Kammergericht schon im September wegen Emotet vom Netz genommen werden musste (vgl. Berlin.de 2019). Im Dezember warnt erneut CERT-Bund vor „currently one of the most dangerous botnets in operation“ und verleiht seinem schon deutlichen Hinweis mit dem Ausruf „Don't be the next“ eine hinreichend eindrückliche Dramaturgie (Twitter.com 2019b).



Abbildung 15: Screenshot des Tweets von CERT-Bund (@certbund, vom 16.12.2019, Quelle: Twitter.com 2019b)

„Aufgrund technischer Probleme“ seien die Dienste der Stadt Frankfurt vorübergehend nicht erreichbar, teilt die Verwaltung selbst am 18. Dezember ebenfalls per Twitter mit (Twitter.com 2019c). Tatsächlich, so zeigt sich kurze Zeit später, ist Emotet auch in diesem Fall die Ursache für die Abschaltung der kommunalen Informationstechnik. Am 24. Januar 2020 dann warnt die RWTH Aachen ihre Studierenden (vgl. RWTH Aachen 2020). Das Niedersächsische Landesamt für Bezüge und Versorgung gibt am selben Tag bekannt, bis auf Weiteres nur eingeschränkt per E-Mail erreichbar zu sein (vgl. Niedersächsisches Landesamt für Bezüge und Versorgung 2020). Wiederum drei Tage später publiziert der Tagesspiegel, dass ein mehrere Monate zurückliegender Emotet-Angriff auf das Berliner Kammergericht „schwerer als erwartet“ sei (Tagesspiegel 2020). Unter Bezugnahme auf eine betroffene niedersächsische Stadtverwaltung wiederholt heise im März 2020 die vom damaligen BSI-Präsident Arne Schönbohm etablierte Bezeichnung Emotets als „König der Schadsoftware“ (heise online 2020b). Schönbohm hatte Emotet bereits 2019 bei der Vorstellung des Lageberichts auf dieses Podest erhoben und prägte damit eine auch international häufig verwendete Betitelung. So lässt sich ableiten, dass Emotet in dieser Zeit, sowohl von staatlich-institutioneller Seite als auch von der Medienöffentlichkeit, in Deutschland deutlich mehr Beachtung findet als in den Niederlanden. Einhergehend wird die Malware deutlicher problematisiert, während sie in den Niederlanden überwiegend von Verantwortlichen diskret behandelt und von der Presse analog dazu lediglich wenig interessiert aufgegriffen wird.

Anfang 2021 verändert sich diese Erzählung und Emotet gelangt in das Scheinwerferlicht der niederländischen und internationalen Öffentlichkeit. Mit der internationalen Polizeioperation Ladybird, geleitet von Europol und unter Beteiligung unter anderem der Niederlande, Deutschlands und der Vereinigten Staaten, schließen sich nationale Polizeibehörden zusammen und zerschlagen eine wesentliche Infrastruktur zur Verbreitung der Schadsoftware (vgl. Europol 2021). Ab diesem Zeitpunkt herrscht in den Niederlanden eine Erfolgserzählung vor, obwohl zwei der drei wichtigsten Server der Distributionsinfrastruktur für die weltweite Emotet-Verbreitung lange Zeit auf niederländischem Boden angesiedelt waren (vgl. Politie.nl 2021a). Nach der Veröffentlichung des Ermittlungserfolgs stellen diverse Institutionen den Erfolg von Ladybird und insbesondere die eigene Rolle in diesem Erfolg heraus. Das NCSC proklamiert für sich, die beschlagnahmten Datensätze analysiert und Betroffene informiert zu haben; das Openbaar Ministerie²²⁷ stellt seine anhaltende Beteiligung an der Operation heraus (vgl. Nationaal Cyber Security Centrum 2021b/vgl. Openbaar Ministerie 2021a). Wenige Tage später meldet die niederländische Polizei in einer weiteren Pressemitteilung, dass sie nun Berichte des Vorgehens in Foren und Onlinerräumen von Cyberkriminellen teilt, um dort Abschreckung zu betreiben sowie zu signalisieren, dass die potenziellen Tätergruppen unter Beobachtung stehen (vgl. Politie.nl 2021b). Der Justizminister fügt dem ein weiteres Narrativ hinzu: „Daarbij hebben de politie en het OM mede gebruik gemaakt van de bevoegdheid tot binnendringen in een geautomatiseerd werk. Uiteindelijk is het netwerk overgenomen en is de Emotet-malware gedeactiveerd“²²⁸ (Officielebekendmakingen 2021). Demnach sei der Coup nur möglich gewesen, weil Computercriminaliteit III der Strafverfolgung umfassende Befugnisse einräumt. Das Openbaar Ministerie, das die Nutzung der hackbevoegdheid genehmigen muss, exponiert die Nutzung dieses Ermittlungsinstruments ebenfalls, sodass beide Institutionen das umstrittene Gesetz stützen (vgl. Openbaar Ministerie 2021a). In mehrfacher Hinsicht bietet sich zu diesem Zeitpunkt ein günstiger Anlass zur Schöpfung einer positiven Geschichte: Erstens leisteten die Institutionen der Niederlande einen wesentlichen Anteil, um die diffuse Bedrohung Emotet zu beseitigen. Zweitens waren die Behörden eine zentrale

²²⁷ Deutsch: Staatsanwaltschaft

²²⁸ Deutsch: Dabei haben die Polizei und die Staatsanwaltschaft von der Befugnis Gebrauch gemacht, in automatisierte Werke einzudringen. Letztlich wurde das Netzwerk übernommen und die Schadsoftware Emotet deaktiviert.

Schnittstelle für die Ermittlungen, indem sie die inländischen Server bloßstellten und Computercriminalität III anlegten. Schließlich unterstreicht die gesamte Operation, drittens, dass die etablierten Hackbefugnisse wirken. Daraus ergibt sich eine Gelegenheit, diese öffentlich als entsprechend sinnhaft zu positionieren. So äußert sich Staatsanwalt Martijn Egberts in der folgenden Berichterstattung durchaus anerkennend:

Dit is een van de eerste zaken waar je kan zien waar de hackbevoegdheid van de politie (die deze bevoegdheid sinds maart 2019 heeft, red.) toe kan leiden. Het beschermt honderdduizenden slachtoffers en voorkomt – dat durf ik wel te stellen – honderden miljoenen aan schade²²⁹ (NU.nl 2021).

Auf deutscher Seite zeigt sich das BKA vorrangig für Ladybird verantwortlich und proklamiert in der zugehörigen Pressemitteilung, dass die Operation „auf Initiative von ZIT²³⁰ und BKA in enger Kooperation mit den betroffenen internationalen Strafverfolgungsbehörden durchgeführt worden“ sei (Bundeskriminalamt 2021). In sozialen Medien kommuniziert das BKA den Vorgang sogar als sei es eine rein deutsche Leistung, dass die Server und Strukturen ausgehoben werden konnten: „Das #BKA hat gemeinsam mit der @GStA_FFM_ZIT die Infrastruktur übernommen und zerschlagen“ (Twitter.com 2021a). Noch am selben Tag berichten zahlreiche Medien über die Operation. heise unterstreicht in diesem Zuge insbesondere das Gefahrenpotenzial von Emotet, indem es festhält, die „erstmals 2014 identifizierte Malware legte in sehr zielgerichteten Angriffen immer wieder ganze Firmen lahm und verursachte Schäden in Millionenhöhe“ (heise online 2021c). Die Deutsche Welle verzichtet dagegen auf Personifizierungen und arbeitet heraus, dass das kriminelle Netzwerk hinter der Software zerschlagen wurde (vgl. Deutsche Welle 2021). Der Spiegel spekuliert unterdessen, wer die mutmaßlich russischen Köpfe hinter Emotet sein könnten beziehungsweise, ob sich die Polizeiaktion als nachhaltiger Schlag gegen die Cyberkriminalität erweist (vgl. Spiegel 2021). Daneben greift die Tagesschau um 20 Uhr das Thema auf. Mit Aussagen wie „Deutschen Ermittlern ist mit Kollegen aus sieben Ländern ein bedeutender Schlag gegen organisierte Cyberkriminalität gelungen“ (TC 8.24-8.30) akzentuiert auch die tägliche Nachrichtensendung den Erfolg der Aktion (Tagesschau – tagesschau 20:00 Uhr 2021). Insgesamt erwecken das BKA sowie die berichtende Presse den Eindruck, die Emotet-Infrastruktur sei zerstört und die Gefahr

²²⁹ Deutsch: Dies ist eine der ersten Gelegenheiten, an der Sie sehen können, wohin die Hackbefugnis der Polizei (die diese Befugnis seit März 2019 hat, red.) führen kann. Sie beschützt hunderttausende Opfer und beugt – das wage ich zu behaupten – hunderten Millionen an Schaden vor.

²³⁰ Zentralstelle zur Bekämpfung der Internetkriminalität – Generalstaatsanwaltschaft Frankfurt am Main

gebannt. Der stetig vor Emotet warnende Duktus kehrt sich in eine Siegeserzählung um – das Gute hat das Böse geschlagen. Umso mehr betonen die Artikel, dass etwa der Schaden in betroffenen Ländern bei „rund 2,5 Milliarden US-Dollar (etwa 2,1 Milliarden Euro)“ liege, sodass die Leistung der Polizeien noch bedeutsamer erscheint (vgl. Deutsche Welle 2021).

Im November 2021 dann titeln die Nachrichtenmagazine „Vindingrijke malware Emotet lijkt teruggekeerd“²³¹ (Emerce 2021) oder „Berucht, beroemd, gevreesd, Emotet malware was het allemaal“²³² (Z-CERT 2021). Schließlich berichtet ESET Nederland im Mai 2022, Ableger eines weltweit agierenden Sicherheitsunternehmens, dass Emotet nicht nur seit Ende 2021 zurück sei, sondern dass sich die Malware explosionsartig verbreite. In einer Pressemitteilung erklärt ESET, dass globale Detektionen um 8600 % gestiegen seien, in den Niederlanden immerhin um 3900 % (vgl. ESET Nederland 2022). Seit dieser Nachricht finden sich in den Niederlanden nur vereinzelte Berichte zur Schadsoftware, aus der öffentlichen Hand wurde die Kommunikation zu Emotet nahezu eingestellt. In der deutschen Öffentlichkeit zeigen sich nur sporadische Berichte darüber, dass die Malware wieder genutzt wird, um Schadsoftware zu verbreiten und in Systeme einzudringen. Bemerkenswert ist vor allem eine gemeinsame Presseerklärung von BKA und BSI, nachdem sich das BKA die Erfolgsmeldung im Januar auf die Fahnen geschrieben hatte. Darin warnen Arne Schönbohm und Holger Münch vor Emotet als eine Komponente im Phänomenbereich Cybercrime-as-a-Service (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021d). Die Bedeutung von Ladybird, die Rolle des BKA oder das Schadensvermögen von Emotet bleiben in dieser einzigen öffentlichen Meldung von Sicherheitsbehörden unmittelbar nach der Emotet-Rückkehr unerwähnt. Gleichzeitig sehen sich die Behörden nun mit Vorwürfen konfrontiert, da mit der Aktion im Januar 2021 einherging, dass Opfersysteme auf niederländischer wie auch auf deutscher Seite automatisiert bereinigt wurden, um eine weitere Verbreitung von Emotet zu unterbinden (vgl. Nationaal Coördinator Terrorismebestrijding en Veiligheid 2022c, 33). Netzsicherheit.org nennt den Vorgang „weltweit einmalig und rechtlich mindestens fragwürdig, wenn nicht sogar rechtswidrig“ (Netzsicherheit.org 2021b). Wenige Monate zuvor wurden die deutschen Strafverfolger noch für ihre Beteiligung an Ladybird gewürdigt; inzwischen geraten sie

²³¹ Deutsch: Erfindungsreiche Malware Emotet scheint zurückgekehrt zu sein.

²³² Deutsch: Berühmt, berühmt, gefürchtet, Emotet-Malware war all das.

unter Erklärungsdruck, indem beispielsweise Fragen aus mehreren Fraktionen an den zuständigen Staatssekretär im BMI, Dr. Markus Richter, gestellt werden (vgl. Bundestag 2021b, 11/vgl. Bundestag 2021c, 41). In den Niederlanden bleibt diese Diskussion derweil gänzlich aus, da die Behörden durch Computercriminaliteit III befugt sind und die Empörung bereits bei der Gesetzeseinführung vorgebracht worden war. In einem Interview für eine Reportage zum Emotet-Takedown äußert Marijn Schuurbiers, Mitarbeiter der niederländischen NHTCU, stattdessen: „The dutch police had this new law that we can basically hack into systems. And I think in this investigation this was one of the big advantages that we had“ (TC 8.32-8.43) (Tomorrow Unlocked – How a global police force took down Emotet 2021). Zur gleichen Zeit greift das Blatt AD den von G DATA eingeführten bildlichen Vergleich Emotets mit einem Schweizer Taschenmesser erneut auf. Im Interview fügt der IT-Sicherheitsexperte Dave Maasland eine Begründung hinzu: „Et kann allerlei trukjes“²³³ (TC 0.28-0.33) und verleiht dem Risikopotenzial der Schadsoftware ein Naturell (AD – Zo werkt het beruchte cybervirus Emotet 2021). Daneben spielt diese Form der Nachrichtengestaltung den Sicherheitsbehörden der Niederlande in die Karten, indem sie die nicht greifbare, multifaktorielle Gefahr vereinfacht, konkretisiert und ihr eine gegenständliche Dramaturgie verleiht. Die beteiligten staatlichen Institutionen beider Länder aber stellen ihre Kommunikation nahezu ein, als die Emotet-Infrastruktur Ende 2021 reaktiviert wird und seitdem erneut starke Verbreitung findet. Die Niederländer kehren damit in ihre Strategie aus der Zeit vor Ladybird zurück, indem sie sich äußerst verhalten zeigen. Wider Erwarten nehmen die Deutschen entgegen ihrer vorherigen Herangehensweise eine ähnlich defensive Kommunikationsstellung wie ihre Nachbarn ein und beschränken sich seit Ende 2021 auf reaktive Veröffentlichungen. Zwischen Deutschland und den Niederlanden treten unterschiedliche Kommunikationsstrategien und damit einhergehend auch abweichende Problemlösungsansätze hervor. Während die verantwortlichen Stellen in den Niederlanden bis Anfang 2021 selten über Emotet gesprochen haben, war die Software in den Erzählungen von BSI, BKA und anderen schon seit Jahren eine der größten digitalen Bedrohungen. Erst mit dem Polizeieinsatz Ladybird öffnen sich die niederländischen Behörden und präsentieren, nicht frei von einem gewissen Stolz, ihren kooperativen Erfolg. Wenngleich auch das BKA diesen Sieg für sich einnimmt, ist der Paradigmenwechsel ob der vorangegangenen

²³³ Deutsch: Es beherrscht allerlei Tricks.

Zurückhaltung auf niederländischer Seite augenfällig. Ab diesem Zeitpunkt nehmen die öffentlichen Beiträge der Politie, der Staatsanwaltschaft und des NCSC über die verfügbaren Kanäle zu. Dies zieht wiederum eine ebenfalls intensivierte Berichterstattung der Informationsmedien nach sich.

In der vergleichenden Betrachtung fallen zwei Hilfsmittel ins Auge, derer sich die Institutionen beider Länder, seien sie staatlich oder gesellschaftlich verortet, bedienen. So ist es äußerst geläufig, Emotet zu personifizieren und der Malware individuelle Wesensarten, eine Persönlichkeit und gar absichtsvolles Handeln zu unterstellen. Emotet wird in beiden Ländern zum Anthroponym für einen Antagonisten statt zur Bezeichnung für ein Werkzeug oder eine Waffe. Das zieht zwei Effekte nach sich: Erstens stilisiert diese Rhetorik Emotet zu etwas Bösem, das leichter artikulierbar wird. Diese Simplifizierung begünstigt die Verbreitung angeschlossener Diskurse und macht die behördliche Verfolgung der Software zu einem unvermeidbaren wie auch logischen Schluss. Zweitens nimmt diese Sprachverwendung Verantwortung von den eigentlichen Tätern und überträgt die Rechenschaftspflicht auf die unbelebte Entität Emotet. Ferner lässt sich beiderseits beobachten, dass Metaphern Anwendung finden. In den Niederlanden wird Emotet vereinzelt einem Schweizer Taschenmesser gleichgesetzt. Derart imaginative Stützen können zwar hilfreich sein, um solch komplexe Sachverhalte herunterzubrechen und das Sprechen darüber zu vereinfachen, allerdings bleibt speziell dieses Bild unzulänglich und trägt nur bedingt. Der in Deutschland geprägte Begriff des Königs der Schadsoftware ist nicht weniger unscharf, dagegen aber deutlich eindrucksstärker. Im Gegensatz zum Erstgenannten ist diese Veranschaulichung figurativ; sie ruft Imaginationen hervor, da sie auf erlernten Narrativen und medialen Interpretationen ruht. Nicht zuletzt verleiht dieses Symbolbild, ganz gleich, ob zutreffend oder nicht, der Schadsoftware neben der benannten Vermenschlichung zwingend auch Autorität, indem es Emotet innerhalb einer eigentlich sozialen Rangordnung arrangiert und dort an die Spitze sortiert. Der *König der Schadsoftware* ermöglicht damit interpersonelle Anschlussfähigkeit, die eine beträchtliche Verbreitung des Themas katalysiert – im Übrigen zeichnet der Ausspruch einen würdigen Gegner, den zu besiegen einen umso größeren Triumph bedeutet.

Resümierend wenden die niederländischen Behörden im Zusammenhang mit Emotet beinahe ausschließlich positive Botschaften an, wie die Erfolgsmeldungen der Polizei gegen die technische Infrastruktur hinter der Malware. Dabei sind diese Botschaften

wenig faktenbasiert. Vielmehr setzen die Tatsachen den Rahmen für eine sentimentaffine, monologische Kommunikation über öffentliche Bekanntmachungen. In diesem Kontext ist anzunehmen, dass die weitestgehende Nichtkommunikation der niederländischen Administration zu den Hochzeiten Emotets den Zweck hatte, die Gefährdung gar nicht erst auf die Agenda zu heben, indem man der Schadsoftware weder zu Aufmerksamkeit noch zu Relevanz verhilft. Demgegenüber herrscht in Deutschland eine erschöpfendere Nachrichtenverbreitung vor, da das BSI und andere Institutionen über Jahre hinweg fortwährend über Emotet sowie dessen Bedrohungspotenzial berichteten. Neben der Verbreitung pessimistischer Risikobeschreibungen fügten die Behörden stets auch Fallbeispiele oder Verbreitungsstatistiken an, um ihre Argumentation zu untermauern. Die öffentlichen Institutionen der BRD legen somit eine transparentere, wenngleich nicht weniger intentionale Kommunikationsstrategie an den Tag. Denn dahinter steckt annehmbar die Absicht, anhaltend für die Risiken von Emotet und anderen Schadprogrammen zu sensibilisieren; also Prävention durch Repetition zu betreiben. Gleichwohl kann an dieser Stelle unterstellt werden, dass das BSI, das BKA oder andere beteiligte Organisationen bei dieser Diskursform mit einer gewissen Geltungsintention aufwarten: Wie bereits in den Erläuterungen zur Legitimierung staatlicher Sicherheitspolitik und -institutionen festzustellen war, zwingt der inhärente Legitimierungsautomatismus jede öffentliche Institution, ihr Daseinsrecht stets zu bekräftigen, um ihre Abschaffung zu verhüten.

3.2 Fallstudie 2: Einführung des 5G-Mobilfunkstandards

Wie schon an anderer Stelle erkannt, hält Nick Couldry Medienkulturen für die verdichteten Abdrücke menschlicher Bedürfnisse (vgl. Couldry 2013, 158). Der Umgang mit Medien, mit Technologie, formt die Kultur rund um diese Hilfsmittel. Aus diesem Grund schlägt Couldry für den Kulturvergleich folgerecht vor, unter anderem auf die Etablierungsprozesse neuer Medien in zu vergleichenden Ländern zu achten (vgl. Couldry 2013, 158). Er stellt also zwei Annahmen voran: Erstens geht Couldry davon aus, dass sich Unterschiede bei der Einführung neuer Techniken ausprägen können, obwohl ebendiese Technik unverändert bleibt. Zweitens – und das ist die entscheidende Prämisse – müssen zum Einführungsmoment ähnliche ökonomische, wissenschaftliche oder regulative Ausgangsbedingungen vorliegen, um die

verschiedenen kulturellen Erscheinungsformen mit wiederum kulturellen Ursachen in Verbindung bringen zu können – ganz nach Detlef Jahns *most similar systems design*.

Während diese Dissertation entsteht, drängt mit dem Mobilfunkstandard 5G eine fundamental neue Technologie auf den weltweiten Markt. Obwohl sich 5G anhört wie eine Weiterentwicklung von 4G/LTE, leitet die Funktechnik perspektivisch nicht weniger als eine Revolution der Internetnutzung ein: 5G potenziert nicht nur die Geschwindigkeit der Datenübertragung um ein Vielfaches, sondern ermöglicht aufgrund der verschwindend geringen Latenzen erst Konzepte wie intelligente Städte, autonome Fahrzeuge, ferngesteuerte Medizinroboter oder kabellos vernetzte Industriemaschinen (vgl. Fraunhofer-Institut für Integrierte Schaltungen IIS 2021). Nebenbei könnten für Endanwender Ladezeiten entfallen und Consumer-Anwendungen, beispielsweise die Integration von Augmented Reality in Fernsehübertragungen, in Echtzeit realisiert werden. Zugleich stellen diese Perspektiven lediglich Mutmaßungen dar; die wahrhaftig bevorstehenden Errungenschaften oder Enttäuschungen, die 5G mit sich bringen wird, sind nur hypothetisch zu fassen. Dabei sind der Standard und die Technik bereits verfügbar. Die Vergabe der Mobilfunkfrequenzen oder die Telekommunikationsnormen legen die Staaten im Prozess des Netzausbaus individuell fest. Dadurch bedingt kann das Prozedere zur Installation der Infrastruktur variieren und sich gegebenenfalls auch zu unterschiedlichen Zeitpunkten vollziehen.

Im Falle des 5G-Ausbaus in Deutschland und den Niederlanden sind die national unterschiedlichen Herangehensweisen bestens anhand der um sie kursierenden Diskussionen abzulesen. Denn 5G repräsentiert nicht nur ein technisches Update des bisherigen Mobilfunkstandards, sondern bietet in vielerlei Hinsicht eine Angriffsfläche zum Beispiel für (außen-)politische, moralische oder sicherheitstaxierende Debatten. Der 5G-Diskurs setzte sich aus fünf Partikulardiskussionen zusammen, die multidimensional, parallel und teils radikal geführt werden.

Erstens besteht auf kommunaler Ebene regelmäßig Gesprächsbedarf darüber, wo die erforderlichen zusätzlichen Sendemasten zu errichten sind. Denn obwohl das 5G-Netz leistungsfähiger ist als die bisherigen Netze, ist seine Reichweite geringer. Somit sind deutlich mehr Senderstandorte als bislang nötig, die Räume auf Privatgrundstücken, in der Nähe von Sehenswürdigkeiten oder neben Schulen einnehmen müssen. Die Türme gelten weithin als unansehnlich und angsteinflößend (vgl. Süddeutsche Zeitung 2020). In Wohngebieten ist der Bau solcher Sendemasten daher ein unliebsames Thema.

Kommunen, Städte und Telekommunikationsdienstleister stehen einer kritischen Zivilbevölkerung gegenüber, die die möglichen Nutzeffekte der Technik anzweifelt und stattdessen persönliche Nachteile erkennt.

Unmittelbar an diese Dynamik reiht sich zweitens der Streit über potenzielle Gesundheitsrisiken für die Anwohner. Denn Bedenkensträger schreiben 5G – wenn auch ohne wissenschaftliche Evidenz – gesundheitsschädigende Wirkung aufgrund von Strahlung zu. Die niederländische Initiative Stop5GNL hat in einem offenen Brief im Dezember 2019 ernstliche Befürchtungen verlauten lassen:

Vele toonaangevende en onafhankelijke onderzoeken tonen aan dat langdurige blootstelling aan elektromagnetische straling leidt tot onder andere tumoren in de hersenen en geslachtsdelen, onvruchtbaarheid, verminking van de spermacellen en DNA, diabetes, autisme, leer- en geheugen stoornissen, adhd, depressies en een toename van Alzheimer²³⁴ (Stop5GNL 2019, 3).

Die Technikevolution trifft auf Radiophobie; ein Phänomen, das in dieser Art immer wieder zum Auftakt neuer Technologien auftritt. Denn mit Akzeptanzhemmnissen hatten aufkommende Medien und Technologien seit jeher zu kämpfen. Das Buch musste sich gegen den Vorwurf behaupten, die Menschen zu zerstreuen und zu verwirren. Während tragbare Musikplayer für den Rückzug von Jugendlichen aus ihrer sozialen Umgebung verantwortlich gemacht wurden, waren Videospiele gleich Auslöser von Amokläufen und Suiziden. Technikskepsis und -enthusiasmus sind Komponenten ein und desselben Verhandlungsprozesses neuer Medien – so auch im Fall von 5G. Diesen Streit führen vor allem Wissenschaft und Politik gegen diverse Bevölkerungsgruppen aus verschiedenen Schichten und Lagern, die konkret Angst vor Strahlung, teils aber auch vor Abstraktem, wie zum Beispiel Veränderung, haben. Obwohl verantwortliche Stellen in beiden Ländern feststellen, dass 5G weder mit „signifikanten Änderungen der durchschnittlichen Exposition“ in Verbindung steht noch in Zusammenhang mit Krebserkrankungen zu bringen ist, bleibt die diffuse Skepsis bestehen (Bundesamt für Strahlenschutz 2021, 2f). In den Niederlanden erreicht diese Skepsis ihre vorzeitige Klimax als im April und Mai 2020 29 Mobilfunksendemasten zusammenhanglos in Brand gesetzt werden (vgl. Openbaar Ministerie 2021b). Die Ermittlungsbehörden stellen einen Katalysator fest, der viele dieser Fälle verbindet: Die ermittelten Täter

²³⁴ Deutsch: Viele führende und unabhängige Studien zeigen, dass eine langfristige Exposition gegenüber elektromagnetischer Strahlung zu Tumoren im Gehirn und in den Genitalien, Unfruchtbarkeit, Verstümmelung von Samenzellen und DNA, Diabetes, Autismus, Lern- und Gedächtnisstörungen, ADHS, Depressionen und einer Zunahme von Alzheimer führt.

haben mutmaßlich eine Verbindung zwischen den neuen 5G-Türmen in ihrer Nachbarschaft und der Corona-Pandemie hergestellt; eine Anschauung, die ihr kriminelles Handeln zu rechtfertigen schien. In Deutschland wird diese Verkettung zwar ebenfalls konstruiert, eine derartige Radikalisierung, wie sie etwa auch in Frankreich oder der Schweiz zu beobachten war, bleibt allerdings aus. Die Proteste beschränken sich überwiegend auf Aktionsbündnisse, Bürgerinitiativen oder Parteiagenden, wie beispielsweise jene der in Bayern verwurzelten ÖDP (vgl. ÖDP 2019). Die Strahlenfurcht geht in den Niederlanden so weit, dass die Autoriteit Nucleaire Veiligheid en Stralingsbescherming²³⁵ Warnungen vor mehreren Produkten ausspricht, die vorgeblich vor 5G-Strahlung schützen sollen, jedoch selbst ionisierende Strahlung abgeben – darunter Armbänder, Ketten oder auch Schlafmasken (vgl. AutoriteitNVS 2021).

Demgegenüber steht als Drittes die Verhandlung über jene Regionen, die zuerst von den neuen Fortschrittmöglichkeiten profitieren sollen. In dieser Kontroverse geht es nicht darum, den Netzausbau aufzuhalten; ganz im Gegenteil stammt die Argumentation zumeist aus dem Lager der 5G-Befürworter. Sie identifizieren 5G als Schlüsseltechnologie und fürchten bei einer späteren Netzintegration ihrer Region einen Standortnachteil für ihre lokale Infrastruktur, ihr Unternehmen oder ihre Wettbewerbsfähigkeit. In Europa ist diese Priorisierungsentscheidung zumeist den Providern überlassen, die wiederum nach wirtschaftlichen Kriterien vorgehen. Eine Untersuchung des Beratungsunternehmens Umlaut mit der Branchenzeitschrift Connect zeigt, dass der europäische 5G-Ausbau bis Ende April 2021 zuvorderst von der Schweiz, Großbritannien, den Niederlanden und Deutschland angetrieben wird (vgl. Rügheimer 2021, 76). Diese Länder liegen sowohl bei der Netzabdeckung als auch bei Datenrate und Latenz im internationalen Vergleich weit vorne. Die Ergebnisse legen nahe, dass die neuen Netze überall dort entstehen, wo viele Menschen in Ballungsräumen zusammenleben, der Ausbau also tatsächlich nach Haushalten und weniger nach Fläche voranschreitet. Das Hochgeschwindigkeitsnetz ist dort besonders rentabel, wo es der Ökonomie zu erhöhter Produktivität verhilft und den Netzbetreibern viele Kunden verspricht. So zeigen auch die Karten der großen Mobilfunkanbieter zum 5G-Ausbau in Deutschland und in den Niederlanden, dass das Netz bevorzugt dort wächst, wo der Raum dicht besiedelt ist. Ein genauerer Blick legt eine differenzierte

²³⁵ Deutsch: Behörde für nukleare Sicherheit und Strahlenschutz

Gemengelage frei: In Deutschland entscheiden die Provider zwar selbst über die Standortfrage der Sendemasten, haben aber bei der Ersteigerung der Frequenzen einem Regulativ zugestimmt. So hat die Bundesnetzagentur festgelegt, dass „bis Ende 2022 mindestens 98 % der Haushalte je Bundesland mit mindestens 100Mbit/s“ versorgt sein müssen (Bundesnetzagentur 2018, 2). Angaben zur Flächenabdeckung wurden hingegen nicht festgehalten. Obwohl deutlich dichter besiedelt, verfolgt die niederländische Regierung eine alternative Strategie zur Distribution: „[T]wee jaar na vergunningverlening 98 % van de oppervlakte van elke Nederlandse gemeente moet zijn voorzien van dekking“²³⁶ (Ministerie van Economische Zaken en Klimaat 2019, 19). Diese Regelung zielt darauf ab, auch ländliche Regionen in den Infrastrukturausbau einzubinden. Hinzu kommt, dass die Niederlande die Versteigerung der Frequenzen anders konzipiert als Deutschland: Die Bundesnetzagentur versteigerte am 12. Juni 2019 alle in der BRD vorgesehenen Frequenzen, einschließlich des 3,6 GHz-Bereichs. Zwar sind die in der Zwischenzeit erzielten Geschwindigkeiten des mobilen Netzes sehr vielversprechend, jedoch ist die Abdeckung noch unbefriedigend. Dagegen fand die Versteigerung in den Niederlanden erst am 21. Juli 2020 statt. Eine Woche später gingen bereits die ersten 5G-Verbindungen ans Netz und im Dezember 2020 war dann das 5G-Netz von T-Mobile landesweit verfügbar (vgl. Overalsnelinternet.nl 2020). Die Antithese, die für diesen Geschwindigkeitsunterschied verantwortlich ist, liegt in der Versteigerungsstrategie begründet: Die niederländische Agentschap Telecom hat zunächst die langsameren, niederfrequenten Bereiche veräußert, sodass der Bau der Netze zügig anlaufen konnte. In Kombination mit der Zweijahresfrist für eine Flächendeckung wurden die Provider gezwungen, den Netzausbau unmittelbar voranzutreiben. Erst Jahre später versteigert die Agentschap 3,5 GHz-Frequenzen, die dann ermöglichen, das bis dahin aufgebaute Netz performanter zu gestalten (vgl. Rijksoverheid 2021a). Zum Vergleich: Vodafone brachte in Deutschland bereits 2021 ein 5G-Kernnetz auf dieser Frequenz auf den Markt (vgl. heise online 2021b). Hier stehen sich der Ausbau einer zügig flächendeckenden Mobilfunkstruktur in den Niederlanden und die Konstruktion eines fragmentarischen und schleppend voranschreitenden, aber gleich sehr leistungsfähigen Netzes in Deutschland gegenüber.

²³⁶ Deutsch: 98 % der Fläche jeder niederländischen Gemeinde muss zwei Jahre nach Erteilung der Konzession abgedeckt werden.

Dabei ist es für ein Mobilfunknetz und insbesondere für eine digitalisierte Gesellschaft wichtig, Telekommunikation auch in entlegenen Gegenden noch zuverlässig und schnell zu ermöglichen. Anja Karliczek, damalige Bundesministerin für Bildung und Forschung, fachte im November 2018 ebendiese Diskussion an, noch bevor die Frequenzen versteigert waren. Mit der Aussage „5G ist nicht an jeder Milchkanne notwendig“ setzte sie einen Stimulus zur Empörung und zeigte zugleich das grundlegend verschiedene Verständnis des Telekommunikationsausbaus im Vergleich zu den Niederlanden auf (Frankfurter Allgemeine Zeitung 2018). Die daraus entstandene Benachteiligungsdebatte griff Klischees von deutscher, bürokratischer Langsamkeit genauso auf wie die Angst vor einem wachsenden Rückstand in der Digitalisierung. Diese Diskussion führen Akteure aus vielfältigen Feldern des gesellschaftlichen Lebens mit unterschiedlichsten Motiven: Provider, Bundesnetzagentur, Anwender, ansässige Unternehmen oder Politiker. So entgegneten etwa der Entwicklungsminister Gerd Müller, der Hauptgeschäftsführer des Deutschen Städte- und Gemeindebundes Gerd Landsberg oder der damalige Ministerpräsident von NRW und spätere Kanzlerkandidat Armin Laschet: „Wir brauchen 5G an jeder Milchkanne“ (Berliner Morgenpost 2018).

Wenn auch nur eine Randnotiz innerhalb des übergeordneten Gesamtdiskurses, bestehen viertens bei Umweltschützern große Bedenken gegen 5G. Aufgrund der höheren Datenraten und der exponentiell wachsenden Datenmenge, die der neue Funkstandard mit sich bringt, erwarten Experten eine Zunahme von Datenzentren, Funkmasten, sowie von Technologien wie der Robotik oder künstlicher Intelligenz und damit einen kräftig zunehmenden Energieverbrauch (vgl. e.on 2019). Wenngleich einige Interessengruppen anmerken, dass 5G viele Prozesse, beispielsweise in der Industrie, effizienter und damit energieschonender gestalten kann, suggerieren Studien, dass der Strombedarf der Gesamtinfrastruktur, unter anderem durch den Mehrbedarf an Funktürmen und einhergehende Rebound-Effekte, stark zunehmen könnte. Eine Untersuchung aus der Schweiz legt nahe, dass das neue Funkverfahren zwar vorerst mehr Energie verbrauchen wird als der bisherige Standard, zugleich aber das langfristige Einsparpotenzial „deutlich höher [ist] als die durch die 5G-Netze verursachten Treibhausgasemissionen“ (Bieser et al. 2020, 10). Auch aufgrund dieser Vielschichtigkeit wird diese Diskussion weniger lautstark geführt als die übrigen. Wissenschaftler und Klimaschützer können die Folgen der dichteren Vernetzung nur erahnen, wohingegen die Betreiber der Netze

von der Klimafreundlichkeit ihrer Produkte überzeugt sind und gar damit werben (vgl. kpn 2021, 15).

