Zentrum für Europäische Integrationsforschung
Center for European Integration Studies
Rheinische Friedrich-Wilhelms Universität Bonn

Discussion Paper

Johannes Wiggen

Chancen und Grenzen europäischer Cybersicherheitspolitik

C261
2020

Johannes Wiggen ist Referent für Cybersicherheit in der Abteilung Internationale Politik und Sicherheit der Konrad-Adenauer-Stiftung e.V. Er studierte Politikwissenschaft und BWL an der Albert-Ludwigs-Universität Freiburg, der Rheinischen-Friedrich-Wilhelms-Universität Bonn und der University of Dundee. Dieses Papier beruht auf seiner Masterarbeit an der Universität Bonn. Der Autor gibt seine persönliche Meinung wieder.

Johannes Wiggen

Chancen und Grenzen europäischer Cybersicherheitspolitik

Angst und Aufrüstung im Cyberspace: Das Cybersicherheitsdilemma

> „Während Attacken physische Infrastruktur in der Ukraine oder dem Iran beschädigten, waren sie bislang nicht darin erfolgreich, Volkswirtschaften oder Gesellschaften massiven und anhaltenden Schaden zuzufügen. Ohne Zweifel ist dies nur eine Frage der Zeit. Cyber ist zweifelsohne eine Waffe der Spionage aber es ist auch eine Waffe die Staaten nutzen, um zu destabilisieren, manipulieren, beeinträchtigen und zu sabotieren. Und das was in Friedenszeiten wahr ist, wird es in Krisen- und Kriegszeiten wahrscheinlich noch mehr sein.“[1]

Der Ausschnitt aus einer Rede der französischen Verteidigungsministerin Florence Parley anlässlich der Teilveröffentlichung der ersten offensiven Cyberdoktrin des Landes im Januar 2019 steht exemplarisch für die Angst europäischer Staaten vor „Cyberattacken“ anderer Staaten, die heute vielfach die vor Terroranschlägen nach „9/11“ abgelöst hat. [2] Staatliche Cyberoperationen – landläufig unpräzise als „Cyberattacken“ bezeichnet – können der Sabotage, Spionage und Subversion dienen und haben ihren

1 Florence Parley: in Ministère des Armées, Madame Florence Parly, ministre des Armées, Stratégie cyber des Armées, Paris, le 18 janvier 2019, S. 3f., Übersetzung J.W., online unter: https://www.defense.gouv.fr/content/download/551517/9394183/20190118%20%20Stratégie%20cyber%20des%20Armées.pdf.

2 Zwar fürchten Staaten auch die heimtückischen Cyberaktivitäten nicht-stattlicher Cyberakteuren bzw. deren Zusammenarbeit mit staatlichen Akteuren (siehe hierzu Tim Maurer: Cyber Mercenaries, The State, Hackers, and Power, Cambridge: Cambridge University Press, 2018). Staatliche Akteure verfügen aber nach wie vor über deutlich weitreichendere Möglichkeiten und Ressourcen, die nationale Sicherheit eines anderen Staates negativ zu beeinflussen (vgl. Erik Gartzke: The Myth of Cyberwar. Bringing War in Cyberspace Back to Earth, in International Security 2 (2013), S. 41-73, hier S. 63; Jon R. Lindsay: Stuxnet and the Limits of Cyber Warfar, in: Security Studies 3 (2013), S. 365-404, hier S. 389.
Internet resources, last date of access: January 2020

Ausgangspunkt in dem Eindringen eines Staates in ein bedeutsames Netzwerk eines anderen Staates.[3] Eine Netzwerkoperation kann dem eindringenden Staat Vorteile bzw. Gewinne bescheren während der von einer Kompromittierung eines Netzwerks betroffene Staat Nachteile bzw. Verluste erleiden kann. Die Sorge von Staaten, dass sich andere Staaten in ihren wichtigen Netzwerken befinden, führt Ben Buchanan zufolge dazu, dass sie zur Optimierung der Sicherheit ihrer eigenen Netzwerke in größerem Umfang in die Netzwerke anderer Staaten eindringen. Diese Dynamik, die ungewollt eskalieren kann, bezeichnet Buchanan das Cybersicherheitsdilemma:

> „To assure their own cybersecurity, states will sometimes intrude into the strategically important networks of other states and will threaten – often unintentionally – the security of those states, risking escalation and undermining stability".[4]

Im Wesentlichen besagt das Sicherheitsdilemma bei Netzwerkoperationen folgendes: Staaten, die über die Option der Durchführung einer Cyberoperation in Krisenfällen verfügen wollen, können aufgrund der operativen Spezifika von Cyberoperationen eine Reihe von Vorbereitungen treffen, die häufig bereits das Eindringen in die Netzwerken fremder Staaten beinhalten.[5] Entgegen der weitläufigen Ansicht, dass Cyberoperationen bei Lichtgeschwindigkeit stattfänden, sind sie größtenteils „human operations", die Zeit, Disziplin, Geduld, ausgebildetes Personal, fortschrittliche Fähigkeiten und folglich der Vorbereitung sowie Planung bedürfen.[6] Daraus

3 Thomas Rid: Cyber War Will Not Take Place, in: Journal of Strategic Studies 1 (2012), S. 5-32; ders., Cyber War Will Not Take Place, Oxford: Oxford University Press. Auf taktischer Ebene beinhaltet eine Cyberoperation den Einsatz von Code bzw. dessen „Hack" über digitale Netzwerke, Systeme und andere verbundene Geräte mit dem Ziel des Diebstahls, der Veränderung oder Zerstörung von Informationen bzw. der Einschränkung oder Unterbindung deren Funktionalität (Sven Herpig: Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cyber Security for the State, Hull: University of Hull 2016, S. 49 f.).

4 Ben Buchanan: The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations, Oxford: Oxford University Press 2017, S. 3.

5 Ebd., S. 44-48. Ausgangspunkt von Buchanans Cybersicherheitsdilemma ist, dass sich die Dynamik des Sicherheitsdilemmas auch auf Geheimdienstoperationen zum Sammeln von Informationen übertragen lässt (Ebd., S. 24; vgl. Michael Herman: Intelligence power in peace and war, Cambridge: Cambridge University Press 1996, S. 371).

6 Buchanan: The Cybersecurity Dilemma, S. 42.

resultiert das Interpretationsdilemma: Der betroffene Staat muss unter imperfekten Informationen beurteilen, ob die Cyberfähigkeiten eines anderen Staates oder dessen Eindringen in ein bedeutendes Netzwerk eine unmittelbar bevorstehende Attacke bedeuten oder nur Ausfluss dessen Aufbaus von Notfallfähigkeiten sind.[7] Aus der Perspektive der Defensive betrachtet führt besagte Angst dazu, dass sogar Staaten, die selbst keine offensiven Fähigkeiten anstreben und andere Staaten nicht bedrohen wollen, defensive Netzwerkoperationen durchführen: Sie dringen großflächig in die Netzwerke anderer Staaten ein, um mit den dort gewonnenen Informationen ihre Netzwerke sicherer zu machen.[8]

Die Notwendigkeit der Durchführung defensiver Netzwerkoperationen ergibt sich daraus, dass die sogenannte „Grundlagensicherheit", bestehend aus automatisierten Systemscans anhand von Signaturen und „aktiver Verteidigung" bzw. „hunting", d. h. die proaktive, menschengestützte Suche nach Schwachstellen und Schadsoftware in den eigenen Netzwerken, für sensible Ziele wie Geheimdienste oder militärische Einrichtungen oftmals nicht ausreicht.[9] Von der Logik des konventionellen Sicherheitsdilemmas weicht dies deutlich ab: Ein Staat, der zum Schutz vor einem anderen Staat in dessen Territorium unilateral eine Militärpräsens unterhält, begeht eine Invasion und verletzt dessen Souveränität mit der hohen Wahrscheinlichkeit der Eskalation. Auch wenn defensive Netzwerkoperationen meist Geheimdienstoperationen sind oder von Militärs wie solche durchgeführt werden, birgt das Eindringen zu defensiven Zwecken in ein Netzwerk eines anderen Staates eine ernst zu nehmende Gefahr, wenn es besonders

7 Ebd. S. 49.
8 Dabei sagt das Konzept des Cybersicherheitsdilemmas nicht, dass Staaten nur zur Erhöhung ihrer eignen Sicherheit in die Netzwerke anderer Staaten eindringen. Sie können auch aus Gier, d. h. zur Erzielung relativer Gewinne in die Netzwerke anderer Staaten eindringen. Dies bedeutet, aber nicht, dass sie sich nicht auch vor den Netzwerkoperationen anderer Staaten fürchten. Daraus ergibt sich: Je gieriger ein Staat, desto weniger relevant ist das Cybersicherheitsdilemma (Ebd., S. 114).
9 Ebd., S. 58; S. 64.

bedrohlich ist oder leicht als eine unmittelbar bevorstehende Attacke missinterpretiert werden kann.[10]

Ohne die Absichten eines Eindringlings zu kennen – sind diese rein defensiver Natur zur Sicherung der eigenen Netzwerke oder hat er offensive Motive und plant eine Attacke? – müssen Staaten die Gefahr, die von einem Eindringling in einem ihrer wichtigen Netzwerke ausgeht, bewerten. In Anbetracht des Potentials von Netzwerkoperationen, das sowohl die Durchführung defensiver wie offensiver Operationen befördert, neigen Staaten, die eine Netzwerkoperation feststellen, schlussendlich dazu, das Schlimmste anzunehmen und entsprechend zu eskalieren.[11]

Als bislang einziges umfassendes politikwissenschaftliches Konzept liefert das Cybersicherheitsdilemma, das auf Robert Jervis Arbeiten zu Fehlwahrnehmungen in den internationalen Beziehungen und zum Sicherheitsdilemma aufbaut, ein Modell, mit dem sich die Logik und Dynamik hinter staatlichen Netzwerkoperationen erklären lässt.[12] Die Mitgliedsstaaten der Europäischen Union (EU) fürchten vor allem staatliche Netzwerkoperationen von Nicht-EU-Staaten. Die EU-Kommission verdeutlichte 2011 erstmals die politische Dimension von staatlichen Cyberoperationen:

> „New and technologically more sophisticated threats have emerged. Their global geo-political dimension is becoming progressively clearer. We are witnessing a trend towards using ICT for political, economic and military predominance, including through offensive capabilities".[13]

10 Ebd., S. 73. Da gezielte Cyberoperationen mit physischen Effekten der Auftakt für einen unmittelbar darauffolgenden konventionellen Konflikt sein können, sie auch weniger gezielt unkalkulierbare Gefahren bergen, sie der Errichtung eines Brückenkopfs und der Gewinnung von Informationen über das entsprechende Netzwerk dienen können, sie durch Cyberspionage zukünftige Konflikte und die Informationsverteilung beeinflussen können und die Gegenspionage bzw. Spionageabwehr negativ beeinflussen können, bewerten Staaten nahezu jedes Eindringen in eines ihrer strategischen Netzwerk als bedrohlich (Ebd., S. 76; S. 96).
11 Ebd., S. 188-191.
12 Robert Jervis: Perception and Misperception in International Relations, Princeton: Princeton University Press 1976; ders.: Cooperation under the Security Dilemma, in: World Politics 2 (1978), S. 167-214.
13 Europäische Kommission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the

Bildlicher illustrierte EU-Kommissionspräsident Jean Claude Juncker im September 2017 die Folgen von Cyberoperationen:

> „Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. […] Cyber-attacks know no borders and no one is immune".[14]

Aufbauend auf dem Konzept des Cybersicherheitsdilemmas untersucht dieses Papier, wie die EU bislang dazu beigetragen hat das Cybersicherheitsdilemma abzuschwächen bzw. wie sie dazu beitragen kann. „[M]any of the means by which a state tries to increase its security decrease the security of others", diese Bedeutung arbeitete Jervis mit dem Konzept des Sicherheitsdilemmas heraus.[15] Ein exemplarischer Blick auf die drei größten EU-Staaten Deutschland, Frankreich und das Vereinigte Königreich zeigt, dass die drei Länder offenbar der Maxime der USA folgen, die ihre militärischen Cyberfähigkeiten massiv aufrüsteten, um gegenüber Akteuren wie Russland, China, Nordkorea und dem Iran der Wahrnehmung vorzubeugen, dass die USA ein leichtes Ziel mit mangelndem Willen der Vergeltung von „Cyberattacken" seien.[16]

So kündigte Großbritannien, das bis 31. Januar 2020 Mitglied der EU war, als Reaktion auf die zunehmenden feindlichen Cyberaktivitäten Russlands, Nordkoreas und des Irans im Herbst 2018 an, seine bestehende Einheit für offensive Cyberoperationen aus Mitarbeitern des für „Signals Intelligence" (SIGINT) zuständigen „Government Communications Headquarters" (GCHQ) und des Militärs von 500 auf 2.000 Mann zu vervierfachen.[17]

Committee of the Regions, on Critical Information Infrastructure Protection, ‚Achievements and next steps: towards global cyber-security', Brussels, 31.03.2011, COM(2011) 163 final, S. 3, online unter: http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-163-EN-F1-1.Pdf.

14 Jean-Claude Juncker: in Europäische Kommission, President Jean-Claude Juncker's State of the Union Adress 2017, 13.09.2017, Updated version following delivery, Speech/17/3165, S. 3, online unter: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm.

15 Jervis: Cooperation under the Security Dilemma, S. 169.

16 David E. Sanger: N.S.A. Nominee Promotes Cyberwar Units, in: The New York Times 11.03.14, online unter: https://www.nytimes.com/2014/03/12/world/europe/nsa-nominee-reports-cyberattacks-on-ukraine-government.html.