Im fünften und hier entscheidenden Subdiskurs, dem über die Sicherheit der Technologie, kumulieren nahezu alle zuvor genannten Streitpunkte: So bestimmt der Standort der Masten unter anderem, ob sie gegen physische Manipulation gesichert sind. Die Angst vor übermäßiger Strahlung und ein gewisser Technikfatalismus unterminieren die Akzeptanz der Bevölkerung und setzen die Infrastruktur einer wachsenden Angriffsfläche, beispielsweise für Vandalismus, aus. Nicht zuletzt korreliert die Ausbaugeschwindigkeit des Netzes mit den Hürden, die vor der Errichtung zu überwinden sind, wie die Implementierung von Sicherheitsmechanismen. Die zunehmende Zahl der Funkmasten, das abzusehen dichtere Internet of Things und die zentrale Rolle von 5G für Echtzeitanwendungen machen diese Architektur außerdem besonders reizvoll für konkurrierende Staaten oder Kriminelle. Trotz dieser nachvollziehbaren Angriffsvektoren konzentriert sich die IT-Sicherheitsdebatte in Deutschland wie auch in den Niederlanden weniger auf konkrete Regularien zu Konstruktion und Betrieb der Netze, sondern vielmehr auf die Auswahl der Marktteilnehmer, also derjenigen Unternehmen, die die Komponenten für die Kernnetze und die technische Peripherie produzieren. 2018 begannen die Vereinigten Staaten damit, ausländische, staatlich subventionierte Telekommunikationsanbieter vom Ausbau ihrer Netze auszuschließen (vgl. New York Times 2018). Effektiv betrifft diese Einschränkung weder amerikanische noch europäische Unternehmen, sondern lediglich chinesische Tech-Konzerne wie Huawei oder ZTE. Dieser amerikanische Impuls trat in Europa eine jahrelang anhaltende Diskussion darüber los, ob chinesische Unternehmen tatsächlich ein Risiko für die Sicherheit westlicher Demokratien darstellen könnten oder ob sie unabdingbar für einen zügigen 5G-Ausbau sind. Obwohl bislang keine Belege für chinesische Backdoors oder Abhöraktionen unter Verwendung von chinesischer Hardware gefunden wurden, besteht weiterhin der Verdacht der Spionage. Wenngleich Deutschland zunächst noch an der Zusammenarbeit mit Huawei festhielt, begann ab 2018 eine mehrjährige Phase intensiver Untersuchungen und politischer wie medialer Auseinandersetzungen (vgl. Tagesspiegel 2018). In den Niederlanden war das Framing von Beginn an kritischer. So forderte die regierende Partei VVD noch 2018, dass chinesische Zulieferer gar aus den Kommunikationssystemen der Rettungsdienste und Polizeien ausgeschlossen werden sollten (vgl. Techzine 2018). Der

Telekommunikationsprovider KPN kam im Frühjahr 2019 einem Ausschluss Huawei durch die Regierung zuvor und beschloss proaktiv, den chinesischen Betrieb für den Aufbau der Kernnetze nicht zu berücksichtigen (vgl. Computable 2019). 2021 wurde ein Bericht publik, nach dem Huawei im Jahr 2011 Zugang zu mehreren Millionen Kundendaten über den niederländischen Mobilfunkanbieter Telfort hatte. Dieser Fall sorgte auch international für Aufregung, da er eine der wenigen Gelegenheiten darstellte, Huawei Spionage und Datenschutzverletzungen anhand eines konkreten Fehlverhaltens nachzuweisen (vgl. NOS 2021). Wenige Wochen später kumulierte der Dissens in den Niederlanden im Ausschluss Huawei aus den 5G-Kernnetzen des Landes (vgl. Tweakers.net 2021). Schon zuvor erklärte die Regierung ihre Pläne, die Verpflichtungen von Telekommunikationsanbietern auszuweiten:

Daarnaast regelt de AMvB dat telecomaanbieders bij beschikking de verplichting kan worden opgelegd om in de zogenaamde kritieke onderdelen van hun netwerken uitsluitend gebruik te maken van producten of diensten van anderen dan in die beschikking genoemde partijen. Daarbij geldt dat partijen kunnen worden aangewezen indien bekend is of vermoed kan worden dat zij de intentie hebben om een in Nederland aangeboden telecomnetwerk of -dienst te misbruiken of uit te laten vallen²³⁷ (Rijksoverheid 2020a).

Hinter diesen Ausschlüssen chinesischer Hochtechnologie steht die Befürchtung, die digitale Souveränität des Landes könne nachhaltig Schaden nehmen. Denn der 5G-Ausbau ist vor allem ein Infrastrukturprogramm: Die 3GPP, die Initiative zur Standardisierung von Mobilfunktechnologien, gibt an, dass das 5G-Kernnetz zu Teilen aus bestehenden wie auch aus neuen Komponenten zusammengesetzt sein wird und damit mehr eine Evolution der Architektur bedeutet als einen Austausch des Bestands (vgl. 3GPP 2021). Sollte das Netz mit schadhafter Hardware versehen sein, ist der Rückbau auf einen Status Quo nicht mehr ohne weiteres möglich. In Deutschland wurde Huawei daher bis zum Ende des Untersuchungszeitraums Anfang 2022 nicht vom deutschen 5G-Ausbau ausgeschlossen. Das Unternehmen bezog mehrfach öffentlich Stellung zu den Vorwürfen und streitet bis heute nicht nur alle Vorhaltungen ab, sondern postuliert obendrein, dass ein Ausschluss Huawei die Netzsicherheit gefährde (vgl. Huawei.com 2019). Diese Debatte überstrahlt in beiden Ländern hingegen weitere

²³⁷ Deutsch: Außerdem sieht die Verordnung des Rates vor, dass Telekommunikationsanbieter durch Beschluss angehalten werden können, in den sogenannten kritischen Teilen ihrer Netze nur Produkte oder Dienstleistungen von anderen als den in dieser Entscheidung genannten Parteien zu verwenden. Dabei gilt, dass Beteiligte benannt werden können, wenn bekannt oder vermutet wird, dass sie beabsichtigen, ein in den Niederlanden angebotenes Telekommunikationsnetz oder einen in den Niederlanden angebotenen Dienst zu missbrauchen oder zu sabotieren.

sicherheitsrelevante Aspekte der 5G-Infrastruktur. Öffentlich wird kaum darüber gesprochen, dass 5G eine verbesserte Kryptografie mit sich bringt, dass sich Energiebedarfe verlagern könnten oder dass Sicherheitslücken des Roamings nun geschlossen werden können. Stattdessen setzen die beteiligten Institutionen je eigene Schwerpunkte und divergente Anliegen auf die Agenda.

Die Netzanbieter proklamieren insbesondere die Vorteile des Funknetzes, häufig aber ohne auf die Technik oder mögliche Seiteneffekte einzugehen. Während etwa die Telekom beteuert, „5G revolutioniert den Mobilfunk!“, lässt sich o2 zu der Kernaussage hinreißen: „o2 Telefónica schafft mit 5G mobile Freiheit“ (Telekom.de 2019/Telefonica.de 2020). Auch Industrieunternehmen wie Bosch oder Audi werben damit, 5G inzwischen auf dem eigenen Firmengelände einzusetzen oder in ihren Produkten zu verbauen, um sie vermeintlich sicherer, vernetzter und zukunftsweisender anzupreisen (vgl. Audi 2021). Einen vergleichbaren Ton schlägt auch das Wirtschaftsministerium NRW an, das eine „bessere Versorgung von Schwerstverletzten, größere Sicherheit für Fahrradfahrer oder in Echtzeit optimierte Schweißprozesse“ prognostiziert und das Bundesland zu einem „5G-Innovationslabor“ entwickeln möchte (Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen 2020). Die Vorteile der Technologie werden zumeist an erwarteten Beispielen und Szenarien dargestellt, auch weil die kryptische Abbreviation kaum dazu geeignet ist, eine lebhaftere Vorstellung des neuen Funknetzes zu schaffen. So sind es häufig Exempel aus den Themengebieten Industrie 4.0, teilautonomes Fahren oder Medizin, die sowohl in absehbarer Zeit realistisch anmuten und zudem hinreichend wünschenswert sind (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021e). Diese Zukunftserwartungen teilt unter anderem auch das BSI, wenn es beschreibt, dass es bereits an der Erforschung des 6G-Standards beteiligt sei und die Absicherung zukünftiger Funktechnologien begleite (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021f). Um auch kritische Stimmen zu Wort kommen zu lassen, hat die Bundesregierung die Dialoginitiative *Deutschland spricht über 5G* ins Leben gerufen. Das Ministerium für Digitales und Verkehr, die Bundesnetzagentur, das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz sowie das Bundesamt für Strahlenschutz gehen in ihrer Onlinekampagne auf Sorgen und Fragen der Bürger ein. Dort sprechen sie Themen wie Umwelt, Gesundheit, Technik oder Datenschutz und -sicherheit an, um Skepsis zu

nehmen und auch Fehlinformationen vorzubeugen (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2019).

Niederländische Netzbetreiber entwerfen ganz ähnliche Imaginationen der Zukunft: „Met het 5G-netwerk kunnen we met meer mensen tegelijk nóg sneller en soepeler muziek downloaden, films streamen en gamen in de cloud via onze smartphones“²³⁸, führt etwa KPN aus (kpn 2019). Das Unternehmen beginnt hier mit eher urbanen Bedürfnissen und fährt fort, indem es stereotype Interessen der Landbevölkerung adressiert: „Hoe preciezer een boer zijn planten kan bespuiten, hoe minder beschermingsmiddel nodig is. Schonere groenten en fruit dankzij gerichte bestrijding met een drone: het kan met 5G“²³⁹ (kpn 2019). Hier konterkariert der Netzanbieter den deutschen Diskurs um einen Mobilfunk, der nicht an jeder Milchkanne obligatorisch verfügbar sein muss – ein Indiz dafür, dass Netzbreite vor Netzgeschwindigkeit geht. Zusätzlich erhielt 2018 im *Actieplan Digitale Connectiviteit*²⁴⁰ der Punkt *Innovatie* eine wesentliche Bedeutung, da das zuständige Ministerie van Economische Zaken en Klimaat davon ausging, dass 5G „innovaties in maatschappelijke domeinen en economische sectoren mogelijk maakt, opdat de Nederlandse economie en samenleving maximaal kunnen profiteren van de digitalisering“²⁴¹ (Ministerie van Economische Zaken en Klimaat 2018, 41). Aus diesem Grund ermunterte die Staatsführung Wirtschafts- und Wissenschaftseinrichtungen, durch Förderprogramme mit 5G und Konnektivität zu experimentieren (vgl. Ministerie van Economische Zaken en Klimaat 2018, 39ff). So etablierte die nationale Regierung Hilfestellungen zur überregionalen Vernetzung relevanter Akteure der Funktechnologie. Das Ministerium errichtete ein Innovationsnetzwerk sowie eine Zusammenarbeit mit der Vereniging van Nederlandse Gemeenten (vgl. Ministerie van Economische Zaken en Klimaat 2018, 42). Das VNG wurde zugleich Ansprechpartner für Telekommunikationsanbieter und Gemeindeverwaltungen; es ermöglichte so obendrein der Staatsadministration, direkt Einfluss auf kommunale Angelegenheit zu nehmen – während die Ausgestaltung der

²³⁸ Deutsch: Mit dem 5G-Netz können wir über unsere Smartphones mit mehr Menschen zugleich noch schneller und reibungsloser Musik herunterladen, Filme streamen und Videospiele in der Cloud spielen.

²³⁹ Deutsch: Je präziser ein Landwirt seine Pflanzen besprühen kann, desto weniger Schutzausrüstung ist erforderlich. Saubereres Gemüse und Obst dank gezielter Steuerung mit einer Drohne: Mit 5G ist das möglich.

²⁴⁰ Deutsch: Aktionsplan digitale Konnektivität.

²⁴¹ Deutsch: Innovationen in sozialen Bereichen und Wirtschaftssektoren ermöglicht, sodass die niederländische Wirtschaft und das Zusammenleben maximal von der Digitalisierung profitieren können.

Ausbauförderung in Deutschland zwischen Bund und Ländern segmentiert ist. Neben jenen Innovationen, die unmittelbar ökonomisch verwertbar und für eine Dienstleistungs- und Wissensgesellschaft substanziell sind, versprach das niederländische Wirtschaftsministerium bereits 2018, zeitnah auch „5G-steden“²⁴² in den Niederlanden aufzubauen und zu subventionieren (Ministerie van Economische Zaken en Klimaat 2018, 39). Zu den Testfeldern gehören unter anderem Groningen, Amsterdam und Enschede. Anne Katrin Bohle, Staatssekretärin im BMI, rief zwei Jahre später zu Ähnlichem auf als das Ministerium ein weiteres Jahr des Förderprojekts Smart Cities verabschiedete: „Wir wollen unsere Kommunen dazu ermutigen, Neues zu wagen, und die Chancen der Digitalisierung zu nutzen“ (Bundesministerium des Innern, für Bau und Heimat 2020b).

An diesen Formulierungen fällt auf, dass 5G als Schlagwort mitsamt seiner zugehörigen Technologien und Zukunftsversprechen sowohl in den Niederlanden als auch in Deutschland eine merkliche Überhöhung erfährt. Die Idealisierung ist auf beiden Seiten ein gebräuchliches Stilmittel, um die Debatten anzuleiten. Gleichwohl scheinen die Diskursführer auf diese Weise jeweils Echokammern auszubilden, die die Argumentation zwar anschieben, aber keinen Umweltkonsens jenseits ihres Systems herbeiführen. Während die Institutionen der Staaten, Unternehmen und Technikenthusiasten die Nutzeffekte von 5G überhöhen und die Technologie teils als Heilsbringer für fehlerhafte Strukturen wie den Straßenverkehr oder das Internet of Things betrachten, werden Bedenkensträger nicht selten als Verschwörungstheoretiker oder „5G-Rebellen“ abgetan (Deutschlandfunk Kultur 2020). Zwar untersuchen die Rijksinspectie Digitale Infrastructuur sowie das Bundesamt für Strahlenschutz die Strahlenemissionen von 5G-Technologie; dem weit verbreiteten Imaginary eines nunmehr um sich greifenden Strahlungsrisikos können die Regierungen mit wissenschaftlichen Erkenntnissen bislang kaum beikommen.

In Fragen der nationalen Informationssicherheit führte das Misstrauen gegen potenziell regimenahe Zulieferer zu tatsächlichem Handeln. Während in den Niederlanden chinesische Komponenten seit 2019 sukzessive und im Jahr 2021 endgültig aus den niederländischen 5G-Netzen ausgeschlossen werden, suchen deutsche Behörden bis 2022 weiter nach Ausschlussgründen, um diese auch politisch getriebene Anforderung

²⁴² Deutsch: 5G-Städte

schließlich tatsachenbasiert durchsetzen zu können. An diesem prominenten Beispiel zeigen sich reale Unterschiede im Umgang mit 5G, vor allem aber mit Sicherheitsherausforderungen. Denn die Niederlande folgen einer, im direkten Vergleich zu Deutschland, populistischeren, weniger sachbezogenen Handlungsweise, die sich beispielsweise in schnellen Entscheidungen und hoher Adaptionfähigkeit äußert. Der 5G-Ausbau verläuft zügig und es herrscht eine klare, für die Bevölkerung nachvollziehbare Priorisierung vor: Zuerst treibt die Regierung den Netzausbau an, anschließend erhöht sie die Leistungsfähigkeit der Infrastruktur. Davon lassen sich die Niederländer auch nicht durch den Huawei-Diskurs abbringen; eine in den USA geformte Debatte über einen chinesischen Tech-Konzern. Das frühe Durchgreifen gegen Huawei ist sogleich eine Sicherheitsmaßnahme wie auch die Botschaft nach innen, dass der Ausbau nicht durch äußere Kräfte zu bremsen ist. Die Niederlande unterstreichen hierdurch erneut, wo ihre Prioritäten liegen: Die nationale Souveränität, damit auch die digitale Unabhängigkeit, ist ein so hohes Gut, dass die Entscheider bereit sind, mögliche Fehlurteile im Zuge der Handlungsschnelligkeit in Kauf zu nehmen. Deutsche Regierungsstellen zeigen sich zögerlicher, wenn es um den Ausschluss eines chinesischen Wettbewerbers geht. Die Verurteilung Huaweis infolge internationaler, politischer Konflikte bei mangelnder Beweislast gilt als so große Hypothek, dass stattdessen ein verlangsamer Netzausbau zu erdulden ist. In diesem Fall folgen deutsche Verantwortliche der Maxime, ausschließlich anhand korrekter, sachgeleiteter Nachweise Entscheidungen zu treffen. Dieses Vorgehen hemmt den Deutschen Netzausbau, dessen Augenmerk ohnehin nicht auf Geschwindigkeit, sondern auf der Leistungsfähigkeit der Infrastruktur liegt. Gewissermaßen stehen sich die opportunistische Adaptivitätsfähigkeit der Niederlande und die sachbetonte Technokratie Deutschlands antithetisch gegenüber. Zu diesen offenkundig sicherheitspolitischen Unterschieden addiert sich in beiden Staaten eine markante Ausprägung einer utopischen 5G-Anschauung, neben der kritische Stimmen nur wenig Platz haben. 5G ist gewissermaßen mit einem Erlösernarrativ behaftet, wonach die Technologie nicht weniger als das autonome Fahren, eklatante Fortschritte in der Medizin oder eine neue Zeit ökonomischer Hegemonie verheißt. Hierin liegt jedoch eine inhärente Sicherheitslücke, da das Streben nach diesem Zukunftsbild die Sicht für Risiken verstellen kann. So bedeutet ein mehr an Funktürmen auch ein mehr an physischen Angriffspunkten; ein mehr an Vernetzung induziert schwerere Schäden bei unbefugtem Zugriff; und schließlich führt die Auslagerung bisher menschlicher Arbeit

auf 5G-vernetzte Maschinen, wie dem Autofahren oder medizinischer Chirurgie, zu größerer Unmündigkeit und Determiniertheit. Diese Anfälligkeiten haben im öffentlichen Diskurs sowohl in den Niederlanden als auch in Deutschland keinen Raum.

Stattdessen bestätigt die vorliegende Betrachtung die in der Zusammenschau der Institutionenanalyse (siehe 2.7) getroffene Beurteilung, dass der Gefahrendiskurs unter staatlichen Institutionen der Niederlande prädominant ist, während die deutsche Administration und Öffentlichkeit zu Normalisierungsdiskursen neigen. Die Bundesnetzagentur, das Bundesinnenministerium sowie die Bundesregierung treten als stoischer Bürokratieapparat auf, der Wettbewerberausschlüsse nur nach langwährender, intensiver Prüfung in Betracht zieht. Bis dahin sind die Publikationen öffentlicher Stellen darauf bedacht, einen Kontrollzustand zu insinuieren; wenngleich dieser womöglich darauf beruht, dass Sicherheitsrisiken bislang entweder nicht erfolgreich ausgenutzt oder nicht entdeckt wurden. Ob es um mutmaßliche Strahlung, den Verdacht ausländischer Spionagetätigkeiten oder um die Furcht vor langfristigen Umweltschäden geht – deutsche Institutionen begreifen sich in diesen Zusammenhängen als deeskalierende Diskursteilnehmer, die zwar durch ihre dogmatische Verlässlichkeit vermitteln, sich von Fakten leiten zu lassen, dafür aber wesentlich an Geschwindigkeit einbüßen. Demgegenüber fassen ihre niederländischen Pendants die Gefahr ins Auge und vertrauen auf Entschlussfreude und Schnelligkeit, um Bedrohungen zuvorzukommen. Dabei besteht das Risiko, dass sich staatliche Einrichtungen zu Entschlüssen durch die Lautstärke gesellschaftlicher Auseinandersetzungen oder durch eine publikative Agenda treiben lassen und so gegebenenfalls zu einer Fehleinschätzung gelangen.

Dieser strategische Unterschied hat eine reelle Konsequenz für die breite Rezeption von 5G- und verwandten Sicherheitsdiskursen: Der niederländisch-risikozentristische Angang betrachtet das drohende Unheil, indem Gut und Böse deutlich konturiert sowie ideologisiert sind; und leistet damit affektgeleiteten Urteilsfindungen Vorschub. Zugleich haftet der Infrastruktur mit diesem Verbot an, dass sie grundsätzlich von Fremdstaaten zu kompromittieren und so stetig zu schützen ist. Währenddessen ist der vermeintlich kontrollierbare Zustand der deutschen Sicherheitsaushandlung ein beruhigendes Scheinbild, bei dem der Staat suggeriert, das die Technologie sicher ist, bis eine Aggression oder ein Eindringen nachgewiesen werden kann. Indem Herausforderungen wissenschaftlich und administrativ zu lösen sind, sind schnelle

Angriffe oder solche, die kaum nachweisbar sind, persistent im Vorteil. Damit ist anzunehmen, dass das 5G-Netz zwar vergleichsweise als weniger anfällig wahrgenommen wird, zugleich aber auch das Sensitivitätsniveau für mögliche Attacken niedriger ist.

3.3 Fallstudie 3: BSI und NCSC inszenieren Cybersicherheit

Für eine letzte Inspektion ist eine Prämisse vorzuschicken, die sich immer wieder im Laufe dieser Arbeit deutlich gezeigt hat: Die Sicherheitslage im Digitalraum und die Cybersicherheitsinstitutionen bedingen einander. Die Behörden begründen ihre Existenz in der anhaltenden Bedrohungslage; gleichzeitig wirken sie auf die Sicherheitsvolatilität ein. Diese Wirkung erzielen etwa das NCSC und das BSI nicht allein durch ihre Detektions- und Reaktionsfähigkeiten, sondern auch indem sie Cybergefahren öffentlich thematisieren, indem sie publizieren, berichten, Content produzieren und indem sie aufklären. Dabei sind diese Einrichtungen unweigerlich Inszenatoren der Informationssicherheit. Denn sie reichern ihre datenbasierte Arbeit mit Botschaften, Absichten und Meinungen an, die ein extensives Bild von Freund und Feind, von Sicherheitsverhältnissen und von möglichen Zukunftsperspektiven geben. Beide Institutionen betreiben Webseiten, veröffentlichen Jahresberichte oder Pressemitteilungen und sind in den sozialen Medien aktiv. Auf diese Weise arrangieren BSI und NCSC Cybersecurity und sind damit wichtige Stimmen und sogar Meinungsbildner für digitale Sicherheitsdiskurse.

Als offensichtliches Instrument ihrer Außenwirkung haben sowohl das NCSC als auch das BSI einen Leitsatz definiert, der die wesentlichen Merkmale und Absichten der Behörden zusammenschnüren soll. Der heute geltende Leitsatz des NCSC enthält eine dramatische Note: „Wij zijn het Nationaal Cyber Security Centrum. De digitale infrastructuur is van levensbelang: voor het betalingsverkeer, voor schoon water uit de kraan en om droge voeten te houden“²⁴³ (Nationaal Cyber Security Centrum 2022a). Die niederländische Behörde verschreibt sich vorrangig dem Schutz vitaler Infrastrukturen und betont unter anderem die Bedeutung der nationalen Hochwasserschutzsysteme. Damit verknüpft das NCSC die Immunität ihrer virtuellen Netze mit existenziellen, physischen Abwehrkräften. Die Botschaft des NCSC lautet: Cybersicherheit ist

²⁴³ Deutsch: Wir sind das Nationale Zentrum für Cybersicherheit. Die digitale Infrastruktur ist lebensnotwendig: für den Zahlungsverkehr, für sauberes Leitungswasser und für trockene Füße.

essenziell, um beispielsweise die Dammanlagen entlang der niederländischen Küsten zu schützen und ist damit auch von fundamentaler Bedeutung, um die Lebensgrundlage der Bevölkerung aufrechtzuerhalten. Mehr noch ist Informationssicherheit nach dieser Lesart die Voraussetzung, damit Bedrohungen wie Stuxnet oder Emotet den Menschen den Zugang zu Trinkwasser, Lebensmittelversorgung und Gesundheitsdiensten nicht abschneiden können – das NCSC erhebt sich damit zu einer Herz-Lungen-Maschine der modernen Zivilgesellschaft. Der Leitsatz des BSI ist dagegen prosaisch ausformulieren: „Das BSI als die Cybersicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft“ (Bundesamt für Sicherheit in der Informationstechnik 2022a). Die Devise ist begrifflich formuliert und gibt nur wenige Botschaften an die Hand. Offenbar ist es der Behörde elementar wichtig, ihre Schlüsselrolle für Belange der Cybersicherheit herauszuarbeiten. Um diesen Anspruch zu verdeutlichen, setzt das BSI auf die technokratischen Termini Prävention, Detektion und Reaktion. Wenngleich für den Leser nicht gleich deutlich wird, welche Tätigkeiten daraus folgen, unterstreichen die Verfasser so, dass das Handeln der Behörde über die reine Abwehr von IT-Angriffen und -Vorfällen hinausgeht. So allumfassend die Aktivitäten des BSI erscheinen, so holistisch skizziert der Leitsatz auch den Adressatenkreis. Diese Zielsetzung scheint damit nur bedingt mit der Größe der Behörde und ihren finanziellen wie regulativen Mitteln in Einklang zu stehen.

Passend zu diesen Ambitionen hat das BSI einen Claim entwickelt, der als Logo auf der Webseite und weiteren Publikationen prangt und den Gedanken kondensiert: *Deutschland. Digital. Sicher. BSI.* Gleichsam haben die Niederländer ein Credo gestaltet, das sehr große Ähnlichkeit aufweist, obwohl die Zuständigkeiten des NCSC deutlich enger gefasst sind: *Nederland digitaal veilig*²⁴⁴. Das NCSC vermittelt ebenso wie das BSI, gesamtverantwortlich für die digitale Sicherheit des Landes zu sein. Das überhöht nicht nur die Befähigung der Behörde, sondern spiegelt erneut die Dimension, die die Niederlande dem Schutz ihrer kritischen Infrastruktur beimessen.

Unter seinem Leitbild präsentiert das BSI darüber hinaus ein Imagevideo, das gleichermaßen auf die Erzählung seiner existenziellen Wichtigkeit einzahlt. Wiederholt

²⁴⁴ Deutsch: Niederlande digital sicher.

fragt die Off-Stimme, wie die Zuschauenden leben möchten, beispielsweise ob sie mobil, hilfsbereit, vernetzt oder schlau sein wollen.



Abbildung 16: Videospot *Digital leben* (Bundesamt für Sicherheit in der Informationstechnik 2022a)

Für all dies, so erzählt das Video, sei Digitalität die Basis. Der aufwändige Film stellt durchweg tendenziöse Fragen, auf die die Zusehenden zu großem Teil übereinstimmend antworten würden, um mit der Nahelegung zu schließen, dass die Arbeit des BSI für Informationssicherheit diese digitale Freiheit erst ermöglicht. Letztlich endet der Sprecher: „Deswegen kümmern wir uns um Deutschlands digitale Sicherheit“ (TC 1.17-1.21) und lässt das Publikum mit dem Gedanken zurück, dass das BSI als alleinige Institution, wenn auch unter Mitwirkung der Nutzenden, dafür Sorge trägt, dass diese Möglichkeiten erhalten bleiben und die User die Vorzüge der Digitalisierung ausschöpfen können (YouTube: Bundesamt für Sicherheit in der Informationstechnik – @bsi_bund 2021b).

Diese Verantwortlichkeitskonzentration des BSI findet sich in der Onlinepräsenz wieder. Die Webseite stellt neben aktuellen Mitteilungen, Pressemeldungen oder Sicherheitswarnungen eigene Seitenbereiche für die Zielgruppen „Staat und Verwaltung“, „Unternehmen und Organisationen“ sowie „Verbraucherinnen und Verbraucher“ bereit (Bundesamt für Sicherheit in der Informationstechnik 2022b). Staatlichen Akteuren liefert das BSI hier Informationen zu Dienstleistungen wie der Sicherheitsberatung und gibt obendrein Empfehlungen zum Umgang mit gegenwärtigen Technologien oder Leitfäden heraus, etwa zur IT-Sicherheit von Kandidierenden und Mandatsträgern bei demokratischen Wahlen. Für Verbraucher stellt das BSI eine

Landingpage zur Verfügung, hinter der sich ein breites Angebot befindet: Dazu gehören Informations- und Empfehlungsartikel für diverse Subzielgruppen, darunter Gamer, Eltern oder Reisende. Im zweiwöchentlich erscheinenden Newsletter *sicher informiert* greifen die Autoren je etwa ein dutzend anwenderrelevante Neuigkeiten der vergangenen 14 Tage für mehr als 200.000 Lesende auf. Darüber hinaus haben Interessierte die Möglichkeit, sogenannte Bürger-CERT-Sicherheitshinweise per RSS-Feed zu abonnieren und so neueste Warnungen und Hinweise unmittelbar bei Bekanntwerden zu erhalten. Für Podcasthörer hält das Amt mit *Update verfügbar* ein Talk-Format auf den bekannten Plattformen bereit, in dem seit 2020 monatlich beispielsweise Schadsoftware, Onlinebetrug oder digitale Alltagsprobleme der Hörer zur Sprache kommen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2020c).



Abbildung 17: Webseite [bsi.bund.de/VerbraucherInnen](https://www.bsi.bund.de/VerbraucherInnen) am 02. Februar 2022 (Bundesamt für Sicherheit in der Informationstechnik 2022c)

Für den Fall, dass Besucher Anliegen haben, die das Spektrum der Seite nicht abbildet, hat die Cyberbehörde ein Servicecenter eingerichtet. Dort bilden Mitarbeitende einen Rückkopplungskanal in das BSI, durch den Interessierte etwa ihre Fragen an Experten richten oder Kritik an den öffentlichen Produkten äußern können.

Das Angebot für Unternehmen und Organisationen fällt ebenso umfangreich aus: Neben Informationen zu 5G, Quantencomputing oder zu industriellen Steuerungssystemen, präsentiert das BSI auch hier stets Hilfestellungen und Gegenmaßnahmen, mit denen sich die Betriebe eigenhändig schützen können. Gleichfalls für diese Klientel unterhält

das BSI mit CYBERSNACS einen spezifischen Podcast, der sich insbesondere an Entscheidungsträger und IT-Verantwortliche im unternehmerischen Zusammenhang wendet. Additiv sind die Zertifizierungsangebote sowie die Allianz für Cyber-Sicherheit zu erwähnen. Das BSI entwickelt dazu unter anderem technische Richtlinien, die die sachgerechte Nutzung und Gestaltung eines IT-Produkts festschreiben. Wenn ein Unternehmen oder ein Dienst eine Zertifizierung in Anspruch nimmt, muss es diesen Richtlinien nachkommen und einen aufwändigen Prüfungsprozess durchlaufen. Die Zertifizierung „bestätigt, dass eine Produktversion bestimmte funktionale und Sicherheitseigenschaften erfüllt“ und kann entsprechend für werbliche Zwecke und einen gewissen Wettbewerbsvorteil verwendet werden, um das IT-Sicherheitsniveau langfristig strukturell anzuheben (Bundesamt für Sicherheit in der Informationstechnik 2022d). Nicht zuletzt unterhält das BSI mit der Allianz für Cyber-Sicherheit eine Public-Private-Partnerschaft, die durch regelmäßige Webtalks, Initiativen, Erfahrungskreise und Vernetzungsevents Wissensaustausch zwischen Unternehmen und Behörden herzustellen versucht. Neben der Verbindung der etwa 5400 Mitglieder²⁴⁵ der Netzwerkplattform dient die ACS dazu, Bedrohungsinformationen vertrauensvoll und effizient an die zuständigen Stellen der Unternehmen zu übermitteln (vgl. Allianz für Cyber-Sicherheit 2022).

Der Auftritt des NCSC fällt erkennbar knapper aus. Die Webseite enthält keine Inhalte, die sich explizit an Privatanwender richten – hier verweist das NCSC schlicht an veiliginternetten.nl. Zwar existieren die sogenannten *Basismaatregelen cybersecurity*, jedoch wenden sich diese ausdrücklich an Unternehmen und Organisationen (vgl. Nationaal Cyber Security Centrum 2021c). Für staatliche Verantwortliche bietet das NCSC das Nationaal Detectie Netwerk²⁴⁶, ein behördliches Netzwerk, in dem Bedrohungsinformationen ähnlich der ACS zwischen den Teilnehmerorganisationen ausgetauscht werden (vgl. Nationaal Cyber Security Centrum 2021d). Darüber hinaus verweist die Webseite lediglich auf eine E-Mail-Adresse des CERT. Für die Wirtschaft bietet das NCSC online Informationen zu ausgewählten Gefahren, darunter Ransomware, Phishing und DDoS. Passend dazu informiert die Webseite Institutionen zu Authentisierungsmöglichkeiten, sicheres Arbeiten im Homeoffice oder über Verbindungsabsicherung. Jedoch bleiben diese Inhalte stets allgemein gehalten und

²⁴⁵ Stand: November 2021

²⁴⁶ Deutsch: Nationales Detektionsnetzwerk

wenig an sachbezogenen Anwendungsfällen ausgerichtet. Einen zentralen Dienst des Internetangebots, den alle Interessierten nutzen können, stellen die Advisories dar. Dabei handelt es sich um aktuelle Warnmeldungen und Gefahrenhinweise. Diese Mitteilungen beinhalten eine Beschreibung, eine Lösungsempfehlung, sowie detaillierte Einschätzungen zu Schäden und Ausnutzungswahrscheinlichkeit (vgl. Nationaal Cyber Security Centrum 2021e). Jedoch werden die Advisories weder in einen Kontext gesetzt, noch in eine Ausdrucksform überführt, die für Privatpersonen verständlich oder gar hilfreich wären.

In Ausnahmefällen veröffentlicht das NCSC zusätzliche Factsheets, Checklisten oder Neuigkeitenartikel. Diese Hilfestellungen entstehen in Folge äußeren Drucks respektive kontemporärer Diskurse. Sie beschreiben das Phänomen, das Gefahrenpotenzial sowie mögliche Absicherungsmaßnahmen, die die Lesenden treffen können. Wenn auch nicht als solche etikettiert, fällt auf, dass sich diese Dokumente an Organisationen und Unternehmen richten, in keinem der überprüften Fälle aber an Endanwender. „Enerzijds kunt u uw werknemers trainen om phishing-mails te herkennen; anderzijds zijn er ook technische maatregelen die u kan nemen“²⁴⁷ (Nationaal Cyber Security Centrum 2020b, 3). Vielmehr sind diese Handreichungen komprimierte Nachweise der Expertise des NCSC, die in dieser generischen Form als Denkanstöße für Unternehmen dienen können.