17 David Bond: Britain preparing to launch new cyber warfare unit, in: Financial Times 21.09.18, online unter: https://www.ft.com/content/eef717f2-bb6e-11e8-8274-

Hierfür sind zusätzlich zu den in der „National Cyber Security Strategy“ für den Zeitraum von 2016-2021 veranschlagten 1,9 Milliarden Pfund 250 Millionen Pfund vorgesehen.[18] Aus dem Bericht des britischen „Intelligence and Security Committee of Parliament“ für den Berichtszeitraum 2016-2017 geht hervor, dass das GCHQ in Kooperation mit dem Verteidigungsministerium im Rahmen des „National Offensive Cyber Programme“ (NOCP) offensive Kapazitäten entwickelt, wie die Fähigkeiten zur Behinderung, Unterbrechung und Zerstörung von Kommunikations- und Waffensystemen, Vergeltungsfähigkeiten zur Beantwortung einer „Cyberattacke“ und Angriffsfähigkeiten gegen Infrastruktur, die auch in physische Effekte resultieren können sollen. [19] All diese offensiven Fähigkeiten sollen zu einer effektiven Abschreckung von „Cyberattacken“ beitragen.

Wie eingangs bereits erwähnt, stellte Frankreich im Januar 2019 seine erste offensive Cyberdoktrin in Teilen öffentlich vor, um zu signalisieren, dass Frankreich bereit ist sich mit seinen Cyberfähigkeiten zu verteidigen und andere abzuschrecken, um Frankreichs militärische Überlegenheit weiterhin zu wahren.[20] Zuvor stellte der „Strategic Review of Defence and National

55b72926558f. Als „Signals Intelligence“ oder kurz SIGINT wird das Abfangen bzw. Abhören von elektronisch übertragenen Daten über Funk, Satellit, Telefonverkehr und Mobilfunk oder auch das Eindringen in Netzwerke zur Erlangung dort gespeicherter oder übertragener Daten bezeichnet (Rid: Cyber War Will Not Take Place, 2017, S. 81.).

18 HM Government: National Cyber Security Strategy 2016-2021, 2016, online unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

19 Intelligence and Security Committee of Parliament: Annual Report *2016-2017*, Chair: The Rt. Hon. Dominic Grieve QC MP, Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013 Ordered by the House of Commons to be printed on 20 December 2017, S. 43 f., online unter: https://b1cba9b3a5e6631fds-sites.googlegroups.com/a/independent.gov.uk/isc/files/2016-2017_ISC_AR.pdf?attachauth=ANoY7crrUHWvI9vXvbwMfO_acGt9YzkglMsfGn5rrsvuWSI5VO1OTqYlim8_EILsC7gI4KIt64OlV-bLACt3rI0wS10CtmaeZ-f-XR7ZkymG1BTGeMjuSMaW2QYh6Rg3pAdB3O4ggtG_JvhA9QqERN521rOirCxjJunrs6n8BaTMAYI6rhKlMvVduGMSlkhU41aadp9D2r4SQCxVSTLg33GCT8f5HsAmE1FvskdaG7XUI0o17mONc0%3D&attredirects=0.

20 Ministère des Armées: „Éléments publics de doctrine militaire de lutte informatique Offensive“, 2019, online unter: https://www.defense.gouv.fr/fre/content/download/551555/9394645/Eléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf.

Security“ von 2017 fest, dass wiederholte „Cyberattacken“ die Verletzlichkeit von französischen Netzwerken gezeigt hätten, weswegen es das 2017 gegründete Cyberkommando (COMCYBER) der französischen Streitkräfte zur Durchführung taktischer und strategischer Cyberoperationen zu befähigen gelte.[21] Als Konsequenz beschloss die französische Regierung im Januar 2018 mit der Budgetplanung des Verteidigungshaushaltes die Ausgaben für das Cyberkommando zwischen 2019 bis 2025 um 1,6 Milliarden Euro zu erhöhen und die Anzahl der „Cyberkämpfer“ von 1.500 auf insgesamt 4.000 im Jahr 2025 nahezu zu verdreifachen.[22]

Selbst Deutschland, das außenpolitische traditionell eher zurückhaltend agiert, rüstet seine Cyberfähigkeiten – wenn auch in kleinerem Umfang – auf. Das Blog „netzpolitik.org“ veröffentlichte im September 2015 die „Strategische Initiative Technik“ des deutschen Auslandsgeheimdienstes „Bundesnachrichtendienst“ (BND). In dem als „VS-Geheim“ eingestuften Dokument heißt es, dass der BND als Reaktion auf die „Bedrohungen“, die von der „Cyber-Aufrüstungen zahlreicher Länder, darunter China und Russland“ ausgehen, seine eigenen Cyberfähigkeiten modernisieren bzw. ausbauen müsse, um „Angriffs- und Spionageversuche“ erfolgreich abzuwehren. [23] Als „SIGINT Support to Cyber Defense“ sollen die Cyberfähigkeiten „die Gewinnung von Zugängen zur Realisierung von Ansatzmöglichkeiten und die Erschließung von technischen Informationen“ ermöglichen, d. h. Netzwerkoperationen sollen die SIGINT-Aktivitäten unterstützen.[24] Militärisch zog Deutschland im April 2017 nach und stellte mit dem „Kommando Cyber- und Informationsraum“ (KdoCIR) einen neuen

21 Ministère des Armées: Strategic Review of Defence and National Security 2017, 2017, S. 80, online unter: https://www.defense.gouv.fr/layout/set/popup/content/download/520198/8733095/version/2/file/DEFENCE+AND+NATIONAL+SECURITY+STRATEGIC+REVIEW+2017.pdf.
22 Ministère des Armées: Draft Military Planning Law 2019/2025. Synopsis. A MPL based on Renewal, 2018, S. 4, online unter: https://www.defense.gouv.fr/content/download/523961/9053454/file/MPL%202019-2025%20-%20Synopsis%20(EN).pdf.
23 Andre Meister: Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will, in: Netzpolitik.org 21.09.15, online unter: https://netzpoliti-k.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/#2014-Strategische-Initiative-Technik.
24 Ebd.

militärischen Organisationsbereich auf. Neben defensiven Aufgaben wie dem Schutz der bundeswehreigenen IT-Systeme und Netzwerke, der Erstellung eines Cyberlagebildes sowie einem vage definierten Beitrag zum Schutz kritischer Infrastruktur, soll die Bundeswehr „zur Durchführung wirkungsvoller Cyber-Maßnahmen“ neben defensiven auch offensive Fähigkeiten besitzen, um Operationen in fremden Netzwerken durchführen zu können.[25]

Auch auf Ebene der EU setzen die Mehrheit der Mitgliedsstaaten auf den Ausbau von Cyberfähigkeiten. Im Rahmen der im Dezember 2017 errichteten „Permanent Structured Cooperation“ (PESCO) beschlossen 25 EU-Staaten (alle außer Großbritannien, Dänemark und Malta) zukünftig eine engere und ambitioniertere Sicherheitspolitik zu betreiben.[26] Eines der zwei von insgesamt 17 im November 2018 beschlossenen „Cyberprojekte“ soll u. a. „more active defence measures“ entwickeln.[27]

Im Kontext der EU lässt sich das Cybersicherheitsdilemma folgendermaßen konzeptionieren: Um in zukünftigen Krisenzeiten über die Option von Cyberoperationen zu verfügen und vermeintlich auch zur Abschreckung von Cyberoperationen, unternehmen die Mitgliedsstaaten und die EU-25 im Rahmen von PESCO erhebliche Vorbereitungen für offensive Netzwerkoperationen, wozu sie oftmals bereits in die Netzwerke anderer Staaten eindringen. Gleichzeitig dringen die EU-27 aus Furcht vor

25 Bundesministerium der Verteidigung: Abschlussbericht Aufbaustab Cyber- und Informationsraum. Empfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung, 2016, S. 5, online unter: https://www.bmvg.de/resource/resource/UlRvcjZYSW1RcEVHaUd4cklzQU4yNWFvejhLjVyYnR1OCt3ZlU1N09FWGxYTVBDcmdDmtjRUxQcS9vTWc2ZTVRV2pzRkw0UkN5Z25NOWtLdUY5a0UyaURHVnFpUjFjSEtOYTVFbm5MTzA9/Abschlussbericht%2 0Aufbaustab%20CIR.pdf.

26 2017/2315/CFSP: Council Decision of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States, in: Official Journal of the European Union L331, 14.12.17, S. 57-77, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:331:FULL&from=DE.

27 Rat der Europäischen Union: Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview – 19 November 2018, S. 9, online unter: https://www.consilium.europa.eu/media/37315/tablePESCO-projects-updated.pdf.

Cyberoperationen in die Netzwerke anderer Staaten ein, um dort Informationen zu sammeln und mit diesen ihre Cybersicherheit zu erhöhen. Ebenso dringen andere Staaten aus rein defensiven Zwecken in die Netzwerke der EU-27 ein. Die Cyberfähigkeitsaufwüchse der einen Seite und die Aufdeckung ihrer Netzwerkoperationen löst bei der anderen Partei, ohne deren Absichten zu kennen, das Interpretationsdilemma aus und umgekehrt: Sind diese Maßnahmen rein defensiver Natur zur Erhöhung der Cybersicherheit bzw. dienen sie dem Aufbau von Kapazitäten für den Notfall oder sind sie böswillig?

In Anbetracht der vielfältigen Einsatzmöglichkeiten von Netzwerkoperationen fürchten die EU-27 wie andere Staaten auch jedes Eindringen in eines ihrer strategischen Netze. Dies verstärkt einerseits die Notwendigkeit von defensiven Netzwerkoperationen und andererseits lässt es sie im Falle der Kompromittierung eines ihrer strategischen Netzwerke dazu neigen, im Dilemma der Beantwortung das Schlimmste anzunehmen:

> „[T]he core of the cybersecurity dilemma is about fear and that the dilemma potentially brings about. This pattern of fear and escalation shapes policy-makers' decisions".[28]

Auch wenn das Cybersicherheitsdilemma, dessen Relevanz aufgrund der voranschreitenden Vernetzung zukünftig noch zunehmen wird, weniger existenziell als das konventionelle Sicherheitsdilemma ist, kann es die politischen und wirtschaftlichen Prioritäten von Staaten beeinflussen.[29] Der dem Sicherheitsdilemma inhärenten Spiraldynamik folgenden können die aufwachsenden Cyberfähigkeiten der EU-27 – ob als Reaktion auf die aggressive Haltung anderer Staaten oder zur Erzielung relativer Gewinne – die Ängste anderer Staaten und damit eine Cyberaufrüstungsspirale sowie Konflikte induzieren.[30] Darüber hinaus verschärfen die operativen Spezifika der Vorbereitung und Durchführung von offensiven Netzwerkoperationen sowie die Notwendigkeit, auch als Verteidiger außerhalb der eigenen Staatsgrenzen zu operieren, d. h. defensive Netzwerkoperationen

28 Buchanan: The Cybersecurity Dilemma, S. 193.
29 Ebd., S. 149; S. 155.
30 Vgl. Jervis: Perception and Misperception in International Relations, S. 64 f.

durchzuführen das Sicherheitsdilemma im Cyberspace.[31] Im Falle der NATO und der EU, die beide recht vage ankündigten, ernste „Cyberattacken“ auch militärisch zu beantworten, kann das Cybersicherheitsdilemma sogar ins Militärische eskalieren.[32]

Wie beim konventionellen Sicherheitsdilemma lassen sich die Angst und die Eskalationsgefahr, die aus dem Cybersicherheitsdilemma in den zwischenstaatlichen Beziehungen resultieren, mit spezifischen politischen Maßnahmen reduzieren, wodurch das Cybersicherheitsdilemma in seiner Wirkung abgeschwächt werden kann. Hierzu bedarf es eines umfassenden politischen Ansatzes, der kurzfristig die Stabilität erhöht, mittelfristig Vertrauen zwischen Staaten aufbaut und langfristig das Risiko von Fehlinterpretationen reduziert.[33] Dementsprechend wird das Cybersicherheitsdilemma in diesem Papier auf den „Sicherheitsakteur EU“ übertragen, der mit seinen Politiken versucht, sich bzw. seine Mitgliedsstaaten vor staatlichen „Cyberattacken“ zu schützen bzw. diese zu vermeiden. Dieses theoretisch-konzeptionell geleitete Vorgehen zur Identifikation und Bewertung der bislang von der EU unternommenen Politiken im Kontext staatlicher Cyberoperationen bietet gegenüber gewöhnlichen „Policy-Papieren“ zu dem Thema Cybersicherheit auf EU-Ebene den Mehrwert, dass es eine systematische Analyse und spezifischere Erkenntnisse über die Effektivität der EU-Politiken ermöglicht.[34]

31 Buchanan: The Cybersecurity Dilemma, S. 32; S. 52.
32 North Atlantic Treaty Organization: Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05.09.14, online unter: https://www.nato.int/cps/en/natohq/official_texts_112964.htm; Rat der Europäischen Union: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, 13007/17, Brussels, 9 October 2017, S. 10, online unter: http://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.
33 Buchanan: The Cybersecurity Dilemma, S. 157.
34 Vgl. Annegret Bendiek/Raphael Bossong/Matthias Schulze: The EU’s Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges, in: SWP Comments 47, November 2017, online unter: https://www.swp-berlin.org/fileadmin/contents/products/comments/2-017C47_bdk_etal.pdf; Erica Moret/Patryk Pawlak: The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?, Hrsg. European Union Institute for Security Studies (EUISS), July 2017, online unter: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20san

Dieses Papier argumentiert, dass sich die Cyber-Diplomatie der EU zur Abschwächung des Cybersicherheitsdilemmas verstärkt auf den Aufbau von Vertrauen mit nicht-gleichgesinnten Staaten und die Etablierung eines zwischenstaatlichen Status quo im Umgang mit Cyberoperationen konzentrieren sollte. Zur Signalisierung ihrer friedvollen Absichten und um so einen Beitrag zur Cybersicherheit aller Staaten zu leisten, sollte die EU einen Schwachstellenmanagementprozess verabschieden sowie sich pro-Verschlüsselung positionieren. Des Weiteren sollten die EU-27 Cybersicherheit defensiv denken, um das Cybersicherheitsdilemma nicht weiter zu befeuern, und deutlich machen, dass nur Cyberoperationen, die vergleichbar eines Militärschlages sind, mit konventioneller Gewalt beantwortet werden.

Die Ambitionen und Möglichkeiten der EU auf dem Feld der Cybersicherheitspolitik

Was sind die Ziele der EU auf dem Feld der Cybersicherheitspolitik und welche Handlungsmöglichkeiten hat sie? Mit dem seit 2009 gültigen Vertrag von Lissabon (TEU-L) ist die Gemeinsame Außen- und Sicherheitspolitik (GSVP) das einzige Politikfeld der EU, das nicht den Prinzipien der qualifizierten Mehrheit (Art. 16 Abs. 4 TEU-L; Art. 238 TFEU), sondern der Einstimmigkeit unterliegt (Art. 24 TEU-L).[35] Grundlage von „operational action“ ist seit dem Vertrag von Lissabon eine Entscheidung, in der der Rat Ziele, Umfang, Mittel, den Zeitraum und die jeweiligen Implementationsbedingungen festlegt (Art. 28 TEU-L). Hierbei kann der Rat

ctions.pdf; Annegret Bendiek: The EU as a Force for Peace in International Cyber Diplomacy, in: SWP Comment No. 19, April 2018, online unter: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19bdk.pdf; Ivan, Paul: Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox, Discussion Paper Europe in the World Programme, 18. March 2019, Hrsg. European Policy Centre, online unter: https://www.epc.eu/documents/uploads/pub_9081_responding_cyb-erattacks.pdf?doc_id=2120.

35 Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community 2007/C 306/01, unterzeichnet am 13.12.2007, in Kraft getreten am 01.12.2009, in: Official Journal of the European Union Information and Notices C 306 50, S. 1-147, online unter: http://eurlex.europa.eu/LexUriServ/LexUriServ .do?uri=OJ:C:2007:306:FULL:EN:PDF.

auch auf restriktive Maßnahmen, d. h. Sanktionen zurückgreifen (Art. 215 TFEU). Ebenfalls kann der Rat Entscheidungen verabschieden, die den Ansatz der EU in einer bestimmten geographischen oder thematischen Sache vorgeben (Art. 29 TEU-L).

Nach wie vor soll die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) der GASP zur Krisenprävention und dem Krisenmanagement nach einstimmigem Beschluss (Art. 42 Abs. 4 TEU-L) zivile und militärische Kapazitäten bereitstellen (Art. 42 Abs. 1 TEU-L), die der EU von den Mitgliedsstaaten bereitgestellt werden sollen (Art. 42 Abs. 3 TEU-L). Mit dem Vertrag von Lissabon wurde die EU gleichzeitig zu einem Verteidigungsbündnis: Er verpflichtet die Mitgliedsstaaten im Falle „einer bewaffneten Aggression auf das Territorium" eines Mitgliedsstaates zur „aid and assistance by all the means in their power" (Art. 42 Abs. 7 TEU-L).

Während die Erwartungen an die EU von außen hochgeredet wurden – und sie sie selber hoch redete – entwickelte sich ihre Fähigkeit nach außen hin zu wirken – „*its ability to agree, its resources, and the instruments at its disposal*" – unterproportional dazu.[36] Ursächlich hierfür ist in erster Linie die Unfähigkeit der EU als ein Akteur aufzutreten und militärische Gewalt, d. h. „hard power" einzusetzen bzw. plausibel damit drohen zu können, um mittels „coercive diplomacy" einen Status quo zu erhalten.[37] Janne Haaland Matlarys Charakterisierung der EU als einem „unstrategischen" Akteur auf dem Gebiet der GASP und vor allem der GSVP scheint einleuchtend. Ihr zufolge zeichnet sich ein strategischer Akteur dadurch aus, dass er sowohl eine Strategie als auch militärische Kapazitäten besitzt, „both the ability to threaten the use of force through coercive diplomacy and the ability to actually deploy such force". [38] Der inkrementelle „„bottom-up"" Fähigkeitsaufwuchs innerhalb der Strukturen der EU sei zwar notwendig für

36 Christopher Hill: The Capability-Expectations Gap, or Conceptualizing Europe's International Role, in: Journal of Common Market Studies 3 (1993), S. 305-328, hier S. 315, (Hervorhebung im Original).
37 Alexander L. George: Coercive Diplomacy: Definition and Characteristics, in: The Limits of Coercive Diplomacy, Hrsg. Alexander L. George und William E. Simons, 7-12, Boulder: Westview Press 1994.
38 Janne H. Matlary: When Soft Power Turns Hard: Is an EU Strategic Culture Possible?, in: Security Dialogue 1 (2006), S. 105-121, hier S. 112.

einen strategischen Akteur.[39] Entscheidend ist Matlary zufolge auf dem intergouvernementalen Politikfeld der CFSP aber eine strategische Kultur, die Fragen nationaler Souveränität berühre und die folglich eine Frage des politischen Willens sei. Ohne eine strategische Kultur bleiben die institutionellen Strukturen der EU auf dem Gebiet der GASP nur ein Wasserkopf. Was bedeutet das für die Möglichkeiten der EU, das Cybersicherheitsdilemma durch politische Maßnahmen abzuschwächen?

Während „Cyber" als Substantiv oder Komposition in der „Europäischen Sicherheitsstrategie" von 2003 noch eine gänzliche Unbekannte ist, kommt das Wort in der sie ersetzenden „Globalstrategie für die europäische Außen- und Sicherheitspolitik" von 2016 in diesen Variationen 23 Mal auf 47 Seiten Fließtext vor.[40] Was aber bedeutet „Cyber" eigentlich? „Cyber" stammt von „Cybernetics" ab: In Anlehnung an das griechische Verb „kybernan", was so viel bedeutet wie „steuern, navigieren oder leiten", bezeichnet „Cybernetics" eine nach dem Zweiten Weltkrieg geprägte Theorie des Mathematikers Norbert Wiener über die Interaktion von Menschen mit Maschinen, deren zunehmende Verbreitung Kommunikation und Steuerung bzw. Kontrolle fundamental veränderten.[41] Wie das Beispiel des von Tesla im November 2019 vorgestellten „Cybertrucks" – einem futuristischen Elektro-SUV – illustriert, ist aus dem facettenreichen Begriff „Cyber" ein Gegenwartsmythos um den technologischen Fortschritt der Zukunft geworden: „The word refuses to be either noun or prefix. Its meaning is equally evasive, hazy, and uncertain. Whatever it is, it is always stirring, it is always about the future, and it always has been".[42]

39 Ebd., S. 112.
40 Europäischer Rat: European Security Strategy. A Secure Europe In A Better World, Brussels, 12. December 2003, online unter: http://www.consilium.europa.eu/uedocs/cmsupload/78367.pdf; Europäische Kommission: Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy, June 2016, S. 9; 20; 26; 37; 42; 43, online unter: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.
41 Thomas Rid: Rise of the Machines. A Cybernetic History, New York: Norton 2016, S. 3.
42 Ebd., S. XI. Siehe zum Cybertruck: Nick Carey/Naomi Tajitsu: Shattered glass: Futuristic design questioned after Tesla Cybertruck launch, in: Reuters 22.11.19, online

Was bedeutet Cybersicherheit im Kontext nationaler Sicherheit? Der Begriff „Cybersecurity“, der in den letzten Jahren einen nahezu kometenhaften Aufstieg hinter sich hat, löste die um die Jahrhundertwende verwendeten Begriffe der „Computer Security“, „IT Security“ oder „Information Security“ zusehends ab.[43] Obwohl der Begriff Cybersicherheit sich mittlerweile nicht nur in der Politik sondern teilweise auch in der Wissenschaft etabliert hat, ist er aufgrund der antiquierten Bedeutung des Begriffs „Cyber“ nicht unumstritten – adäquater wäre es von „information security“ zu sprechen.[44] Daniel Schatz, Rabih Bashroush und Julie Wall entwickeln anhand der Untersuchung heute existierender, aber häufig inkongruenter Erklärungen von staatlicher Cybersicherheit, eine repräsentativste Definition von Cybersicherheit, die auf die Bedeutung sozialer und politischer Maßnahmen zur Gewährleistung der Sicherheit von Daten eingeht:

> „The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users“.[45]

Als Politikfeld befasst sich Cybersicherheitspolitik mit defensiven wie offensiven Maßnahmen zum Schutz des Cyberspace, d. h. des technischen Mediums Internet, mit ihm verbundener und nicht verbundener Computer sowie Netzwerke vor feindlichen Aktionen sowie daraus resultierender sozialer und politischer Effekte. Des Weiteren kann Cybersicherheit bzw.

unter: https://www.reuters.com/article/us-tesla-truck-windows/shattered-glass-futuristic-design-questioned-after-tesla-cybertruck-launch-idUSKBN1XW1CU.

43 Daniel Schatz/Rabih Bashroush/Julie Wall: Towards a more Representative Definition of Cyber Security, in: Journal of Digital Forensics, Security and Law 2 (2017), S. 53-74, hier S. 66.

44 Thomas Rid/Ben Buchanan: Hacking democracy, in SAIS Review of International Affairs 1 (2018) 38: S. 3-16, hier S. 7.

45 Schatz/ Bashroush/Wall: Towards a more Representative Definition of Cyber Security, S. 66. Diese Definition von Cybersicherheit beruht – wie die meisten andere auch – auf der sogenannten „CIA-Traide“, d. h. den Konzepten der „confidentiality“ (Vertraulichkeit), „integrety“ (Integrität) und „availability“ (Verfügbarkeit) von Daten (vgl. Jason Andress: The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice, Zweite Auflage, Elsevier: Amsterdam 2014, S. 5-7).

Cyberverteidigung, wenn Aspekte dieser Definition in das Aufgabengebiet des Militärs fallen, einen Zustand bezeichnen, d. h. die Abwesenheit bzw. Reduzierung unautorisierter Netzwerkoperationen auf ein annehmbares Niveau.[46]

Was sind folglich die Ziele europäischer Cybersicherheits- bzw. Cyberverteidigungspolitik? In ihrer „Globalstrategie" für die europäische Außen- und Sicherheitspolitik vom Sommer 2016 bestätigt die EU den Trend, „Cyber" als nichtssagendes Schlagwort zu verwenden.[47] So verkündete die EU, ihre Anstrengungen auf dem Feld „Cyber" zum Schutz der Union im Inneren zu verstärken:

> „The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace".[48]

Dazu will die EU ihre technologischen Fähigkeiten zur Reduzierung von Gefahren und der Erhöhung der Resilienz von kritischer Infrastruktur sowie Informations- und Kommunikationssystemen (ICTs) stärken.[49] „[C]yber issues" sollen Bestandteil aller Politiken werden und „cyber elements" in den GSVP-Missionen und -Operationen verstärkt werden.[50] Des Weiteren will die EU Kooperationsplattformen weiterentwickeln, die Mitgliedsstaaten bei der politischen, technischen und operativen Kooperation unterstützen sowie deren Austausch mit EU-Institution fördern. Ebenso soll die Zusammenarbeit zwischen der EU und Partnern wie der NATO sowie den USA auf dem Gebiet der Cybersicherheit gestärkt werden. Hierbei sollen auch die Privatwirtschaft und die Zivilgesellschaft eingebunden werden.

Nach außen ist der Anspruch der EU nicht minder klein: „Without global norms and the means to enforce them, peace and security, prosperity and democracy – our vital interests – are at risk".[51]

46 Vgl. Lucas Kello: The Virtual Weapon and International Order, New Haven: Yale University Press 2018, S. 46.
47 Europäische Kommission: A Global Strategy, S. 9; 20; 26; 37; 42; 43.
48 Ebd., S. 21.
49 Ebd., S. 22.
50 Ebd., S. 22.
51 Ebd., S. 39.

Auf dem Politikfeld „Cyber“, „at the frontiers of global affairs“, will die EU als „forward-looking cyber player“ durch die Förderung eines freien und sicheren Internets sowie der Weiterentwicklung von Regeln dazu beitragen, die Sicherheit zu gewährleisten und den Zugang zu Gemeingütern aufrechtzuerhalten sowie ihre eigenen „critical assesments and values“ schützen:

> „We will engage in cyber diplomacy and capacity building with our partners, and seek agreements on responsible state behaviour in cyberspace based on existing international law. We will support multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information“.[52]

Verglichen mit konventionellen Konflikten, mit denen die GASP bisher konfrontiert und stets überfordert war, bedarf eine Abschwächung des Cybersicherheitsdilemmas keiner militärischen Mittel, sondern viel mehr einer umfassenden politischen Mitigationsstrategie. Einerseits könnte die EU ohne eigene operative militärische und geheimdienstliche Cyberfähigkeiten, die andere Staaten fürchten müssten, ein glaubwürdiger und – nach der Herstellung von Einigkeit – ein gewichtiger diplomatischer Akteur sein, der ggf. auch mit restriktiven Maßnahmen (Art. 215 TFEU) einen Beitrag zur Abschwächung des Cybersicherheitsdilemmas der EU-27 in den internationalen Beziehungen leisten könnte.[53] Dies sehen auch Brandon Valeriano und Ryan Maness so: „The EU already has an exceptional framework for cooperation and collaboration; using this institution as a steppingstone to further deepen international cyber agreements might be a beneficial path“.[54] Andererseits ist die EU auch das, was ihre Mitgliedsstaaten sind. Die rüsten, wie die Beispiele Großbritanniens, Frankreichs und Deutschlands gezeigt haben, ihre Cyberfähigkeiten auf und könnten auf dem sensiblen Feld der Cybersicherheit nationale Vorbehalte und Interessen haben, die

52 Ebd., S. 42.
53 Vgl. Kristof Clerix: Ikka Salmi, the EU’s spymaster, in: Mondiaal Nieuws 04.03.14, online unter: https://www.mo.be/en/interview/ilkka-salmi-eu-s-007.
54 Brandon Valeriano/Ryan C. Maness: Cyber War versus Cyber Realities, Oxford: Oxford University Press 2015, S. 43.

geschlossenes Handeln der EU-27 in der intergouvernementalen GASP konterkarieren könnten.