Umso mehr fällt auf, dass das NCSC im Juni 2021 mit der nationalen IT-Krisenübung ISIDOOR auf sich aufmerksam macht und den Hergang öffentlichkeitswirksam zur Schau stellt. Die Übung schließt 96 Organisationen aus den Bereichen der kritischen Infrastrukturen und der Regierung ein, um den *Nationaal Crisisplan Digitaal*²⁴⁸ einerseits zu erproben und andererseits mithilfe der Teilnehmenden fortzuschreiben (vgl. Nationaal Cyber Security Centrum 2021a). Begleitend zu dieser Übungssituation veröffentlichen NCSC und NCTV ein Video, das weniger informativen als vielmehr katastrophischen Charakter hat. Der Sprecher leitet mit dramatisch, ernsthafter Stimme ein:

²⁴⁷ Deutsch: Einerseits können Sie Ihre Arbeitnehmenden schulen, damit sie Phishing erkennen können; andererseits existieren technische Maßnahmen, die sie ergreifen können.

²⁴⁸ Deutsch: Nationaler, digitaler Krisenplan

Begin juni 2021. Nederland wordt getroffen door meerdere cyberaanvallen. Met grote gevolgen voor de samenleving: Geen of vervuild water uit de kraan, uitval van energie en uitval van digitaal betaalverkeer. Er ontstaan problemen in de transportsector op Schiphol en in de havens. Een ziekenhuis heeft een patiëntenstop omdat ze geen nieuwe patiënten meer kunnen registreren. Bij het zoeken naar oplossingen blijkt een kwaadwillende partij gevoelige data van een groot aantal getroffen vitale organisaties buit te maken. Maar met welk doel²⁴⁹ (Nationaal Cyber Security Centrum 2021a)?

Die Ersteller des Videos machen die Zuschauer glauben, die Niederlande seien just in diesem Moment, da sie es schauen, einem schwerwiegenden Cyberangriff nationaler Tragweite zum Opfer gefallen, der unverzichtbare Dienste wie die Energieversorgung oder die Pflege von Kranken sabotiert. Erst nach 43 Sekunden löst das NCSC auf, dass es sich bei dieser Erzählung lediglich um das spekulative Szenario handelt, in dem ISIDOOR durchgeführt wird. Das Video, in dem zu Beginn ein digitales Fadenkreuz auf eine niederländische Industrielandschaft zielt, entwirft also eine Dramaturgie der Angst.



Abbildung 18: Terugblik ISIDOOR III (Nationaal Cyber Security Centrum 2021a)

Der Informationsgehalt bleibt durchgehend gering, die Dichte der vermittelten Emotionen ist aber greifbar: Eine existenzielle Gefährdung unbekannter Herkunft bedroht alle Bereiche des öffentlichen Lebens und erzeugt eine diffuse Verunsicherung. Schließlich beendet der Sprecher seine Schilderungen, indem er die Klimax mit den Worten „En nog erger. Dit blijkt al maanden aan de gang“²⁵⁰ erreicht (Nationaal Cyber

²⁴⁹ Deutsch: Anfang Juni 2021. Die Niederlande werden von mehreren Cyberangriffen heimgesucht, mit großen Folgen für die Gesellschaft: Kein oder verschmutztes Wasser aus dem Wasserhahn, Stromausfall und Ausfall des digitalen Zahlungsverkehrs. Probleme treten im Transportsektor in Schiphol und in den Häfen auf. Ein Krankenhaus hat einen Patientenstopp, weil es keine neuen Patienten mehr registrieren kann. Bei der Suche nach Lösungen stellt sich heraus, dass ein Angreifer sensible Daten von einer großen Anzahl betroffener lebenswichtiger Organisationen erbeutet. Aber zu welchem Zweck?

²⁵⁰ Deutsch: Schlimmer noch, das geht schon seit Monaten so.

Security Centrum 2021a). Nachdem der Sprecher daraufhin erläutert, welche Intentionen hinter ISIDOOR stehen und von welcher Größenordnung die Übung ist, endet das Video damit, dass die Zuschauer direkt angesprochen und schlussendlich gefragt werden: „Welke rol speel jij“²⁵¹ (Nationaal Cyber Security Centrum 2021a)? NCSC und NCTV lassen die Zusehenden mit der Frage zurück, inwiefern sie ganz persönlich an der Unversehrtheit der Niederlande mitwirken oder sie im Gegenteil aufs Spiel setzen. Die Argumentation entspinnt sich entlang der gefühlten Sicherheit, frei von quantifizierbaren Anhaltspunkten. Dies suggeriert, die Gefahr lauere dauerhaft und jederzeit könne ein schwerwiegendes Ereignis eintreten. Dieses Katastrophenszenario sei allerdings dann abwendbar, wenn das NCSC die relevanten Organisationen der Niederlande auf den Ernstfall vorbereitet und wenn jede und jeder Einzelne diese Ordnung annimmt. Diese mediale Inszenierung von ISIDOOR ist ein Indiz dafür, dass ein gewisses dystopisches Narrativ respektive eine emotionalisierte Erzählung eines weitestgehend sachlichen Vorgangs, wie einer Übung, in den Niederlanden zuträglich sein kann, um für Cybersicherheit zu sensibilisieren.

Sowohl das NCSC als auch das BSI fallen online mit ihren Darstellungen von Gefahren und hauseigenen Diensten auf. So halten sie Advisories bereit, die einzig Bedrohungen thematisieren, aus Gründen der Marktneutralität aber nie auf zum Beispiel Schutzprodukte referenzieren. Sie offerieren Vernetzung, Informationen zur Wiederherstellung betroffener Systeme sowie eine große Fülle an Warnungen, Mahnungen und Risikobeschreibungen. Schon durch diese Quantität tragen die Institutionen zu einer dystopischen Imagination zukünftiger Digitalrealitäten bei. Zugleich versuchen sie, Vertrauen in Staat und Technik zu schaffen, indem sie fortwährend suggerieren, dass es möglich sei, durch gewisse Systembedingungen und sensibles Handeln Sicherheit herzustellen. In der Vorgehensweise lassen sich erhebliche Unterschiede ausmachen: Während das BSI stetig zahlreiche Angebote, Informationen und Medienadaptionen lanciert, die sich im Gegensatz zum NCSC auch an Verbraucher richten, zementieren die Niederländer auf ihren Webseiten die Verantwortlichkeit von Wirtschaft und Staat. Damit reflektieren sie grundverschiedene Institutionalisierungen der Problemauffassung: Das BSI ist Abbild einer Gemeinschaftsaufgabe, bei der jede beteiligte Entität und jede involvierte Person von Belang ist, um die Herausforderungen angehen zu können. Dagegen steht die niederländische Vorstellung einer nicht

²⁵¹ Deutsch: Welche Rolle spielst du?

kollektiven, sondern einer Verwaltungs- beziehungsweise Infrastrukturaufgabe, auf die Anwender kaum Einfluss haben.

Diese Grundkonfigurationen der Cybersicherheitsämter findet sich in diversen Veröffentlichungen wieder. Demgemäß bilden die Titelseiten der letzten fünf Cybersecuritybeeld Nederland überwiegend Küstenmotive oder mit dem Hochwasserschutz verbundene Aufnahmen ab. Sie zeigen das Schützenswerte, den Grund für den betriebenen Aufwand rund um sichere Informationstechnik und rekurren zugleich auf ein Stück niederländische Identität. Abgedruckt sind Brücken, Windkraftanlagen, Hochwasserschutzsysteme oder gewässernahe Städte. Damit stellt das NCSC einen konkreten Bezug zwischen der Lebenswelt der Niederländer und den ungegenständlichen Cyberherausforderungen her. Einhergehend stärkt diese Botschaft das Daseinsrecht der Behörde, da sie suggeriert, für die Sicherheit und das Bestehen dieser essenziellen Strukturen verantwortlich zu sein.



Abbildung 19: Titelbilder des *Cybersecuritybeeld Nederland* 2017–2021 (eigene Collage)

Die Titelblätter des BSI-Lageberichts sind völlig anders arrangiert: Die Motive sind abstrakt, wenig ausdrucksstark und sind weniger erzählend gestaltet. Stattdessen zeigen sie häufig geometrische oder fließende Formen ohne sichtbare Kohärenz, sodass die verwendeten Abbildungen ebenso für andere Sinnzusammenhänge nutzbar wären. Erst 2020 und 2021 bieten die Cover eine modifizierte Karte Deutschlands je mit fiktiven Knotenpunkten an, die annehmbar Städte oder wichtige Infrastrukturzentren darstellen sollen. Damit bleiben auch diese Abbildungen weniger greifbar als die niederländischen.

Zwar legt das BSI so nahe, dass es für die Sicherheit ganz Deutschlands verantwortlich sei, gibt den Lesenden aber keine Vorstellung davon an die Hand, was diese Verantwortung realiter einschließt.



Abbildung 20: Titelblätter des Berichts zur *Lage der IT-Sicherheit in Deutschland* 2017–2021 (eigene Collage)

Die Wahl eines derart generischen Titelbildes lässt hinreichend Spekulationsraum über die Schwere der berichteten Situation, über den inhaltlichen Fokus und sogar über die angesprochene Leserschaft des Berichts. Schließlich gleichen die Titel nahezu denen des Bundeslagebilds Cybercrime des BKA. In dem vermeintlichen Versuch, alle Deutschen zu adressieren, geht die konstituierende Botschaft unter und das BSI lässt eine Gelegenheit zum Agendasetting und zur Positionierung innerhalb des Behördenspektrums aus. Gewissermaßen spiegeln die Titelbilder der Berichte die jeweilige erzählerische Form des Inhalts. Während in den Niederlanden Narrative rund um unmittelbare, greifbare Bedrohungsszenarien sowie etablierte Wendungen wie *digitale dijkverzwaring*²⁵² kursieren, herrschen in Deutschland konturlose und zudem segmentierte Diskurse über vage Ereignisse vor, die zunächst wenig individuelle Betroffenheit erzeugen. Hier bestätigt sich, was bereits in vorausgegangenen Kapiteln erfasst wurde: Staatliche Institutionen der Niederlande, so auch das NCSC, neigen zu einer emotionalisierenden, medienwirksamen Kommunikation, unter anderem da das Land geografisch und systemisch noch stärker von IT abhängt. Das BSI, aber auch andere öffentliche Einrichtungen legen vornehmlich sprachliche und gestalterische Zurückhaltung sowie größere Sachlichkeit an den Tag.

²⁵² Deutsch: Digitale Deichstärkung

Um einerseits das Augenmerk auf das BSI zu lenken und andererseits die Sicherheitsbotschaften der Behörde zu verbreiten, beschließen BMI und BSI Anfang 2021 gemeinsam, die öffentlichkeitswirksame Kampagne #einfachaBSIchern mit einem Budget von 1,5 Mio. Euro zu initiieren. „Hierfür zeigen und thematisieren die Motive der Kampagne typische digitale Nutzungsszenarien aus der alltäglichen Lebenswelt der Verbraucherinnen und Verbraucher“ (Bundesamt für Sicherheit in der Informationstechnik 2021g). Dabei setzte das BSI in den ersten Monaten der Aktion auf Themen, die in Relation zur Corona-Pandemie standen und entsprechend zeitgeistig gestaltet waren. Zum Erscheinen dieser Maßnahmen wurden Anwender nicht nur mit den plötzlichen Anforderungen einer neuen Arbeitswelt konfrontiert, sondern erfuhren aus der Presse regelmäßig von Sicherheitslücken und Datenschutzverstößen von großen Videokonferenzanbietern.



Abbildung 21: Kampagnenmotiv #einfachaBSIchern 2021 (Bundesamt für Sicherheit in der Informationstechnik 2021g)

Die Gestaltung suggeriert eine Verzahnung von realen Lebensherausforderungen und Digitalität, um zugleich vorzugeben, dass eine sichere Nutzung entsprechender Dienste unaufwändig zu realisieren ist. Das BSI tritt neben den abgebildeten Personen und den nur zu erahnenden Cyberkriminellen als unsichtbarer Protagonist auf, der an dem Punkt Hilfe anbietet, an dem bei gewöhnlichen Usern mutmaßlich Überforderung einsetzt. In

zugehörigen Kurzvideos, die in den sozialen Medien wie auch in Streamingdiensten als Werbung ausgespielt wurden, erhebt das BSI die Angesprochenen gar zu Helden, indem es sie zu Verteidigern ihrer Dienste und Geräte erklärt und als schillernde, befähigte Herren ihrer Informationstechnik zeichnet.



Abbildung 22: Video: Cyber-Held*innen der Kampagne #einfachaBSIchern 2021 (Bundesamt für Sicherheit in der Informationstechnik 2021g)

Die Filme zeigen ebenso Menschen in ihren heimischen Umgebungen, in denen sie allerdings nicht durch die Pandemie paralysiert zum Warten gezwungen sind, sondern sich bemächtigen und als Helden ihre eigene IT sichern und durch ihre Potenz überdies zu Beschützern des digitalen Gemeinwohls werden. Erneut ist das BSI als mittelbarer Akteur zugegen, indem es nicht auf die Bühne tritt, aber sich durch #einfachaBSIchern unaufdringlich als Ausbilder ebendieser Cyberhelden geriert. Noch im selben Jahr legt das BSI Videos und Motive zum Onlineshopping nach, die völlig konträre Botschaften tragen: Die Kunden agieren im analogen Einzelhandel wie unbedachte Onlinekäufer, indem sie naiv Passwörter preisgeben oder auf unseriöse Preisgestaltung hereinfallen (vgl. KNSK.de 2021). In diesem Szenario zeigen sich die Verbraucher nicht heldenhaft, sondern sind und bleiben leichte Opfer für ihre Gegenspieler. Mit einem Voice Over wie „Wir helfen Ihnen, im Netz sicher zu zahlen“ verhält sich das BSI belehrend, um sich über die Protagonisten ihrer Geschichten und damit auch über die Zusehenden zu erheben (KNSK.de 2021). Das BSI bietet die allegorische Krücke für jene Menschen, die selbst nicht imstande sind, digital zu laufen. Während Cyberkriminelle in der Heldendarstellung machtlos daherkommen, liegt hier das Augenmerk auf der

Bedrohung. Die Heldenkampagne zielt darauf auf, Ängste vor dem Cyberraum abzubauen und ein berechtigtes Selbstbewusstsein vermitteln. Die Onlineshopping-Inhalte hingegen entreißen dem Zuschauer seine gewonnenen Fähigkeiten wieder, um ihn letztlich als unwissenden Gehilfen seiner selbstverschuldeten Misere darzubieten. Gemeinsam haben beide Kommunikationsprodukte, dass sie ihrer Zielgruppe nahebringen, dass sie selbst großen Einfluss darauf haben, ihre Opferwerdung zu vermeiden – oder umgekehrt: Sie haben die Verantwortung, ihren Anteil zur Cybersicherheit beizutragen. Das BSI präsentiert sich zunächst als Ausbildungsstätte für Cyberhelden, die wiederum ihr Umfeld schützen und sensibilisieren; wenige Monate später ist es eine instruierende Institution, die offenlegt, dass sie zumindest vereinzelt Usern geringes Zutrauen schenkt. Darüber hinaus erscheint das BSI im Grunde machtlos, da es implizit nicht in der Lage ist, unsichere Geräte und Dienste a priori zu verhüten. Die Behörde gesteht mit der Darstellung ihrer Klientel ein, dass sie selbst nur bedingt handeln kann und auf die Mithilfe aller angewiesen ist, um sich der Utopie einer demokratisierten Digitalgesellschaft überhaupt annähern zu können.

#einfachBSIchern ist eine der aufwändigsten und langwährendsten Sensibilisierungsmaßnahmen zur Informationssicherheit, die es in der Bundesrepublik bis heute gab. In den Niederlanden besteht kein Pendant, das durch das NCSC initiiert, von ähnlicher Stelle produziert oder mit einem vergleichbaren Ressourcenaufkommen hinterlegt ist, auch da eine solche Kampagne einen nennenswerten Teil des NCSC-Jahresetats verlangen würde. Stattdessen greift das Nationaal Cyber Security Centrum auf eine weniger kostenintensive, aber nicht weniger anspruchsvolle Methodik zur Selbstdarstellung zurück. Die Behörde belohnt Hacker und Computerexperten, die Sicherheitslücken in der niederländischen IT-Infrastruktur ausmachen und dem NCSC melden mit einem Shirt, das mit *I hacked the Dutch government, and all I got was this lousy T-shirt* bedruckt ist.

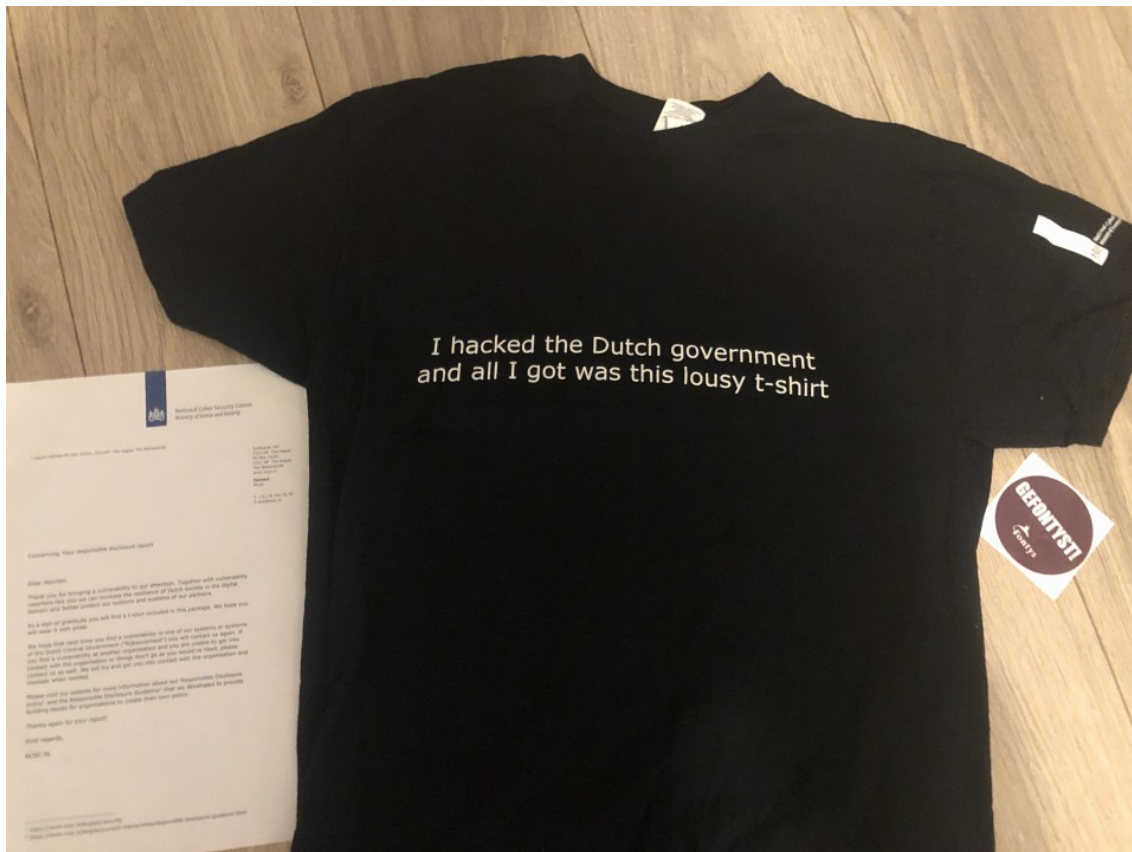


Abbildung 23: Sanders, Koen (LinkedIn 2020)

Dieser simple, weiße Druck auf schwarzem Untergrund trägt gleich mehrere Botschaften: Das NCSC thematisiert seine eigene Ressourcenknappheit in Design und Aussage, indem es selbst das Shirt als zu geringe Anerkennung darbietet. Auf einer weiteren Ebene wird auch der Hacker zwangsläufig zu Selbstironie gezwungen, da das Tragen des Kleidungsstücks betont, dass er eine wertvollere Entlohnung erwartet hatte. Dabei ist der Besitz des Shirts ein Statusinstrument, das distinguert und den Träger in einen elitären Kreis weniger Personen aufnimmt. Es suggeriert, dass der Besitzer Hacker mit besonderen Fähigkeiten ist, und dass er dieses Know-how in den Dienst der Gesellschaft gestellt hat. Somit kann das Shirt als Kompetenzetikett fungieren, dass zum einen den Träger erhebt und zum anderen zum begehrten Objekt innerhalb der Community wird. Diesen Effekt macht sich das NCSC zunutze, indem es Shirt und Begleitbrief lediglich per Post versendet und auf öffentliche Auszeichnungen verzichtet.

Das führt dazu, dass die prämierten Personen ihren Erfolg selbst publik machen und zu Multiplikatoren der Initiative sowie schließlich des NCSC mutieren. Jacob Riggs, ein Hacker, der selbst mit einem NCSC-Shirt honoriert wurde, stellt heraus, dass derartige Belohnungen unüblich und Strafandrohungen dagegen die Regel sind: „This was a pleasant response to receive and illustrates a far better approach to engaging with ethical

hackers than traditional threats of prosecution“ (jacobriggs.io 2021). Indem die Niederlande solche sogenannten White Hats auszeichnen, statt sie abzustrafen, machen sie diese Gruppe nicht nur zu ihren Mitstreitern, sondern gehen gegen verhärtete Stereotypen vor, die diesen Personenkreis zumeist als Kapuzenpullover tragende Kriminelle porträtieren. Das Shirt ist zeitgleich Ansporn, Anerkennung und gefällige Werbemaßnahme und verfügt somit über die Eigenschaft, sich selbst zu replizieren. Auf diese Weise präsentiert sich das NCSC als pragmatische Behörde mit Blick für opportune Nutzeffekte, ohne offenzulegen, welche Erträge durch diesen Synergismus tatsächlich entstehen.

Diese niederländische Kommunikationsstrategie, die mit wenigen finanziellen und personellen Ressourcen umsetzbar ist, spiegelt sich in den sozialen Netzwerken wider. Das NCSC betreibt seine Kanäle bei Twitter sowie LinkedIn und gibt damit eine Programmatik vor – die Behörde adressiert Fachleute, Journalisten, Unternehmensvertreter und Talente. Demgegenüber ist das BSI bei Facebook, Twitter, LinkedIn, Youtube, Mastodon, Instagram und Xing anzutreffen. Daraus lässt sich ableiten, dass sowohl ein Interesse besteht, verschiedenartige Personengruppen anzusprechen als auch größere Mittel vorhanden sind, um die Kommunikationsträger mit der notwendigen Menge an Inhalten befüllen und sie administrieren zu können. Das NCSC nutzt die Plattformen, um größtenteils reine Textbeiträge ohne multimediale Begleitung abzusetzen. Sie spielen dort vorwiegend eigene Inhalte, Arbeitserzeugnisse und Agenden aus, die sie gewissermaßen für Social Media reproduzieren (vgl. Twitter.com 2019d). Ebenso sehr gibt das NCSC über Twitter konkrete Bedrohungsmeldungen heraus, damit diese über die Lesenden vervielfacht werden (vgl. Twitter.com 2021b). Konträr zu der Idee, dass User, Follower und letztlich Hacker die Botschaften organisch vervielfältigen, einzig weil diese relevant sind, verfügt das BSI über eigens hergestellte Social Media-Formate, wie einen Adventskalender mit 24 Kurzvideos oder Gaming-Talks für Youtube (vgl. YouTube: Bundesamt für Sicherheit in der Informationstechnik – @bsi_bund 2021a). Mit Zitatkacheln, wiederkehrenden Posting-Formaten, darunter Begriffsklärungen, Fakten aus der Welt der Cybersicherheit, interaktive Ratespiele oder Sicherheitsirrtümer, kann das BSI sowohl dem Genre Social Media als auch jedem seiner Kanäle präziser entsprechen.

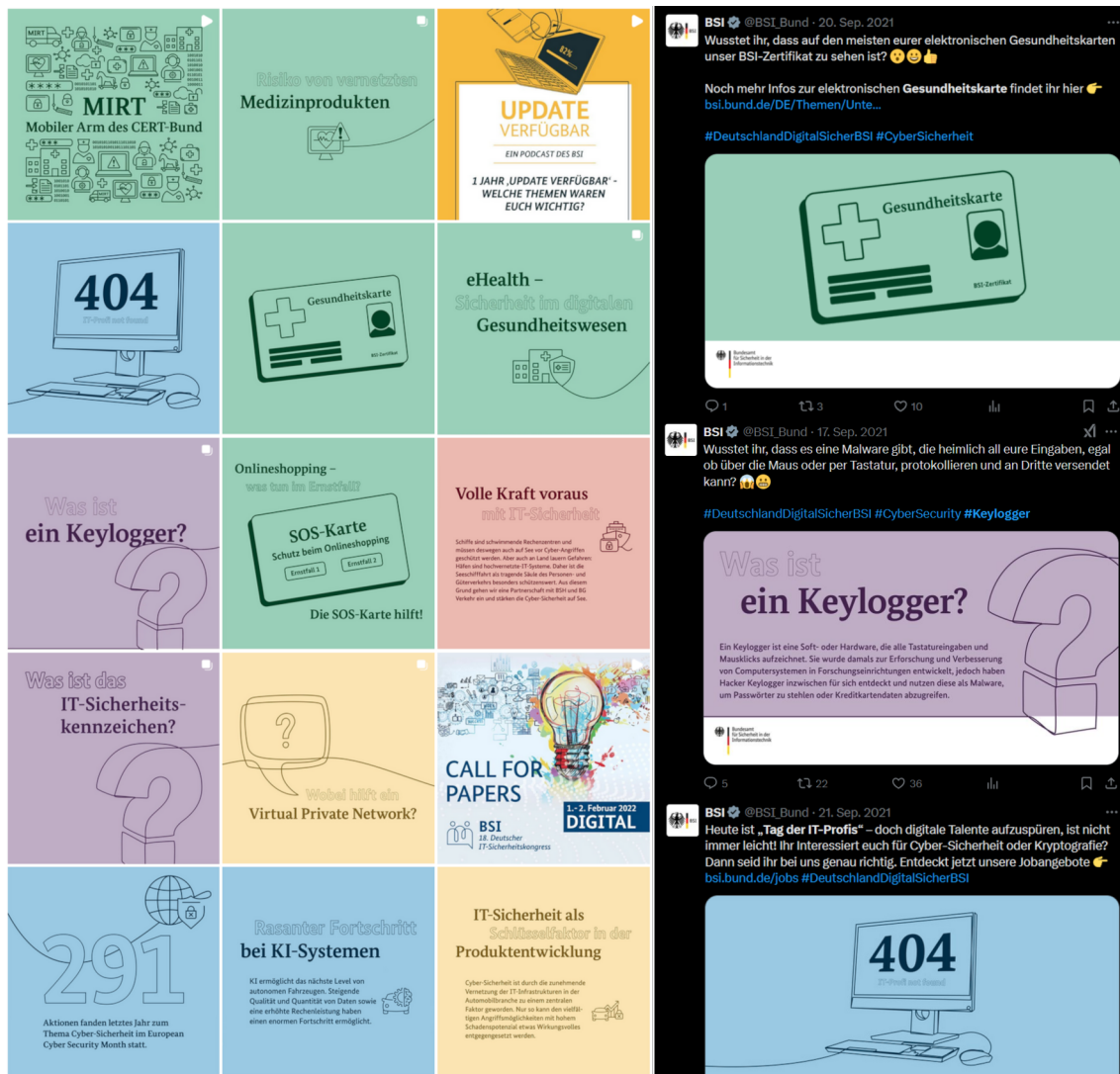


Abbildung 24: eigene Darstellung: Links der Instagram-Feed bsi_bund aus dem September 2021 - rechts einzelne Tweets von @bsi_bund | beides aus dem September 2021

Zusätzlich hilft das Corporate Design der Behörde, den Kanälen eine erkennbare Figuration nebst einer erleichterten Wiederverwendbarkeit zu verleihen. Inhalte, die unter anderem auf Instagram erscheinen, können so mit geringen Mitteln für weitere Medien adaptiert und zweitverwertet werden.

In nahezu allen Belangen ist ersichtlich, dass die Instrumente des NCSC signifikant limitiert sind, wenn die vorhandenen Social Media-Präsenzen in Rubriken wie Gestaltungsvielfalt, Mediendiversität, Frequenz oder inhaltlicher Breite nebeneinanderstehen. Schlussendlich spricht hieraus nicht nur die ungleiche Verfügbarkeit von Finanzmitteln, sondern erneut die je behördeneigene Identität: Das Nationaal Cyber Security Centrum legt sein Augenmerk auf Betreiber kritischer Infrastrukturen, Experten sowie Verantwortungsträger und begnügt sich damit, innerhalb dieser Netzwerke Aufmerksamkeit und Reputation hinzuzugewinnen. Das

BSI erweist sich demgegenüber bemüht, auch jenseits dieser bedeutsamen, aber überschaubaren Zirkel zu operieren und so auf eine denkbar stärkere Inklusion aller Entitäten des Landes zu bauen.

Zweifellos belegt diese Gegenüberstellung die unterschiedliche Leistungsfähigkeit der Öffentlichkeitsarbeit beider nationaler Cybersicherheitsbehörden. Das BSI kann sowohl in der Breite als auch in der Tiefe umfassender Inhalte sowie vielfältigere Distributionswege vorhalten und erreicht damit annehmbar eine größere Wirkung bei seinen Zielgruppen. Der Mangel an diesen Produktionsmitteln zwingt das NCSC wiederum zu kreativeren Umsetzungen und Kooperationskonzepten. Noch erhellender ist aber, dass aus diesen Einsichten allem voran unterschiedliche Grundannahmen von Cybersicherheit sprechen: Während die Niederlande von einer technischen Lösbarkeit digitaler Sicherheitsaufgaben ausgehen, herrscht auf deutscher Seite das Axiom vor, diese Herausforderungen nur als kollaborative Gesellschaftsaufgabe angehen zu können. Dementsprechend legt das BSI den Anspruch und die Ressourcen an den Tag, die Gesellschaft kommunikativ durchdringen und das Thema Informationssicherheit bei jeder Gelegenheit auf die Agenda heben zu wollen. Das NCSC folgt einer anderen Maßgabe; es zeigt sich weniger transparent und mitteilksam, da es sich explizit an ausgewählte Zielgruppen, unter anderem wichtige Infrastrukturakteure, wendet. Die Behörde agiert verdeckter und mutet daher vergleichsweise geheimdienstlich an. Letztlich perpetuieren beide Cybersicherheitsämter die sie jeweils legitimierenden Imaginationen; das einer im BSI konzentrierten Omnikompetenz sowie das einer an das NCSC delegierten Administrationsherausforderung ohne notwendiges Zutun der Bevölkerung.

Infolgedessen produziert und inszeniert das BSI Zukunftsvorstellungen für ein vielfach größeres Publikum. Wo das NCSC in eine Echokammer konsenspflegender IT-Fachleute sendet, zielt die Außendarstellung des BSI darauf ab, bestehende Vorstellungswelten der Gesellschaft zu verändern und so auch Imaginaries zu lenken. Dazu lohnt es sich, einen Gedanken neu zu formieren, den Ernst und Schröter in ihrem Aufsatz über die Möglichkeit einer anderen Technik dargelegt haben:

Medien werden in letzter Konsequenz als die Instanzen und Institutionen angesehen, die durch die Umgestaltung von Kommunikations- und Informationsprozessen neue Öffentlichkeiten, neue Lebensformen, neue Politiken etc. praktisch ermöglichen sollen (Ernst/Schröter 2022b, 171).

Denn mehr als das haben die vergangenen Kapitel aufgezeigt, dass nicht nur den Medien, sondern ebenjenen Institutionen, die ebenso als Medien gelesen werden können, die immanente und unauslöschliche Wirkung anhaftet, den way of life zu verändern. So machen BSI und NCSC die körperlose Informationssicherheit durch ihre Veröffentlichungen und ihre Präsenz erlebbar, indem sie je eine glaubhafte Perspektive kommunizieren; allerdings nur eine Perspektive. Das Nationaal Cyber Security Centrum vernimmt Cyberbedrohungen als technisch lösbare Aufgaben, für deren Bewältigung das Zutun der Endanwender weitestgehend obsolet ist. Das Bundesamt für Sicherheit in der Informationstechnik verkörpert die Ausdeutung, dass User sehr wohl elementarer Bestandteil der Sicherheitsarchitektur sind. Resultierend daraus imaginiert die deutsche Behörde andere Techniken – gewissermaßen Paralleltechniken, deren Existenz sie anstrebt – um ihre Appetenz nach Usable Security oder Security-by-Design zu einem allgemeinen Bedürfnis zu entwickeln. Es ist anzunehmen, dass das BSI verinnerlicht hat, dass Imagination „mithin immer auch das ›Medium‹ für die »Andersheit« bzw. das »Anderswerden« gesellschaftlicher Ordnung“ ist (Ernst/Schröter 2022a, 13). Gleichwohl kann dem NCSC diese Erkenntnis nicht abgesprochen werden, wenn die Cyberbehörde ihren medialen Wirkungsgrad punktuell einsetzt, um ihre Fähigkeiten mittels Krisenübungen oder Erfolgsmeldungen hervorzuheben. Stattdessen handelt es sich um einen Beleg dafür, dass sich eine Gesellschaft „ein Anderswerden von Technik nur als von ihren jeweiligen identitätslogischen Prämissen ausgehend vorstellen“ kann (Ernst/Schröter 2022b, 166). Das NCSC stellt also im Gegensatz zum BSI in Aussicht, dass die ökonomische Leistungsfähigkeit sowie die ökologische Überlebensfähigkeit der Niederlande ohne exzeptionell professionalisierte Behörde sowie rasches Handeln dauerhaft in Gefahr sein werden, um anschließend aus diesem Szenario fast schon unumgänglich die Vision abzuleiten, dass „Nederland wil behoren tot de wereldtop“²⁵³ (Tweede Kamer der Staten-Generaal 2011, 2). Der schon eingangs dieser Textpassage zitierte NCSC-Leitsatz legt zusätzlich nahe, dass die Behörde die existenzielle Gradwanderung zwischen digitalisiertem Zusammenleben und gefährdeten Lebensgrundlagen lenken könnte: „De digitale infrastructuur is van levensbelang: voor het betalingsverkeer, voor schoon water uit de kraan en om droge voeten te houden“²⁵⁴ (Nationaal Cyber Security Centrum 2022a). Das NCSC errichtet als Folge dessen das

²⁵³ Deutsch: die Niederlande zur Weltspitze gehören wird

²⁵⁴ Deutsch: Die digitale Infrastruktur ist lebensnotwendig: für den Zahlungsverkehr, für sauberes Leitungswasser und für trockene Füße.

Narrativ einer externalisierbaren Verantwortung für die Sicherheit in der virtuellen Sphäre und ruft die Vorstellung einer zukünftig unbeschwerten und unter Betreuung gestellten Bevölkerung aus. Diesen Erfolg versprechen sich die Niederlande nicht zuletzt durch möglichst wenig Regulierung: „Ook de overheid heeft een rol“²⁵⁵ (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021a, 46). In dieser Lesart ist die Regierung respektive das NCSC nur ein, mitunter paritätischer, Akteur unter Vielen, die gemeinsam die Cybersicherheit der Niederlande schultern.

Die Entschleierung von Informationssicherheitskultur über drei reale Kasus hat markante Merkmale offengelegt, die sich aus den obigen Diskursen ableiten lassen. Diese Attribute sind nicht allesamt über sämtliche Exempel festzustellen, fallen aber bei der Untersuchung als derart wirkungsvolle Triebfeder der jeweiligen Kulturadaption auf, dass sie womöglich als Charakteristika solcher Transferprozesse klassifiziert werden können:

1. In der Öffentlichkeit kursieren sinnfällige Vergleiche oder Metaphern.
So ist Emotet das Schweizer Taschenmesser oder wahlweise der König der Cyberkriminalität, während 5G mit Radioaktivität gleichgesetzt und unter anderem für Krankheiten wie Krebs, Diabetes oder Autismus verantwortlich gemacht wurde. Der Vergleich komplexer Hergänge oder Technologien mit alltäglichen Begrifflichkeiten lässt diese weniger kolossal erscheinen und nimmt Distanz.
2. Es existiert ein dominanter Überhöhungskonsens.
Relevante Akteure induzieren Sicherheitsvorstellungen entweder über Diskreditierung oder Idealisierung einer Zukunftsimagination, indem sie Positiverwartungen oder Fürchte auch abseits der Fakten zur bevorstehenden Tatsache stilisieren. So zeigte sich, dass 5G nicht selten entweder als Allheilmittel für autonomes Fahren und die Medizin oder als gewaltiges Risiko für Gesundheit und Natur aufgefasst wird. In dieser Mechanik verhaftete Diskursteilnehmer neigen dazu, Gegenstimmen zu diffamieren und so Debatten zu ersticken.
3. Die Schadsoftware, der Angriff oder der Vorfall erhalten bewusst handelnde, gar menschenähnliche Züge.

²⁵⁵ Deutsch: Auch die Regierung spielt eine Rolle.

Die Zuweisung humaner Eigenschaften geht mit erkennbaren Protagonisten- und Antagonistenzuschreibungen einher. So attribuierte die Debatte um Emotet die Schadsoftware immer wieder mit Titeln oder mit absichtsvollem Handeln, das wiederum den Anschein gewisser Menschenähnlichkeit hervorrief. Auf diese Weise kann das leblose Technikprodukt als Leinwand für Ideologie und Aversion dienen.

In Summe beleuchten diese Kennzeichen, welcher Hilfsmittel es bedarf, damit sich komplizierte Gegenstände kulturell niederschlagen und in der Gesellschaft verstetigen können. Mithin haben alle drei Merkmale gemein, dass sie übersetzen und derart simplifizieren, dass sich die Zugänglichkeit so lange erleichtert bis eine Begebenheit fassbar und nachhaltig einprägsam wird. Sie sind Werkzeuge, um Situationen aufzugreifen, zu kommunizieren und letztlich zu bewältigen. Schließlich gibt die Ausprägung dieser Indikatoren Hinweise auf die „shared perceptions of futures that should or should not be realized“, wie Sheila Jasanoff es ausdrückt (Jasanoff 2015a, 8). Wie nachhaltig sich Vorfälle kulturell verfestigen und welche Schlüsse die beteiligten Institutionen und Öffentlichkeiten aus diesen Vorgängen respektive ihrer Bewältigung ziehen, geben die Charakteristika nicht preis.

IV. Conclusio

Zu Beginn dieser Dissertationsschrift steht die Annahme, dass Deutschland und die Niederlande auf verschiedene Weise Cybersicherheit herstellen. Um diese Präsumption überprüfen zu können, wurden drei hinleitende Fragestellungen formuliert, um sowohl auf das Erkenntnisziel einzuzahlen als auch das akademische Feld einzugrenzen, das es zu bestellen galt.

1. Was ist eine Cybersecurity Culture?

Cybersicherheitskultur ist der Begegnungsrahmen, also das kulturelle System, in dem IT-Sicherheit besprochen und fortgeschrieben wird. Sie ist der Raum, in dem Menschen intersubjektiv ordnen, wie sie mit Cyberunsicherheit umgehen. Sie ist sogleich der Ort, an dem sie sich mit digitalen Risiken konfrontiert sehen, an dem sie politisches Treiben erfahren, an dem sie militärische Konflikte wahrnehmen, in den sie ihre eigene Rolle und so auch ihre individuelle wie kollektive Herkunft eintragen. Cybersecurity Culture ist nicht zuletzt die Dimension, in der die (Teil-)Gesellschaft Einfluss auf Cybersicherheit nimmt und ihr Form verleiht. Auf dieser Bühne – die einige Akteure unbewusst, andere absichtsvoll, betreten – bestimmen die Partizipatoren, ob der Status quo als sicher oder unsicher wahrgenommen wird, ob Cybersicherheit auch jenseits von Fachdebatten Aufmerksamkeit erlangt; und welche Zukunftsarrangements die Vorstellungswelt jener Gemeinschaft einfassen. Innerhalb dieser Cybersicherheitskulturen sind Imaginationen ein wesentliches Instrument zur Reduzierung oder Ausdehnung des denkbar Möglichen einer Gesellschaft. Wie sich zeigte, existiert nicht das eine imaginierte Leitmotiv einer Konsensgesellschaft, dem dann wiederum alle handelnden Personen nacheifern. Vielmehr sind Imaginaries pluralistische Akkumulationen von zukunftsidealistischen Fiktionen, die interpersonell derartige Schnittmengen aufweisen, dass sie in weiten Teilen eines jeweiligen Diskurses auszumachen sind. Und tatsächlich bestätigt diese Untersuchung diese inhärente Eigenschaft von allem Imaginierten: „Historisch-kulturelle Denk- und Handlungspfade kanalisieren das Handlungsrepertoire politischer Akteure“ und sind so, wie bereits festgestellt wurde, Produkt und Produzent der Cybersicherheitskultur (siehe S. 87) (Hegemann/Kahl 2012, 166). Denn diese zirkulierenden Imaginationen bedingen, wie die Gemeinschaft unter anderem auf Institutionen, innere wie äußere Einflussnehmer, politische Kultur, Technologieentstehung, Ökonomie, Normen oder Digitalisierung

blickt und ob sie die dominanten Imaginaries selbst als Leitbilder wahrnehmen kann. Es tritt zu Tage, dass Informationssicherheitskultur selbst Medium ist, eine diskursive Masse, mit der sich IT-Sicherheit aushandeln und rejustieren lässt. Als solches naturalisiert Cybersicherheitskultur Abbilder von Bedrohung und Sicherheit, kongruiert als Schauspiel und Bühne, als Botschaft und zugleich als Botschaftsträger. Sie beherbergt und formt gleichermaßen über Jahrzehnte gewachsene Moralitäten und institutionalisierte Direktiven, die „die aktuellen Wertevorstellungen unserer Gesellschaften“ verfassen (Pohlmann 2016, 40).

Dieses (mediale) Vorstellungsvermögen des Kollektivs konstituiert maßgeblich, wie Cybersicherheit oder Cyberbedrohungen wahrgenommen, wie ernst sie aufgefasst und in welchem Maße sie gemeinschaftlich erörtert werden – letztlich welche Wirkung IT-Sicherheit auf die Lebenswirklichkeit eines jeden Einzelnen hat. Denn daran kann nach der Lektüre dieser Dissertation kein Zweifel sein: Cybersecurity Culture ist eine unsichtbare Ordnungsmacht, die jedem Individuum eine dynamische Position innerhalb dieses Kultursystems zuweist und diese Person etikettiert. Sie ist Expertin, unbedarfter Konsument, wissenschaftliche Betrachterin, vielleicht Hersteller von Informationssicherheit, Laie oder aber Außenstehende. Wie jede Erscheinung, die mit menschlicher Interaktion verknüpft ist, wird das Naturell von IT-Sicherheit besonders von solchen Akteuren bestimmt, die sie initiativ ausfüllen. So sind es zum Beispiel Staat und Gesellschaft als intranationale Funktionsgattungen sowie ausländische Nachrichtendienste, Hackergruppen, Kriminelle oder Techkonzerne, die international oder gar supranational agieren, sodass sich nunmehr der gewohnte Charakter staatlicher Verantwortlichkeit transformiert und bisherige Grenzziehungen an Relevanz einbüßen. Cybersicherheitskultur ist dynamische Kommunikation, überträgt Erlerntes und fungiert als Medium zwischen den Partizipatoren einer Gesellschaft ebenso wie zwischen Mensch und Technologie – all das kumuliert in *IT-Sicherheitskultur*.

2. Wie organisieren die beiden Länder IT-Sicherheit?

Daran knüpft die Frage an, welche Institutionenlandschaften in Deutschland und den Niederlanden mit der Sicherung des Digitalraums beauftragt sind und wie diese Administrationen miteinander im Verhältnis stehen. Aber nicht nur die offensichtlichen Institutionen, wie Behörden oder Anstalten der Staaten, unterzogen sich der kritischen Auseinandersetzung, sondern ebenso wurden die jeweiligen Rechtszustände, die Bedrohungskontexte, strategische Absichten oder auch zivilgesellschaftliche Akteure als

Institutionen gefasst und entsprechend betrachtet. Zuvorderst konnten die strukturell-organisatorischen Dispositionen mithilfe der Added Values systematisiert werden, sodass maßgebliche Narrative der Cybersicherheit in beiden Ländern bloßgelegt werden konnten. Dabei wurde offenbar, dass zwischen Deutschland und den Niederlanden Einigkeit über gleich mehrere strukturelle Funktionsmerkmale eines nationalen IT-Sicherheitsgerüsts bestand. So scheint es in der Natur der untersuchten Institutionen und Regeln zu liegen, dass ihre Bemühungen auf das Makrogefüge abzielten und Mikroorganisation zumeist außer Acht ließen. Wie einzelne Anwender mit der Digitalisierung zurechtkommen, wie Vereine ihre Mitgliederdaten sicher verwalten oder wie Kleinunternehmer die IT ihres Betriebs sicher konfigurieren, spielte in beiden Ländern allenfalls eine untergeordnete Rolle. Stattdessen konzentrierten beide Nationen ihre Kapazitäten auf die Absicherung kritischer Infrastrukturen, auf die Regulierung ökonomisch tragender Branchen und auf die Protektion staatlicher Institutionen und Geheimnisse gegen fremde Aggressoren. Die staatliche Weichenstellung wirkte auf technisch-strukturelle Absicherungsmaßnahmen hin und ignorierte weitestgehend die Befähigung eines jeden Einzelnen, beispielsweise über medienpädagogische oder didaktische Instrumente der Individualbildung – die universellen Entscheidungen der politischen Makroebene wurden den unzähligen Einzelbedürfnissen übergestülpt. Private Antreiber der Cybersicherheit oder gesellschaftliche Institutionen handelten überwiegend ebenso generalisierend, indem sie das jeweils staatliche Angebot um etwa Hinweise für Anwender ergänzten. Ebendarum legen die Resultate an den Tag, dass die untersuchten Dokumente und Institutionen deutlich mehrheitlich technische Maßnahmen, Zertifizierungen und strategische Schutzbarrieren vorsahen und nur in einigen Fällen den Blick auf soziale Faktoren der IT-Sicherheit oder auf Stolpersteine der Mensch-Maschine-Interaktion richteten.

In den Gesetzen und Strategien der Länder zeichnete sich diese Grundhaltung deutlich ab – und zugleich waren hier große Differenzen zwischen den Niederlanden und Deutschland auszumachen: So ermächtigt das IT-Sicherheitsgesetz das BSI zu Portscans oder macht es zur zentralen Meldestelle für IT-Sicherheit in Deutschland. Das Wbni befähigt das NCSC, mögliche Schwachstellen zu analysieren oder auch, Unternehmen der kritischen Infrastrukturen zu Meldungen oder Sicherungsmaßnahmen zu verpflichten. Das Zentrum der Aufmerksamkeit lag in beiden Staaten in der technischen Überwindung der vielschichtig verschränkten Aufgaben der Informationssicherheit.

Abweichungen ließen sich dagegen in der rhetorischen Ausdifferenzierung der offiziellen Dokumente ausmachen: Während der deutsche Lagebericht stets komplex formuliert, mit Statistiken angereichert und mit Fachtermini gespickt war und sich somit an Experten, Organisationen und staatliche Institutionen richtete, war das niederländische CSBN einfacher strukturiert, bestand aus leicht verständlichen Botschaften und adressierte mit diesen sowohl Laien als auch außenpolitische Akteure. Das ist unter anderem damit zu erklären, dass das deutsche Cybersicherheitsgerüst, insbesondere innerhalb des BSI, breiter aufgestellt war und die Möglichkeit hatte, Adressaten zu differenzieren, wohingegen die Niederländer angesichts eingeschränkter Ressourcen weniger Kommunikationsmaßnahmen kuratieren konnten. So pflegte das BSI eigene Webseitenbereiche, Podcasts oder Newsletter für Verbraucher und Unternehmen, während das NCSC diese Gruppen nur unregelmäßig bediente.

Darüber hinaus erwies sich die Kommunikationsweise der untersuchten Institutionen als auffallend verschieden. Deutsche Behörden veröffentlichten vornehmlich Kommunikationsprodukte und Medieninhalte, die sowohl in ihrer Gestaltung als auch in der Sprache von großer Sachlichkeit waren. Die staatlichen Cybersicherheitseinrichtungen der Niederlande fielen demgegenüber regelmäßig mit sichtlich dramatischeren Ausdrucksformen auf, die nicht selten eine Bedrohung von Leib und Leben erklärten, da das Land systemisch von Informationstechnik abhängt, wie zum Beispiel bei der Steuerung seiner Deichanlagen. Genau gegenläufig präsentierten sich die zivilgesellschaftlichen Institutionen, die in Deutschland durch laute Kritik auf sich aufmerksam machten und in den Niederlanden kaum hörbar waren. Diese liegt inter alia in ihren engen funktionalen Verstrickungen mit dem niederländischen Staat begründet. So lässt sich festhalten, dass relevante staatliche Administrationen wie auch gesellschaftliche Organisationen national grundlegend unterschiedliche Auffassungen idealer Ansprache, Selbstrepräsentation und gegenseitiger Interaktion vertraten.

Die wohl gewichtigste Differenz zwischen den Cybersicherheitsstrukturen beider waren die jeweiligen staatlichen Organisationsprinzipien. Während die Bundesrepublik mit einem komplexen, föderalistischen Geflecht und unzähligen Beteiligten aufwartete, zeigte sich der niederländische, dezentrale Einheitsstaat beweglicher. Die Abstimmung von Bund, Ländern und Kommunen hemmte nicht nur die Geschwindigkeit und kostete viel Geld, sondern verhinderte manches Ansinnen, beispielsweise die Einführung eines

bundesweit verpflichtenden Informatikunterrichts, bereits in ihrer Entstehung. Allerdings wurde auch deutlich, dass die Bundesrepublik eminent mehr Betriebsmittel in Cybersecurity investierte. Dieses Mehr an Behörden, Finanz- und Personalmitteln bot wiederum ein Mehr an Handlungsräumen und Betätigungsfeldern. Die übersichtlichen Strukturen der Niederlande verlangten demgegenüber weniger Abstimmungsaufwände. Jedoch öffnete die geringere Verfügbarkeit von Geld und Experten größere Unsicherheitsräume und zwang die Beteiligten häufiger zu freier Momentgestaltung mit allen Vor- und Nachteilen dieser Methodik. Auch daraus rührt, dass die Niederlande versuchten, diesen augenscheinlichen Mangel durch eine ausgeprägte Kooperation mit der Wirtschaft zu assimilieren und das NCSC gar als „joint venture between government bodies and business enterprises“ anzulegen (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020b).

3. Wie formatieren die Institutionen die Logik der Informationssicherheit?

Unter Zuhilfenahme der drei Fallbeispiele der 5G-Einführung, der Schadsoftware Emotet und der behördeneigenen Öffentlichkeitsarbeit konnte die vor vielen Seiten referierte These Ulrike Felts erhärtet werden, dass Staaten technopolitische Identitäten ausbilden, die maßgeblich beeinflussen, welche Technologien und Innovationen auf welche Weise in Kulturräume implementiert werden. Denn Technologie „potenziert [...] ethische Fragestellungen“, sodass die Beantwortung oder wenigstens Besprechung dieser Fragen unter anderem den Konsens, oder auch Dissens, einer Gesellschaft abbildet (Stubbe et al. 2019, 248). Solche Verhandlungen von Moralität, soziotechnischen Zukunftsvariationen und politischen Programmatiken finden sich in der Beobachtung kürzlich vergangener Hergänge. Die Fallbeispiele 5G und Emotet eigneten sich besonders, um die Verwebung von Technologie und (Politik-)Kultur zu dechiffrieren. Das technische Produkt Emotet animierte in Deutschland sowohl gesellschaftliche als auch staatliche Akteure zu einer Unzahl an Mitteilungen und Verlautbarungen. Durch die stete Reproduktion und die Berichte über weitere schwere Vorfälle wurde die Schadsoftware zu einer anthropomorphen, nie dagewesenen Bedrohung, die im Titel *König der Schadsoftware* gipfelte. Somit veränderte Emotet die deutsche Perspektive auf Malware: Seit das Programm derartige Popularität erlangt hatte, kämpften das BSI und andere nicht mehr nur gegen eine Masse gesichts- und namenloser Täter, sondern gegen einen unbelebten, aber adressierbaren Widersacher. Emotet wurde damit zur Projektionsfläche möglicher Bedrohungs- aber auch

Retternarrative, die es beispielsweise dem BSI ermöglichten, eine intendierte Imagination von einer unheilvollen Emotet-Übermacht aufzubauen und weiter zu schüren. Diesem Bild folgend wurde Emotet gigantesk, sodass die allgemeine Erzählung einen impliziten Scheideweg enthielt: Das Schadprogramm müsse zerschlagen werden oder dem Medium E-Mail sei im Grunde nicht mehr zu trauen. Zu diesem Zeitpunkt war nicht nur objektiv die Cybersicherheitslage bedroht, sondern auch das digitale Sicherheitsempfinden in der Öffentlichkeit gab diese Gefährdung wieder, wie die breite Berichterstattung erkennen ließ. Die langanhaltende Machtlosigkeit von BSI und BKA entlud sich in entsprechend ausufernden Erfolgsmeldungen infolge des internationalen Ermittlungsdurchbruchs. Demgemäß haben die bestimmenden Akteure bereitwillig Imaginationen forciert und verbreitet, die das Schadprogramm zunehmend ikonisch werden ließen. In den Niederlanden traf Emotet dagegen auf keinen vergleichbaren Nährboden, obwohl sich die objektive Bedrohungssituation kaum von der deutschen unterschied. Das führte dazu, dass sich nur wenig Berichterstattung oder behördliche Kommunikation finden ließen. Die nahezu Nichtbenennung von Emotet verhütete, dass die Bevölkerung ein Interesse für die Causa entwickelte und sich damit belastete. Das NCSC und die Regierung perpetuierten auf diese Weise ihre arbeitsteilige Auffassung von Informationssicherheit: Der Staat bekämpft Gefährdungen wie Emotet – und feiert diese im Erfolgsfall mit der Öffentlichkeit – wohingegen die Endanwender konsumieren und sich in ihrer Nutzungsweise nicht eingeschränkt sehen sollen. Dies verhindert, dass das subjektive Unsicherheitssentiment zunimmt, obwohl die objektiv mögliche Schadeinwirkung existent ist.

Im Falle der Neueinführung des 5G-Mobilfunkstandards legte sich ebenfalls ein sehr ähnlicher Status quo beider Länder bei völlig unterschiedlichen nationalen Aufgabenadaptionen offen. Der Netzausbau in Deutschland verlief langsam und der dahingestellte Ausschluss chinesischer Komponentenhersteller zog eine lange, aber sachbezogene Debatte nach sich, wohingegen die Niederländer schnell ausbauten und ebenso schnell entschieden, Bauteile von Zulieferern wie Huawei aus dem Kern der Kommunikationsnetze zu verbannen. Während also der deutsche Kontrolldiskurs zu dem Schluss kam, über einen Huawei-Ausschluss erst nach andauernder Prüfung entscheiden zu wollen, war die niederländische Administration bereit, schon im Mai 2021 die Notbremse zu ziehen. Obwohl zu dieser Zeit keine akute Gefahr von derartigen Komponenten ausging, war das subjektive Bedrohungsempfinden in der

niederländischen Öffentlichkeit und bei den Verantwortlichen groß genug, um diese Entscheidung mit ihren möglicherweise nachteiligen Nebeneffekten in Kauf zu nehmen. Im Zuge dessen zeigte sich, dass die untersuchten Institutionen und ihre Öffentlichkeitsarbeit den eingangs resümierten Diskurstypen nach Reiner Keller gewissermaßen idealtypisch folgten und so die Ergebnisse der vorangegangenen Kapitel stützten. Unter den niederländischen staatlichen Institutionen war der Gefahrendiskurs dominant, der die Bedrohung ins Zentrum der öffentlichen Diskussion stellt, um davon ausgehend politische Beschlüsse in emotionalisierten Teilöffentlichkeiten, Parlamenten und Medien zu diskutieren. In Deutschland dagegen überwog der Kontroll- oder Normalisierungsdiskurs. Zwar sprachen deutsche Institutionen nicht davon, dass Cybersicherheit hergestellt sei, jedoch gaben sie zumeist vor, einen kontrollierbaren Zustand erreicht zu haben. „Denn erfolgreiche Cyber-Sicherheit ist unsichtbar. Nur wenn sie nicht funktioniert, wird sie sichtbar“, formulierte Arne Schönbohm 2021 für das Vorwort des Lageberichts (Bundesamt für Sicherheit in der Informationstechnik 2021a, 4). Die Institutionen normalisierten die grundsätzliche Angreifbarkeit der deutschen Infrastruktur, indem die bestehenden Sicherheitseinrichtungen als passgenaue Antwort auf die sich stetig wandelnden Bedrohungen inszeniert wurden. Im Normalfall funktionieren die Abwehrmechanismen und die Menschen im Land sind nicht beeinflusst von digitalen Vorfällen. In Einzelfällen allerdings kann selbst der beste Schutz nicht das Unglück verhindern, so das häufig zugrundeliegende Narrativ. Damit geht die Erzählung der Schuldlosigkeit der Sicherheitsinstitutionen einher, die nahezu ausschließlich mithilfe technischer Lösungen versuchten, möglicher Bedrohungslagen Herr zu werden – beides ebenso kennzeichnende Merkmale von Normalisierungsdiskursen.

Die vielfach herangezogenen Imaginaries sind nun die Brücke zwischen solchen Diskursen und dem manifestierten Kultursystem. Ganz im castoriadisichen oder später im jasanoffschen Sinne zeigte dieses Exempel sehr offenkundig Realeffekte politisch-technischer Wechselwirkungen auf. Denn obwohl Deutschland und die Niederlande, respektive ihre verantwortlichen Aufsichtsbehörden, vor der nahezu identischen Aufgabenstellung standen, haben sie diese Herausforderung unterschiedlich aufgefasst, in den öffentlichen Diskurs eingetragen und schließlich daraus abweichende Handlungserfordernisse abgeleitet, die unmittelbare Auswirkungen auf die 5G-Infrastruktur beider Länder sowie auf deren Abhängigkeit von der Technologie

politisch-ideologisch gelenkter Konzerne aus China hatten. Das leigen, also das Vorstellen und das Besprechen eines Mobilfunks mit oder ohne chinesische Komponenten, hat über das teukein, dem Verbot oder der vorläufigen Zulassung entsprechender Bauteile, Imaginationen zu Dominanz verholfen, die die Weichen in beiden Nationen in praxi disparat gestellt haben und deren langfristige Folgen nicht abzusehen sind.

In diesen Momenten verformt sich Cybersicherheitskultur. Aus soziotechnischer Betrachtung hat der divergente Eintrag von 5G in die nationalen Vorstellungswelten neue Konventionen geschaffen, die alternative Technologieexpressionen bevorzugen. Dabei kommt den Institutionen sichtlich die Funktion zu, übereinstimmende Anliegen zu transkribieren – und zwar in beide Richtungen. Das bedeutet, behördliche Institutionen sind ein Medium zur Aufnahme des Bevölkerungswillens, den sie wiederum bestenfalls mit Expertise anreichern, um so tragfähige Entscheidungen treffen zu können. Dieser vermeintlich demokratisierende Vorgang vollzieht sich allerdings genauso umgekehrt: Die Institutionen setzen ihre Agenda in tendenziöse Kommunikation und Einflussnahme um, damit ihr Konvolut aus politischen, gesellschaftlichen und technischen Zukunftsvorstellungen belastbare Zustimmung findet.

Diese gegenwärtige Technopolitik kommt nicht aus einem luftleeren Raum, sondern beruht, so eine der initialen Hypothesen, auf einem bestellten Feld aus Kultur und Tradition. Denn wie eingangs in aller Breite dargestellt, haben die Niederlande verinnerlicht, dass sie aufgrund ihrer Größe, ihrer geografischen Lage und ihrer Rolle im internationalen Staatsgefüge ein zugleich kleiner Staat mit begrenzten Mitteln wie auch ein progressives und wandelbares Kollektiv sind. Die Niederlande zeigen sich als ein vergangenheitsbewusstes Königreich mit Okkupationshistorie sowie starken konservativen Strömungen. Sie sind aber auch ein Land, das sich Technologien schnell nutzbar macht und sich durch eine Resilienz gegen externe Kräfte auszeichnet; seien es maritime Naturgewalten oder physische und digitale Attacken durch Russland, gegen die sich die Niederlande zur Wehr zu setzen wissen. Das zwang sie an vielen Zeitpunkten der jüngeren Vergangenheit zu gleichsinnigem Pragmatismus nach innen und einer erlernten Schutzhaltung nach außen. Diese Sensitivität gegenüber globalen Geschehnissen bei simultanem Festhalten an bewährten Traditionen hat sich kulturell stabilisiert (vgl. Wielenga 2020, 286).

Daher müssen im Befund zwei Kulturpraktiken erwähnt sein, die die Niederlande in ihrer Historie wiederholt angewandt haben und jetzt anlegen, um sich nunmehr in der digitalen Lebenswelt zu behaupten. Erstere zeigte sich bereits kurz nach dem Krieg: Das Land erfuhr einen Modernisierungsschub, weil es sich die Imagination zu eigen machte, ein modernes Land und künftig noch fortschrittlicher zu sein. Daraus resultierte ein ökonomischer und wissenschaftlicher Aufschwung, der dieses Zielbild realisierte. Später verhielten sich die Niederländer vergleichbar als sie die Verzuiling aufbrachen, indem sie einen Konsens heraufbeschworen. Lediglich der Ruf nach einer Konsensgesellschaft zu Zeiten tiefer Gräben zwischen den Säulen führte zu Jahren der Eintracht. Nun wenden die Niederlande diese Mechanik erneut an: Besonders die Regierung produziert Leitbilder und baut darauf, dass dieser Impuls ausreicht, um technologisch Schritt halten und sich gegen Gefahren abschirmen zu können.

Zweitens stülpt das Land ein weiteres erlerntes Prinzip staatlichen und gesellschaftlichen Handelns über das Digitale: Der Staat ist, wie festgestellt werden konnte, teilhabendes Korrektiv, indem er sich mit Regulierungen und Verboten zurückhält und die Weichen zum Gelingen einer Zukunftsvorstellung stellt. Das bedeutet für die digitale Sicherheitspolitik, dass die staatlichen Stellen nur für jene Lebensbereiche Regelungen treffen, die essenziell sind. So gibt die Regierung der Wirtschaft und den Privathaushalten nahezu freie Hand, weil sie der Annahme anhängt, auf diese Weise Innovationen und Prosperität zu begünstigen. Reguliert werden dagegen allen voran die kritischen Infrastrukturen, die in der niederländischen Gemeinschaft als lebenswichtiges Netzwerk verankert sind.

Hans Simons möchte in dieser außergewöhnlichen Konstellation einen Schöpfermechanismus für die niederländische Identität erkannt haben:

[T]he Netherlands is an increasingly important player in the field of cyber security, which in itself is an interesting development given its more limited resources compared to countries like the US, the UK or Germany. At the root of this development, as will be seen, is the desire to preserve Dutch identity (Simons 2014, 59).

Jedoch weisen die Resultate dieser Dissertation daraufhin, dass die Niederlande ihr Engagement in Cybersicherheit nicht ausschließlich betreiben, um eine Identität zu erhalten, sondern vielmehr um eine leichtgewichtige, dynamische, risikoaffine und somit handlungsfähige Cybersicherheitskultur in ihr zu assimilieren; trotz und wegen der vorhandenen Limitationen.

Demgegenüber steht mit der Bundesrepublik ein Land, das kaum über eine zentrale Identität verfügt. Mehr noch liegt die größte kulturelle Eigenheit der Deutschen, neben ihrer verbindenden Sprache, im Erleben ihrer eigenen Brüchigkeit etwa durch Teilung und spätere Wiedervereinigung. Exakt in dieser Phase der jüngeren deutschen Vergangenheit etablierte sich eher eine lange ideologische Zweiteilung statt einer Stabilisierung verbindender Identitätsmotive. Daher befindet sich Deutschland bis heute kulturell wohl auf der Suche nach identitätsstiftenden Leitmotiven jenseits vielfach reproduzierter Stereotypen vom Land der Autobauer, der Dichter und Denker, vom Exportweltmeister oder bis heute vom Land des Nationalsozialismus. So gehören Wirtschaft und Sport immer wieder zu den wenigen identitätsbildenden Sphären, die ihre Funktion daraus schöpfen, die Deutschen zum Beispiel unter dem Siegel Made in Germany ökonomisch herausragen zu lassen oder sie im kompetitiven Wettstreit zusammenführen. Demnach besäße die Bundesrepublik aufgrund der angestammten Technologiekompetenz und des zugeschriebenen Forschergeistes eigentlich beste Voraussetzungen für eine sichere Digitalisierung. Indes zeigte sich jedoch, dass Deutschland – insbesondere in der direkten Gegenüberstellung mit den Niederlanden – langsam und immobil agiert. Seine ökonomische Stärke erzielt Deutschland bis heute mit industriellen Erzeugnissen aus Stahl, Chemikalien oder Elektrotechnik. Diese konventionelle Generierung von Werten durch Produktion kann nur sukzessive digitalisiert und kaum virtuell kommerzialisiert werden. In der Vergangenheit zeichnete sich das politische Deutschland zusätzlich durch einen strategischen und technologischen Konservatismus aus, der mehrere Hemmnisse für eine sichere Digitalisierung ausgebildet hat. So rang das Land mit einem Modernisierungsstau seiner Infrastrukturen, zum Beispiel beim Ausbau schneller Glasfaseranbindungen, die wiederum substanziell für den Aufbau von tragfähigen Mobilfunknetzen sind. Anstatt Digitales als integralen Bestandteil aller Ressorts zu betrachten und zu zentralisieren, wurde das Handlungsfeld an die bestehenden interdependenten Behördenstrukturen gekoppelt und auf verschiedene Häuser, darunter BNetzA, BfDI, Innenministerium oder Verkehrsministerium verteilt. Die IT-Sicherheit als Spezifikum ist nach wie vor horizontal im Bund auf mehrere Kompetenznehmer zerstreut. Vertikal wurde Informationssicherheit in den föderalistischen Kategorien nicht planvoll bedacht und ist jedem Bundesland und jeder Kommune in großen Teilen selbst überlassen. Gleichzeitig fassten deutsche, staatliche Institutionen die Cybersicherheit im Gegensatz zu den Niederlanden holistisch auf: Allen voran BMI und BSI etablierten

Informationssicherheit als eine Herausforderung, die alle Menschen und Lebenswelten betrifft, sodass die Behörden nicht nur den Schutz elementarer Strukturen oder Netzwerkpunkte anvisierten, sondern beispielsweise auch den Verbraucherinnen und Verbrauchern Hilfestellungen anboten oder technische Richtlinien für digitale Produkte herstellten.

Insgesamt lassen die Untersuchungsergebnisse die Bemerkung zu, dass deutsche Institutionen, politische Entscheider und letztlich Teile der Gesellschaft den Versuch unternehmen, erlernte Erfolgsmechanismen auf Digitalisierung und Informationssicherheit zu übertragen. Denn in den Jahrzehnten nach dem Zweiten Weltkrieg hatten sich Prosperität und Sicherheitsempfinden durch den Produktionsausbau materieller Wirtschaftsgüter, durch eine stabile Verwaltungsordnung und durch defensive Außenpolitik bei offensiver Wirtschaftspolitik eingestellt. Wenngleich Deutschland in Europa über viele Jahre eine ökonomische wie politische Führungsrolle, beispielsweise während der Einführung des Euro, während der europäischen Finanzkrise oder in der Migrationskrise, eingenommen hatte, fehlen dem Land in der Digitalisierung sowie in der Sicherung der digitalen Lebenswelt nun Erfolgsfaktoren wie Geschwindigkeit oder Innovation. Diese Trägheit innerhalb des technologischen Umbruchs von Verwaltung, Verkehr oder Kommunikation verkommt in Deutschland allmählich zu einem imagebildenden Klischee, das positiv besetzten Voraussetzungen im Wege steht. Mithin mündet diese wenig adaptionsfähige Ordnung der letzten Dekaden heute in ein Land, das über großes monetäres, wissenschaftliches und ökonomisches Vermögen verfügt, zugleich aber mit den Regeln der erlernten Weltordnung versucht, im digitalen Zeitalter gleichsam erfolgreich zu sein oder den bisherigen way of life wenigstens konservieren zu können.

Im Ergebnis drückt sich aus, dass die grundlegende Prämisse zutrifft: Deutschland und die Niederlande verfolgen tatsächlich unterschiedliche Modi zur Synthese von Cybersicherheit. Beide Länder pflegen eigene Vorstellungen und Regelungen in Bezug auf Datensicherheit und agieren aus ihrer individuellen Historie heraus. Sie verfolgen diverse Strategien, werden von unterschiedlichen Motivationen angetrieben und zielen dennoch auf vergleichbare Intentionen ab. Sie unterscheiden sich in den Maßstäben ihrer Anstrengungen, in der Finanzierung von Sicherungsmitteln und in der Komplexität der Organisation von IT-Sicherheit. Wenn in Deutschland von staatlicher Zuständigkeit der Cyberabwehr die Rede ist, ist damit eine erheblich tiefere Intervention in weite

Gesellschaftsbereiche adressiert als in den liberalistischen Niederlanden. Wenn niederländische Behörden mit Informationssicherheit betraut sind, neigen sie zu ausgeprägterer Risikoaffinität und Konfrontationsbereitschaft, setzen auf intensivere Kooperationsarbeit mit Initiativen sowie Verbänden und initiieren vorzugsweise privat-öffentliche Partnerschaften, um Problemstellungen anzugehen. Selbst die Inzentive zur Errichtung digitaler Sicherheitsstrukturen divergieren: Die Niederlande sehen sich existenziell bedroht, da massive Cyberangriffe schlimmstenfalls ökologisch bedingte Katastrophen herbeiführen oder zumindest die Integrität der Niederlande bedrohen könnten. Deutsche Schutzbemühungen zielen dagegen darauf ab, die Gewissheiten ökonomischen Handelns und damit die Lebensgrundlage der Wirtschaft zu behüten.