Die Verortung des Cybersicherheitsdilemma in den internationalen Beziehungen

Für das Cybersicherheitsdilemma relevant sind Cyberoperationen zu Friedenszeiten, die oftmals von Geheimdiensten oder mit bzw. von Militärs klandestin durchgeführt werden.[55] Sie erfüllen formal nicht die Kriterien eines Krieges nach Carl von Clausewitz: Cyberoperationen sind weder potentiell tödlich, da sie sich nur gegen ein computergestütztes System und nicht direkt gegen einen Menschen richten können, womit ihre Schadmöglichkeiten auf die physische Kraft oder Energie, die in diesem vorhanden oder von diesem geschaffen wird begrenzt sind, sie sind weder instrumentell im Sinne der Erreichung eines Ziels, noch sind sie politisch, da Staaten für sie meist keine Verantwortung übernehmen.[56]

Cyberoperationen, die Thomas Rid als politische Gewalt klassifiziert, dienen in Friedenszeiten der Sabotage, Spionage und Subversion mit dem übergeordneten Ziel der Zersetzung von Vertrauen zwischen Personen sowie dem Vertrauen von Personen in Institutionen.[57] Solche Cyberoperationen signalisieren Ausdruck von Unzufriedenheit mit dem Handeln eines anderen Staates, sollen diesem „Nadelstiche“ zufügen, erweitern die für Staaten zur Verfügung stehenden Optionen für kompetitives und aggressives Verhalten oder erweitern im Krisenfall die militärischen Optionen eines Staates. Möchten Sabotage, Spionage und Subversion effektiv sein, müssen sie

55 Rid: Cyber War Will Not Take Place, 2012, S. 15; Lindsay: Stuxnet and the Limits of Cyber Warfar, S. 43; 2015, Valeriano/Maness: Cyber War versus Cyber Realities, S.68.
56 Rid: Cyber War Will Not Take Place, 2012, S. 6; S. 10. Dementsprechend sind Cyberoperationen kein Ersatz für konventionelle Kriege, sie erweitern aber deren Spektrum z. B. um die Störung oder Zerstörung der Kommando- und Kommunikationsstruktur eines Gegners oder die Sabotage kritischer Infrastruktur.
57 Rid: Cyber War Will Not Take Place, 2012, S. 15; ders.: More Attacks, Less Violence, in: Journal of Strategic Studies 1 (2013), S.139-142, hier S. 142; ders. 2017: S. 26. Dennoch können auch die unmittelbaren physischen Effekte einer Cyberoperation, z. B. von Cybersabotage, in der Praxis von politischen Entscheidungsträgern als ein Akt des Krieges wahrgenommen werden.

unerkannt bleiben, da die andere Partei sonst Gegenmaßnahmen ergreift und sie unterbindet. [58] In Friedenszeiten sind die physischen Effekte von Cybersabotage durch die Gefahr der militärischen Vergeltung und hohe politische Kosten begrenzt.[59] Auch wenn solche verborgenen, strategischen Interaktionen kein Krieg sind, sind sie „alles andere als pazifistisch“.[60] In diesem Kontext zwischenstaatlicher Beziehungen lässt sich das Cybersicherheitsdilemma verorten.

Das Scheitern traditioneller Mitigationsmaßnahmen

Anders als das konventionelle Sicherheitsdilemma, lässt sich das Cybersicherheitsdilemma nicht mit den von Jervis herausgearbeiteten Ansatzpunkten der „Offense-Defense-Balance“, die das Verhältnis offensiver Waffen und Politiken einerseits sowie defensiver Waffen und Politiken andererseits im Hinblick auf die Überlegenheit einer Haltung beschreibt, und der Differenzierung offensiver von defensiven Militärpolitiken abschwächen. [61] Die Überlegenheit der Offensive oder Defensive betreffend, die von der Geographie und der Technologie beeinflusst wird, gibt es keine geographischen Barrieren vergleichbar mit Bergen oder Meeren, die den Verteidigern im Cyberspace einen Vorteil bieten würden. „The intruders, uninhibited by difficult geography, therefore enjoy greater freedom of action“. [62] Auch die Möglichkeit, künstliche Barrieren wie eine Firewall zur Trennung von Netzwerkbereichen zu errichten, ergibt beim Cybersicherheitsdilemma nur Sinn, wenn diese Barrieren Schutz vor Angriffen bieten und gleichzeitig die eigenen Möglichkeiten, anzugreifen, verringern.[63] Eine verbesserte Firewall, die die

58 Eric Gartzke/Jon R. Lindsay: Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace, in: Security Studies 2 (2015), S. 316-348, hier S. 346.
59 Lindsay: Stuxnet and the Limits of Cyber Warfar, S. 397 f.; Valeriano/Maness: Cyber War versus Cyber Realities, S. 64.
60 Eric Gartzke/Jon R. Lindsay: Weaving Tangled Webs, S. 346; vgl. Kello: The Virtual Weapon and International Order, S. 56; S. 78.
61 Jervis: Cooperation under the Security Dilemma, S. 187-199.
62 Buchanan: The Cybersecurity Dilemma, S. 106.
63 Jervis: Cooperation under the Security Dilemma, S. 195.

eigene Netzwerksicherheit erhöht und vergleichbar ist mit einer künstlichen Barriere, ist deswegen schlicht eine defensive Technologie.[64]

Die Technologie betreffend, die die Überlegenheit der Offensive oder Defensive bestimmt, ist das Wissen über „zero days", d. h. unbekannte Schwachstellen, die für das Eindringen in ein System mittels eines „exploit" genutzt werden können, für die Defensive beschränkt: Möchte ein Staat sie gleichzeitig für offensive Netzwerkoperationen nutzen, kann er nur dafür sorgen, dass die Software der wichtigsten Computer unter seiner Kontrolle gepatcht ist, da eine breitere Veröffentlichung der Schwachstelle ihren Wert für offensive Operationen mindern würde. Für Staaten mit Kenntnissen über unbekannte Schwachstellen bestehen deswegen Anreize diese zu verwenden.[65] Da eine unbekannte Schwachstelle und ein entsprechender „zero day exploit" nur mit viel Zeit sowie entsprechendem Wissen zu finden bzw. zu programmieren ist, ergibt sich kein genereller Vorteil für die Offensive.[66]

Wie Jervis verdeutlichte, bestimmt sich die Überlegenheit der Offensive oder Defensive allerdings weniger auf Grundlage von Tatsachen, als vielmehr durch subjektive Wahrnehmungen.[67] Neben Vertretern aus der Wissenschaft wird die Offensive auch von Praktikern aufgrund der technischen Infrastruktur des Internets und der vermeintlich leichteren Durchführbarkeit von offensiven Netzwerkoperationen als überlegen wahrgenommen.[68] So äußerte 2015 der damalige US-Präsident Barack Obama: „Offense is moving

64 Buchanan: The Cybersecurity Dilemma, S. 106.
65 Ebd., S. 107 f.
66 Die IT-Sicherheitsfirma „Symatec" stellte fest, dass im Jahr 2018 nur 23% der 155 bekannten „attack groups" Zero-Day-Exploits nutzten, was eine Verringerung um 4% zum Jahr 2017 ist. Die meisten offensiven Netzwerkoperationen nutzen bekannte Schwachstellen oder Spear-Phishing-E-Mails (Symatec: Internet Security Threat Report, Volume 24, February 2019, online unter: https://www.symantec.com/content/dam /symantec/docs/reports/istr-24-2019-en.pdf.).
67 Jervis: Cooperation under the Security Dilemma, S. 189-191.
68 Vgl. Nazli Choucri: Cyberpolitics in International Relations, Cambridge: MIT Press 2012; Kello: The Virtual Weapon and International Order.

faster than defense“.[69] In China wird die Offensive ebenfalls als im Vorteil wahrgenommen, konstatiert Lindsay: „Chinese doctrine stresses that striking fast and striking hard against the most important networked targets is essential, because victory at the beginning of a war will determine its end“.[70] Die offensiven Cyberfähigkeitsaufwüchse Deutschlands, Frankreichs und Großbritanniens, können ebenfalls als Ausdruck einer wahrgenommenen Überlegenheit der Offensive interpretiert werden, der die europäischen Staaten zum Aufrüsten animiert. Vergleichbar mit der Situation vor dem ersten Weltkrieg, als die Offensive ebenfalls als überlegen wahrgenommen wurde, verstärkt solch eine Perzeption die Triebkräfte des Cybersicherheitsdilemmas.[71]

Die Unterscheidbarkeit offensiver von defensiven Waffen, die bereits im konventionellen Sicherheitsdilemma nicht einfach ist und stets von deren Einsatzkontext abhängt, lässt sich auf das Cybersicherheitsdilemma nahezu nicht anwenden.[72] Als Bestandteil der Grundlagensicherheit können z. B. Virenscanner, Firewalls und Software-Patches als rein defensive Technologien betrachtet werden, die außerhalb der eigenen Netzwerke nahezu keinen Nutzen haben.[73] Um ihre Cybersicherheit zu erhöhen, dringen die Geheimdienste einiger Staaten allerdings in die Netzwerke fremder Staaten ein, um dort Informationen zu sammeln. Der selbe Code, der in diesem Kontext einem defensiven Zweck dient, kann in einem anderen Fall auch offensiv eingesetzt werden. Erneut verdeutlichte US-Präsident Obama die Problematik in einem Interview:

> „This is more like basketball than football, in the sense that there’s no clear line between offense and defense. Things are going back and forth all the time [...].

69 In U.S.-Department of Defense: Obama Discusses National Security During Worldwide Troop Talk, 11.09.15, online unter: https://dod.defense.gov/News/Article/Article/616987/obama-discusses-national-security-during-worldwide-troop-talk/.
70 Lindsay, Jon R: The Impact of China on Cybersecurity, in: International Security 3 (2015), S. 7-47, hier S. 36.
71 Buchanan: The Cybersecurity Dilemma, S. 110.
72 Jervis: Cooperation under the Security Dilemma, S. 203 f.
73 Buchanan: The Cybersecurity Dilemma, S. 111 f.

> [...] Because when you develop sufficient defenses, the same sophistication you need for defenses means that, potentially, you can engage in offense".[74]

Die Ambivalenz von Code als Mittel, das sowohl offensiv als auch defensiv eingesetzt werden kann, ist noch keine Abweichung vom traditionellen Sicherheitsdilemma. Problematisch ist, dass eine offensive Technologie, d. h. das Eindringen in ein fremdes Netzwerk, im Cyberspace einem defensiven Zweck dienen kann.[75] Dies widerspricht der Grundidee der Differenzierung offensiver von defensiven Waffen. Da eine ausschließlich zu defensiven Zwecken durchgeführte Netzwerkoperation – anders als andere defensive Technologien wie z. B. Artillerie mit einer begrenzten Reichweite – dem Eindringling in dem fremden Netzwerk dennoch eine Vielzahl von Möglichkeiten eröffnet, wird der davon betroffenen Staat stets verunsichert sein. Hinzu kommt, dass ein Verteidiger, der einen Eindringling als einen unsicheren Staat identifiziert, der nur aus defensiven Motiven Informationen sammeln möchte, sich dessen Absichten in seinem Netzwerk für die Zukunft nicht sicher sein kann: „The nature of an intrusion can change with a state's intention".[76] Eine Unterscheidung zwischen offensiven und defensiven Waffen anhand deren Zwecks ist im Cyberspace deshalb kaum möglich.

Das Cybersicherheitsdilemma durch das Signalisieren friedvoller Absichten mittels der gezielten Beeinflussung der eigenen Cybersicherheits- und Cyberverteidigungspolitik abzuschwächen, wie es Charles Glaser für das konventionelle Dilemma vorschlug, ist ebenfalls von begrenzter Wirkung.[77] Waffenkontrollabkommen sind aufgrund der schwierigen Verifikation und der verhältnismäßig niedrigen Einstiegshürden im Cyberspace nur begrenzt wirksam. Das unilaterale Absenken defensiver Fähigkeiten birgt die Gefahr, den ohnehin niedrigen Sicherheitsstandard der Grundlagensicherheit weiter abzusenken und ist ohnehin schwierig von einer oftmals unzureichenden

74 In Liz Gannes: How Cyber Security Is Like Basketball, According to Barack Obama, in: *Vox* 14.02.15, online unter: https://www.vox.com/2015/2/14/11559050/how-cyber-security-is-like-basketball-according-to-barack-obama.
75 Buchanan: The Cybersecurity Dilemma, S. 64-69.
76 Ebd., S. 113.
77 Charles Glaser: The Security Dilemma Revisited, in: World Politics 1 (1997), S. 171-201, hier S. 181.