Die Bundesrepublik investiert dafür hunderte Millionen Euro jährlich in IT-Sicherheit, beschäftigt tausende Menschen mit der Absicherung von Technologien und formuliert den Anspruch, Staat, Wirtschaft und Gesellschaft gleichermaßen zu schützen – ihr Handeln ist durchaus effektiv. Das Königreich der Niederlande demgegenüber agiert effizient, indem es seine ohnedies geringeren Kapazitäten selbsttätig auf ein Minimum an finanziellen Mitteln, personellen Ressourcen sowie Institutionen beschränkt, dies allerdings durch unkonventionelle Entwürfe auszugleichen versucht.

IV.I. Evaluation des Forschungsdesigns

Zunächst einmal hat die Wortneubildung *Cybersicherheitskultur* den Grundstein für die eigentliche Untersuchung gelegt. Die wissenschaftliche Herleitung dieses Neologismus stellte erstmalig den überfälligen Konnex zwischen der Cybersicherheit und ihrer kulturellen Einbettung her. Mehr noch öffnete dies das Interpretationsfeld, das zur Betrachtung der Untersuchungsgegenstände nötig war. Der systematische Dreiklang aus Begriffsklärung respektive -schöpfung, der darauf aufbauenden Institutionenanalyse und abschließend der Auswertung jüngster Vorkommnisse vermittelte eine Draufsicht auf den Umgang beider Länder mit digitalen Sicherheitsherausforderungen. Aus dieser Methodik resultierten drei wesentliche Leistungen.

1. Das Vorgehen hat aufgezeigt, dass Institutionen selbst Medien zur Reproduktion von Imaginationen sind. Institutionen sind Ausdruck interpersoneller Stabilisierungsmechanismen und erhärten soziale Habitus und Anschauungen weiter. Als Kulturmedien erfüllen sie den Zweck, Motive gesellschaftlicher Konformität abzubilden und zu priorisieren. Aus der, in diesem Fall demokratischen, Legitimation

einer Institution spricht die Übereinkunft, dass diese Entität notwendige, mindestens aber sinnvolle, Funktionen für das Gelingen des sozialen Gefüges beiträgt. Mit dem Vergleich analoger Institutionen der Niederlande und Deutschlands konnten also belastbare Rückschlüsse auf die Prioritäten, die Organisationsweise und die interpersonellen Wirkungen im Umgang mit Cyber(un)sicherheit innerhalb der jeweiligen Kollektive gezogen werden; letztlich untermauert dies die Reliabilität der Methodik.

2. Die Dissertation hat die signifikanten Unterschiede sowie Gemeinsamkeiten der Forschungsobjekte offenbart: So hat sich die Annahme bestätigt, dass ähnliche Umstände, wie Wohlstand, geografische Lage in Europa oder ein vergleichbares Bedrohungsszenario zu ähnlichen Defensivstrategien und einhergehend zu verwandten Handlungs-, Institutionalisierungs- und Kommunikationsmustern führen. Gleichmaßen zeigte sich, dass zwischen allen Similaritäten auch Spezifika zu finden sind, die sich teils erheblich voneinander unterscheiden und in der vergleichenden Methode entsprechend herausragten. Schließlich konnte mit dieser Praktik ein Nexus zwischen den Vergangenheitserfahrungen Deutschlands und der Niederlande, den daraus erwachsenen Kultursphären sowie ihrem Transfer auf die neue Gegenwartsaufgabe Informationssicherheit hergestellt werden.

3. Es entstand ein systematisches Verfahren, dass ausreichend generalisierbar und anpassungsfähig ist, um es nutzbringend auf zusätzliche Vergleichsoperationen anlegen zu können. Der Begriff der Cybersicherheitskultur erwies sich als eine Aggregation bedingungsvoller Korrelationen aus neben anderem Technologie, Politik, Ökonomie, Exposition, Prosperität und Medien. Um also diese Aspekte sinnvoll in Relation setzen zu können, war es unerlässlich, eine neue Methode zu entwickeln oder bereits erprobte Ansätze zu adaptieren und zu modifizieren.

Die Grundlage der Untersuchung bildete zunächst eine Aufstellung und Betrachtung der maßgeblichen Institutionen innerhalb Deutschlands und der Niederlande. Daraus resultierte zugleich eine Übersicht über identifizierte Herausforderungen, denen mit diesen Behörden, Verbänden oder Ministerien begegnet werden soll. Dies führte zu Erkenntnissen darüber, welches Gewicht diesen Institutionen im Einzelnen beigemessen wird, wenn der Blick auf den Haushalt, die Personaldichte oder das Aufgabenspektrum fällt. Mithilfe der Added Values ließen sich die Texte, Strategien und Agenden jeweils

binären Polen zuordnen. Das führte notwendigerweise zu starken Vereinfachungen komplexer Gesellschafts- oder Politikgebilde, erlaubte aber auch eine erste, noch unpräzise Identifizierung substanzieller Unterschiede beider Kulturen. Vervollständigt wurde die Triangulation mit der Identifizierung sogenannter Imaginaries, die unterstrichen, dass in jeder Gesellschaft oder kulturellen Gruppe Bilder der Welt existieren, die mit Erwartungen, Ängsten oder Hoffnungen verbunden sind. Bei der Erkundung dieser Imaginationen fiel der Blick auf leitende Handlungsmotive der beiden Staaten und speziell darauf, inwiefern diese Imaginaries auf die Realität rekurren.

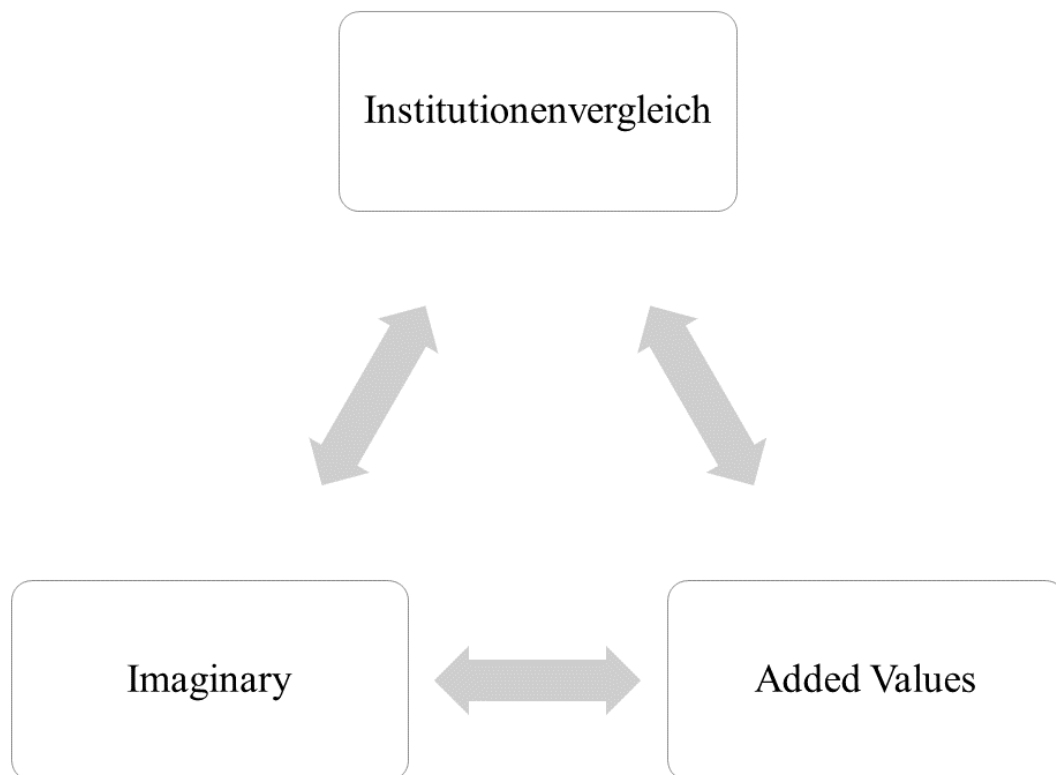


Abbildung 25: eigene Darstellung

Triangulation meint in diesem Sachzusammenhang, dass die unterschiedlichen Informationen und Einsichten, die aus den drei Methoden zusammenlaufen, wiederum ein neues Abbild ergeben, wenn man sie verkettet. So gibt etwa die Verbindung der identifizierten Vergleichsinstitutionen mit den Added Values, also der Abgleich der Institutionen mit den kulturbeschreibenden Polen, Auskunft über Ursache und Wirkung, über die Relation von Gesinnung und Handeln. Dies wird dann angereichert mit dem Konzept des Imaginary, also mit bildhaften Zukunftskonstellationen, die die Lebensrealität beeinflussen. Die Imaginaries zeigten zuvorderst auf, inwieweit sich die Institutionen über Narrative legitimierten. Denn unbestritten zahlen Imaginaries auf

kollektive Ideen von Verantwortung, Bedrohung, Gut und Böse, Gemeinschaft und Sicherheit ein und führen so kulturelle Tendenzen herbei, die dann wieder die Entstehung von Institutionen prägen. Aus diesem Widerhall formten sich die Konterfeie zweier Kulturen, zweier Cybersicherheitskulturen, mit ihren wesentlichen Attributen. Vor allem im direkten Gegenschnitt zur je anderen Vergleichskultur materialisieren sich die bedeutenden, immanenten Kontraste. Letzten Endes entstand ein Typus, der die jeweilige Kultur nicht in ihrer Gänze abbildet, aber dafür Vergleichbarkeit sowie Übersicht herstellt. Das Schema ist hinreichend flexibel und somit auf nahezu jeden Ländervergleich oder auch Vergleich von zum Beispiel Kulturräumen oder gar anderer Vergleichsobjekte zweckdienlich applizierbar.

IV.II. Kritische Auseinandersetzung

Notwendigerweise hinterlässt diese Analyse theoretische wie auch forschungspraktische Implikationen. Es ist beispielsweise gelungen, eine neue Anschauungsweise der zwei Untersuchungsobjekte aufzubauen, die die Konzepte von Motivation, Kultur und Cybersicherheit enger verknüpft als bislang. Dazu trägt die überfällige Anfüllung des Begriffs Cybersecurity Culture mit Sinngehalten außerhalb von artifiziellen, organisationsspezifischen Regelsystemen bei. Cybersecurity Culture war in der Wissenschaft bislang nur als Phänomen innerhalb kapitalistischer Ordnungen, also innerhalb von Unternehmen oder Märkten, nie aber als einer der unzähligen inhärenten Bausteine gesellschaftlichen Zusammenlebens erfasst worden. Die Öffnung des Terminus zu einer Domäne von Kultur mit holistischer Geltung löst Cybersicherheitskultur aus der Organisationstheorie heraus und bricht einen Zugang zu interpersonellen, sozialen Kategorien von IT-Sicherheit auf.

In diesem Zuge wurde offenbar, dass sowohl Castoriadis Gedanken zu Imaginärem, insbesondere seine Ausdeutung der Radikalität, als auch Jasanoffs soziotechnische Imaginaries weiterhin anschlussfähig sind, indem sie Anwendenden nicht nur Perspektivwechsel ermöglichen, sondern sich durch die Anwendung selbst fortschreiben und expandieren. Denn verbunden mit den Added Values nach Daase, Junk und Rauer verhelfen ihre Theoreme zu neuen Interpretationsräumen und Untersuchungsmöglichkeiten, die jenseits von harter Empirie dennoch reliable Resultate produzieren.

Diese Form des Vergleichens hat darüber hinaus ganz praktische Vorzüge für die Untersuchten. Denn auch die gegenübergestellten Länder und Institutionen können nun deutlicher sehen, wo eigene Stärken und Schwächen liegen; sie können sich aber vor allem an den besonderen Fähigkeiten des jeweils Anderen orientieren. Gegebenenfalls könnte gar der Versuch unternommen werden, Imaginationen, Kommunikationsmodi oder Organisationssystematiken zu übernehmen, um die eigene Cybersicherheitskultur umzugestalten. Manche Funde dieser Arbeit – darunter die niederländische Zentralisierung von IT-Sicherheitskompetenz oder die deutsche Verantwortlichkeit für alle Anspruchsgruppen der Gesellschaft – haben das Potenzial, in die Methoden und Praktiken des Nachbarn zu migrieren, andere sind dagegen höchst landesspezifisch.

Bei allen Nutzeffekten, die sich gezeigt haben, weist das Vorgehen Limitierungen auf. Eine Insuffizienz ist unvermeidbarer Teil der Added Values: Zwar lässt die Zuordnung zu den Polen der Binärpaare grundsätzliche Aberrationen erkennen, jedoch verstellt dieses Vorgehen den Blick für graduelle Unterschiede. So ergibt die Analyse, dass das deutsche IT-Sicherheitsgesetz als restaurativ zu werten war, wohingegen das niederländische Wet beveiliging netwerk- en informatiesystemen (Wbni) progressiv gesehen wurde. Wie sehr beide Gesetze den ihr zugeteilten Polen entsprachen, bleibt in der bloßen Betrachtung ihrer Verortung unsichtbar. Die Added Values zeigen demnach an, welcher Seite der Polarität ein Untersuchungsobjekt überwiegend entspricht. Sie sagen zunächst aber wenig darüber aus, in welchem Ausmaß oder in welcher Intensität es in dieser Hälfte der Dichotomie liegt. Hier könnte die Ergänzung durch eine zusätzliche Methode Abhilfe schaffen.

Der Vergleich, dem die Added Values schließlich untergeordnet sind, birgt dabei ebenfalls Unzulänglichkeiten, die bedacht werden müssen. Es handelt sich bei dieser Arbeit um die weitestgehend isolierte Begutachtung lediglich zweier Untersuchungsgegenstände. Gleichzeitig bestehen diese vielschichtigen Objekte, also Deutschland und die Niederlande, in einer dynamischen und brüchigen Systemumwelt. Für den Vergleich müssen nun sowohl die Untersuchten als auch ihre Umwelt simplifiziert werden, um den Fokus der Analyse nicht zu verlieren. Hinzuzurechnen ist, dass der Forschende diese Dissertationsschrift zeitlich wie auch kulturell aus der individuellen Perspektive seines sozialen Milieus, eines erlernten westeuropäischen Zentralismus sowie seiner Erfahrungen und angeeigneten Kapazitäten antrat. Das wiederum beeinflusste die Auswahl der Vergleichsgrößen und -variablen und birgt

immer das Risiko von unausgewogener Distanz zwischen Forschendem und Forschungsobjekt in sich (vgl. Layes 2005, 72). Zumal der Vergleich sogenannte Nachbarschaftsauswirkungen, also die gegenseitige Beeinflussung physisch nahe liegender Objekte, wie auch die Interaktionseffekte durch unterschiedlich skalierte Entitäten nicht exakt abbilden kann (vgl. Berg-Schlosser 2016, 11). Schließlich ergibt sich aus der hier notwendigen Abstraktion, dass weder regionale noch transnationale Kultureffekte oder Imaginaries sinnhaft herausgestellt werden konnten.

Einen Mangel stellt das unvermeidliche Ende des Untersuchungszeitraums dar. In diesem Fall setzte der Überfall Russlands auf die Ukraine den Endpunkt der Betrachtungsperiode, sodass diese Arbeit als Blick auf ein historisches Intervall zu verstehen ist. Diese inhärente Limitierung ist zugleich erster Anknüpfungspunkt für möglicherweise aufbauende Analysen: Diese Dissertation stellt Werkzeuge bereit, um beispielsweise auf der temporalen Achse zu untersuchen, wie deutsche und niederländische Cybersicherheitsbemühungen seit Beginn 2022 fortgeschritten sind. Ebenso gut ist es möglich, die Methodik auf weitere Vergleichskonstellationen anzuwenden, um etwa andere Staaten heranzuziehen oder mit völlig neuen Vergleichsobjekten zu iterieren. Sie bedarf Verfeinerungen, beispielsweise bei der passgenauen Auswahl der Added Values-Pole, erlaubt dann aber sowohl tiefer gehende Studien des hier bemühten Vergleichs als auch breitere Forschungsvorhaben mit mehr als zwei Objekten. Wohl wissend, dass diese Arbeit nie Vollständigkeit zu erreichen vermag, kontribuiert sie doch eine wertvolle Vorgehensweise zur aussagekräftigen Betrachtung von Cybersicherheitskulturen und überlässt es kommender Episteme, die Leerstellen geeignet zu füllen.

IV.III. Ausblick

Da sowohl der Begriff der Cybersicherheitskultur erarbeitet ist als auch eine Schablone für einen Institutionenvergleich geschaffen wurde, ist der Weg für anknüpfende Arbeiten, wenn nicht geebnet, dann wenigstens von Hindernissen geräumt. Schlussendlich, und darin liegt eine persönliche Hoffnung, können zukünftige Abhandlungen diese Verfahrensweise weiterentwickeln, um sie schlanker und anwenderfreundlicher zu adaptieren. Es bleibt zudem abzuwarten, wie Deutschland und die Niederlande kommenden Herausforderungen begegnen. Die gerade erst begonnene digitale Transformation aufbauend auf Technologien wie künstlicher Intelligenz,

Quantencomputing und Automation zieht eine Vervielfachung der Rechenleistung und damit auch der Möglichkeiten nach sich – auch für Kriminelle. So finden sich sowohl die Niederlande als auch Deutschland in dem ständigen Bemühen wieder, ein Equilibrium aus tradierten Identitäten und rasender Erneuerung aufrechtzuerhalten, damit „moralische Integration und Konsens gegen die Logik der Modernisierung weiterhin gewährleistet werden“ (Sander 1998, 50). Diese Anstrengungen unternehmen beide Kulturräume und Staaten während multipler Krisen und komplexer werdender Lebenswelten. Sie sind konfrontiert mit dem globalen Aufstieg des Populismus und einem verheerenden Krieg in Europa, der die Sicherheitstektonik irreversibel umgestoßen hat. Hinzukommen geopolitische Verschiebungen, die unter anderem von China und den USA forciert werden und schließlich ökonomische und politische Bedrängnisse, die die angestammten Demokratien unter Druck setzen. Auch deshalb lohnt sich in den kommenden Jahren sowohl eine Wiederholung dieses Vergleichs als auch die Durchführung weiterer solcher Studien. Denn zweifelsfrei war schon während der Anfertigung dieser Dissertationsschrift zu beobachten, dass sich Umstände in einer Rasanz veränderten, die absehbar Konsequenzen für die Cybersicherheitskulturen und die vorherrschenden Imaginaries haben werden.

Dank

Am Ende dieses Forschungs- und Lernprozesses steht die Erkenntnis, dass diese Arbeit zwar von einer Person verfasst, aber von vielen geschultert wurde. Während der Ideenfindung, Recherche, Lektüre, Niederschrift, während Freude und Verzweiflung hatte ich in den zurückliegenden Jahren liebe Menschen um mich, die mir mit Rat, Tat, wirksamer Ablenkung, gleißenden Fragen, ehrlichen Hilfsangeboten, liebevoller Kinderbetreuung, gutem Essen oder einem Lächeln zur Seite standen.

Zu diesen Menschen gehört Prof. Dr. Jens Schröter, der mich durch inspirierende Lehrveranstaltungen überhaupt erst mit dem Gedanken anfreunden ließ, nach meinem Studium ein Promotionsprojekt mit dem passenden Betreuer in Angriff nehmen zu wollen. Seinen sprudelnden Denkanstößen verdanke ich so manche Sorgenfalte der Überforderung, aber vor allem die entscheidenden Kurswechsel und die Courage zu grundstürzenden Entscheidungen. In diesem Zuge möchte ich mich bei allen Mitgliedern der Prüfungskommission bedanken: Prof. Dr. Britta Hartmann, Dr. Christoph Ernst sowie Prof. Dr. Adrian Hermann halfen mir vor allem dabei, die Dissertation über die Ziellinie zu bringen.

Auch die mitleidenden Doktoranden des begleitenden Kolloquiums möchte ich honorieren, weil ich unsere regelmäßigen Treffen oft mit neuem Mut verlassen habe und sie mich wissen ließen, dass nicht nur ich wiederholt im Dunkeln tappe. Genauso motivierend waren Freunde, Kollegen und Verwandte, die immer wieder gestichelt und sich sechs Jahre lang nach meiner baldigen Abgabe erkundigt haben.

Meinen Eltern sage ich danke, weil sie mich auf meinem langen Bildungsweg unterstützt haben, beispielsweise indem sie den Schuldirektor unfreiwillig gut kennenlernten, indem sie mir das Studieren in einer fremden Stadt ermöglichten und indem sie mich darin bestärkt haben, zu promovieren. Ihnen und auch meinen Schwiegereltern danke ich nicht zuletzt für die bedingungslose Betreuung unserer Tochter Selma, wenn uns das Wasser bis zum Hals stand.

Am wichtigsten für den Abschluss dieser Dissertation war aber meine Frau Meike. Du hast mich in den schwierigen Phasen aufgebaut und in glänzenden Zeiten geerdet. Du hast mir immer Gelegenheiten gegeben, mich zurückziehen und konzentrieren zu können. Vor allem aber hast du stets mehr an das gute Ende geglaubt als ich.

Danke.

Hilfsmittel

Zur Prüfung von Rechtschreibung und Grammatik wurde das Programm Languagetool verwendet, das sich unter anderem auf Künstliche Intelligenz stützt. Analog zu üblichen automatischen Rechtschreibkorrekturen überprüft das Programm den regelgerechten Einsatz der deutschen Sprache. Zu keinem Zeitpunkt wurde von generativen Funktionen Künstlicher Intelligenz zur Erstellung von Inhalten, Argumenten oder Phrasen Gebrauch gemacht.

Literatur

- Abbate, Janet (2010): Privatizing the Internet: Competing Visions and Chaotic Events, 1987–1995. In: *IEEE annals of the history of computing*, Bd. 14, Nr. 1, S. 10–22.
- Adorno, Theodor W./Horkheimer, Max (2019): *Dialektik der Aufklärung. Philosophische Fragmente*. 24. Aufl. Frankfurt am Main: Fischer Taschenbuch Verlag.
- Aiken, Mary (2018): *Der Cyber-Effekt. Wie das Internet unser Denken, Fühlen und Handeln verändert*. Frankfurt am Main: Fischer Taschenbuch Verlag.
- Andersson, Magdalena/Blümel, Gernot/Hoekstra, Wopke/Matovič, Igor/Reirs, Jānis/Saarikko, Annika/Schillerová, Alena/Wammen, Nicolai (2021): *Common views on the future of the Stability and Growth Pact*.
- Auerbach, Benedikt/Kiltz, Eike/Shnayien, Mary/Tuschling, Anna (2019): Zwei Betrachtungen von Sicherheit und Privatheit nach Snowden. In: *Datenschutz und Datensicherheit*, Bd. 43, Nr. 11, S. 706–712.
- Badke-Schaub, Petra/Hofinger, Gesine/Lauche, Kristina (Hrsg.) (2008): *Human Factors. Psychologie sicheren Handelns in Risikobereichen*. Heidelberg: Springer Medizin.
- Balzacq, Thierry (2005): The Three Faces of Securitization: Political Agency, Audience and Context. In: *European Journal of International Relations*, Bd. 11, Nr. 2, S. 171–201.
- Baudrillard, Jean (1991): Simulacra and Science Fiction. In: *Science Fiction Studies*, Bd. 18, Nr. 3, S. 309–313.
- Bauman, Zygmunt (2000): *Flüchtige Moderne*. Wiesbaden: Springer.
- Bauman, Zygmunt/Lyon, David (2013): *Daten, Drohnen, Disziplin*. Berlin: Suhrkamp.
- Beck, Klaus (2014): Kommunikationsforschung/Medienwirkungsforschung. In: Ruschmeyer, Simon/Schröter, Jens (Hrsg.)/Walke, Elisabeth: *Handbuch Medienwissenschaft*. Stuttgart: J. B. Metzler'sche Verlagsbuchhandlung und Carl Ernst Poeschel Verlag GmbH, S. 453–460.
- Beißel, Stefan (2019): *Security Awareness: Grundlagen, Maßnahmen und Programme für die Informationssicherheit*. Berlin/Boston: Walter de Gruyter GmbH.
- Benjamin, Walter (2010): *Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit*. Berlin: Suhrkamp.
- Berg-Schlosser, Dirk (2016): Historische Entwicklungen und Grundlagen der Vergleichenden Politikwissenschaft. In: Lauth, Hans-Joachim (Hrsg.)/Kneuer, Marianne (Hrsg.)/Pickel, Gert (Hrsg.): *Handbuch Vergleichende Politikwissenschaft*. Wiesbaden: Springer, S. 3–22.
- Bergem, Wolfgang (Hrsg.)/Diehl, Paula (Hrsg.)/Lietzmann, Hans J. (Hrsg.) (2019): *Politische Kulturforschung reloaded: Neue Theorien, Methoden und Ergebnisse*. Bielefeld: transcript Verlag.

- Berger, Peter L./Luckmann, Thomas (2018): *Die gesellschaftliche Konstruktion der Wirklichkeit: Eine Theorie der Wissenssoziologie*. 27. Aufl. Frankfurt am Main: Fischer Taschenbuch Verlag.
- Bieser, Jan/Salieri, Beatrice/Hischier, Roland/Hilty, Lorenz M. (2020): *Next generation mobile networks: Problem or opportunity for climate protection?* Zürich: University of Zurich/Empa.
- Boaru, Gheorghe / Iorga, Benedictos (2015): Security Culture – The first line of Cyber Defense. In: *Annals – Series on Military Sciences*, Bd. 7, Nr. 2, S. 31–46.
- Bonacker, Thorsten (2009): Konflikttheorien. In: Kneer, Georg/Schroer, Markus (Hrsg.): *Handbuch Soziologische Theorien*. Wiesbaden: Springer, S. 179–198.
- Broschek, Jörg (2009): *Der kanadische Föderalismus. Interstaatlicher und Intrastaatlicher Föderalismus*. Wiesbaden: Springer.
- Broschek, Jörg (2016): Staatsstrukturen in der Vergleichenden Politikwissenschaft: Föderal- und Einheitsstaat. In: Lauth, Hans-Joachim (Hrsg.)/Kneuer, Marianne (Hrsg.)/Pickel, Gert (Hrsg.): *Handbuch Vergleichende Politikwissenschaft*. Wiesbaden: Springer, S. 331–344.
- Brünker, Felix/Deitelhoff, Fabian/Mirbabaie, Milad (2019): *Collective Identity Formation on Instagram – Investigating the Social Movement Fridays for Future*. Perth Western Australia: Australasian Conference on Information Systems.
- Bulanova-Hristova, Gergana (Hrsg.)/Kasper, Karsten (Hrsg.)/Korsell, Lars (Hrsg.)/Odinot, Geralda (Hrsg.)/Pool, Ronald (Hrsg.)/de Poot, Christianne (Hrsg.)/Verhoeven, Maite (Hrsg.)/Werner, Yael (Hrsg.) (2016): *Cyber-OC – Scope and manifestations in selected EU member states*. Wiesbaden: Bundeskriminalamt.
- Buras, Piotr/Puglierin, Jana (2021): *Beyond Merkelism: What Europeans expect from post-election Germany*. London: European Council on Foreign Relations.
- Burri, Regula Valérie (2015): Imaginaries of Science and Society: Framing Nanotechnology Governance in Germany and the United States. In: Jasanoff, Sheila (Hrsg.)/Kim, Sang-Hyun (Hrsg.): *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: The University of Chicago Press, S. 233–253.
- Busse, Dietrich (1987): *Historische Semantik: Analyse eines Programms*. Stuttgart: Klett-Cotta.
- Buzan, Barry/Hansen, Lene (2010): Beyond The Evolution of International Security Studies? In: *Security Dialogue*, Bd. 41, Nr. 6, S. 659–667.
- Castoriadis, Cornelius (1990): *Gesellschaft als imaginäre Institution*. Frankfurt am Main: Suhrkamp Verlag.
- Cohen, Elizabeth F. (2018): *The Political Value of Time Citizenship, Duration, and Democratic Justice*. Cambridge: Cambridge University Press.
- Couldry, Nick (2012): *Media, society, world: Social theory and digital media practice*. Cambridge: Polity Press.

- Daase, Christopher (2010): *Der erweiterte Sicherheitsbegriff*. Frankfurt am Main: Goethe-Universität Frankfurt.
- Daase, Christopher (2012): Sicherheitskultur als interdisziplinäres Forschungsprogramm. In: Daase, Christopher (Hrsg.)/Offermann, Philipp (Hrsg.)/Rauer, Valentin (Hrsg.): *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*. Frankfurt am Main: Campus Verlag, S. 23–44.
- Daase, Christopher/Junk, Julian/Rauer, Valentin (2014): Konjunkturen des Kulturbegriffs: Von der politischen und strategischen Kultur zur Sicherheitskultur. In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.)/Endreß, Christian (Hrsg.): *Dimensionen der Sicherheitskultur*. Wiesbaden: Springer, S. 33–56.
- De Hoon, Marieke (2019): Pursuing Justice for MH17: The Role of the Netherlands. In: Nijman, Janne E. (Hrsg.)/Werner, Wouter G. (Hrsg.): *Netherlands Yearbook of International Law 2018. Populism and International Law*. Den Haag: Asser Press, S. 245–270.
- Derrida, Jacques (1972): *Die Schrift und die Differenz*. Frankfurt am Main: Suhrkamp Verlag.
- Diekstra, René (2009): Steeds minder ruimte. Hoe publiek verliest van privaat. In: Boutellier, Hans (Hrsg.)/Boonstra, Nanne (Hrsg.)/Ham, Marcel (Hrsg.): *Omstreden ruimte. Over de organisatie van spontaniteit en veiligheid*. Amsterdam: Van Genneep, S. 211–224.
- Edelmann, David (2014): *Dezentrale Regierungs- und Verwaltungssysteme: bürgerlich, demokratisch und leistungsfähig. Beratungsansatz und Beispielvorbereiten in den Bereichen Dezentralisierung, lokale Selbstverwaltung und Föderalismus*. Bonn: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.
- Endreß, Christian/Feißt, Martin (2014): Von der Sicherheit zur Sicherheitskultur - Über den Umgang mit Komplexität im Sicherheitsdiskurs. In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.)/Endreß, Christian (Hrsg.): *Dimensionen der Sicherheitskultur*. Wiesbaden: Springer, S. 19–32.
- Ernst, Christoph/Schröter, Jens (2020): *Zukünftige Medien. Eine Einführung*. Wiesbaden: Springer.
- Ernst, Christoph/Schröter, Jens (2022a): Radikale Imagination. Zum 100. Geburtstag von Cornelius Castoriadis. In: *Zeitschrift für Kulturwissenschaften. Radikale Imaginationen*, Bd. 16, Nr. 2, S. 11–17.
- Ernst, Christoph/Schröter, Jens (2022b): Ist eine andere Technik möglich? Zum Verhältnis von Imagination, zukünftiger Technik und implizitem Wissen bei Cornelius Castoriadis. In: *Zeitschrift für Kulturwissenschaften. Radikale Imaginationen*, Bd. 16, Nr. 2, S. 161–176.
- Fehr, Sonja/Vobruba, Georg (2011): Die Arbeitslosigkeitsfalle vor und nach der Hartz-IV-Reform. In: *WSI Mitteilungen*, Bd. 5, S. 211–217.
- Felder, Ekkehard (2013): Faktizitätsherstellung mittels handlungsleitender Konzepte und agonaler Zentren. Der diskursive Wettkampf um Geltungsansprüche. In: Felder, Ekkehard (Hrsg.): *Faktizitätsherstellung in Diskursen. Die Macht des Deklarativen*. Berlin: De Gruyter, S. 13–28.

- Felt, Ulrike (2015): Keeping Technologies Out: Sociotechnical Imaginaries and the Formation of Austria's Technopolitical Identity. In: Jasanoff, Sheila/Kim, Sang-Hyun: *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: The University of Chicago Press, S. 103–125.
- Floren, Franz Josef (2006): *Wirtschaft – Gesellschaft – Politik*. Paderborn: Schöningh-Verlag.
- Floyd, Rita (2007): Security as Practice – Discourse Analysis and the Bosnian War. In: *Journal of International Relations and Development*, Nr. 10, S. 214–217.
- Flusser, Vilém (1989): Gedächtnisse. In: Baudrillard, Jean/Böhringer, Hannes/Flusser, Vilém/von Foerster, Heinz/Kittler, Friedrich/Weibel, Peter: *Philosophien der neuen Technologien*. Berlin: Merve-Verlag, S. 41–56.
- Foucault, Michel (1970): *Die Ordnung des Diskurses*. Inauguralvorlesung am Collège de France am 02.12.1970.
- Foucault, Michel (1978): *Dispositive der Macht. Über Sexualität, Wissen und Wahrheit*. Berlin: Merve-Verlag.
- Foucault, Michel (2004): *Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I*. Frankfurt am Main: Suhrkamp Verlag.
- Frank, Michael C. (2019): Antizipationen des nächsten Anschlags: Zur Rolle der Imagination im Sicherheitsdiskurs nach 9/11. In: Becker, Johannes (Hrsg.)/Bühler, Benjamin (Hrsg.)/Pravica, Sandra (Hrsg.)/Willer, Stefan (Hrsg.) (2019): *Zukunftssicherung: Kulturwissenschaftliche Perspektiven*. Bielefeld: Transcript, S. 123–145.
- Friedrich, Steffen/Hellmig, Lutz/Schwarz, Richard (2020): *Informatikunterricht in Deutschland – Eine Übersicht*. Rostock: Universität Rostock.
- Frohman, Larry (2017): Eine unerkennbare Zukunft regieren: Recht, Ausnahme und die Logik der präventiven Überwachung. In: Kampmann, Christoph (Hrsg.)/Marciniak, Angela (Hrsg.)/Meteling, Wencke (Hrsg.) (2017): *"Security turns its eye exclusively to the future": Zum Verhältnis von Sicherheit und Zukunft in der Geschichte*. Baden-Baden: Nomos, S. 285–304.
- Fuhse, Jan (2011): Welche kulturellen Formationen entstehen in mediatisierten Kommunikationsnetzwerken? In: Fuhse, Jan/Stegbauer, Christian (Hrsg.): *Kultur und mediale Kommunikation in sozialen Netzwerken*. Wiesbaden: Springer, S. 31–54.
- Gadamer, Hans-Georg (1986): *Hermeneutik I – Wahrheit und Methode. Grundzüge einer philosophischen Hermeneutik*. Tübingen: J.C.B. Mohr.
- Gengnagel, Vincent/Hirschfeld, Alexander (2016): Die Herrschaft und „das Politische“. Machtanalyse zwischen Konsens und Konflikt. In: Hofmann, Wilhelm/Martinsen, Renate (Hrsg.): *Die andere Seite der Politik. Theorien kultureller Konstruktion des Politischen*. Wiesbaden: Springer, S. 85–112.
- George, Alexander L./Bennett, Andrew (2005): *Case Studies and Theory Development in the Social Sciences*. Cambridge: The MIT Press.