Netzwerkverteidigung zu unterscheiden.[78] Auf das Eindringen in fremde Netzwerke zu verzichten könnte eine vertrauensbildende Maßnahme sein. Ohne wiederum in die Netzwerke dieses Staates einzudringen ist dies allerdings schwierig zu verifizieren. Ausschließlich eine defensive Haltung mit mehr Personal zur Netzwerkverteidigung einzunehmen, erhöht die Grundlagensicherheit. Eine rein defensive Cybersicherheitshaltung, die ein über die Grundlagensicherheit hinausgehendes Sicherheitsniveau gewährleisten möchte, ist allerdings von defensiven Netzwerkoperationen abhängig. Solche defensiven Operationen sind schwierig von böswilligen Netzwerkoperationen zu unterscheiden, weswegen eine unilaterale Verteidigungshaltung ihre Effektivität verliert.[79]

Eine Rechtsgrundlage und daraus ableitbare Normen sowie Regeln, die das Cybersicherheitsdilemma nachhaltig mitigieren und als Ausgangslage zur Beurteilung inakzeptablen Verhaltens fungieren könnten, existieren mit Blick auf das Internet nicht: Es gibt hier keinen Status quo, obwohl die Vereinten Nationen (UN) seit 1999 versuchen den Missbrauch von ICTs durch internationale Kooperation, vertrauensbildende Maßnahmen und die Verrechtlichung sowie Herausbildung von Normen zu verhindern.[80] Die sogenannten „Groupe of Governmental Experts“ (GGEs) – Experten aus den UN-Mitgliedsstaaten – einigten sich 2013 u. a. darauf, dass internationales Völkerrecht und die Charta der Vereinten Nationen im Cyberspace gelten sollen.[81] Ebenso sollen sich die Staaten an die „non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment” halten.[82] In der

78 Buchanan: The Cybersecurity Dilemma, S. 115. Hinzu kommt, dass nicht-staatliche Akteure die verringerte Grundlagensicherheit ausnutzen könnten.
79 Ebd., S. 116.
80 A/RES/53/70: United Nations, Resolution Adopted by General Assembly, Developments in the field of information and telecommunications in the context of international security, 4. January 1999, online unter: https://undocs.org/A/RES/53/70. Zugegriffen: 25.06.19
81 A/68/98: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, S. 8, in United Nations General Assembly A/68/98* 24.06.13, online unter: http://undocs.org/A/68/98.
82 A/70/174, 2015, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International

Praxis zeigt sich, dass z. B. Russland und die USA mit ihren Aufklärungsoperationen in den Netzwerken von Stromkraftwerken des jeweils anderen gegen die von den UN-Experten vorgeschlagene Norm, dass Staaten nicht die kritische Infrastruktur anderer Staaten zum Ziel von Netzwerkoperationen machen sollen, verstoßen. [83] Insgesamt bleibt die Einhaltung der Experten-Kompromisse freiwillig und die genaue Anwendbarkeit von Völkerrecht, an deren Ausarbeitung eine weitere Sachverständigengruppe 2017 scheiterte, vage.[84]

Ansatzpunkte zur Mitigation des Cybersicherheitsdilemmas

Wie können die negativen Folgen des Cybersicherheitsdilemmas effektiv abgeschwächt werden? Notwendig aber alleine nicht hinreichend zur Mitigation des Cybersicherheitsdilemmas ist die Grundlagensicherheit (automatisierte Systemscans und aktive Verteidigung). Auf dieser Grundlagensicherheit basieren alle weiteren Maßnahmen zur Abschwächung des Cybersicherheitsdilemmas. [85] Der Ausbau der Grundlagensicherheit beeinflusst nicht die Offense-Defence-Balance, da defensive Technologien wie Scans und Firewalls anders als konventionelle Waffen keine offensiven Aktivitäten zulassen. [86] Eine aktive, menschengestützte Verteidigung zum Aufspüren von Eindringlingen in einem Netzwerk kann auch ohne Informationen, die in fremden Netzwerken

Security, S. 7, in United Nations General Assembly 22.07.15. https://undocs.org/A/70/174.

83 A/70/174, 8; vgl. David E. Sanger/Nicole Perlroth: U.S. Escalates Online Attacks on Russia's Power Grid, in: The New York Times 15.06.19, online unter: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

84 Adam Segal: Cyber Norms at the United Nations Ends in Deadlock. Now What?, in: Council on Foreign Relations 29.06.17, online unter: https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what; Arun M. Sukumar: The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?, in: lawfareblog.com 04.07.17, online unter: https://www.lawfareblog.com/un-gge-failed-inter-national-law-cyberspace-doomed-well.

85 Buchanan: The Cybersecurity Dilemma, S. 161.

86 Ebd., S. 158.

gewonnen wurden, ein adäquates Mittel gegen eine Vielzahl von Gefahrenakteuren sein.

Für diesen zeit- und ressourcenintensiven Prozess bedarf es mehr und besser ausgebildetes Personal. Dieses trägt zur Erhöhung der eigenen Cybersicherheit bei ohne die der anderen Staaten zu reduzieren und verringert zusätzlich die Notwendigkeit von defensiven Netzwerkoperationen. [87] Darüber hinaus verbessert ein Ausbau der Grundlagensicherheit komplexe Cybersicherheitsentscheidungsstrukturen, indem die kleine Anzahl relevanter Gefahren in der Mehrheit irrelevanter Gefahren wie Scans zur Zielaufklärung identifiziert werden kann.[88] Durch die Beschränkung auf potentiell gefährliche Staaten und Netzwerkoperationen lässt sich das Cybersicherheitsdilemma dort womöglich vermeiden und insgesamt handhabbarer machen. Anders als bei Nuklearwaffen, bei denen defensive Waffen das stabilisierende Gleichgewicht der gegenseitigen Zerstörung empfindlich stören, sind es im Cyberspace offensive Waffen, die andere Staaten fürchten und das Cybersicherheitsdilemma animieren:

> „By contrast, cybersecurity baseline defenses are universally recognized as non-threatening and part of professional best practice“.[89]

Da das Cybersicherheitsdilemma besonders mächtig bei starken Staaten operiert, die als Sicherheitsgarant für schwache und mittelstarke Staaten fungieren, kann die Vertiefung bilateralen Vertrauens zwischen diesen Staaten ähnlich wie im Kalten Krieg das Cybersicherheitsdilemma partiell abschwächen und die Stabilität erhöhen. Maßnahmen wie die Einrichtung eines „roten Telefons“ oder niederschwellige Austauschmechanismen für operative Angelegenheiten bieten die Möglichkeit, Fehlinterpretationen zu verringern und Vertrauen aufzubauen. Vertrauensvolle bilaterale Beziehungen, die z. B. Experten und Politiker mit Abkommen befördern und durch Verifikationsmechanismen weiter stärken können, fungieren auch als eine gute Grundlage, um in der Zukunft liegende Herausforderungen besser

87 Ebd., S. 161.
88 Ebd., S. 162.
89 Ebd., S. 163.

zu meistern.[90] Neben einem Notfallkanal sollten Staaten zur Entschärfung von akuten Cybervorfällen aufgrund deren großer Anzahl zur Minimierung der Risiken von Spannungen und um das Interpretationsdilemma der anderen Seite zu informieren, ihre Positionen und Fähigkeiten kommunizieren.[91]

Staaten können auch unilaterale Schritte unternehmen, die die Cybersicherheit aller Akteure im System mehren und gleichzeitig die Vertrauenswürdigkeit und das Ansehen des entsprechenden Staates steigern. So können gezielte Maßnahmen, die mit hohen Kosten für den signalisierenden Staat verbunden sind, sogenannte „costly signals", anderen Staaten etwas über dessen Absichten signalisieren und folglich ein Beitrag zur systemweiten Sicherheit sein.[92] Signale, die für den entsprechenden Staat mit bedeutenden Kosten verbunden sind, haben folglich für andere Staat einen gewissen Wert, der friedvolle und kooperative Absichten indizieren kann:

> „If the cost of the signal is sufficiently meaningful, other states are likely to see it as a sign of trustworthiness and consider taking reciprocal action".[93]

Im Zweifel wird das Handeln eines vertrauenswürdigen Staates zu seinen Gunsten ausgelegt. Auf dem Gebiet der Wahrnehmung der Offensive und Defensive sowie des Motivs der Gier eines anderen Staates verfügen Staaten

90 Hürden beim Aufbau bilateralen Vertrauens bzw. dem Schließen von Abkommen sind die Ambivalenz operativer Begriffe, der Dual-Use-Charakter von Sicherheitssoftware oder die Entwicklung und Verwendung von Software, mit der Schwachstellen aufgedeckt und ausgenutzt werden, um die eigene Netzwerksicherheit zu verbessern (Ebd., S. 167). Die Möglichkeit des Betrugs erschwert die Verifikation von Abkommen und macht sie gleichzeitig noch bedeutsamer. Aufgrund der Option, Cyberfähigkeiten zu verstecken, wird kein Staat einem anderen Staat vollen Zugang zu all dessen Netzwerken geben, um die Einhaltung der Nicht-Entwicklung bestimmter Cyberfähigkeiten zu verifizieren (Ebd., S. 168). Nicht-staatliche Akteure erschweren Abkommen zusätzlich, da ein Staat diese einerseits nicht gänzlich kontrollieren kann bzw. sie ihm die Möglichkeit bieten, unter plausibler Abstreitbarkeit ein Abkommen zu verletzen.

91 Ebd., S. 166.

92 Dass Signale Vertrauen hervorrufen können setzt voraus, dass politische Entscheidungsträger ihre Verzerrungen ausblenden können, um „costly signals" als solche zu erkennen, und sie selbst dazu bereit sind, solche Signale zu senden (Ebd., S. 170).

93 Ebd., S. 170.

über die meisten Handlungsoptionen, um mittelfristig – wie beim Aufbau bilateralen Vertrauens – die systemweite Stabilität zu erhöhen.

Eine Möglichkeit Absichten zu signalisieren, ist der Umgang eines Staates mit unbekannten Schwachstellen. Sie können entweder operativ für anspruchsvolle Netzwerkoperation genutzt werden oder sie können an die Softwarehersteller gemeldet werden, sodass diese sie beheben können.[94] So nutzte die NSA eine unbekannte Schwachstelle mit dem Exploit „EternalBlue“ operativ jahrelang für gezielte Cyberoperationen aus, bis die bis heute nicht zweifelsfrei identifizierte Gruppe „The Shadow Brokers“ den Exploit im April 2017 im Internet veröffentlichte.[95] Sowohl „WannaCry“, mit der Nordkorea im Mai 2017 hunderttausende Computer infizierte und den Inhalt derer Festplatten löschte, als auch die kurz darauf ähnlich operierende russische Schadsoftware „NotPetya“, „the most destructive and costly cyber-attack in history“, basierten auf „Eternal-Blue“.[96]

Ähnlich können Staaten beim Thema Verschlüsselung, die es ermöglicht Daten auszutauschen oder zu kommunizieren ohne dass eine dritte Partei, die diese Informationen abfängt, sie auslesen kann, unterschiedliche Wege einschlagen. [97] Verschlüsselungstechnologien können die Arbeit von Geheimdiensten einschränken: Ihre Ziele können

94 Das Wissen über eine Schwachstelle und die Verfügbarkeit eines entsprechenden Exploits kann für einen fähigen Staat zur Durchführung von Netzwerkoperationen gegen „harte Ziele“ ein bedeutender Vorteil sein. Die Veröffentlichung eines Zero-Days durch einen Staat, den dieser operativ nicht immer mit anderen Methoden ausgleichen kann, bringt ihm hingegen keine Vorteile ein, die nicht auch anderen Staaten zu Gute kommen. Stattdessen verliert dieser Staat dadurch die Möglichkeit, die Schwachstelle auszunutzen und „near tearm intelligence gains“ zu realisieren (Ebd., S. 172).
95 Thomas Rid/Ben Buchanan: Hacking democracy, in: SAIS Review of International Affairs 1 (2018), S. 11 f.
96 The White House: Statement from the Press Secretary, Foreign Policy 15.02.18, online unter: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/; Dustin Volz: U.S. blames North Korea for „WannaCry“, in: Reuters 19.10.17, online unter: https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wan-nacry-cyber-attack-idUSKBN1ED00Q; Nicole Perlroth/Mark Scott/Sheera Frenkel: Cyberattack Hits Ukraine Then Spreads Internationally, in: The New York Times 27.06.17, online unter: https://www.nytimes.com/2017-/06/27/technology/ransomware-hackers.html.
97 Buchanan: The Cybersecurity Dilemma, S. 174.

Verschlüsselungstechnologien nutzen, die sie aus dem spionierenden Land importiert haben. Eine Option für Staaten ist es, Verschlüsselungstechnologien als sicher zu zertifizieren und in diese anschließend Schwachstellen zu implementieren. Nutzen andere Staaten diese Verschlüsselungssoftware, kann der Staat deren sensible Daten abfangen und entschlüsseln.

Ein anderer Weg im Umgang mit Verschlüsselung ist es, Schwachstellen gesetzlich für illegal zu erklären und sichere Verschlüsselungstechnologien zu fördern. Hierdurch erhöht sich die Sicherheit aller Akteure. Anders als eine indifferente Einstellung zu Verschlüsselungstechnologien, bei der die Frage der Sicherheit von Verschlüsselungstechnologien privaten Anbietern überlassen wird, erhöht die eindeutige Positionierung einer Regierung pro-Verschlüsselung langfristig ebenfalls das Vertrauen in diesen Staat, da sie mit realen Kosten für ihn verbunden ist und bis zu einem gewissen Grad Aufschluss über dessen Haltung zu Netzwerkoperationen gibt: Ein Staat, der für sichere Verschlüsselungstechnologien eintritt, die mit seinen Geheimdienstoperationen zur Sammlung von Informationen unvereinbar sind, erkennt Limitierungen für seine Geheimdienste an und akzeptiert die Existenz von Informationen außerhalb seines Zugriffs, während er gleichzeitig einen Beitrag zur Sicherheit aller Staaten leistet.[98]

Die Entwicklung einer Cybersicherheitsdoktrin kann einem Staat bei der Interpretation und der Beantwortung von Cyberoperationen helfen und damit die interne Politikformulierung leiten.[99] Wird sie nach außen kommuniziert, kann sie auch als Orientierungshilfe für andere Staaten im Umgang mit diesem Staat dienen und so gefährliche Fehlinterpretationen reduzieren. Teilen mehrere Staaten eine ähnliche Haltung, kann dies in einen stabilen Status quo münden, der die Folgen des Cybersicherheitsdilemmas versucht zu reduzieren. Einzelne Maßnahmen können deshalb der längerfristigen Etablierung eines Status quos, einer „stable multi-lateral baseline of behaviour“ dienen.[100]

98 Ebd., S. 177.
99 Ebd., S. 178.
100 Ebd., S. 185.

Eine Cybersicherheitsdoktrin sollte darlegen, wie ein Staat mit Netzwerkoperationen umgeht, bei denen ein anderer Staat aus defensiven Motiven in großem Umfang in die Netzwerke ökonomischer und politischer Ziele sowie kritische Infrastruktur eines anderen Staates eindringt, um dort Informationen über seine Gegner zu sammeln, die er ebenfalls in diesen Netzwerken vermutet. Diese sogenannten „third-party Counter-Computer Network Exploitation“ (CCNE) resultieren nach der Detektion durch den Drittstaat bei diesem in das Interpretationsdilemma, da dieser entscheiden muss, ob es sich um eine defensive CCNE-Operation handelt oder eine für ihn gefährliche Operation.[101] CCNE-Operationen erweitern folglich den Umfang des Cybersicherheitsdilemmas, das ansonsten auf eine vergleichsweise kleine Anzahl defensiver Netzwerkoperationen, bei denen Staaten nur in die Netzwerke potentieller Gegner eindringen, beschränkt wäre. Um das Cybersicherheitsdilemma zu minimieren, können starke Staaten präventiv kommunizieren, dass sie jegliches Eindringen in eines ihrer bedeutenden Netzwerke, das nicht unmittelbar mit ihren eigenen operativen Cyberoperationseinheiten in Verbindung steht, als Gefahr werten und nicht als defensive CCNE-Operation. Solche Staaten, die ihre Position gegenüber CCNE-Operationen glaubhaft kommuniziert haben, können aufgedeckte Netzwerkoperationen folglich mit höherer Gewissheit als für sie gefährlich identifizieren und entschlossener darauf reagieren.[102]