- Giebel, Daniela (2014): Sicherheitskultur - Resilienz durch Sicherheitskommunikation. In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.)/Endreß, Christian (Hrsg.): *Dimensionen der Sicherheitskultur*. Wiesbaden: Springer, S. 359–380.
- Grabbe, Katharina (2014): *Deutschland – Image und Imaginäres. Zur Dynamik der nationalen Identifizierung nach 1990*. Berlin/Boston: Walter de Gruyter GmbH.
- Gusy, Christoph (2010): Sicherheitskultur – Sicherheitspolitik – Sicherheitsrecht. In: *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, Bd. 93, Nr. 2, S. 111–128.
- Habermas, Jürgen (1990): *Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Frankfurt am Main: Suhrkamp Verlag.
- Habermas, Jürgen (1992): *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Frankfurt am Main: Suhrkamp Verlag.
- Hallin, Daniel C./Mancini Paolo (2004): *Comparing Media Systems. Three Models of Media and Politics*. Cambridge: Cambridge University Press.
- Handwerker, W. Penn (2009): *The Origin of Cultures*. Walnut Creek, Kalifornien: Left Coast Press, Inc.
- Hansel, Mischa (2011): Stuxnet und die Sabotage des iranischen Atomprogramms: Ein neuer Kriegsschauplatz im Cyberspace? In: Beckmann, Rasmus (Hrsg.)/Jäger, Thomas (Hrsg.): *Handbuch Kriegstheorien*. Wiesbaden: Springer, S. 564–576.
- Hansen, Lene (2006): *Security as Practice. Discourse Analysis and the Bosnian War*. London: Routledge.
- Hansen, Lene/Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School. In: *Kritische International Studies Quarterly*, Bd. 53, Nr. 4, S. 1155–1175.
- Hasse, Raimund/Krücken, Georg (2009): Neo-institutionalistische Theorie. In: Kneer, Georg/Schroer, Markus (Hrsg.): *Handbuch Soziologische Theorien*. Wiesbaden: Springer, S. 237–251.
- Haverkamp, Rita (2014): Human Security im Rahmen von Sicherheitskultur und Technisierung von Sicherheit? In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.)/Endreß, Christian (Hrsg.): *Dimensionen der Sicherheitskultur*. Wiesbaden: Springer, S. 179–196.
- Hegemann, Hendrik/Kahl, Martin (2012): Politische Entscheidungen und das Risiko Terrorismus. Terrorismusbekämpfung als kulturbedingte Praxis, politischer Möglichkeitsraum und symbolisches Handeln. In: Daase, Christopher (Hrsg.)/Offermann, Philipp (Hrsg.)/Rauer, Valentin (Hrsg.): *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*. Frankfurt am Main: Campus Verlag, S. 159–181.
- Hepp, Andreas (2011): *Medienkultur. Die Kultur mediatisierter Welten*. Wiesbaden: Springer.
- Hoffmann, Dagmar (2014): Kommunikationswissenschaftliche Medientheorien. In: Ruschmeyer, Simon/Schröter, Jens (Hrsg.)/Walke, Elisabeth: *Handbuch*

Medienwissenschaft. Stuttgart: J. B. Metzler'sche Verlagsbuchhandlung und Carl Ernst Poeschel Verlag GmbH, S. 88–95.

Hofstede, Geert/Minkov, Michael (2016): *Allemaal andersdenkenden. Omgaan met cultuurverschillen*. 4. Aufl. Amsterdam: Business Contact.

Horn, Eva (2007): *Der geheime Krieg: Verrat, Spionage und moderne Fiktion*. Frankfurt am Main: Fischer Taschenbuch Verlag.

Hooyman, Paula (2019): *Het ware gezicht van gezichtsherkenningstechnologie*. Amsterdam: Bits of Freedom.

Jahn, Detlef (2013): *Einführung in die vergleichende Politikwissenschaft*. 2. Aufl. Wiesbaden: Springer.

Jasanoff, Sheila (2015a): Future Imperfect: Science, Technology and the Imaginations of Modernity. In: Jasanoff, Sheila/Kim, Sang-Hyun: *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: The University of Chicago Press, S. 1–33.

Jasanoff, Sheila (2015b): Imagined and Invented Worlds. In: Jasanoff, Sheila/Kim, Sang-Hyun: *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: The University of Chicago Press, S. 321–342.

Kaal, Bertie/Krouwel, André/Maks, Isa/van Elfrinkhof, Annemarie (2009): Steeds minder ruimte. Hoe publiek verliest van privaat. In: Boutellier, Hans/Boonstra, Nanne/Ham, Marcel: *Omstreden ruimte. Over de organisatie van spontaniteit en veiligheid*. Amsterdam: Van Gennep, S. 211–224.

Kant, Immanuel (2011): *Kritik der praktischen Vernunft*. Köln: Anaconda Verlag.

Kaspersen, Henrik W. K. (2004): Bestrijding van Cybercrime en de noodzaak van internationale regelingen, in deel: Cybercrime, In: *Justitiële Verkenningen*, Bd. 8, S. 58–75.

Kastler, Holger A. (2015): *Föderaler Rechtsschutz. Personenbezogene Daten in einem Raum der Freiheit, der Sicherheit und des Rechts*. Wiesbaden: Springer.

Kaufhold, Marc-André/Reuter, Christian (Hrsg.) (2018): Usable Safety Engineering sicherheitskritischer interaktiver Systeme. In: Reuter, Christian (Hrsg.): *Sicherheitskritische Mensch-Computer-Interaktion. Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement*. Wiesbaden: Springer, S. 19–40.

Keller, Reiner (2003): Wissenssoziologische Diskursanalyse. Gundlegung eines Forschungsprogramms. In: *Berliner Journal für Soziologie*, Bd. 13, Nr. 3, S. 395–414.

Keller, Reiner (2005): *Wissenssoziologische Diskursanalyse. Gundlegung eines Forschungsprogramms*. Wiesbaden: Springer.

Kennedy, James C. (2017): *En beknopte geschiedenis van Nederland*. Amsterdam: Prometheus.

Kepplinger, Hans Mathias (2011): Der Nachrichtenwert der Nachrichtenfaktoren. In: Kepplinger, Hans Mathias (Hrsg.): *Journalismus als Beruf*. Wiesbaden: Springer, S. 61–76.

- Kittler, Friedrich (1993): *Draculas Vermächtnis*. Leipzig: Reclam Verlag.
- Kleinert, Hubert (2019): *Das geteilte Deutschland. Die Geschichte 1945–1990*. Wiesbaden: Springer.
- Kleinert, Hubert (2020): *Das vereinte Deutschland. Die Geschichte 1990–2020*. Wiesbaden: Springer.
- Klenk, Tanja (2019): Akteure der Sozialpolitik. In: Obinger, Herbert/Schmidt, Manfred G. (Hrsg.): *Handbuch Sozialpolitik*. Wiesbaden: Springer, S. 77–96.
- Klimke, Martin (2010): 1968 als transnationales Ereignis. In: Rathkolb, Oliver/Stadler, Friedrich (Hrsg.): *Das Jahr 1968 – Ereignis, Symbol, Chiffre*. Wien: V&R unipress GmbH, S. 21–30.
- Krüger, Uwe (2017): Der neue Strukturwandel der Öffentlichkeit und die German Angst. In: Hooffacker, Gabriele/Kenntemich, Wolfgang/Kulisch, Uwe (Hrsg.): *Die neue Öffentlichkeit. Wie Bots, Bürger und Big Data den Journalismus verändern*. Wiesbaden: Springer, S. 9–26.
- Kundnani, Hans (2016): *German Power. Das Paradox der deutschen Stärke*. München: C.H.Beck oHG.
- Kurz, Constanze/Rieger, Frank (2018): *Cyberwar – die Gefahr aus dem Netz: Wer uns bedroht und wie wir uns wehren können*. München: C. Bertelsmann Verlag.
- Lademacher, Horst (1993): *Die Niederlande. Politische Kultur zwischen Individualität und Anpassung*. Berlin: Propyläen-Verlag.
- Landwehr, Achim (2008): *Historische Diskursanalyse*. Frankfurt/New York: Campus Verlag.
- Lange, Hans-Jürgen (2010): Zum Wandel der Institutionen und Steuerungsformen des staatlichen Sicherheitssystems. In: Zoche, Peter (Hrsg.)/Kaufmann, Stefan (Hrsg.)/Haverkamp, Rita (Hrsg.): *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. Bielefeld: transcript Verlag, S. 319–340.
- Layes, Gabriel (2005): Kulturdimensionen. In: Thomas, Alexander (Hrsg.)/Schroll-Machl, Sylvia (Hrsg.)/Kammhuber, Stefan (Hrsg.)/Kinast, Eva-Ulrike (Hrsg.): *Handbuch Interkulturelle Kommunikation und Kooperation: Band 1 und 2*. 2. Aufl. Göttingen: Vandenhoeck & Ruprecht, S. 60–73.
- Lem, Stanislaw (1981): *Imaginäre Größe*. Frankfurt am Main: Suhrkamp Verlag.
- Lijphart, Arend (1969): Consociational Democracy. In: *World politics*, Bd. 21, Nr. 2, S. 207–225.
- Lo Iacono, Luigi/Smith, Matthew (2018): Werkzeuge für Usable (Cyber-)Security. In: Reuter, Christian (Hrsg.): *Sicherheitskritische Mensch-Computer-Interaktion. Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement*. Wiesbaden: Springer, S. 99–118.
- Luhmann, Niklas (1985): *Soziale Systeme: Grundriß einer allgemeinen Theorie*. 2. Aufl. Frankfurt am Main: Suhrkamp Verlag.

- Luhmann, Niklas (1997): *Die Gesellschaft der Gesellschaft. 2 Teilbände*. Frankfurt am Main: Suhrkamp.
- Luhmann, Niklas (2017): *Die Realität der Massenmedien*. 5. Aufl. Wiesbaden: Springer.
- Lyon, David (2015): *Surveillance after Snowden*. Cambridge: Polity Press.
- Mai, Gunther (1977): *Westliche Sicherheitspolitik im Kalten Krieg. Der Korea-Krieg und die deutsche Wiederbewaffnung 1950*. Boppard am Rhein: Boldt Verlag.
- Maier, Michaela (2003): Auslandsberichterstattung nach dem 11. September 2001. Bewertung der deutschen Medienberichterstattung durch deutsche, US-amerikanische, afghanische und türkische Rezipienten. In: *Kommunikation & Management*, Bd. 3, S. 5–80.
- Maierhofer, Martina (2003): *Zur Genealogie des Imaginären: Montaigne, Pascal, Rousseau*, Tübingen: Gunter Narr Verlag.
- Maslow, Abraham H. (1966): *The psychology of science. A reconnaissance*, New York: Harper & Row.
- McLuhan, Marshall (1964): *Understanding Media: The Extensions of Man*, London: Routledge.
- Meyer, Katrin/Purtschert, Patricia/Winter, Yves (2008): Einleitung. In: ders. (Hrsg.): *Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault*. Bielefeld: transcript Verlag, S. 7–18.
- Miller, Clark A. (2015): Globalizing Security: Science and the Transformation of Contemporary Political Imagination. In: Jasanoff, Sheila/Kim, Sang-Hyun: *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: The University of Chicago Press, S. 277–299.
- Moebius, Stephan/Quadflieg, Dirk (Hrsg.) (2011): *Kultur. Theorien der Gegenwart*. 2. Aufl. Wiesbaden: Springer.
- Moravcsik, Andrew (1997): Taking Preferences Seriously: A Liberal Theory of International Politics. In: *International Organization*, Bd. 51, Nr. 4, S. 513–553.
- Müller, Markus M. (2012): Beschützer und Big Brother. Regierungshandeln in Sicherheitskrisen. In: Jansen, Stephan A./Stehr, Nico/Schröter, Eckhard (Hrsg.): *Positive Distanz? Multidisziplinäre Annäherungen an den wahren Abstand und das Abstandswahren in Theorie und Praxis*. Wiesbaden: Springer, S. 223–240.
- Odinot, Geralda/Pool, Ronald/Poot, Christianne/Verhoeven, Maite (2017): *Organised Cybercrime in the Netherlands. Empirical findings and implications for law enforcement*. Den Haag: Ministerie van Veiligheid en Justitie.
- Oerlemans, Jan-Jaap (2019): Jurisdictie en grensoverschrijdende digitale opsporing. In: Kooops, Bert-Jaap/Oerlemans, Jan-Jaap (Hrsg.): *Strafrecht en ICT*. Den Haag: Sdu, S. 209–232.
- Oram, Andy/Viega, John (2009): *Beautiful Security*. Sebastopol: O'Reilly Media, Inc.
- Otte, Gunnar (2018): Was ist Kultur und wie sollen wir sie untersuchen? Entwurf einer sozialwissenschaftlichen Sozialstruktur- und Kulturanalyse. In: Böcker, Julia/Dreier,

- Lena/Eulitz, Melanie/Frank, Anja/Jakob, Maria/Leistner, Alexander: *Zum Verhältnis von Empirie und kultursoziologischer Theoriebildung. Stand und Perspektiven*. Weinheim: Beltz Juventa, S. 74–104.
- Parnas, David Lorge (1985): Software Aspects of Strategic Defense Systems. In: *Software Engineering Notes*, Bd. 10, Nr. 5, S. 432–440.
- Parsons, Talcott/Shils, Edward/Allport, Gordon/Kluckholm, Clyde/Murray, Henry/Sears, Robert/Sheldon, Richard/Stouffer, Samuel/Tolman, Edward: (1951): Some fundamental categories of the theory of action: A general statement. In: Parsons, Talcott/Shils, Edward/Allport, Gordon/Kluckholm, Clyde/Murray, Henry/Sears, Robert/Sheldon, Richard/Stouffer, Samuel/Tolman, Edward: *Toward a general theory of action*. Cambridge: Harvard University Press, S. 3–29.
- Piontek, Dorota/Kopka, Artur (2019): Politikberatung und Lobbyismus in der Mediendemokratie: Die Mediatisierung von Expertenwissen als Element des politischen Entscheidungsprozesses am Beispiel Deutschlands und Polens. In: Kopka, Artur/Minkenber, Michael (Hrsg.)/Piontek, Dorota: *Politikberatung und Lobbyismus im parlamentarischen Entscheidungsprozess*. Wiesbaden: Springer, S. 239–254.
- Pohlmann, Norbert (2016): Zur Entwicklung einer IT-Sicherheitskultur. In: *Datenschutz und Datensicherheit*, Bd. 40, Nr. 1, S. 38–42.
- Ramge, Thomas (2018): *Mensch und Maschine. Wie Künstliche Intelligenz und Roboter unser Leben verändern*. Ditzingen: Reclam Verlag.
- Reutter, Werner (2020): *Die deutschen Länder. Eine Einführung*. Wiesbaden: Springer.
- Rieckhoff, Henning (2007): *Der Vorbehalt des Gesetzes im Europarecht*. Tübingen: Mohr Siebeck.
- Ritter, Gerhard A. (2009): Die Deutsche Wiedervereinigung. In: *Historische Zeitschrift*, Bd. 286, Nr. 2, S. 289–339.
- Röbken, Heinke/Wetzel, Kathrin (2016): *Qualitative und quantitative Forschungsmethoden*. 2. Aufl. Oldenburg: Universität Oldenburg.
- Rudolf, Dennis Bastian (2018): *Analyse und Vergleich politischer Mythen. Ein systematischer Theorierahmen für Demokratien und Autokratien*. Wiesbaden: Springer.
- Rügheimer, Hannes (2021): 5G in Global Comparison. In: *Connect*, Nr. 7, S. 72–76.
- Sander, Uwe (1998): *Die Bindung der Unverbindlichkeit. Mediatisierte Kommunikation in modernen Gesellschaften*. Frankfurt am Main: Suhrkamp Verlag.
- Sandhu, Swaran (2012): *Public Relations und Legitimität. Der Beitrag des organisationalen Neo-Institutionalismus für die PR-Forschung*. Wiesbaden: Springer.
- Schaar, Peter (2009): *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft*. München: Wilhelm Goldmann Verlag.
- Schaar, Peter (2015): *Das digitale Wir. Unser Weg in die transparente Gesellschaft*. Hamburg: edition Körber.
- Schaar, Peter (2017): *Trügerische Sicherheit. Wie die Terrorangst uns in den Ausnahmezustand treibt*. Hamburg: edition Körber.

- Schäller, Steven/Vorländer, Hans (Hrsg.) (2013): *Föderalismus und Souveränität im Bundesstaat. Ideengeschichtliche Grundlagen und die Rechtsprechung des Bundesverfassungsgerichts*. Wiesbaden: Springer.
- Scheffer, Jörg (2009): Gefangen im Container – Kulturvergleiche und ihre räumliche Vorbestimmung am Beispiel des Filmes „Willkommen bei den Sch’tis“. In: *Interculture Journal*, Bd. 8, Nr. 10, S. 19–34.
- Schipper, Ori (2017): Der kleine, unfeine Unterschied. In: *Unipress – Das Unbekannte*, Bd. 170, S. 30–31.
- Schmidt, Siegfried Johannes (2000): *Kalte Faszination. Medien, Kultur, Wissenschaft in der Mediengesellschaft*. Weilerswist: Velbrück Wissenschaft.
- Schmitt, Carl (1982): *Der Leviathan in der Staatslehre des Thomas Hobbes. Sinn und Fehlschlag eines politischen Symbols*. 3. Aufl. Stuttgart: Klett Cotta.
- Schneckener, Ulrich (2003): *War on terrorism. Die Bush-Regierung im Kampf gegen den internationalen Terrorismus*. Berlin: Stiftung Wissenschaft und Politik.
- Schnettler, Bernt (2011): Thomas Luckmann: Kultur zwischen Konstitution, Konstruktion und Kommunikation. In: Moebius, Stephan/Quadflieg, Dirk (Hrsg.): *Kultur. Theorien der Gegenwart*. Wiesbaden: Springer, S. 212–226.
- Schölzel, Hagen (2016): Das Politische als Kommunikationspraxis. Über Interventionen der „Kommunikationsguerilla“ in die „Kulturelle Grammatik“. In: Hofmann, Wilhelm/Martinsen, Renate (Hrsg.): *Die andere Seite der Politik. Theorien kultureller Konstruktion des Politischen*. Wiesbaden: Springer, S. 33–54.
- Schönherr-Mann, Hans-Martin (2016): Kulturelle symbolische Einheit und die Mikrophysik der Macht. Cassirer und Foucault. In: Hofmann, Wilhelm/Martinsen, Renate (Hrsg.): *Die andere Seite der Politik. Theorien kultureller Konstruktion des Politischen*. Wiesbaden: Springer, S. 15–32.
- Schrödel, Tobias (2014): *Ich glaube, es hackt! Ein Blick auf die irrwitzige Realität der IT-Sicherheit*. 3. Aufl. Wiesbaden: Springer.
- Schröter, Jens (2014): Einleitung. In: Ruschmeyer, Simon/Schröter, Jens (Hrsg.)/Walke, Elisabeth: *Handbuch Medienwissenschaft*. Stuttgart: J. B. Metzler'sche Verlagsbuchhandlung und Carl Ernst Poeschel Verlag GmbH, S. 1–11.
- Schröter, Jens (2018): Das Geld und die Medientheorie. In: *Zeitschrift für Medienwissenschaft*, Bd. 10, Nr. 18, S. 59–72.
- Schröter, Jens (2019): *Medien und Ökonomie. Eine Einführung*. Wiesbaden: Springer.
- Schulz, Andreas (2005): *Lebenswelt und Kultur des Bürgertums im 19. und 20. Jahrhundert*. München: R. Oldenbourg Verlag.
- Schüttpelz, Erhard (2016): *Infrastrukturelle Medien und öffentliche Medien*. Universität Siegen.
- Schwaneck, Stefan (2019): *Lobbyismus und Transparenz. Eine vergleichende Studie einer komplexen Beziehung*. Wiesbaden: Springer.

- Schwarz, Martin (2014): Der objektivierte Mensch und die Sicherheitskultur in Deutschland. In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.): *Postfaktische Sicherheitspolitik. Gewährleistung von Sicherheit in unübersichtlichen Zeiten*. Wiesbaden: Springer, S. 75–102.
- Siedschlag, Alexander/Jerković, Andrea (2014): Sicherheitskulturanalyse jenseits der Begleitforschung. In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.)/Endreß, Christian (Hrsg.): *Dimensionen der Sicherheitskultur*. Wiesbaden: Springer, S. 303–322.
- Simons, Hans (2014): *Consensual Hallucinations. The Politics of Identity in Dutch Cyber Security Policy*. Nijmegen: Radboud University.
- Sprenger, Florian (2017): Warum ist das Medium die Botschaft? In: Heilmann, Till A. (Hrsg.)/Schröter, Jens (Hrsg.): *Medien verstehen: Marshall McLuhans Understanding Media*. Lüneburg: meson press, S. 39–49.
- Stauff, Markus (2014): Cultural Studies. In: Ruschmeyer, Simon/Schröter, Jens (Hrsg.)/Walke, Elisabeth: *Handbuch Medienwissenschaft*. Stuttgart: J. B. Metzler'sche Verlagsbuchhandlung und Carl Ernst Poeschel Verlag GmbH, S. 516–522.
- Strohschneider, Stefan (2010): Technisierungsstrategien und der Human Factor. In: Zoche, Peter (Hrsg.)/Kaufmann, Stefan (Hrsg.)/Haverkamp, Rita (Hrsg.): *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. Bielefeld: transcript Verlag, S. 161–178.
- Stubbe, Julian/Wessels, Jan/Zinke, Guido (2019): Neue Intelligenz, neue Ethik? In: Wittpahl, Volker (Hrsg.): *Künstliche Intelligenz. Technologie, Anwendung, Gesellschaft*. Berlin: Springer, S. 239–254.
- Tassis, Theofanis (2007): *Cornelius Castoriadis*. Berlin: Freie Universität Berlin.
- Terberl, Christina/Wendekamm, Michaela (2014): Un/Sicherheit als Un/Sichtbarkeit – Sicherheitskultur als Sichtbarkeitskultur. In: Lange, Hans-Jürgen (Hrsg.)/Wendekamm, Michaela (Hrsg.)/Endreß, Christian (Hrsg.): *Dimensionen der Sicherheitskultur*. Wiesbaden: Springer, S. 323–340.
- Verbeek, Sanne (2016): *Case studie – De 'Moeders van Srebrenica'*. Gent: Universiteit Gent.
- von Foerster, Heinz (1989): Wahrnehmung. In: Baudrillard, Jean/Böhringer, Hannes/Flusser, Vilém/von Foerster, Heinz/Kittler, Friedrich/Weibel, Peter: *Philosophien der neuen Technologien*. Berlin: Merve-Verlag, S. 27–40.
- von Humboldt, Wilhelm (1851): *Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staats zu bestimmen*. Breslau: Trewendt.
- Weber, Max (2016): *Die protestantische Ethik und der "Geist" des Kapitalismus. Neuauflage der ersten Fassung von 1904–05 mit einem Verzeichnis der wichtigsten Zusätze und Veränderungen aus der zweiten Fassung von 1920. Herausgegeben und eingeleitet von Klaus Lichtblau und Johannes Weiß*. Wiesbaden: Springer.
- Wenzel, Harald (1998): Parasozialität und Vertrauen. Zur Bedeutung elektronischer Massenmedien für die soziale Integration der amerikanischen Gesellschaft. In: ders.

- (Hrsg.): *Die Amerikanisierung des Medienalltags*. Frankfurt am Main/New York: Campus Verlag, S. 80–126.
- Wichmann, Peter (2014): *Al-Qaida und der globale Dihad. Eine vergleichende Betrachtung des transnationalen Terrorismus*. Wiesbaden: Springer.
- Wielenga, Friso (2020): *A history of the netherlands. From the Sixteenth Century to the Present Day*. 2. Aufl. London: Bloomsbury Academic.
- Williams, Michael C. (2003): Words, Images, Enemies: Securitization and International Politics. In: *International Studies Quarterly*, Bd. 47, Nr. 4, S. 511–531.
- Williams, Raymond (1960): *Culture and Society. 1780–1950*. New York: Anchor Books Doubleday & Company, Inc..
- Williams, Raymond (1961): *The Long Revolution*. New York: Columbia University Press.
- Williams, Raymond (1985): *Keywords. A vocabulary of culture and society*. New York: Oxford University Press.
- Winter, Rainer (2009): Cultural Studies. In: Kneer, Georg/Schroer, Markus (Hrsg.): *Handbuch Soziologische Theorien*. Wiesbaden: Springer, S. 67–86.
- Winter, Rainer (2011): Cultural Studies. In: Ayaß, Ruth (Hrsg.)/Bergmann, Jörg (Hrsg.): *Qualitative Methoden der Medienforschung*. Mannheim: Verlag für Gesprächsforschung, S. 423–434.
- Zerubavel, Eviatar (2012): *Time Maps. Collective Memory and the Social Shape of the Past*. Chicago: University of Chicago Press.
- Ziemann, Andreas (2011): *Medienkultur und Gesellschaftsstruktur*. Wiesbaden: Springer.

Quellen

- Adviesraad Internationale Vraagstukken (2018): *Coalitievorming na de Brexit. Allianties voor een europese Unie die moderniseert en beschermt*. Den Haag: AIV.
- Algemene Rekenkamer (2019): *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*. Den Haag.
- Amtsblatt der Europäischen Union (2016): *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*. Brüssel: Europäische Union.
- Amtsblatt der Europäischen Union (2018): *Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation*. Brüssel: Europäische Union.
- Bayerische Staatsregierung (2018): *Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz) vom 18. Mai 2018*. München: Bayern.Recht.
- Bild (2018): *Wenn er abgeschoben worden wäre, würde sie noch leben*. 08. Juni 2018 Berlin: Axel Springer SE.
- Bitkom (2020): *Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt*. Berlin.
- Bitkom (2021a): *Wirtschaftsschutz 2021*. Berlin.
- Bitkom (2022): *Wirtschaftsschutz 2022*. Berlin.
- Bolte-Richter, Matthias (2020): *Kleine Anfrage 3326 – des Abgeordneten Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN. Wie steht es um die IT-Sicherheit an den nordrhein-westfälischen Hochschulen?* Düsseldorf: Landtag NRW.
- Bundesamt für Sicherheit in der Informationstechnik (2019a): *Die Lage der IT-Sicherheit in Deutschland 2019*. Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (2020a): *Die Lage der IT-Sicherheit in Deutschland 2020*. Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (2021a): *Die Lage der IT-Sicherheit in Deutschland 2021*. Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (BSI)/Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (2020): *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit*. Bonn.
- Bundesamt für Strahlenschutz (2021): *5G – Die 5. Mobilfunk-Generation*. Salzgitter.
- Bundesgesetzblatt (1990): *Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik*. Jahrgang 1990 Teil I Nr. 71, 2009, S. 2834–2836.
- Bundesgesetzblatt (2009): *Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes*. Jahrgang 2009 Teil I Nr. 54, 2009, S. 2821–2826.

Bundesgesetzblatt (2015): *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. Jahrgang 2015 Teil I Nr. 31, 2015, S. 1324–1331.

Bundesgesetzblatt (2021): *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*. Jahrgang 2021 Teil I Nr. 25, 2021, S. 1122–1138.

Bundeskriminalamt (2017): *Bundeslagebild Kriminalität im Kontext von Zuwanderung 2016*. Wiesbaden.

Bundeskriminalamt (2020): *Polizeiliche Kriminalstatistik – Jahrbuch 2019*. Wiesbaden.

Bundeskriminalamt (2022a): *Bundeslagebild Cybercrime 2021*. Wiesbaden.

Bundesministerium des Innern (2016): *Cyber-Sicherheitsstrategie für Deutschland 2016*. Berlin.

Bundesministerium des Innern, für Bau und Heimat (2019): *Verfassungsschutzbericht 2019*. Berlin.

Bundesministerium des Innern, für Bau und Heimat (2021a): *Cyber-Sicherheitsstrategie für Deutschland 2021*. Berlin.

Bundesnetzagentur (2018): *Entscheidung der Präsidentenkammer der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 26. November 2018 über die Festlegungen und Regeln im Einzelnen (Vergaberegeln) und über die Festlegungen und Regelungen für die Durchführung des Verfahrens (Auktionsregeln) zur Vergabe von Frequenzen in den Bereichen 2 GHz und 3,6 GHz*. Bonn.

Bundesregierung (2016): *Weißbuch. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr*. Berlin.

Bundesregierung (2018): *Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode*. Berlin.

Bundesregierung (2019): *Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949*. Berlin: Presse- und Informationsamt der Bundesregierung.

Bundestag (2021a): *Haushaltsgesetz 2021*. Berlin.

Bundestag (2021b): *Schriftliche Fragen mit den in der Woche vom 1. Februar 2021 eingegangenen Antworten der Bundesregierung*. Berlin.

Bundestag (2021c): *Schriftliche Fragen mit den in der Woche vom 8. Februar 2021 eingegangenen Antworten der Bundesregierung*. Berlin.

Cyber Security Raad (2020): *Jaaroverzicht 2019*. Den Haag.

Cyber Security Raad (2021): *Adviesrapport. Integrale Aanpak Cyberweerbaarheid*. Den Haag.

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) (2018): *Deutschland in den Augen der Welt. Ergebnisse der GIZ-Erhebung 2017/2018*. Bonn: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

El Ouassil, Samira/Karig, Friedemann (2021): *Erzählende Affen. Mythen, Lügen, Utopien – wie Geschichten unser Leben bestimmen*. Berlin: Ullstein.

- European Commission (2021a): *Digital Economy and Society Index 2021. The Netherlands*. Brüssel.
- European Commission (2021b): *European Innovation Scoreboard 2021. The Netherlands*. Brüssel.
- European Education and Culture Executive Agency (2022): *Informatics education at school in Europe. Eurydice report*. Publications Office of the European Union. Luxemburg.
- European Union Agency for Network and Information Security (ENISA) (2017): *Cyber Security Culture in organisations*. Marousi.
- European Union Agency for Network and Information Security (ENISA) (2018): *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. Marousi.
- European Security Research and Innovation Forum (ESRIF) (2009): *Final Report*. Brüssel.
- Gesellschaft für Informatik e. V. (2021): *Informatik-Monitor*. Berlin.
- Heumann, Stefan (2021): *Scheinlösung Digitalministerium. Welche tiefgreifende [sic!] Reformen von Regierung und Verwaltung für eine erfolgreiche Digitalpolitik nötig sind*. Berlin: Stiftung Neue Verantwortung e. V..
- Herpig, Sven/Rupp, Christina (2022): *Deutschlands staatliche Cybersicherheitsarchitektur*. 9. Aufl. Berlin: Stiftung Neue Verantwortung e. V..
- kpn (2021): *Duurzaamheid – Technologie maakt het mogelijk*. Rotterdam: kpn.
- LOAD e. V. (2021b): *Stellungnahme zur Konsultation zum Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und Gefahrenabwehr*. Berlin: LOAD e. V. – Verein für liberale Netzpolitik.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2019): *Grondwet voor het Koninkrijk der Nederlanden 2018*. Den Haag: Rijksoverheid.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2021): *Kabinetsreactie op de notitie ICT-investeringen door de overheid*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
- Ministerie van Economische Zaken en Klimaat (2018): *Actieplan Digitale Connectiviteit*. Den Haag.
- Ministerie van Economische Zaken en Klimaat (2019): *Nota mobiele communicatie 2019*. Den Haag.
- Ministerie van Economische Zaken en Klimaat (2021): *Terugblik Digital Trust Center 2021. Terugkijken naar het jaar, samenwerken aan de toekomst*. Den Haag.
- Ministerie van Financiën (2020): *Miljoenennota 2021*. Den Haag.
- Ministerie van Onderwijs, Cultuur en Wetenschap (2021): *Tendrapportage Arbeidsmarkt Leraren po, vo en mbo 2021*. Den Haag.
- Ministerie van Onderwijs, Cultuur en Wetenschap (2022): *Kamerbrief Onderwijsakkoord Samen voor het beste onderwijs*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018a): *Cybersecuritybeeld Nederland 2018*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018b): *Nederlandse Cybersecurity Agenda. Nederland digitaal veilig*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2019a): *Cybersecuritybeeld Nederland 2019*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2019b): *Χίμαιρα – Een duiding van het fenomeen ‘hybride dreiging’*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020a): *Cybersecuritybeeld Nederland 2020*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2021a): *Cybersecuritybeeld Nederland 2021*. Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022c): *Cyber Security Assessment Netherlands*. Den Haag.

Nationaal Cyber Security Centrum (2019): *NCSC Onderzoeksagenda 2019 – 2022*. Den Haag.

Nationaal Cyber Security Centrum (2020b): *Ransomware. Maatregelen voor het voorkomen, beperken en herstellen van een ransomware-aanval*. Den Haag.

OECD (2020): *Bildung auf einen Blick 2020. OECD-Indikatoren*. Paris.

OECD (2022): *Bildung auf einen Blick 2022. OECD-Indikatoren*. Paris.

Sociaal en Cultureel Planbureau (2019): *Denkend aan Nederland – Sociaal en Cultureel Rapport 2019*. Den Haag.

Staatsblad van het Koninkrijk der Nederlanden (1993): *Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit)*. Den Haag: Staatsblad.

Staatsblad van het Koninkrijk der Nederlanden (2018a): *Wet van 27 juni 2018 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)*. Den Haag: Staatsblad.

Staatsblad van het Koninkrijk der Nederlanden (2018b): *Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)*. Den Haag: Staatsblad.

Statistisches Bundesamt (2021a): *Niederlande. Statistisches Länderprofil*. Wiesbaden: Statistisches Bundesamt.

Statistisches Bundesamt (2021b): *Bildung und Kultur. Studierende an Hochschulen*. Wiesbaden: Statistisches Bundesamt.

Tweede Kamer der Staten-Generaal (2011): *De Nationale Cyber Security Strategie (NCSS). Slagkracht door samenwerking*. Den Haag.

Tweede Kamer der Staten-Generaal (2020a): *Vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2021*. Den Haag.

Tweede Kamer der Staten-Generaal (2020b): *Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2021*. Den Haag.

Tweede Kamer der Staten-Generaal (2020c): *Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2021*. Den Haag.

Tweede Kamer der Staten-Generaal (2021): *Stafnotitie over ICT-investeringen door de overheid*. Den Haag.

Verbraucherzentrale NRW (2020): *Jahresbericht 2019*. Düsseldorf: Verbraucherzentrale Nordrhein-Westfalen.

VNG (2020): *Agenda Digitale Veiligheid 2020 – 2024. Een veilige (digitale) gemeente*. Den Haag: Vereniging van Nederlandse Gemeenten.