Grundsätzlich kann das Cybersicherheitsdilemma abgeschwächt werden, wenn Staaten sich bewusst sind, wie sie mit einem Eindringling in einem ihrer strategischen Netzwerke umgehen.[103] Drei Ansatzpunkte bestehen hier zur Mitigation des Cybersicherheitsdilemmas: Erstens müssen sich Staaten bewusst werden, dass sie unter einer gewissen Bedeutungsschwelle wahrscheinlich über keine adäquaten Mittel verfügen, einen Eindringling zu

101 Ebd., S. 179.
102 Ebd., S. 180.
103 Diese Notwendigkeit resultiert daraus, dass selbst Staaten mit einer guten Grundlagensicherheit nicht vor allen Netzwerkoperationen geschützt sind, was sie dazu verleitet, in die Netzwerke anderer Staaten einzudringen, um ihre eigene Netzwerksicherheit zu erhöhen. Gleichzeitig detektieren Staaten einen Teil der Eindringlinge noch bevor diese ihre Missionsziele erreichen konnten, weswegen sie sich bewusst sein sollten, wie sie in solch einem Fall reagieren (Ebd., 180).

bestrafen, d. h. sie können nicht alles unerwünschte Verhalten vor allem gegen weniger bedeutende Netzwerke bestrafen oder erfolgreich abschrecken. [104] Da das Cybersicherheitsdilemma nur bei Netzwerkoperationen gegen strategisch bedeutsame Netzwerke eines Staates operiert, muss die Reaktion auf das Eindringen in solch ein Netzwerk sich fundamental von der auf weniger bedeutende Netzwerke unterscheiden: „Recognize this difference internally – the additional options available and the additional risk that arise – is the first step".[105]

Für Netzwerke von strategischer Bedeutung müssen Staaten zweitens ihr Verständnis von Proportionalität überdenken. Da ein Staat vermutlich nicht alle Netzwerkoperationen in seinen strategisch bedeutsamen Netzwerken entdeckt, muss er bei denen, die er aufdeckt, seine Reaktion hochskalieren, um durch die Kumulation der Maßnahmen auf das künftige Verhalten des Gegners abzuzielen:

> „[T]he cumulative deterrence paradigm does not unrealistically seek to prevent cyber-attacks from ever occurring. Instead, it takes for granted the inevitability of some acts of cyber aggression and strives to shape and limit them by attacking the rival repeatedly in response to specific behaviors, over a long period of time, sometimes even disproportionally to its aggressive actions".[106]

Netzwerkoperationen separat zu untersuchen, ihre Folgen aber in Form von Bewertungsberichten – vergleichbar mit denen über Menschenrechtsverletzungen – zusammenzuführen, die Aufschluss über die Prioritäten eines Staates, dessen Fähigkeiten und künftiges Verhalten liefern, kann als Grundlage der kumulierten Bestrafung des Verhaltens eines Staates dienen, das von dem Status quo, den der betreffende Staat versucht zu etablieren, abweicht.[107]

Cyberoperation, die nicht vergleichbar sind mit einem konventionellen Militärschlag, sollten nicht mit Maßnahmen beantwortet werden, die unmittelbar Leben gefährden oder die Sorge vor einem kurz bevorstehenden militärischen Konflikt nähren. Sowohl auf der operativen als auch der

104 Ebd., S. 180 f.
105 Ebd., S. 181.
106 Uri Tor, 2017, 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, in: Journal of Strategic Studies 1 (2015): S. 92-117, hier S. 95).
107 Buchanan: The Cybersecurity Dilemma, S. 182.

strategischen Ebene verfügen Staaten über die Option der „cross-domain-deterrence“, „the use of threats of one type, or some combination of different types, to dissuade a target from taking actions of another type to attempt to change the status quo“.[108] Auf operativer Ebene kann die kurzfristige Beantwortung einer Cyberoperation das Veröffentlichen der Fähigkeiten eines anderen Staates beinhalten, um deren Effektivität zu reduzieren. Dies bedroht den Eindringling nicht, erschwert aber dessen künftige Netzwerkoperationen und macht diese teurer.[109]

Neben diesen kurzfristig angelegten Reaktionen auf Cyberoperationen sollte die strategische Reaktion von Staaten nicht das Eindringen in dessen Netzwerke beinhalten, sondern unter Bezugnahme auf die Verhaltensberichte auf Mittel wie politische und wirtschaftliche Sanktionen zurückgreifen, die das Cybersicherheitsdilemma nicht animieren. Dies können Sanktionen gegen eine Firma sein, die an Cyberoperationen beteiligt ist, eine diplomatische Protestnote oder eine Anklage, mit dem Ziel einen Akteur, der eine „rote Linie“ überschritten hat, zu isolieren oder zu verurteilen.[110] Diese nichtinvasiven Maßnahmen animieren – genauso wie potentielle Gegensanktionen – nicht das Cybersicherheitsdilemma. Dennoch sollten Staaten in einem akuten Bedrohungsszenario, in dem ein Eindringling ein strategisch bedeutendes Netzwerk kompromittiert hat, auf eine „harte Antwort“ setzen – wenn diese keine militärische oder geheimdienstliche Eskalation birgt –, um anderen Staaten ihre Entschlossenheit zu signalisieren und so zukünftig weniger wahrscheinlich das Ziel von gefürchteten Netzwerkoperationen zu werden.[111]

108 Jon R. Lindsay/Erik Gartzke: Cross-Domain Deterrence. Strategy in an Era of Complexity, Oxford: Oxford University Press 2019, S. 4.
109 Eine weitere Möglichkeit ist es, unerwünschte Aktivitäten während deren Durchführung in der Infrastruktur des Internets zu unterbinden (Buchanan: The Cybersecurity Dilemma, S. 183). Diese Option kommt für die EU ohne eigene operative Cyberfähigkeiten nicht in Frage.
110 Ebd., S. 184.
111 Ebd., S. 184.

Europäische Mitigationsstrategien

Wie hat die EU bislang dazu beigetragen, das Cybersicherheitsdilemma abzuschwächen und wie kann sie effektiv zu dessen Mitigation beitragen? Mit der 2013 beschlossenen Cybersicherheitsstrategie „An Open, Safe and Secure Cyberspace" benannte die EU den Ansatz bzw. Prozess der Verrechtlichung und Regelsetzung im Cyberspace auf UN-Ebene als eine ihrer Top-Priorität, den sie vor allem mit ihrer 2015 beschlossenen „Cyber Diplomacy" aktiv unterstützen sowie weiterentwickeln will.[112] Die Aussichten darauf, dass es in Bezug auf die Verrechtlichung und Normenbildung im Cyberspace in naher Zukunft Erfolge zu vermelden gibt, sind aufgrund der verhärteten Fronten zwischen den USA und ihren Verbündeten einerseits sowie Russland und ihm nahestehenden Staaten andererseits schlecht.[113] Hinzu kommt, dass die vergleichsweise subtilen Effekte von Cyberoperationen, die nicht zwangsläufig unmittelbar physische Auswirkungen haben müssen, Staaten unter einer gewissen Schwelle Anreize bieten diese einzusetzen. Dies ist vermutlich die Ursache für die Stagnation des UN-Prozesses: Verglichen mit den Effekten von Nuklear-, Bio- oder Chemiewaffen sind die Effekte von Cyberoperationen mit Blick auf Tote und Zerstörung zu gering, weswegen für Staaten keine Anreize

112 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final, Brussels, 7.2.2013, S. 15, online unter: https://eeas.europa.eu/archives/d-ocs/policies/eu-cyber-security/cybsec_comm_en.pdf; Rat der Europäischen Union: Council Conclusions on Cyber Diplomacy, 6122/15, Brussels, 11 February 2015, S. 7, online unter: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf; Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Joint Communication to the European Parliament and the Council, JOIN(2017) 450 final, Brussels, 13.9.2017, S. 18, online unter: https://eur-lex.europa.eu/legal-content/EN/T-XT/PDF/?uri=CELEX:52017JC0450&from=en.

113 Alex Grigsby: Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations, in: Council on Foreign Relations 29.10.18, online unter: https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations?utm_medium-=social_share&utm_source=tw.

bestehen, sich ernsthaft auf Regeln und Beschränkungen bei ihrem Einsatz einzulassen. Ebenfalls lassen sich „wrongful acts“ – will man eine Definition unterhalb der bestehenden Schwelle eines bewaffneten Konflikts finden – schwierig definieren ohne gleichzeitig einen effektiven Sanktionsmechanismus zu entwickeln.[114] Dies steigert die Relevanz alternativer Ansätze zur Abschwächung des Cybersicherheitsdilemmas.

Mit dem Ausbau der Grundlagensicherheit kann die Cybersicherheit kurzfristig so erhöht werden, dass ein Staat gegen das Gros der Netzwerkoperationen geschützt ist. Alles in allem beeinflusst der Ausbau der Grundlagensicherheit nicht die Offense-Defense-Balance. Als erste strukturelle Maßnahme zum Ausbau der breiteren Grundlagensicherheit in der EU wurde 2004 die „European Network and Information Security Agency“ (ENISA) gegründet. Die Agentur sollte die Fähigkeiten der EU, der Mitgliedsstaaten und von Unternehmen, mit ICT-Vorfällen umzugehen, weiterentwickeln.[115] Als Top-Priorität und Schlagwort, das bis heute nicht näher definiert ist, führte die EU kurz darauf den Begriff der „resilience“ von ICT-Systemen ein.[116] Die, kündigte die EU 2009 an, gelte es vor allem im Kontext kritischer Infrastruktur aber auch darüber hinaus zu erhöhen, um die Cybersicherheit zu steigern.[117]

114 A/70/174, S. 8.
115 2004/460/EC: Regulation of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, in: Official Journal of the European Union L77, 13.03.04, S. 1-11, hier S. 4, online unter: https://eur-lex.europa.eu/legal-content/EN/T-XT/PDF/?ur-i=OJ:L:2004:077:FULL&from=EN.
116 Europäische Kommission: A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2006) 251, S. 6 f., online unter: http://ec.europa.eu/information_society/doc/com2006251.pdf.
117 Europäische Kommission: „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience“, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2009) 149 final, Brussels, 30.3.2009, S. 5, online unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF; Europäische Kommission, und die Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Cybersecurity Strategy of the European Union, S. 4.

Die bedeutendste und erste legislative Maßnahme zum Ausbau der Grundlagensicherheit ist die im Juli 2016 verabschiedete, sogenannte „NIS-Richtlinie“ („Network and Information Security“), die die Mitgliedstaaten bis Mai 2018 umsetzen sollten.[118] Mit ihr sollten die EU-Staaten die Betreiber von „essential services“ identifizieren, die zur Einführung organisationaler und technischer Mindeststandards sowie der Meldung von ICT-Vorfällen an nationale Behörden verpflichtet wurden.[119]

Ebenso verpflichtete die NIS-Richtlinie die Mitgliedsstaaten dazu, nationale Cybersicherheitsstrategien zu entwickeln und mindestens ein „Computer Emergency Response Team“ (CERT) aufzustellen.[120] Diese Maßnahme engte das Cybersicherheitsdilemma ein, da sich die Mitgliedsstaaten über ihre essentiellen Dienstleister bewusst werden mussten. Gleichzeitig erhöhte die NIS-Richtlinie durch die Einführung von Mindeststandards die Grundlagensicherheit bei strategisch bedeutenden Zielen.

Zur Erhöhung der „cyber resilience“ verabschiedete die Kommission im September 2017 ein größeres Maßnahmenpaket, das u. a. eine Reform von ENISA beinhaltete.[121] Der sogenannte „Cybersecurity Act“ trat im Juni 2019 in Kraft.[122] Mit der Verordnung forcierte die Kommission die Errichtung einer dauerhaften „European Union Agency for Cybersecurity“ und die

118 2016/1148/EU: Directive of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. In Official Journal of the European Union L194, 19.07.16, S. 1-30, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=-NL. Zugegriffen: 06.07.19.
119 Ebd., S. 6; S. 12; S. 16.
120 Ebd., S. 15 f.; S. 26.
121 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, S. 3, siehe auch S. 4.
122 2019/881/EU: Regulation of the European Parliament and of the Coucil of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). In Official Journal of the European Union L 151, 07.06.19, S. 15-96, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&f-rom=EN.

Einführung eines „European Cybersecurity Certification Framework“.[123] Die „neue“ ENISA soll erheblich sichtbarer und mit einem dauerhaften Mandat ausgestattet zukünftig bei der Formulierung und Implementation von Politiken mit Cybersicherheitsbezug mitwirken. Des Weiteren sieht der „Cybersecurity Act“ eine freiwillige Zertifizierung von ICT-Produkten und -Lösungen vor, mit der die EU das Ziel der Erhöhung von Sicherheitsstandards und die Vereinheitlichung von Zertifikaten sowie Standardisierungen zur Beförderung eines Binnenmarktes für Cybersicherheit verfolgt.[124] Das Parlament verschärfte den Vorschlag der Kommission dahingehend, dass die Zertifizierung von spezifischen ICT-Produkten und Lösungen künftig nicht mehr nur freiwillig, sondern verpflichtend sein könnte, um die Cybersicherheit in der EU zu erhöhen.[125] Dies wäre mit Blick auf den Ausbau der Grundlagensicherheit begrüßenswert.

Die Errichtung von ENISA und deren Weiterentwicklung zu einer dauerhaften und leistungsstärkeren „European Union Agency for Cybersecurity“, die NIS-Richtlinie und die Einführung eines europäischen Zertifizierungssystems sind sinnvolle Schritte mit Blick auf den Ausbau der breiteren Grundlagensicherheit in der EU. Alle diese Maßnahmen wurden jedoch vor dem Hintergrund des Binnenmarktes beschlossen und die Zuständigkeiten für die sensibelsten Netzwerke, die für das

123 Europäische Kommission: Proposal for a Regulation on the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final, Brussels, 13.9.2017, S. 4; 10, online unter: https://eur-lex.europa.eu/resource.html?uri=cellar:1985b4b4-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_4&format=PDF.

124 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, S. 4.

125 Europäisches Parlament: EU Cybersecurity Act ***I. European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)), P8_TA-PROV(2019)0151, S. 56, online unter: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirect#top.

Cybersicherheitsdilemma am relevantesten sind, liegt weiterhin bei den Nationalstaaten. Das zeigt, dass die Möglichkeiten der EU, das Cybersicherheitsdilemma durch den praktischen Ausbau der Grundlagensicherheit abzuschwächen, begrenzt sind.

Cyber-Capacity-Building, das mit der 2017 vom Rat beschlossene „Cyber-Diplomacy-Toolbox" zur Beantwortung von „heimtückischen Cyberaktivitäten" ein praktischer Bestandteil der EU-Cyber-Diplomatie wurde, könnte einen wertvollen Beitrag zur Verbesserung der globalen Grundlagensicherheit leisten. [126] Allerdings fehlt hier immer noch ein entsprechender Politikrahmen. So verfügt ENISA über keinerlei Mandat für Cyber-Capacity-Building in Drittstaaten.[127] Dies gilt es zu ändern und den Ausbau der Grundlagensicherheit in das breite Feld der EU-Entwicklungspolitik zu intergieren.

Als weitere Maßnahme zur Stärkung der Grundlagensicherheit formulierte die EU die Förderung von Forschung und Entwicklung auf dem Feld der Cybersicherheit, bei der die Europäische Verteidigungsagentur (EDA) eine zentrale Rolle spielen soll.[128] Hierbei sollte die EU daran denken, dass viele Cybersicherheitstechnologien einen Dual-Use-Charakter haben und die EU durch die Entwicklung ebensolcher Technologien unweigerlich die Offense-Defence-Balance – und damit das Cybersicherheitsdilemma – beeinflusst.

Nicht förderlich zur Mitigation des Cybersicherheitsdilemmas ist die zunehmend militärische bzw. offensive Denkweise der EU von

126 Vgl. Rat der Europäischen Union: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, S. 6.
127 Vgl. 2019/881/EU: S. 150 f.
128 Vgl. Europäische Kommission: Network and Information Security: Proposal for a European Policy Approach, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2001)298 final, Brussels 6.6.2001, S. 21, online unter: http://ec.europa.eu/transparency/regdoc/rep/1/20-01/EN/1-2001-298-EN-F1-1.Pdf;
Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Cybersecurity Strategy of the European Union: S. 5; vgl. Rat der Europäischen Union: EU Cyber Defence Policy Framework, 15585/14, Brussels, 18 November 2014, S. 9, online unter: https://www.europarl.europa.eu/meetdocs/2014_201-9/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyber defencepolicy framework_en.pdf.

Cybersicherheit, was vom Grundgedanken des Ausbaus der Grundlagensicherheit abweicht. Dies zeigt sich daran, dass die EU die Cyberverteidigungskapazitäten der EU-Staaten auch als einen Beitrag zu einer „effektiven“ Abschreckung verstanden wissen will.[129] Ebenfalls wollen die EU-25 im Rahmen von PESCO offensivere Verteidigungsmaßnahmen entwickeln.[130] Diese offensiveren Verteidigungsfähigkeiten dienen wahrscheinlich der Durchführung defensiver Netzwerkoperationen zur Erhöhung der Cybersicherheit. Defensive Netzwerkoperationen sind allerdings eine der treibenden Kräfte des Cybersicherheitsdilemmas. Die dazu notwendigen offensiven Fähigkeiten, die auch zur nicht praktikablen Abschreckung im Cyberspace aufgebaut werden, befördern das Cybersicherheitsdilemma. Auf EU-Ebene ist ihr Aufbau deswegen als kontraproduktiv zu erachten – möchte die EU weiterhin als möglichst neutraler Mittler auftreten.

Ein weiterer Ansatzpunkt zur Mitigation des Cybersicherheitsdilemmas ist der Aufbau bilateralen Vertrauens, z. B. durch die Einrichtung von Notfallkanälen, vertrauensbildenden Maßnahmen (VBM) oder der Kooperation bei gemeinsamen Herausforderungen. Vertrauen kann das Cybersicherheitsdilemma partiell abschwächen und die Stabilität erhöhen. Ebenfalls in ihrer Cybersicherheitsstrategie von 2013 formulierte die EU die Herausbildung strategischer Partnerschaften mittels einer von den Werten, Normen und Prinzipien der EU geleiteten „coherent [...] international cyberspace policy“ mit Partnerstaaten, internationalen Organisationen und Akteuren aus dem Privatsektor sowie der Zivilgesellschaft als Ziel.[131] Diese Vertiefung bilateraler Beziehungen, die sich auf Themen wie Datenschutz konzentrieren sollte, wurde vor allem mit gleichgesinnten Staaten und Regionalorganisationen angestrebt. Unterstützt wird die Cyber-Diplomatie der EU von „EU Cyber Direct“, einer von der Kommission finanzierten und dem „European Union Institute for Security Studies“ (ISS), dem „German

129 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, S. 17.
130 Rat der Europäischen Union: Permanent Structured Cooperation (PESCO), S. 9.
131 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Cybersecurity Strategy of the European Union, S. 15.

Marshall Fund of the United States“ sowie der „Stiftung Neue Verantwortung“ umgesetzten Initiative. „EU Cyber Direct“ soll u. a. durch Forschung auf den Feldern Anwendbarkeit internationalen Rechts auf den Cyberspace und Normen verantwortungsvollen Staatsverhaltens im Cyberspace sowie der Durchführung von Dialogveranstaltungen in den Partnerländern (USA, Brasilien, Indien, China, Japan und Südkorea) und Partnerregionen (Lateinamerika, Europa und der Region Asien-Pazifik) zur Entwicklung einer „secure, stable, and rules-based international order“ beitragen.[132]

Das Engagement der EU zum Aufbau bilateralen Vertrauens ist ausbaufähig. Hier bieten sich der EU eigentlich mehr Möglichkeiten, da sie auf diesem Feld im Gegensatz zum Einsatz militärischer Mittel über eine gewisse Glaubwürdigkeit verfügt. Bislang konzentrierte sich das Engagement der EU allerdings primär auf die Verrechtlichung und Normenbildung im Cyberspace. Auch wenn das Cybersicherheitsdilemma dadurch nachhaltig mitigiert werden könnte, zeichnen sich hier perspektivisch keine Fortschritte ab, da die USA und die EU-27 einerseits sowie China und Russland andererseits hier gegensätzliche Positionen vertreten. In Bezug auf Maßnahmen zum kurz- bzw. mittelfristigen Aufbau von Vertrauen sind die Aktivitäten der EU auf die strukturierten Dialoge mit den mehrheitlich gleichgesinnten Partnern USA, China, Japan, Indien, Südkorea und Brasilien begrenzt. [133] Dementsprechend fokussieren sich diese Dialoge auf die Verrechtlichung und Regelsetzung im Cyberspace.

Wie die EU die von der OSZE 2013 verabschiedeten und 2016 weiterentwickelten VBM außerhalb ihrer Partnerländer und -Regionen

132 EU Cyber Direct: Mission, 2018, online unter: https://eucyberdirect.eu/mission/; siehe auch European Union Institute for Security Studies: EU Cyber Direct. Supporting EU Cyber Diplomacy https://www.iss.europa.eu/sites/default/files/Cyber%20 Direct%20leaflet_0.pdf.

133 Rat der Europäischen Union: Council Conclusions on Cyber Diplomacy, S. 12; Europäische Kommission: Commission Staff Working Document. Assessment of the EU 2013 Cybersecurity Strategy, SWD(2017) 295 final, Brussels, 13.9.2017, S. 18, online unter: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

strategisch einsetzt, bleibt vage.[134] Initiativen zur Vertiefung des Vertrauens mit nicht-gleichgesinnten Staaten gibt es – abgesehen von China – nicht. Die in der Cyber-Diplomacy-Toolbox benannten Maßnahmen der politischen und thematischen Dialoge oder diplomatischen Protestnoten zur Signalisierung von Absichten sollten folglich verstärkt eingesetzt werden.[135] Vertrauensbildende Maßnahmen wie die Errichtung spezifischer Notfallkanäle, bilaterale Abkommen zur Kooperation bei gemeinsamen Herausforderungen wie Cyberkriminalität, der Austausch von Informationen über die eigenen Cyberfähigkeiten und -strategien oder die gegenseitige Unterstützung bei ICT-Vorfällen wären erste Schritte, mit denen die EU mit nicht-gleichgesinnten Cyberakteuren eine erste Vertrauensbasis aufbauen könnte. Die Cyber-Diplomatie der EU sollte sich zur Mitigation des Cybersicherheitsdilemmas folglich weniger auf Partner, sondern verstärkt auf den Aufbau einer rudimentären Vertrauensbasis mit nicht-gleichgesinnten Staaten konzentrieren.

Beiträge zur systemweiten Sicherheit zielen darauf ab, durch kostspielige Signale friedvolle und kooperative Absichten zu signalisieren. Werden sie reziprok beantwortet, können sie die Cybersicherheit aller Staaten erhöhen. Beiträge zur systemweiten Sicherheit hat die EU bislang nicht als Maßnahme zur Abschwächung des Cybersicherheitsdilemmas begriffen – dabei bieten sie großes Abschwächungspotential. Das Thema Schwachstellenmanagement hat die EU bislang sträflich vernachlässigt. Im „Cybersecurity Act“ wird zwar die Bedeutung der Feststellung und koordinierten Publikation von Schwachstellen angeführt. [136] Wie die

134 Ständiger Rat der Organisation für Sicherheit und Zusammenarbeit in Europa: Decision No. 1106, Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1106, 3 December 2013, online unter: https://www.osce.org/pc/109168?download=true; Ständiger Rat der Organisation für Sicherheit und Zusammenarbeit in Europa: Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologie*s*, PC.DEC/1202, 10 March 2016, online unter: https://www.osce.org/pc/227281?download=true.

135 Rat der Europäischen Union 2017: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, S. 7.

136 2019/881/EU: S. 19.

Regierungen der EU-27 mit gefundenen Schwachstellen umgehen, bleibt allerdings offen: Halten sie sie zurück, um sie für offensive Netzwerkoperationen zu nutzen, oder priorisieren sie deren Veröffentlichung und opfern dafür kurzfristige Geheimdienstgewinne zu Gunsten von längerfristigen Gewinnen an Glaubwürdigkeit sowie Vertrauen?

Dass die EU-27 sich in Brüssel darauf einigen können, alle „zero days", die in ihrem Besitz sind, unmittelbar zu veröffentlichen, erscheint angesichts der Cyberaufrüstungsbestrebungen der Mitgliedsstaaten unrealistisch. Einen wie von den USA im November 2017 teilveröffentlichten Schwachstellenmanagementprozess, der in einem interbehördlichen Prozess die konkurrierenden Interessen unterschiedlicher Behörden zusammenführt, um die Risiken der Verbreitung einer unbekannten Schwachstelle, die Vorteile deren Nutzung durch die Regierung und die Vor- und Nachteile einer Teilveröffentlichung abzuwägen, gibt es auf EU-Ebene nicht.[137] Ein möglichst transparenter und von einer unabhängigen Instanz überwachter europäischer Schwachstellenmanagementprozess, der die Nutzung von Schwachstellen für bedeutenden nationale Sicherheitsangelegenheiten temporär begrenzt und ansonsten deren unmittelbare Veröffentlichung auf EU-Ebene priorisiert, könnte ein Kompromiss sein.[138] Hiermit könnten die EU-27 ein – wenn auch weniger – kostspieliges Signal senden, das auch ihre restriktivere Haltung zu offensiven Netzwerkoperationen kommuniziert. Im besten Fall können die EU-27 so unilateral Glaubwürdigkeit und Vertrauen aufbauen, im schlechtesten Fall im Interpretationsdilemma den Vorteil des Zweifels gewinnen.

Mit einer Positionierung pro-Verschlüsselung können Staaten ebenfalls ein teures Signal senden und ihre friedvollen Absichten, d. h. die Akzeptanz von

137 The White House: Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017, Unclassified, S. 1, online unter: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

138 Vgl. Herpig, Sven: Governmental Vulnerability Assessment and Management. Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities. A proposal supported by the Transatlantic Cyber Forum, August 2018, online unter: https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf.

Grenzen für die Arbeit der eigenen Geheimdienste, signalisieren. Solch eine eindeutige Haltung pro-Verschlüsselung könnte, wenn sie reziprok beantwortet werden würde, ebenfalls einen Beitrag zur systemweiten Sicherheit leisten. Die EU verfolgt diese Abschwächungsstrategie des Cybersicherheitsdilemmas bislang auch nicht – schlimmer noch, sie hat keine eindeutige Haltung zum Thema Verschlüsselung. Zwar verfolgt die EU den Ansatz der Förderung der Forschung, Entwicklung und Nutzung von Verschlüsselungstechnologien.[139] Die Position pro-Verschlüsselung, die die EU z. B. in einer Richtlinie zum Schutz personenbezogener Daten eingenommen hat, die vorsieht, dass Dienstleister, die Daten transportieren oder verarbeiten, diese verschlüsseln, konterkariert die EU aber an anderer Stelle: In Rücksprache mit den EU-Staaten kündigte die EU 2017 an, Maßnahmen wie die Förderung von Entschlüsselungstechnologien oder die Entwicklung alternativer Maßnahmen zum Erlangen von Daten zu ergreifen, um die Arbeit von Strafverfolgungsbehörden zu erleichtern.[140]

Dies steht im Widerspruch zu der praktizierten Strategie der EU, Forschungsprojekte und die Entwicklung von Verschlüsselungstechnologien zu fördern.[141]

139 Europäische Kommission: Network and Information Security: Proposal for a European Policy Approach, S. 22 f.; Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Cybersecurity Strategy of the European Union, S. 9 f.; S. 14.