VVD-CDA (2010): *Vrijheid en verantwoordelijkheid. Regeerakkoord VVD-CDA*. Den Haag.

Wetenschappelijke Raad voor het Regeringsbeleid (2017): *Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid*. Den Haag: WRR.

Weltorganisation für geistiges Eigentum (2021): *GII 2021 results*. Genf: WIPO.

Wissenschaftsrat (2020): *Perspektiven der Informatik in Deutschland*. Köln: Wissenschaftsrat.

Onlinequellen

3GPP (2021): *The Evolved Packet Core*. <https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core>, abgerufen am 17. Juli 2021.

accountant.nl (2021): *Nederland waarschuwt Brussel tegen versoepeling staatssteunregels*. <https://www.accountant.nl/nieuws/2021/11/nederland-waarschuwt-brussel-tegen-versoepeling-staatssteunregels/>, abgerufen am 05. Dezember 2021.

adviesraadinternationalevraagstukken.nl (2021): *Home*. <https://www.adviesraadinternationalevraagstukken.nl/>, abgerufen am 07. Dezember 2021.

AD.nl (2017): *Moeten we onze smartphonecamera afplakken tegen hackers?* <https://www.ad.nl/economie/moeten-we-onze-smartphonecamera-afplakken-tegen-hackers~aec9569c/>, abgerufen am 16. Oktober 2023.

Advocatenblad.nl (2017): *Wet computercriminaliteit: wie controleert de hackende politieagent?* <https://www.advocatenblad.nl/2017/09/29/controleert-hackende-politieagent/>, abgerufen am 16. Oktober 2023.

Algemene Inlichtingen- en Veiligheidsdienst (2011): *Nationale Cyber Security strategie*. <https://www.aivd.nl/actueel/nieuws/2011/02/23/nationale-cyber-security-strategie>, abgerufen am 19. April 2022.

Allianz für Cyber-Sicherheit (2022): *Allianz für Cyber-Sicherheit*. https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html, abgerufen am 01. Februar 2022.

Apple (2020a): *Datenschutz*. <https://www.apple.com/de/privacy/features/>, abgerufen am 09. Mai 2020.

Apple (2020b): *iPhone*. <https://www.apple.com/in/iphone/only-iphone/>, abgerufen am 09. Mai 2020.

Audi (2021): *Warum wir unsere Fahrzeuge jetzt mit dem neuen Mobilfunkstandard 5G vernetzen*. <https://www.audi-mediacyber.com/de/pressemitteilungen/warum-wir-unsere-fahrzeuge-jetzt-mit-dem-neuen-mobilfunkstandard-5g-vernetzen-14189>, abgerufen am 13. November 2024.

AutoriteitNVS (2021): *Heeft u een 'Quantum Pendant' (anti-5G) hanger of 'negatief ionen' sieraad of slaapmasker? Leg deze veilig weg*. <https://www.autoriteitnvs.nl/actueel/nieuws/2021/12/16/heeft-u-een-quantum-pendant-anti-5g-hanger-of-negatief-ionen-sieraad-of-slaapmasker-leg-deze-veilig-weg>, abgerufen am 30. November 2024.

BAGSO (2021): *Digitalisierung*. <https://www.bagso.de/themen/digitalisierung/>, abgerufen am 27. Februar 2021.

Bappert, Jens/Borck, Martin/Tigges, Johanna (2006a): *Die Zentralgewalt – het rijk*. <https://www.uni-muenster.de/NiederlandeNet/nl-wissen/politik/verwaltungsstrukturen/rijk.html>, abgerufen am 18. November 2021.

Bappert, Jens/Borck, Martin/Tigges, Johanna (2006b): *Gesetzgebungsprozess*. <https://www.uni-muenster.de/NiederlandeNet/nl-wissen/politik/verwaltungsstrukturen/gesetzgebung.html>, abgerufen am 18. November 2021.

Bappert, Jens/Borck, Martin/Tigges, Johanna (2006c): *Die Provinzen – de provincies*. <https://www.uni-muenster.de/NiederlandeNet/nl-wissen/politik/verwaltungsstrukturen/provincies.html>, abgerufen am 18. November 2021.

Behörden-Spiegel (2020): *Bundeskanzleramt startet “Bundeszentrale für digitale Aufklärung”*. <https://www.behoerden-spiegel.de/2020/07/31/bundeskanzleramt-startet-bundeszentrale-fuer-digitale-aufklaerung/>, abgerufen am 24. Januar 2021.

Berlin.de (2019): *Emotet – oder wie Cyber-Kriminelle Computersysteme lahmlegen*. <https://www.berlin.de/moderne-verwaltung/prozesse-und-technik/ikt-sicherheit/aktuelles/artikel.947571.php>, abgerufen am 04. Oktober 2024.

Berliner Morgenpost (2018): *Laschet warnt neuen CDU-Vorsitzenden vor Richtungswechsel*. <https://www.morgenpost.de/politik/article215924741/Laschet-warnt-neuen-CDU-Vorsitzenden-vor-Richtungswechsel.html>, abgerufen am 07. November 2024.

Bitkom (2021b): *IT-Sicherheitsgesetz 2.0 nimmt Kollateralschäden in Kauf*. <https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheitsgesetz-20-nimmt-Kollateralschaeden-in-Kauf>, abgerufen am 07. Januar 2022.

Bits of Freedom (2016): *Stop Het Hackvoorstel*. <https://www.stophethackvoorstel.nl/>, abgerufen am 15. Oktober 2023.

Bits of Freedom (2022): *Werkwijze*. <https://www.bitsoffreedom.nl/hoel/>, abgerufen am 12. August 2023.

Bundesamt für Sicherheit in der Informationstechnik (2019b): *Historie*. https://www.bsi.bund.de/DE/DasBSI/Historie/historie_node.html, abgerufen am 28. April 2020.

Bundesamt für Sicherheit in der Informationstechnik (2020b): *Das Nationale Cyber-Abwehrzentrum*. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html, abgerufen am 17. Juli 2020.

Bundesamt für Sicherheit in der Informationstechnik (2020c): *„Update verfügbar“ – der BSI-Podcast für Verbraucherinnen und Verbraucher*. https://www.bsi.bund.de/DE/Service-Navi/Mediathek/Podcast/podcast_node.html, abgerufen am 10. Januar 2025.

Bundesamt für Sicherheit in der Informationstechnik (2021b): *Abteilung WG – Cyber-Sicherheit für Wirtschaft und Gesellschaft*. https://www.bsi.bund.de/DE/DasBSI/Organisation-und-Aufbau/Abteilungen-inkl-Organigramm/Abteilung-WG/abteilung-wg_node.html, abgerufen am 28. Dezember 2021.

Bundesamt für Sicherheit in der Informationstechnik (2021c): *BSI-Lagebericht 2021: Bedrohungslage angespannt bis kritisch*. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211021_Lagebericht.html, abgerufen am 12. Januar 2022.

Bundesamt für Sicherheit in der Informationstechnik (2021d): *Informationen zur Schadsoftware Emotet. Wie man sich schützt und was Betroffene tun können*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Sonderfall-Emotet/sonderfall-emotet_node.html, abgerufen am 01. Oktober 2024.

Bundesamt für Sicherheit in der Informationstechnik (2021e): *Was versteht man unter 5G?* https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/5G/5g-was-versteht-man-darunter_node.html, abgerufen am 13. November 2024.

Bundesamt für Sicherheit in der Informationstechnik (2021f): *Moderne Telekommunikationsinfrastrukturen (5G und 6G)*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/5-g_node.html, abgerufen am 13. November 2024.

Bundesamt für Sicherheit in der Informationstechnik (2021g): *Unsere deutschlandweite IT-Sicherheitskampagne*. https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/Ueber-die-Kampagne/die-kampagne_node.html, abgerufen am 30. Januar 2025.

Bundesamt für Sicherheit in der Informationstechnik (2022a): *Unser Leitbild*. https://www.bsi.bund.de/DE/Das-BSI/Leitbild/leitbild_node.html, abgerufen am 29. Januar 2022.

Bundesamt für Sicherheit in der Informationstechnik (2022b): *Themen*. https://www.bsi.bund.de/DE/Themen/themen_node.html, abgerufen am 30. Januar 2022.

Bundesamt für Sicherheit in der Informationstechnik (2022c): *Verbraucherinnen und Verbraucher*. <https://www.bsi.bund.de/VerbraucherInnen>, abgerufen am 07. Januar 2022.

Bundesamt für Sicherheit in der Informationstechnik (2022d): *Der Wert der Informationssicherheit: Zertifizierung und Anerkennung durch das BSI*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html, abgerufen am 01. Februar 2022.

Bundesamt für Sicherheit in der Informationstechnik (2022e): *Staat und Verwaltung*. https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/oeffentliche-verwaltung_node.html, abgerufen am 24. Juni 2023.

Bundesamt für Verfassungsschutz (2021): *Informationsbeschaffung*. https://www.verfassungsschutz.de/DE/verfassungsschutz/auftrag/informationsbeschaffung/informationsbeschaffung_node.html, abgerufen am 29. Dezember 2021.

Bundeshaushalt (2021): *Bundeshaushalt digital*. <https://www.bundeshaushalt.de/DE/Bundeshaushalt-digital/bundeshaushalt-digital.html>, abgerufen am 21. Januar 2023.

Bundeskriminalamt (2021): *Infrastruktur der Emotet-Schadsoftware zerschlagen*. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html, abgerufen am 08. Oktober 2024.

Bundeskriminalamt (2022b): *Abteilung "Cybercrime" (CC)*.
https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html, abgerufen am 01. Dezember 2022.

Bundesministerium für Arbeit und Soziales (2019): *Arbeitslosengeld*.
<https://www.bmas.de/DE/Themen/Arbeitsmarkt/Arbeitslosengeld/arbeitslosengeld.html>, abgerufen am 02. November 2020.

Bundesministerium für Verkehr und digitale Infrastruktur (2019): *Online-Dialog*.
<https://www.deutschland-spricht-ueber-5g.de/online-dialog/>, abgerufen am 15. November 2024.

Bundesministerium für Verkehr und digitale Infrastruktur (2020): *Das Ministerium stellt sich vor*. <https://www.bmvi.de/DE/Ministerium/Aufgaben-Struktur/aufgaben-struktur.html>, abgerufen am 31. Dezember 2020.

Bundesministerium für Verkehr und digitale Infrastruktur (2021): *Die Breitbandförderung des Bundes*.
<https://www.bmvi.de/SharedDocs/DE/Artikel/DG/relaunch-des-breitbandfoerderprogramms.html>, abgerufen am 26. November 2021.

Bundesministerium der Verteidigung (2021a): *Cybersicherheit*.
<https://www.bmvg.de/de/themen/cybersicherheit>, abgerufen am 02. Januar 2021.

Bundesministerium der Verteidigung (2021b): *Cyber-Sicherheitsrat*.
<https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsrat>, abgerufen am 22. Januar 2021.

Bundesministerium der Verteidigung (2021c): *Verteidigungshaushalt 2021*.
<https://www.bmvg.de/de/themen/verteidigungshaushalt/verteidigungshaushalt-2021>, abgerufen am 11. März 2021.

Bundesministerium des Innern, für Bau und Heimat (2020a): *Sicherheit*.
<https://www.bmi.bund.de/DE/themen/sicherheit/sicherheit-node.html>, abgerufen am 29. Dezember 2020.

Bundesministerium des Innern, für Bau und Heimat (2020b): *Modellprojekte Smart Cities: Aufruf für Bewerbungen zur dritten Staffel*.
<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/smart-cities.html>, abgerufen am 09. März 2023.

Bundesministerium des Innern, für Bau und Heimat (2021b): *Startschuss für die Cyberagentur*.
<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/08/startschuss-cyberagentur.html>, abgerufen am 23. Januar 2021.

Bundesministerium des Innern, für Bau und Heimat (2021c): *Jetzt Stellung nehmen: Entwurf der Cybersicherheitsstrategie 2021*.
<https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2021/06/css-2021-beteiligungsformat.html>, abgerufen am 25. Januar 2022.

Bundesministerium des Innern, für Bau und Heimat (2021d): *BMI und BSI starten Informations- und Sensibilisierungskampagne zur IT-Sicherheit*.
<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/03/kampagne-it-sicherheit.html>, abgerufen am 06. Februar 2024.

Bundesministerium für Wirtschaft und Energie (2020): *Den digitalen Wandel gestalten*. <https://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html>, abgerufen am 29. Dezember 2020.

Bundesnachrichtendienst (2021): *Aufrüstung im Cyberspace*. https://www.bnd.bund.de/DE/Die_Themen/Cybersicherheit/cybersicherheit_node.html, abgerufen am 02. Januar 2021.

Bundesnetzagentur (2020a): *Versorgung der Bevölkerung mit funkgestützten Breitbandanschlüssen*. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/MobilesBreitband-node.html, abgerufen am 31. Dezember 2020.

Bundesnetzagentur (2020b): *Bundesnetzagentur veröffentlicht den Katalog von Sicherheitsanforderungen für Telekommunikationsnetze*. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2020/20200811_sicherheitskatalogliste.html, abgerufen am 31. Dezember 2020.

Bundesregierung (2015): *Sommerpressekonferenz von Bundeskanzlerin Merkel*. <https://www.bundesregierung.de/breg-de/aktuelles/pressekonferenzen/sommerpressekonferenz-von-bundeskanzlerin-merkel-848300>, abgerufen am 09. November 2021.

Bundesregierung (2020): *Die Bundeszentrale für Digitale Aufklärung – eine Initiative der Staatsministerin für Digitalisierung*. <https://www.bundesregierung.de/breg-de/bundesregierung/staatsministerin-fuer-digitalisierung/bundeszentrale-fuer-digitale-aufklaerung>, abgerufen am 24. Januar 2021.

Bundestag (2020): *Einspruchs- und Zustimmungsgesetze*. <https://www.bundestag.de/parlament/grundgesetz/gg-serie-05-bundesrat-634568>, abgerufen am 18. Oktober 2020.

Bundesverband der Deutschen Industrie e. V. (BDI) (2021): *Pressemitteilungen und Statements*. https://bdi.eu/presse/pressemitteilungen?tx_solr%5Bpage%5D=6, abgerufen am 04. August 2023.

Bundesverband IT-Mittelstand e. V. (BITMi) (2021a): *Der Bundesverband IT-Mittelstand e. V. stellt sich vor (BITMi)*. <https://www.bitmi.de/ueber-uns/>, abgerufen am 05. März 2021.

Bundesverband IT-Mittelstand e. V. (BITMi) (2021b): *Ein eigenes Digitalministerium sollte Konsens sein*. <https://www.bitmi.de/digitalministerium/>, abgerufen am 29. Mai 2023.

Bundeswehr (2020): *Der Auftrag des Organisationsbereich Cyber- und Informationsraum*. <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag>, abgerufen am 16. September 2020.

Bundeszentrale für politische Bildung (2020): *Subsidiaritätsprinzip*. <https://www.bpb.de/nachschlagen/lexika/pocket-europa/16951/subsidiaritaetsprinzip>, abgerufen am 17. Oktober 2020.

Bundeszentrale für politische Bildung (2021): *Der Zweite Weltkrieg*. <https://www.bpb.de/geschichte/deutsche-geschichte/der-zweite-weltkrieg/>, abgerufen am 05. Februar 2021.

Bundesverfassungsgericht (2021): *Verfassungsbeschwerden gegen das Klimaschutzgesetz teilweise erfolgreich*. <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2021/bvg21-031.html>, abgerufen am 01. August 2021.

Bündnis 90/Die Grünen (2021): *Rede von Dr. Konstantin von Notz - IT-Sicherheit*. <https://www.gruene-bundestag.de/parlament/bundestagsreden/it-sicherheit-1>, abgerufen am 27. Dezember 2021.

Business Insider Deutschland (2022): *Kein Wodka mehr: Nach Netto verbannen auch Aldi, Rewe und Edeka russische Waren aus den Regalen*. <https://www.businessinsider.de/wirtschaft/handel/kein-wodka-mehr-nach-netto-verbannen-auch-aldi-rewe-und-edeka-russische-waren-aus-den-regalen-a/>, abgerufen am 09. April 2022.

BVDW (2021): *Vorteile der Mitgliedschaft*. <https://www.bvdw.org/der-bvdw/gremien/mitglied-werden/vorteile-der-mitgliedschaft/?L=#jump>, abgerufen am 24. Februar 2021.

Chaos Computer Club (2010): *Forderungen für ein lebenswertes Netz*. <https://www.ccc.de/de/updates/2010/forderungen-lebenswertes-netz>, abgerufen am 03. Dezember 2020.

Chaos Computer Club (2018): *Offener Brief: Europäische Upload-Filter-Regelung verhindern*. <https://www.ccc.de/de/updates/2018/upload-filter>, abgerufen am 26. Februar 2021.

Chaos Computer Club (2020): *Reclaim Your Face! Gegen biometrische Massenüberwachung*. <https://www.ccc.de/de/updates/2020/reclaim-your-face-gegen-biometrische-massenuberwachung>, abgerufen am 06. Mai 2024.

Chaos Computer Club (2021a): *Topics*. <https://www.ccc.de/de/topics>, abgerufen am 25. Februar 2021.

Chaos Computer Club (2021b): *Stellungnahme zum ITSIG2: „Sicherheit gestalten statt Unsicherheit verwalten“*. <https://www.ccc.de/de/topics>, abgerufen am 07. Januar 2022.

Chaos Computer Club (2021c): *Pressemitteilungen des CCC*. <https://www.ccc.de/pressemitteilungen>, abgerufen am 04. August 2023.

Centraal Bureau voor de Statistiek (CBS) (2020): *ICT en economie*. <https://longreads.cbs.nl/ict-kennis-en-economie-2019/ict-en-economie/>, abgerufen am 07. Dezember 2020.

Centraal Bureau voor de Statistiek (CBS) (2022): *40 procent eerstejaars universiteit is internationale student*. https://www.cbs.nl/item?sc_itemid=3aa1a3c1-5efc-4fe9-9f2d-d7524fa3353c&sc_lang=nl-nl, abgerufen am 20. März 2023.

CERT-WM (2022): *Over het CERT-WM*. <https://www.cert-wm.nl/over>, abgerufen am 22. März 2023.

Clingendael Spectator (2018): *Why a new Hanseatic League will not be enough*. <https://spectator.clingendael.org/en/publication/why-new-hanseatic-league-will-not-be-enough>, abgerufen am 12. Dezember 2021.

Collins Dictionary (2021): *Definition von go Dutch*. <https://www.collinsdictionary.com/de/worterbuch/englisch/go-dutch>, abgerufen am 18. Dezember 2021.

Computable (2010): *Stuxnet-worm is elektronische oorlogsvoering*. <https://www.computable.nl/artikel/nieuws/security/3539497/250449/stuxnet-worm-is-elektronische-oorlogsvoering.html>, abgerufen am 23. Juli 2022.

Computable (2019): *KPN sluit Huawei uit voor core-netwerk 5G*. <https://www.computable.nl/artikel/nieuws/mobility/6652075/250449/kpn-sluit-huawei-uit-voor-core-netwerk-5g.html>, abgerufen am 21. Juli 2021.

Computerwoche (2021): *BSI Lagebericht 2021 – Sicherheitslage bleibt kritisch*. <https://www.computerwoche.de/a/sicherheitslage-bleibt-kritisch,3552028>, abgerufen am 19. Juni 2023.

Consumentenbond (2023a): *Facebook in de fout*. <https://www.consumentenbond.nl/acties/facebook>, abgerufen am 20. März 2023.

Consumentenbond (2023b): *Google volgt je stiekem: jij weet van niks*. <https://www.consumentenbond.nl/acties/zeker-online>, abgerufen am 20. März 2023.

Coöperatie OnsNet Nuenen (2012): Home. <https://www.connuenen.nl/>, abgerufen am 22. Februar 2024.

Coronavirus-Update (2020): *Coronavirus-Update: Wir müssen weiter geduldig sein*. <https://www.ndr.de/nachrichten/info/24-Coronavirus-Update-Wir-muessen-weiter-geduldig-sein,podcastcoronavirus166.html>, abgerufen am 07. Mai 2020.

Cyber Security Raad (2022a): *Over de CSR*. <https://www.cybersecurityraad.nl/over-de-csr>, abgerufen am 23. November 2022.

Cyber Security Raad (2022b): *Samenwerken is noodzaak in het beschermen van onze digitale dijken*. <https://magazines.cybersecurityraad.nl/csrmagazine/2022/01/12.-samenwerken-is-noodzaak-in-het-beschermen-van-onze-digitale-dijken>, abgerufen am 27. Februar 2024.

Cybersprint (2021): *Hack The Hague 2021 in the media*. <https://www.cybersprint.com/hth/hack-the-hague-in-the-media>, abgerufen am 12. März 2023.

Cybersprint (2022): *Hack The Hague*. <https://www.cybersprint.com/hack-the-hague>, abgerufen am 12. März 2023.

Cyberveilig Nederland (2021): *Dé belangenorganisatie voor een optimaal ondernemingsklimaat voor cybersecuritybedrijven*. <https://cyberveilignederland.nl/over-ons>, abgerufen am 17. März 2023.

Defensie.nl (2009): *The Dutch contribution to the International Security Assistance Force (ISAF)*. <https://english.defensie.nl/topics/historical-missions/mission-overview/2002/international-security-assistance-force-isaf/dutch-contribution>, abgerufen am 07. Mai 2023.

Defensie.nl (2016): *Zijn onze digitale dijken hoog genoeg?*
<https://magazines.defensie.nl/defensiekrant/2016/25/digitale-dijken>, abgerufen am 27. Februar 2024.

Defensie.nl (2022): *Defensie Cyber Commando*.
<https://www.defensie.nl/onderwerpen/cyber-security/cyber-commando>, abgerufen am 29. November 2022.

De Haagse Hogeschool (2022): *Lectoraten*.
<https://www.dehaagsehogeschool.nl/onderzoek/lectoraten>, abgerufen am 21. Januar 2022.

Destatis (2020): *Schüler/-innen an allgemeinbildenden und beruflichen Schulen*.
<https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Schulen/Tabellen/allgemeinbildende-beruflicheschulen-schularten-schueler.html>,
abgerufen am 28. Februar 2021.

Destatis (2021a): *Europa – Deutschland im EU-Vergleich 2021*.
<https://www.destatis.de/Europa/DE/Thema/Basistabelle/Uebersicht.html>, abgerufen am 07. Dezember 2021.

Destatis (2021b): *Kassenmäßige Steuereinnahmen des Bundes, der Länder und der Gemeinden nach Steuerarten*.
<https://www.destatis.de/DE/Themen/Staat/Steuern/Steuereinnahmen/Tabellen/steuerhaushalt-kassenmaessige-steuereinnahmen-nach-steuerverteilung.html>, abgerufen am 07. Dezember 2021.

Destatis (2021c): *Konjunkturindikatoren – Erwerbstätige im Inland nach Wirtschaftssektoren*.
<https://www.destatis.de/DE/Themen/Wirtschaft/Konjunkturindikatoren/Lange-Reihen/Arbeitsmarkt/lrwrw13a.html>, abgerufen am 22. Oktober 2021.

De Stentor (2021): *Heeft het virus vrij spel in de Biblebelt? 'Wij lopen niet klakkeloos achter de meute aan'*. <https://www.destentor.nl/regio/heeft-het-virus-vrij-spel-in-de-biblebelt-wij-lopen-niet-klakkeloos-achter-de-meute-aan~a090e935/>, abgerufen am 18. Dezember 2021.

Der Beauftragte der Bundesregierung für Informationstechnik (2021): *Beauftragter für Informationstechnik*.
https://www.cio.bund.de/Web/DE/Politische-Aufgaben/BfIT/bfit_node.html, abgerufen am 24. Januar 2021.

Deutscher Industrie- und Handelskammertag e. V. (DIHK) (2021): *DIHK weist auf Lücke im geplanten Corona-Steuerhilfegesetz hin*. <https://www.dihk.de/de/aktuelles-und-presse/aktuelle-informationen/dihk-weist-auf-luecke-im-geplanten-corona-steuerhilfegesetz-hin-37124>, abgerufen am 05. März 2021.

Deutsch-Niederländische Handelskammer (DNHK) (2019): *Wirtschaftsstandort Niederlande*. <https://www.dnhk.org/beratung/marktinformationen/wirtschaftsstandort-niederlande>, abgerufen am 25. Juni 2019.

Deutsche Welle (2005): *Klares Nein der Niederlande*. <https://www.dw.com/de/klares-nein-der-niederlande/a-1603125>, abgerufen am 05. Dezember 2021.

Deutsche Welle (2019): *Steinmeier bekennt sich zu deutscher Kriegsschuld*. <https://www.dw.com/de/steinmeier-bekannt-sich-zu-deutscher-kriegsschuld/a-50244009>, abgerufen am 10. Februar 2021.

Deutsche Welle (2021): *Schadsoftware "Emotet" unschädlich gemacht*. <https://www.dw.com/de/schadsoftware-emotet-unschädlich-gemacht/a-56362153>, abgerufen am 10. Oktober 2021.

Deutschlandfunk Kultur (2017): *Debatte um die deutsche Leitkultur. Wer sind wir – und was wollen wir sein?* <https://www.deutschlandfunkkultur.de/debatte-um-die-deutsche-leitkultur-wer-sind-wir-und-was-100.html>, abgerufen am 02. Oktober 2021.

Deutschlandfunk Kultur (2020): *5G-Technologie. Der härteste Widerstand kommt aus Bayern*. <https://www.deutschlandfunkkultur.de/5g-technologie-der-haerteste-widerstand-kommt-aus-bayern-100.html>, abgerufen am 18. November 2024.

Deutschlandfunk Kultur (2021): *Datensicherheit oder Abwehr von Cyberkriminalität. Politik und Gesellschaft müssen sich mal entscheiden*. <https://www.deutschlandfunkkultur.de/datensicherheit-oder-abwehr-von-cyberkriminalitaet-politik-100.html>, abgerufen am 07. Januar 2022.

De Volkskrant (2021a): *Raad van Europa wil gekozen burgemeesters in Nederland* <https://www.volkskrant.nl/nieuws-achtergrond/raad-van-europa-wil-gekozen-burgemeesters-in-nederland~b46e6eee/>, abgerufen am 20. November 2021.

De Volkskrant (2021b): *Russen zaten ten tijde van MH17-onderzoek door hack diep in systemen politie*. <https://www.volkskrant.nl/nieuws-achtergrond/russen-zaten-ten-tijde-van-mh17-onderzoek-door-hack-diep-in-systemen-politie~b0e044e1/>, abgerufen am 25. Februar 2024.

Digitalministerium.org (2021): *Gesucht: Digitalminister (m/w)*. <https://digitalministerium.org/>, abgerufen am 15. April 2021.

Digital Trust Center (2021): *Digital Trust Center start met actief informeren bedrijven over digitale dreigingen*. <https://www.digitaltrustcenter.nl/nieuws/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen>, abgerufen am 22. März 2023.

Digital Trust Center (2022a): *Over het Digital Trust Center*. <https://www.digitaltrustcenter.nl/over-het-digital-trust-center>, abgerufen am 19. April 2022.

Digital Trust Center (2022b): *Doe de Basisscan Cyberweerbaarheid*. <https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid>, abgerufen am 23. November 2022.

Duden (2019): *Kultur, die*. <https://www.duden.de/rechtschreibung/Kultur>, abgerufen am 21. Juni 2019.

eco – Verband der Internetwirtschaft e. V. (2019): *Studie IT-Sicherheit 2019: Immer mehr Unternehmen planen für den IT-Notfall*. <https://www.eco.de/presse/immer-mehr-unternehmen-planen-fuer-den-it-notfall/>, abgerufen am 13. April 2020.

ECP | Platform voor de InformatieSamenleving (2021): *Wat doet ECP*. <https://ecp.nl/over-ecp/wat-doet-ecp/>, abgerufen am 06. März 2023.

Eerste Kamer der Staten-Generaal (2007): *Toezegging Bestuurlijke Vernieuwing*. https://www.eerstekamer.nl/toezegging/bestuurlijke_vernieuwing, abgerufen am 20. November 2021.

Eerste Kamer der Staten-Generaal (2017): *Computercriminaliteit III*. https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii#p0, abgerufen am 15. Mai 2024.

Eerste Kamer der Staten-Generaal (2018): *Motie-Strik (GroenLinks) c.s. over de instelling van een onafhankelijke toetsingscommissie*. <https://www.staten-generaal.nl/9370000/1/j9vvkfj6b325az/vkrgejc49qzg>, abgerufen am 18. Oktober 2023.

Eindhoven University of Technology (2020): *Eindhoven Artificial Intelligence Systems Institute*. <https://www.tue.nl/en/research/institutes/eindhoven-artificial-intelligence-systems-institute>, abgerufen am 26. März 2024.

Emerce (2021): *Vindingrijke malware Emotet lijkt teruggekeerd*. <https://www.emerce.nl/nieuws/vindingrijke-malware-emotet-lijt-teruggekeerd>, abgerufen am 10. Oktober 2024.

e.on (2019): *Neue Studie sieht drastisch erhöhten Energieverbrauch von Rechenzentren durch neuen Mobilfunkstandard 5G*. <https://www.eon.com/de/ueber-uns/presse/pressemitteilungen/2019/neue-studie-sieht-drastisch-erhoehten-energieverbrauch-von-rechenzentren-durch-neuen-mobilfunkstandard-5G.html>, abgerufen am 15. Juli 2021.

ESET Nederland (2022): *Emotet botnet is aan een enorme opmars bezig in Nederland.* <https://www.eset.com/nl/over/newsroom/persberichten-overzicht/persberichten/eset-bevestigt-opmars-emotet/>, abgerufen am 20. Oktober 2024.

Euronews (2021): *Niederlande fühlen sich nach Brexit allein in der EU*. <https://de.euronews.com/2021/03/15/niederlande-fuehlen-sich-nach-brexit-allein-in-der-eu>, abgerufen am 07. Dezember 2021.

Europarat (2001): *Übereinkommen über Computerkriminalität*. <https://www.coe.int/de/web/conventions/full-list/-/conventions/rms/090000168008157a>, abgerufen am 13. Juni 2021.

Europol (2021): *World's most dangerous malware EMOTET disrupted through global action*. <https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action>, abgerufen am 06. Oktober 2024.

Flaßpöhler, Svenja (2018): *Derrida und die Dekonstruktion*. <https://www.philomag.de/artikel/derrida-und-die-dekonstruktion>, abgerufen am 24. Juni 2020.

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (2021a): *Wir über uns*. <https://www.fiff.de/about>, abgerufen am 05. März 2021.

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (2021b): *Offener Brief an die Deutsche Bundesregierung*. <https://www.fiff.de/presse/Cyberunsicherheitsstrategie-offBrief>, abgerufen am 23. Januar 2022.

Frankfurter Allgemeine Zeitung (2018): „5G ist nicht an jeder Milchkanne notwendig“. <https://www.faz.net/aktuell/wirtschaft/digitec/anja-karliczek-5g-muss-an-zentralen-stellen-vorhanden-sein-15902015.html>, abgerufen am 05. Juli 2021.

Fraunhofer-Institut für Integrierte Schaltungen IIS (2021): *5G-Lokalisierung*. <https://www.iis.fraunhofer.de/de/ff/lv/lok/5g.html>, abgerufen am 02. Juli 2021.

Freie Hansestadt Bremen (2021): *Anforderungs- und Sicherheitsmanagement (Compliance)*. https://www.finanzen.bremen.de/digitalisierung/it_recht_und_compliance-37241, abgerufen am 14. Februar 2021.

G DATA (2019): *G DATA ziet explosieve toename van Emotet malware*. <https://www.gdata.nl/news/g-data-ziet-explosieve-toename-van-emotet-malware>, abgerufen am 04. Oktober 2024.

Gesamtverband der Versicherer (2022): *Deutschland muss sich auf heftigere Unwetter und Naturgefahren einstellen*. <https://www.gdv.de/gdv/themen/klima/naturgefahren>, abgerufen am 18. Februar 2024.

Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) (2021): *Aktuelles*. <https://www.gdd.de/aktuelles>, abgerufen am 05. März 2021.

Gesellschaft für deutsche Sprache e. V. (2021): *Wort des Jahres*. <https://gfds.de/aktionen/wort-des-jahres/>, abgerufen am 21. April 2021.

golem.de (2020): *Unser Leitbild*. <https://www.golem.de/sonstiges/leitbild.html>, abgerufen am 27. September 2020.

golem.de (2021): *Home*. <https://www.golem.de>, abgerufen am 06. März 2021.

Greenpeace (2011): *Deutsche Umweltverbände einstimmig für Atomausstieg ohne Wenn und Aber*. <https://www.greenpeace.de/themen/atomkraft/deutsche-umweltverbaende-einstimmig-fuer-atomausstieg-ohne-wenn-und-aber>, abgerufen am 20. Februar 2021.

HackFlag (2022): *Wat is HackFlag?* <https://hackflag.org/about>, abgerufen am 09. August 2023.

Handelsblatt (2011): *Die Angst vor dem digitalen Pearl Harbor*. <https://www.handelsblatt.com/technik/it-internet/cyberattacken-die-angst-vor-dem-digitalen-pearl-harbor/3823836.html>, abgerufen am 23. Juli 2022.

Handelsblatt (2017): *Hochwasserschutz-Technik als niederländischer Exportschlager*. <https://www.handelsblatt.com/technik/forschung-innovation/klimawandel-hochwasserschutz-technik-als-niederlaendischer-exportschlager/20574806.html>, abgerufen am 16. Dezember 2020.

Handelsblatt (2020a): *Die Niederlande sind mit ihrer Blockadehaltung zu weit gegangen*. <https://www.handelsblatt.com/meinung/kommentare/kommentar-die-niederlande-sind-mit-ihrer-blockadehaltung-zu-weit-gegangen/26019264.html>, abgerufen am 07. Dezember 2020.

Handelsblatt (2020b): *Nach Aussagen von Staatsministerin Bär: Debatte über Digitalministerium gewinnt an Fahrt*. <https://www.handelsblatt.com/politik/deutschland/digitalisierung-nach-aussagen-von->

staatsministerin-baer-debatte-ueber-digitalministerium-gewinnt-an-fahrt/
25975344.html, abgerufen am 17. Januar 2021.

Handelsblatt (2020c): *BSI: Angespante IT-Sicherheitslage in Deutschland*.
<https://www.handelsblatt.com/politik/deutschland/hackerangriffe-bsi-angespannte-it-sicherheitslage-in-deutschland/26291164.html>, abgerufen am 19. Juni 2023.

heise online (2019a): *Online-Banking: Nach wie vor Beschwerden wegen PSD2-Umstellung*. <https://www.heise.de/newsticker/meldung/Online-Banking-Nach-wie-vor-Beschwerden-wegen-PSD2-Umstellung-4546850.html>, abgerufen am 25. Oktober 2020.

heise online (2019b): *Trojaner-Befall: Emotet bei Heise*.
<https://www.heise.de/news/Emotet-bei-Heise-4437807.html>, abgerufen am 04. Oktober 2024.

heise online (2020a): *Bundesregierung: BSI soll mit IT-Sicherheitsgesetz 2.0 hacken dürfen*. <https://www.heise.de/news/Bundesregierung-BSI-soll-mit-IT-Sicherheitsgesetz-2-0-hacken-duerfen-4991753.html>, abgerufen am 27. Dezember 2021.

heise online (2020b): *Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen*. <https://www.heise.de/hintergrund/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html>, abgerufen am 04. Oktober 2024.

heise online (2021a): *Heise Online*. <https://www.heise.de/>, abgerufen am 06. März 2021.

heise online (2021b): *Vodafone stellt erste Netzbereiche auf 5G Standalone um*.
<https://www.heise.de/news/Vodafone-stellt-erste-Netzbereiche-auf-5G-Standalone-um-6011740.html>, abgerufen am 06. Juli 2021.

heise online (2021c): *Emotet: Strafverfolger zerschlagen Malware-Infrastruktur*.
<https://www.heise.de/news/Emotet-Strafverfolger-zerschlagen-Malware-Infrastruktur-5038233.html>, abgerufen am 10. Oktober 2024.

Hessisches Ministerium des Innern und für Sport (2021): *Der Bereich Cybersecurity im Hessen3C*. <https://innen.hessen.de/sicherheit/hessen3c/cert>, abgerufen am 14. Februar 2021.

Holland.com (2021): *The country as small as a city*.
<https://www.holland.com/global/tourism.htm>, abgerufen am 20. Dezember 2021.

Houwing, Lotte (2020): *Facial recognition: a 'convenient' and 'efficient' solution looking for a problem?* <https://www.bitsoffreedom.nl/2020/01/29/facial-recognition-a-convenient-and-efficient-solution-looking-for-a-problem/>, abgerufen am 12. August 2023.

HSD Campus (2021): *De broedplaats voor internationale groei. Waarom HSD campus?*
<https://hsdcampus.nl/over-ons>, abgerufen am 12. März 2023.

Huawei.com (2019): *Huawei ist das am besten geprüfte Unternehmen der Welt*.
<https://www.huawei.com/de/deu/magazin/aktuelles/offener-brief>, abgerufen am 07. November 2024.

iBestuur (2019): *'Het is tijd voor digitale dijkverzwaring'*. <https://ibestuur.nl/artikel/het-is-tijd-voor-digitale-dijkverzwaring/>, abgerufen am 02. März 2024.

iBestuur (2022): *NCSC-directeur Hans de Vries: 'Soms neem ik de ruimte om te doen wat niet mag'*. <https://ibestuur.nl/artikel/ncsc-directeur-hans-de-vries-soms-neem-ik-de-ruimte-om-te-doen-wat-niet-mag/>, abgerufen am 30. Juni 2024.

Initiative Europäischer Netzbetreiber (IEN) (2019): *Über die IEN*. <https://www.ien-berlin.de/>, abgerufen am 05. März 2021.

Informationstechnikzentrum Bund (2021a): *IT-Konsolidierung Bund*. https://www.itzbund.de/DE/digitalemission/itkonsolidierungbund/itkonsolidierungbund_node.html, abgerufen am 22. Dezember 2021.

Informationstechnikzentrum Bund (2021b): *IT-Sicherheit*. https://www.itzbund.de/DE/digitalemission/itsicherheit/itsicherheit_node.html, abgerufen am 22. Dezember 2021.

IT-Planungsrat (2019): *Aufgaben des IT-Planungsrats*. https://www.it-planungsrat.de/DE/ITPlanungsrat/Aufgabenspektrum/aufgabenspektrum_node.html, abgerufen am 14. Februar 2021.

jacobriggs.io (2021): *I hacked the Dutch government and all I got was this t-shirt*. <https://jacobriggs.io/blog/posts/i-hacked-the-dutch-government-and-all-i-got-was-this-t-shirt-24>, abgerufen am 07. Februar 2025.

Johns Hopkins University (2020): *COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)*. <https://coronavirus.jhu.edu/map.html>, abgerufen am 25. Oktober 2020.

Kenniscentrum voor beleid en regelgeving (2019): *Decentralisatie*. <https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/index-10>, abgerufen am 13. November 2021.

KNSK.de (2021): *Shopping-Fails*. <https://www.knsk.de/arbeiten/bsi-online-shopping/>, abgerufen am 05. Februar 2025.

kpn (2019): *5G-netwerk en abonnement van KPN*. <https://www.kpn.com/netwerk/5g>, abgerufen am 29. November 2024.

kpn (2020): *Pas op: Emotet is weer volop actief*. <https://www.kpn.com/zakelijk/blog/pas-op-emotet-is-weer-volop-actief.htm>, abgerufen am 15. September 2024.

Landeszentrale für politische Bildung Baden-Württemberg (2005): *9/11 - die Folgen der Terroranschläge auf die USA*. <https://www.lpb-bw.de/terrorusa>, abgerufen am 25. Oktober 2020.

LOAD e. V. (2021a): *LOAD e. V. – Verein für liberale Netzpolitik*. <https://www.load-ev.de/>, abgerufen am 05. März 2021.

Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht (2012): *Studien zur Sicherheit in Deutschland*. https://www.mpg.de/6841890/stra_jb_2012, abgerufen am 10. November 2020.

Mediawijsheid.nl (2017): *Voor scholen – Lesmateriaal*. <https://www.mediawijsheid.nl/lesmateriaal/>, abgerufen am 21. März 2023.

Ministerium für Verkehr des Landes Nordrhein-Westfalen (2021): *Die Organisation des Ministeriums für Verkehr*. <https://www.vm.nrw.de/ministerium/impressum/index.php>, abgerufen am 24. Januar 2021.

Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (2020): *Wettbewerb 5G.NRW: Landesregierung fördert 13 herausragende 5G-Projekte mit bis zu 26 Millionen Euro*.

<https://www.wirtschaft.nrw/pressemitteilung/wettbewerb-5gnrw-landesregierung-foerdert-13-herausragende-5g-projekte-mit-bis-zu>, abgerufen am 13. November 2024.

MKB-Nederland (2018): *MKB-Nederland: voor een kansrijk ondernemersklimaat!* <https://www.mkb.nl/over-mkb-nederland>, abgerufen am 20. März 2023.

MKB-Nederland (2019): *Cybersecurity*. <https://www.mkb.nl/standpunten/cybersecurity>, abgerufen am 20. März 2023.

MKB-Nederland (2021): *Begrotingsbehandeling Justitie en Veiligheid, brief aan de VC voor Justitie en Veiligheid van de Tweede Kamer*. <https://www.mkb.nl/brieven-en-commentaren/begrotingsbehandeling-justitie-en-veiligheid-2021>, abgerufen am 20. März 2023.

Nationaalarchief (2010): *Ministerie van Justitie en Veiligheid: 2010*. <https://actorenregister.nationaalarchief.nl/actor-organisatie/ministerie-van-justitie-en-veiligheid>, abgerufen am 22. März 2023.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020b): *Cyber security*. <https://english.nctv.nl/themes/cyber-security>, abgerufen am 11. Februar 2025.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2021b): *Nationaal Cyber Security Centrum*. <https://www.nctv.nl/onderwerpen/nationaal-cyber-security-centrum>, abgerufen am 19. April 2022.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022a): *Studenten*. <https://www.nctv.nl/onderwerpen/studenten>, abgerufen am 09. Oktober 2022.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022b): *Organisatie*. <https://www.nctv.nl/organisatie>, abgerufen am 09. Oktober 2022.

Nationaal Cyber Security Centrum (2018a): *Wetgeving cybersecurity*. <https://www.ncsc.nl/actueel/dossiers/wetgeving-cybersecurity.html>, abgerufen am 29. Mai 2019.

Nationaal Cyber Security Centrum (2018b): *Wat is het NCSC?* <https://www.ncsc.nl/organisatie/>, abgerufen am 15. Juni 2019.

Nationaal Cyber Security Centrum (2020a): *Toename spam-campagnes met Emotet malware*. <https://www.ncsc.nl/actueel/nieuws/2020/september/16/toename-spam-campagnes-emotet>, abgerufen am 19. September 2024.

Nationaal Cyber Security Centrum (2021a): *Cyberoefening ISIDOOR*. <https://www.ncsc.nl/onderwerpen/isidoor2021>, abgerufen am 24. April 2022.

Nationaal Cyber Security Centrum (2021b): *Wereldwijd botnet Emotet ontmanteld*. <https://www.ncsc.nl/actueel/nieuws/2021/februari/12/wereldwijd-botnet-emotet-ontmanteld>, abgerufen am 06. Oktober 2024.

Nationaal Cyber Security Centrum (2021c): *Basismaatregelen cybersecurity*. <https://www.ncsc.nl/onderwerpen/basismaatregelen>, abgerufen am 28. Oktober 2021.

Nationaal Cyber Security Centrum (2021d): *Aansluiting bij het Nationaal Detectie Netwerk betekent deelname aan een uniek samenwerkingsverband*. <https://www.ncsc.nl/onderwerpen/nationaal-detectie-netwerk-ndn>, abgerufen am 28. Oktober 2021.

Nationaal Cyber Security Centrum (2021e): *Overzicht gepubliceerde Advisories*. <https://advisories.ncsc.nl/advisories>, abgerufen am 19. September 2021.

Nationaal Cyber Security Centrum (2022a): *Home*. <https://www.ncsc.nl>, abgerufen am 08. Oktober 2022.

Nationaal Cyber Security Centrum (2022b): *Wettelijke taak*. <https://www.ncsc.nl/over-ncsc/wettelijke-taak>, abgerufen am 08. Oktober 2022.

Nationaal Cyber Security Centrum (2022c): *Security Centrum – Aansluiting op het Landelijk Dekkend Stelsel (LDS)*. <https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds>, abgerufen am 09. Oktober 2022.

Netwerk Democratie (2019): *Masterclass Netpolitiek*. <https://netdem.nl/nl/projects/masterclass-netpolitiek-3/>, abgerufen am 12. August 2023.

Netzpolitik.org (2021a): *Über uns*. <https://netzpolitik.org/ueber-uns>, abgerufen am 27. Februar 2021.

Netzpolitik.org (2021b): *BKA nutzt Emotet-Takedown als Türöffner für mehr Befugnisse und neue Gesetze*. <https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/>, abgerufen am 10. Oktober 2024.

New York Times (2011): *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>, abgerufen am 23. Juli 2022.

New York Times (2018): *Huawei, Failing to Crack U.S. Market, Signals a Change in Tactics*. <https://www.nytimes.com/2018/04/17/technology/china-huawei-washington.html>, abgerufen am 17. Juli 2021.

New York Times (2020): *Germany Tries to Solve a Coronavirus Puzzle With ‘Endless Pieces’*. <https://www.nytimes.com/2020/02/27/world/europe/germany-coronavirus.html>, abgerufen am 03. August 2020.

Niedersächsisches Landesamt für Bezüge und Versorgung (2020): *Eingeschränkter E-Mail-Verkehr*. https://www.nlbv.niedersachsen.de/wir_ueber_uns/eingeschränkter-e-mail-verkehr-184298.html, abgerufen am 04. Oktober 2024.

NOS (2018a): *'Opmerking cyberoorlog met Rusland is pikant, maar vooral figuurlijk*. <https://nos.nl/artikel/2254781-opmerking-cyberoorlog-met-rusland-is-pikant-maar-vooral-figuurlijk>, abgerufen am 24. November 2022.

NOS (2018b): *Wet aangenomen waardoor politie verdachten mag gaan hacken*. <https://nos.nl/artikel/2238524-wet-aangenomen-waardoor-politie-verdachten-mag-gaan-hacken>, abgerufen am 08. Oktober 2023.

NOS (2018c): *Hackteam AIVD gaf FBI cruciale info over Russische inmenging verkiezingen*. <https://nos.nl/nieuwsuur/artikel/2213762-hackteam-aivd-gaf-fbi-cruciale-info-over-russische-inmenging-verkiezingen>, abgerufen am 24. Februar 2024.

NOS (2019): *De nieuwe politieke kaart van Nederland: versnippering in beeld*. <https://nos.nl/artikel/2277253-de-nieuwe-politieke-kaart-van-nederland-versnippering-in-beeld.html>, abgerufen am 16. Dezember 2020.

NOS (2021): *'Huawei had onbeperkt toegang tot miljoenen klantgegevens van Telfort'*. <https://nos.nl/artikel/2374551-huawei-had-onbeperkt-toegang-tot-miljoenen-klantgegevens-van-telfort>, abgerufen am 19. Juli 2021.

NPO Kennis (2017): *Wat gebeurde er in Srebrenica?* <https://npokennis.nl/longread/7526/wat-gebeurde-er-in-srebrenica>, abgerufen am 21. Juni 2023.

n-tv (2016): *Wohin mit kriminellen Flüchtlingen? Abschieben in die Türkei ist nicht so einfach*. <https://www.n-tv.de/politik/Abschieben-in-die-Tuerkei-ist-nicht-so-einfach-article16904761.html>, abgerufen am 17. Juli 2019.

NU.nl (2021): *Politie vindt 600.000 slachtoffers van Emotet-malware op servers in Nederland*. <https://www.nu.nl/tech/6112795/politie-vindt-600000-slachtoffers-van-emotet-malware-op-servers-in-nederland.html>, abgerufen am 06. Oktober 2024.

NWO (2015): *Cyber Security*. <https://www.nwo.nl/en/researchprogrammes/cybersecurity>, abgerufen am 12. März 2023.

oecd.org (2019): *Internet access*. <https://data.oecd.org/ict/internet-access.htm>, abgerufen am 12. Februar 2021.

oecd.org (2021a): *Percentage of fibre connections in total broadband*. <https://www.oecd.org/digital/broadband/broadband-statistics/OECD-Indikatoren>, abgerufen am 25. November 2021.

oecd.org (2021b): *OECD Fixed broadband subscriptions per 100 inhabitants, by technology, December 2021*. <https://www.oecd.org/digital/broadband/broadband-statistics/>, abgerufen am 16. Februar 2024.

oecdbetterlifeindex.org (2020): *Niederlande*. <https://www.oecdbetterlifeindex.org/de/countries/netherlands-de/>, abgerufen am 17. Dezember 2021.

ÖDP (2019): *Bundesweite Protestaktion gegen Mobilfunkstandard 5G*. <https://www.oedp.de/aktuelles/termine/detailansicht/news/bundesweite-protestaktion-gegen-mobilfunkstandard>, abgerufen am 29. November 2024.

Officiële bekendmakingen (2018): *Kamerstuk 34 372 – Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)*. <https://zoek.officiëlebekendmakingen.nl/kst-34372-G.html>, abgerufen am 11. Oktober 2023.

Officiële bekendmakingen (2021): *Kamerstuk 26 643 – Informatie- en communicatietechnologie (ICT) / 29 911 – Bestrijding georganiseerde criminaliteit / Nr.*

768 - *Bief van de Ministervan Justitie en Veiligheid.*

<https://zoek.officielebekendmakingen.nl/kst-26643-768.html>, abgerufen am 10. April 2022.

One Conference (2019a): *Cyber Resilient Cities.*

<https://one-conference.nl/schedule-2019/day-1/keynote-4>, abgerufen am 17. Dezember 2020.

One Conference (2019b): *Cyber Security: Prevent, Detect and Respond.* <https://one-conference.nl/schedule-2019/day-2/keynote-2>, abgerufen am 15. Dezember 2020.

Openbaar Ministerie (2016): *Wet computercriminaliteit III noodzakelijk in de opsporing van criminelen.* <https://www.om.nl/actueel/nieuws/2016/01/27/wet-computercriminaliteit-iii-noodzakelijk-in-de-opsporing-van-criminelen>, abgerufen am 28. November 2023.

Openbaar Ministerie (2018): *Hack Right.*

https://www.om.nl/onderwerpen/cybercrime/hack_right, abgerufen am 01. März 2022.

Openbaar Ministerie (2021a): *Internationale politieoperatie LadyBird: botnet Emotet wereldwijd ontmanteld.*

<https://www.om.nl/onderwerpen/cybercrime/nieuws/2021/01/27/internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld>, abgerufen am 06. Oktober 2024.

Openbaar Ministerie (2021b): *Eerste zendmastbrandzaak: OM eist 12 maanden cel.*

<https://www.om.nl/actueel/nieuws/2021/03/09/eerste-zendmastbrandzaak-om-eist-12-maanden-cel>, abgerufen am 30. November 2024.

Overalsnelinternet.nl (2020): *Tijdljn snelle mobiele connectiviteit.*

<https://www.overalsnelinternet.nl/onderwerpen/tijdljn-snelle-mobiele-connectiviteit>, abgerufen am 14. Juli 2021.

Overheid (1954): *Statuut voor het Koninkrijk der Nederlanden.*

<https://wetten.overheid.nl/BWBR0002154/2017-11-17>, abgerufen am 13. Dezember 2020.

Overheid (1992a): *Aanwijzingen voor de regelgeving.*

<https://wetten.overheid.nl/BWBR0005730/2018-01-01>, abgerufen am 13. November 2021.

Overheid (1992b): *Gemeentewet.* https://wetten.overheid.nl/BWBR0005416/2021-07-10/#TiteldeelIII_HoofdstukVIII_Paragraaf2_Artikel116, abgerufen am 13. November 2021.

Overheid (2021): *Wetboek van Strafvordering.*

<https://wetten.overheid.nl/BWBR0001903/2021-01-01/>, abgerufen am 05. Oktober 2023.

Politie.nl (2021a): *Internationale politieoperatie LadyBird: wereldwijd botnet Emotet ontmanteld.* <https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html>, abgerufen am 26. November 2023.

Politie.nl (2021b): *Politie bestrijdt cybercrime via Nederlandse infrastructuur*.
<https://www.politie.nl/nieuws/2021/februari/17/politie-bestrijdt-cybercrime-via-nederlandse-infrastructuur.html>, abgerufen am 06. Oktober 2024.

Redaktionsnetzwerk Deutschland (2021): *Letztes Triell vor der Wahl: Wo konnten Baerbock, Scholz und Laschet überzeugen?* <https://www.rnd.de/politik/analyse-zum-tv-triell-wo-konnten-baerbock-scholz-und-laschet-ueberzeugen-QOUAPTT5CJDENIHNQFZX4DO2WQ.html>, abgerufen am 22. September 2021.

Reporters without borders (2021): *2021 World Press Freedom Index*.
<https://rsf.org/en/netherlands>, abgerufen am 17. Dezember 2021.

Reuters (2016): *EU-Ukraine-Abkommen droht Aus durch Niederlande*.
<https://www.reuters.com/article/niederlande-ukraine-idDEKCN12S23G>, abgerufen am 05. Dezember 2021.

Rijksoverheid (2018): *Kamerbrief over Nederlandse Cybersecurity Agenda (NCSA)*.
<https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/21/kamerbrief-over-nederlandse-cybersecurity-agenda-ncsa>, abgerufen am 05. Juni 2019.

Rijksoverheid (2019): *Nieuwe wet versterkt bestrijding computercriminaliteit*.
<https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit>, abgerufen am 04. Oktober 2023.

Rijksoverheid (2020a): *Kamerbrief over Reactie op bericht Nederland kiest harde lijn tegen Huawei in 5G-netwerk*.
<https://www.rijksoverheid.nl/documenten/kamerstukken/2020/02/03/kamerbrief-met-reactie-op-bericht-nederland-kiest-harde-lijn-tegen-huawei-in-5g-netwerk>, abgerufen am 27. September 2021.

Rijksoverheid (2020b): *OCW stelt € 1,4 miljoen beschikbaar voor innovatief online hoger onderwijs*. <https://www.rijksoverheid.nl/actueel/nieuws/2020/05/28/ocw-stelt-e14-miljoen-beschikbaar-voor-innovatief-online-hoger-onderwijs>, abgerufen am 21. März 2023.

Rijksoverheid (2021a): *Veiling frequenties voor 5G*.
<https://www.rijksoverheid.nl/onderwerpen/telecommunicatie/invoering-5g/veiling-frequenties-voor-5g>, abgerufen am 17. September 2021.

Rijksoverheid (2021b): *NCTV: Cyberaanvallen tasten zenuwstelsel maatschappij aan*.
<https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/nctv-cyberaanvallen-tasten-zenuwstelsel-maatschappij-aan>, abgerufen am 23. November 2022.

Rijksoverheid (2023a): *Rijks ICT-dashboard*.
<https://www.rijksictdashboard.nl/ictkosten/>, abgerufen am 20. Januar 2023.

Rijksoverheid (2023b): *Diensten en instellingen ministerie van Economische Zaken en Klimaat*. <https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/organisatie/diensten-en-instellingen>, abgerufen am 21. März 2023.

Rijkswaterstaat (2020): *Waterkeringen*.
<https://www.rijkswaterstaat.nl/water/waterbeheer/bescherming-tegen-het-water/waterkeringen/index.aspx>, abgerufen am 15. Dezember 2020.

Rijkswaterstaat (2022): *Veiligheid*. <https://www.rijkswaterstaat.nl/over-ons/onze-organisatie/onze-missie/veiligheid>, abgerufen am 22. März 2023.

rtl nieuws (2016): *3 argumenten tegen de hackwet*. <https://www.rtlnieuws.nl/tech/artikel/3942116/3-argumenten-tegen-de-hackwet>, abgerufen am 15. Oktober 2023.

RWTH Aachen (2020): *Achtung – Angriffswelle!* <https://blog.rwth-aachen.de/itc/2020/01/24/achtung-angriffswelle/>, abgerufen am 04. Oktober 2024.

Sanders, Koen (2020): *Hacking the Dutch government. (SQLi -> RCE)*. <https://www.linkedin.com/pulse/hacking-dutch-government-sqli-rce-koen-sanders>, abgerufen am 07. Februar 2025.

Security Delta (2019): *79 Hackers Attack the Municipality of The Hague for 6 Hours*. <https://securitydelta.nl/news/overview/79-hackers-attack-the-municipality-of-the-hague-for-6-hours>, abgerufen am 12. März 2023.

Security Delta (2022): *Over HSD*. <https://securitydelta.nl/nl/over/over-hsd>, abgerufen am 01. März 2022.

Security Delta (2022): *Geschiedenis*. <https://securitydelta.nl/nl/over/geschiedenis>, abgerufen am 12. März 2023.

SeniorWeb (2020): *Computerhulp in begrijpelijke taal*. <https://www.seniorweb.nl/pchulp>, abgerufen am 13. August 2023.

Spiegel.de (2010): *Der Wurm, der aus dem Nichts kam*. <https://www.spiegel.de/netzwelt/web/computervirus-stuxnet-der-wurm-der-aus-dem-nichts-kam-a-718927.html>, abgerufen am 23. Juli 2022.

Spiegel.de (2016): *Schlüsselmomente im Irakkrieg. Der Kreuzzug*. <https://www.spiegel.de/geschichte/irakkrieg-2003-george-w-bush-und-der-krieg-gegen-terror-a-1101543.html>, abgerufen am 29. Mai 2021.

Spiegel.de (2021): *Infrastruktur von Emotet abgeschaltet. Strafverfolger stoppen die gefährlichste Schadsoftware der Welt*. <https://www.spiegel.de/netzwelt/web/emotet-gestoppt-straftverfolger-zerschlagen-infrastruktur-der-beruechtigten-schadsoftware-a-dbc45b2a-11d5-453e-a8b2-f56088c85133>, abgerufen am 10. Oktober 2024.

Stop5GNL (2019): *Brief aan Ministerie van Economische Zaken en Klimaat*. <https://www.stop5gnl.nl/wp-content/uploads/2020/01/brief-aan-Ministerie-EZK-Wiebes-19-12-19-3.pdf>, abgerufen am 05. Juli 2021.

Süddeutsche Zeitung (2019): *Deutsche Krankenhäuser mit Ransomware infiziert*. <https://www.sueddeutsche.de/digital/krankenhaeuser-schadsoftware-ransomware-virus-drk-1.4529406>, abgerufen am 18. Oktober 2019.

Süddeutsche Zeitung (2020): *Ein Funkmasten, eine Straße und jede Menge Ärger*. <https://www.sueddeutsche.de/muenchen/muenchen-fuerstenried-mobilfunkmast-5g-protest-1.5005012>, abgerufen am 04. Juli 2021.

SURF (2021a): *Wat vindt SURF?* <https://www.surf.nl/over-surf/wat-vindt-surf>, abgerufen am 21. März 2023.

SURF (2021b): *Wat vindt SURF?* <https://www.surf.nl/snellius-de-nationale-supercomputer>, abgerufen am 21. März 2023.

SURF (2021c): *Leden van SURF*. <https://www.surf.nl/over-surf/leden-van-surf>, abgerufen am 21. März 2023.

Tagesschau (2020): *"Erstaunlich schlecht informiert"*. <https://www.tagesschau.de/investigativ/anonymousnews-103.html>, abgerufen am 24. Oktober 2020.

Tagesspiegel (2018): *Beim 5G-Ausbau wächst die Angst vor Chinas Spionen*. <https://www.tagesspiegel.de/wirtschaft/diskussion-um-huawei-beim-5g-ausbau-waechst-die-angst-vor-chinas-spionen/23699284.html>, abgerufen am 17. Juli 2021.

Tagesspiegel (2020): *Nach Emotet-Virusbefall: Datenproblem an Berliner Kammergericht schwerer als erwartet*. <https://www.tagesspiegel.de/berlin/datenproblem-an-berliner-kammergericht-schwerer-als-erwartet-4139422.html>, abgerufen am 04. Oktober 2024.

Tagesspiegel (2021): *Wen der Bundestag repräsentiert. Das Parlament der Akademiker*. <https://www.tagesspiegel.de/themen/agenda/wen-der-bundestag-repraesentiert-das-parlament-der-akademiker/27735784.html>, abgerufen am 27. Oktober 2021.

Technische Universiteit Delft (2020): *Cybersecurity at the Faculty of Electrical Engineering, Mathematics, and Computer Science*. <https://www.tudelft.nl/ewi/over-de-faculteit/afdelingen/intelligent-systems/cybersecurity>, abgerufen am 26. März 2024.

Techzine (2018): *GroenLinks en VVD willen geen Chinese systemen bij politie en andere hulpdiensten*. <https://www.techzine.nl/nieuws/security/414494/groenlinks-en-vvd-willen-geen-chinese-systemen-bij-politie-en-andere-hulpdiensten/>, abgerufen am 19. Juli 2021.

Telefonica.de (2020): *Unser 5G Netz*. <https://www.telefonica.de/5g.html>, abgerufen am 13. November 2024.

Telegraph.co.uk (2011): *Stuxnet virus attack: Russia warns of 'Iranian Chernobyl'*. <https://www.telegraph.co.uk/news/worldnews/europe/russia/8262853/Stuxnet-virus-attack-Russia-warns-of-Iranian-Chernobyl.html>, abgerufen am 23. Juli 2022.

Telekom.de (2019): *Was ist 5G?* <https://www.telekom.de/unterwegs/was-ist-5g>, abgerufen am 13. November 2024.

Transparency.org (2020): *Country data*. <https://www.transparency.org/en/countries/netherlands>, abgerufen am 17. Dezember 2021.

Transparency International Deutschland (2020): *Transparency Deutschland begrüßt Prüfung der Gesetze zur Auswertung von Patientendaten durch das Bundesverfassungsgericht*. <https://www.transparency.de/aktuelles/detail/article/transparency-deutschland-begruesst-pruefung-der-gesetze-zur-auswertung-von-patientendaten-durch-das-bun/>, abgerufen am 05. März 2021.

Transparency International Deutschland (2021): *Einigung beim Lobbyregister – Transparenz geht anders*. <https://www.transparency.de/aktuelles/detail/article/einigung-beim-lobbyregister-transparenz-geht-anders/>, abgerufen am 05. März 2021.

Tweakers.net (2021): *Huawei bevestigt in Nederland geen coretechnologie voor 5G-netwerken te leveren*. <https://tweakers.net/nieuws/181980/huawei-bevestigt-in-nederland-geen-coretechnologie-voor-5g-netwerken-te-leveren.html>, abgerufen am 27. September 2021.

Twitter.com (2019a): @certbund. <https://x.com/certbund/status/1164803474497761286>, abgerufen am 04. Oktober 2024.

Twitter.com (2019b): @certbund. <https://x.com/certbund/status/1206577491281895424>, abgerufen am 04. Oktober 2024.

Twitter.com (2019c): @Stadt_FFM. https://x.com/Stadt_FFM/status/1207314656123129856, abgerufen am 04. Oktober 2024.

Twitter.com (2019d): @NCSC-NL. https://x.com/ncsc_nl/status/1120600632673615872, abgerufen am 09. Februar 2025.

Twitter.com (2019e): @Honkhase. <https://twitter.com/honkhase/status/1209785079796551680>, abgerufen am 07. August 2022.

Twitter.com (2021a): @bka. <https://x.com/bka/status/1354400213868441600>, abgerufen am 08. Oktober 2024.

Twitter.com (2021b): @NCSC-NL. https://x.com/ncsc_nl/status/1470118189786976259, abgerufen am 09. Februar 2025.

usnews.com (2021): *Overview of Netherlands*. <https://www.usnews.com/news/best-countries/netherlands>, abgerufen am 16. Dezember 2021.

van Dam, Peter (2012): *Von Polarisierung zum Poldermodell*. <https://www.uni-muenster.de/NiederlandeNet/nl-wissen/geschichte/versaeulung/poldermodell.html>, abgerufen am 12. Dezember 2020.

van Tiel, Bram (2021): *Verhoog juist digitale dijken nu cybercrime toeneemt*. <https://www.pwc.nl/nl/themas/blogs/verhoog-juist-digitale-dijken-nu-cybercrime-toeneemt.html>, abgerufen am 27. Februar 2024.

VDE (2021): *VDE + Politik*. <https://www.vde.com/de/arbeitsfelder/politik>, abgerufen am 23. Februar 2021.

Veilig Internetten (2015): *Over Veiliginternetten.nl* <https://veiliginternetten.nl/uitleg/>, abgerufen am 05. März 2023.

Veilig Internetten (2021): *Antwoord op vragen en hulp bij problemen. Voor iedereen*. <https://veiliginternetten.nl/>, abgerufen am 05. März 2023.

Veilig Internetten (2022): *Vandaag is het Safer Internet Day*. veiliginternetten.nl/nieuws/vandaag-is-het-safer-internet-day/, abgerufen am 05. März 2023.

verdi (2021): *Homeoffice in Pandemie-Zeiten*.
<https://tk-it.verdi.de/themen/nachrichten/++co++392c3b5c-bbab-11ea-b47e-001a4a160117>, abgerufen am 23. Februar 2021.

VNG.nl (2020): *Oprichting Vereniging van Nederlandse Gemeenten (1912)*.
<https://vng.nl/artikelen/oprichting-vereniging-van-nederlandse-gemeenten-1912>,
abgerufen am 06. März 2023.

VO-Raad (2022): *Praktijk & Ondersteuning*.
<https://www.vo-raad.nl/onderwerpen/digitalisering/praktijk-ondersteuning>, abgerufen
am 27. Oktober 2023.

Wielenga, Friso (2004): *Ein Strich unter die Vergangenheit? Die Normalisierung der bilateralen politischen Beziehungen*. https://www.uni-muenster.de/NiederlandeNet/nl-wissen/geschichte/beziehungen_nach45/strich.html, abgerufen am 05. Februar 2021.

Wielenga, Friso (2007): *Versäulung*. <https://www.uni-muenster.de/NiederlandeNet/nl-wissen/geschichte/nachkriegszeit/versaehlung.html>, abgerufen am 12. Dezember 2020.

WDR (2020a): *Lockerung des Datenschutzes für bessere Pandemiebekämpfung?*
<https://www1.wdr.de/nachrichten/themen/coronavirus/datenschutz-corona-virus-100.html>, abgerufen am 14. November 2020.

WDR (2020b): *Absturz Germanwings Flug 9525*. <https://reportage.wdr.de/absturz-germanwings>, abgerufen am 28. Mai 2021.

Welt (2011): *11. September - Wie Deutschland Gesetze verschärfte*.
<https://www.welt.de/politik/specials/911/article13588746/11-September-Wie-Deutschland-Gesetze-verschaerfte.html>, abgerufen am 25. Oktober 2020.

Welt (2018): *Dieser Fall entscheidet, ob Hacken eine Kriegswaffe ist*.
<https://www.welt.de/wirtschaft/article185510234/Notpetya-Dieser-Fall-entscheidet-ob-Hacken-eine-Kriegswaffe-ist.html>, abgerufen am 25. Juli 2020.

Welt (2019): *„Identitätsdiebstähle sind an der Tagesordnung“*.
<https://www.welt.de/politik/deutschland/article202045274/Internetkriminalitaet-Identitaetsdiebstaehe-sind-an-der-Tagesordnung.html>, abgerufen am 19. Juni 2023.

Wired (2001): *Dutch Prepare for Hacker Invasion*.
<https://www.wired.com/2001/08/dutch-prepare-for-hacker-invasion/>, abgerufen am 09. August 2023.

Z-CERT (2021): *Emotet; de digitale plaaggeest is terug van weggeweest*. <https://z-cert.nl/actueel/nieuws/emotet-de-digitale-plaaggeest-is-terug-van-weggeweest>,
abgerufen am 10. Oktober 2024.

ZDF (2020): *IT-Sicherheitsgesetz beschlossen - 5G in Deutschland: Hohe Hürde für Huawei*. <https://www.zdf.de/nachrichten/wirtschaft/5g-huawei-sicherheit-deutschland-100.html>, abgerufen am 07. Januar 2022.

ZEIT ONLINE (2010): *Stuxnet: Wer war's? Und wozu?*
<https://www.zeit.de/2010/48/Computerwurm-Stuxnet>, abgerufen am 21. April 2022.

ZITiS (2020): *Aufgaben & Ziele*.
https://www.zitis.bund.de/DE/ZITiS/Aufgaben/aufgaben_node.html, abgerufen am 20. August 2020.

Videografie

AD – Zo werkt het beruchte cybervirus Emotet (2021):

<https://www.ad.nl/video/productie/zo-werkt-het-beruchte-cybervirus-emotet-265469-265469>

Bundesamt für Sicherheit in der Informationstechnik – @bsi_bund (2021a):

https://www.youtube.com/@bsi_bund

Bundesamt für Sicherheit in der Informationstechnik – @bsi_bund (2021b):

<https://www.youtube.com/watch?v=9H-fGSRRoPY>

NOS Live – LIVE: MIVD: Russische hack van OPCW voorkomen, MH17-onderzoek ook doelwit (2018): <https://www.youtube.com/watch?v=Qg2bSVkWVNs>

Tagesschau – tagesschau 20:00 Uhr (2021):

https://www.tagesschau.de/multimedia/sendung/tagesschau_20_uhr/video-815779.html

Tomorrow Unlocked – How a global police force took down Emotet (2021):

<https://www.youtube.com/watch?v=s3o3qOipHhk>

WNL Op Zondag – Defensie-minister Bijleveld: ‘Nederland is in cyberoorlog met Rusland’ (2018): <https://www.youtube.com/watch?v=q39GkUgi7bQ>