140 2016/679/EU: Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in: Official Journal of the European Union L119, 04.05.16, S. 1-88, hier S. 16; 36 f.; 51, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN;
Europäische Kommission: Eleventh progress report towards an effective and genuine Security Union. Communication from the Commission to the European Parliament, the European Council and the Council, COM(2017) 608 final, Brussels, 18.10.2017, S. 9 f., online unter: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine-_security_union_en.pdf.

141 Europäische Kommission: Post-quantum cryptography for long-term security, 30.05.2017, online unter: https://cordis.europa.eu/project/rcn/194347/factsheet/en; Europäische Kommission: Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and

Nach außen signalisiert diese inkohärente Haltung keinerlei Absichten der EU zum Thema Verschlüsselung, sondern sät stattdessen eher Zweifel in Bezug auf die Haltung der EU-27 zur Durchführung von offensiven Netzwerkoperationen. Hier leistet die EU keinerlei Beitrag zur Abschwächung des Cybersicherheitsdilemmas. Würde sich die EU dezidiert pro-Verschlüsselung positionieren und hierzu eine Richtlinie verabschieden, die EU-weite Standards für Verschlüsselungstechnologien vorgibt, und die Hintertüren in Verschlüsselungstechnologien sowie ICT-Produkten und -Lösungen verbietet, könnte sie ein kostspieliges Signal senden – und somit einen gewichtigen Beitrag zur Abschwächung des Cybersicherheitsdilemmas leisten.

Die Entwicklung einer Cybersicherheitsdoktrin kann nach innen die Interpretation und die Beantwortung von Netzwerkoperationen erleichtern. Nach außen kann sie für andere Staaten eine Orientierungshilfe im Umgang mit dem betreffenden Staat sein und so dazu beitragen Fehlinterpretationen zu vermeiden. Hier, bei der Entwicklung einer Cybersicherheitsdoktrin, hat die EU bislang die beachtlichste Entwicklung vollzogen. Nicht näher definierte „Cyberattacken" behandelte die EU zunächst unter dem Gesichtspunkt der Cyberkriminalität – sie wurden als eine Gefahr für die europäischen Wirtschaften und das Funktionieren des Binnenmarktes gesehen.[142] Ab 2009 wandelte sich die Wahrnehmung von „Cyberattacken", die fortan als eine Gefahr für gesellschaftlich und wirtschaftlich relevante kritische Infrastruktur beschrieben wurden.[143] 2013 definierte die EU „Cyberattacken", d. h. das illegale Eindringen in ein System, die

Research Competence Centre and the Network of National Coordination Centres, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. COM(2018) 630 final, Brussels, 12.9.2018, S. 2, online unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54252.

142 Europäische Kommission: Network and Information Security: Proposal for a European Policy Approach, S. 24-26; Europäische Kommission: A strategy for a Secure Information Society – "Dialogue, partnership and empowerment", Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2006) 251, S. 6 f., online unter: http://ec.europa.eu/information_society/doc/com200625-1.pdf.

143 Europäische Kommission: „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", S. 2; S. 4.

Beeinflussung eines Systems und das Löschen, Verändern oder Zerstören von Daten sowie deren illegales Abfangen als „criminal offences“. [144] Sanktioniert werden sollten diese Vergehen mit strafrechtlichen Maßnahmen.

Die 2015 ins Leben gerufene EU-Cyber-Diplomatie stellt die erste Anstrengung der EU dar, ein außenpolitisches Instrument im Kontext von Netzwerkoperationen zu entwickeln.[145] Mit ihr will die EU ganz im Sinne ihres Glaubens an die Stärke von Recht und Verträgen einen Beitrag zur Verrechtlichung und Normensetzung im Cyberspace leisten. Den Umgang mit staatlichen Cyberoperationen und deren Beantwortung zum Schutz der EU, ihrer Mitgliedsstaaten und Bürger thematisierte der Rat erstmals prioritär 2017 im Kontext der Entwicklung einer „Cyber Diplomacy Toolbox“. [146] Mit diesem „Werkzeugkasten“ zur Beantwortung heimtückischer Cyberaktivitäten will die EU im Einklang mit ihrem Selbst- und Fremdverständnis als Friedensmacht Konflikte im Cyberspace mit friedlichen Mitteln beilegen, um Sicherheit und Frieden im Cyberspace zu fördern.

Herausragend für die Herausbildung einer Cybersicherheitsdoktrin ist die Ratsschlussfolgerung, weil sie erstmals deutlich machte, dass die EU Netzwerkoperationen in Einklang mit EU-Recht und in Anlehnung an internationales Recht nicht duldet und Staaten diese auch in keiner Form unterstützen sollten. Ein weiterer bedeutender Punkt ist, dass die EU das offene Kommunizieren von möglichen Konsequenzen als Mittel begreift, um das künftige Verhalten eines „potential aggressors“ in ihrem Sinne EU zu verändern. [147] Schlussendlich benannte die EU mit den Instrumenten der

144 2013/40/EU: Directive of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, in: Official Journal of the European Union L218, 14.08.13, S. 8-14, hier S. 12, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2013:218:FULL&from=-EN.
145 Rat der Europäischen Union: Council Conclusions on Cyber Diplomacy, S. 6 f.
146 Rat der Europäischen Union: Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 10474/17, Brussels, 19 June 2017, S. 3, online unter: http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf.
147 Ebd., S. 4.

GASP inklusive der Sanktionen erstmals außenpolitische Mittel, um auf Netzwerkoperationen zu reagieren.[148]

Zur weiteren Operationalisierung der Beantwortung von Netzwerkoperationen beschloss der Rat einen Implementationsleitfaden zur Cyber-Diplomacy-Toolbox, der deutlich machte, dass Sabotage- und Spionageoperationen einer Antwort bedürften, die über kommunikative Maßnahmen hinaus gehen muss.[149] Der breite EU-Ansatz umfasst u. a. präventive, kooperative, sensibilisierende und restriktiven Maßnahmen, die sowohl der unmittelbaren als auch der strategischen Beantwortung einer Cyberoperation dienen können.[150] Im Einklang mit dem Konzept der Cross-Domain-Deterrence setzt die EU zur Beantwortung von Cyberoperationen auf politische, diplomatische und wirtschaftliche Maßnahmen wie Konsultationen, Protestnoten, Cyber-Capacity-Building sowie Sanktionen.[151] Diese nicht-invasiven Maßnahmen animieren nicht das Cybersicherheitsdilemma und reduzieren die Gefahr der militärischen Eskalation.

Im Mai 2019 verschärfte der Rat die Wirksamkeit restriktiver Maßnahmen: Der ein Jahr gültige Ratsbeschluss sieht als Reaktion auf Cyberoperationen und zur Erreichung der Ziele der CFSP gezielte Sanktionen wie das Einfrieren von Vermögen oder die Verhängung von Reisebeschränkungen vor.[152] Darüber hinaus konkretisierte der Ratsbeschluss Cyberoperationen im außenpolitischen Kontext und stellte mit dem Indikator der „significant effects“ Kriterien auf, wann sowie in welchen Sektoren – z. B. kritische Infrastruktur und kritische Staatsfunktionen – diese eine Gefahr für die EU sind.[153] Durch diese Maßnahmen signalisiert die EU nach außen „rote

148 Ebd., S. 5.
149 Rat der Europäischen Union: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, S. 2.
150 Ebd., S. 4.
151 Ebd., S. 7-9.
152 2019/797/CFSP: Council Decision of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, in Official Journal of the European Union L 129 I, 17.05.19, S. 13-19, hier S. 15 f., online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF-/?uri=OJ:L:2019:129I:FULL&from=EN.
153 Ebd., S. 14.

Linien“ und verinnerlicht nach innen, auf welche Netzwerkoperationen sie dezidiert reagieren muss. Stärken könnte die EU ihre unmittelbare Beantwortung von Netzwerkoperationen, indem sie die genutzten Cyberfähigkeiten und Infrastruktur (z. B. Server) des entsprechenden Staates öffentlich macht, um sie für diesen Staat unbrauchbar zu machen.

Ein weiteres Defizit ist, dass die EU keine – zumindest öffentliche – Position zu CCNE-Operationen hat. Gäben die EU-27 die Devise aus, dass sie alle Netzwerkoperationen, die nicht mit ihren eigenen Cyberoperationseinheiten in Verbindung stehen, als Gefahr werten, könnten sie auf eine entdeckte Netzwerkoperationen – die sie dann als nicht defensiv einstufen – mit mehr Nachdruck reagieren. Überarbeiten sollte die EU die Grundlage der Beantwortung von Netzwerkoperationen. Bislang soll die Reaktion proportional zu den verursachten Effekten sein.[154] Da die EU-27 nicht alle Netzwerkoperationen detektieren werden, sollten sie ihre Reaktion bei den Netzwerkoperationen, die sie beantworten können, hochskalieren, um einen Ausgleich zu schaffen, der darauf abzielt, das langfristige Verhalten eines Staates zu verändern. Vom „European External Action Service“ (EEAS) erarbeitete „Cyberverhaltensberichte“, die die Effekte der Netzwerkoperationen eines Staates in den Mitgliedsstaaten auf EU-Ebene zusammenfassen, könnten hierfür eine adäquate Orientierungshilfe sein.

Mit dem vagen Beschluss der EU, eine „ernsthafte“ Cyberoperation auch als Auslöser für die militärische Beistandsklausel des Lissabonner Vertrags (Art. 42 Abs. 7 TEU-L) zu behandeln, erhöhte die EU den „Wetteinsatz“ für potentielle Gegner.[155] Gleichzeitig birgt dies die vermeidbare Gefahr der Eskalation. So sollen die Mitgliedsstaaten auf freiwilliger Basis ein Verständnis dafür entwickeln, wann der EU-Artikel-5 auf dem „Cyberfeld“

154 Rat der Europäischen Union: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, S. 4.
155 Ebd., S. 10; Rat der Europäischen Union: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 14435/17, Brussels, 20 November 2017, S. 10, online unter: https://www.consilium.europa.eu/media/31666/st14435 en17.pdf.

angewendet werden soll – „while preserving its flexibility“.[156] Hier sollte die EU die Haltung einnehmen, dass Netzwerkoperationen erst ab den Effekten, die äquivalent eines Einsatzes militärischer Gewalt sind, ebenso beantwortet werden. „Strategische Ambivalenz“, die Entscheidungsträger oftmals fordern, ist kontraproduktiv und birgt die unnötige Gefahr der ungewollten Eskalation des Cybersicherheitsdilemmas.

Alles in allem können die Cyber-Diplomacy-Toolbox und der Ratsbeschluss zur Weiterentwicklung restriktiver Maßnahmen (2019/797/CFSP) als solide Grundlage einer Cybersicherheitsdoktrin auf EU-Ebene gewertet werden. Sie signalisieren nach außen, welches Verhalten die EU im Cyberspace als unerwünscht ansieht und machen die Folgen von Cyberoperationen gegen die EU-27 deutlich. So können Fehlwahrnehmungen anderer Staaten im Umgang mit den EU-Staaten reduziert werden. Dieser Effekt könnte noch verstärkt werden, wenn die entsprechenden Dokumente in einem herausgehobenen Dokument zusammengefasst werden. Dieses ausschließlich auf staatliche Netzwerkoperationen zugeschnittene Dokument sollte regelmäßig evaluiert und in politischen Dialogen mit Drittstaaten so transparent wie möglich kommuniziert werden. Den „EU-Status quo“ zu Netzwerkoperationen sollten die EU versuchen in bi- und multilateralen Formaten zu verbreiten, um so nach Möglichkeit seine internationale Akzeptanz zu steigern. Ein international bekannter „EU-Cyber-Status-Quo“ könnte zukünftig Ausgangsgrundlage zur Sanktionierung nicht erwünschten staatlichen Verhaltens sein.

Fazit

Als Gesamtfazit lässt sich konkludieren, dass es für die EU vor allem auf den Feldern der Vertiefung bilateralen Vertrauens und dem unilateralen Signalisieren von Motiven zur Erhöhung der systemweiten Sicherheit noch erheblichen Spielraum gibt, um das Cybersicherheitsdilemma in den Beziehungen mit Drittstaaten zu reduzieren. Maßnahmen zum Ausbau der

156 Rat der Europäischen Union: EU Cyber Defence Policy Framework (2018 update), 14413/18, Brussels, 19 November 2018, S. 11, online unter: https://www.consilium.europa.eu/media/37-024/st14413-en18.pdf.

Grundlagensicherheit in der EU werden sich stets auf die Breite der ICT-Systeme vor dem Hintergrund des Binnenmarktes beziehen und weniger auf die strategischen Netzwerke, die von Bedeutung für das Cybersicherheitsdilemma sind. Auf dem Feld der Cybersicherheitsdoktrin ist die EU gegenwärtig ordentlich aufgestellt. Hier gilt es die Einzeldokumente in eine kohärente Doktrin zusammenzuführen, die diesen Namen verdient, und die strategisch nach außen kommuniziert werden sollte.

Diese Erkenntnisse, die begrenzt sind durch den klandestinen Charakter des Politikfeldes, geben Grund für Optimismus im Hinblick auf die Möglichkeiten der EU, das Cybersicherheitsdilemma mit Drittstaaten abzuschwächen: Auf den Defizitfeldern des Aufbaus von bilateralem Vertrauen und dem unilateralen Signalisieren von friedvollen Absichten zur Erhöhung der systemweiten Sicherheit hat der Sicherheitsakteur EU, der im konventionellen Konfliktmanagement bislang einen durchwachsenen „track record“ zu verzeichnen hat, die größten Möglichkeiten das Cybersicherheitsdilemma abzuschwächen. Die Verhandlungsmacht und Glaubwürdigkeit der EU erleichtert z. B. das Schließen von Abkommen, während die nicht-vorhandenen eigenen Cyberfähigkeiten der EU sowie der Zusammenschluss von 27 Staaten einem teuren Signal mehr Wert verleihen können. Andererseits ist die EU auch das, was ihre Mitgliedsstaaten sind. Und die rüsten ihre Cyberfähigkeiten in dem Glauben, andere Staaten abschrecken zu können, und um im Notfall souverän zu sein, munter auf.

Das **Zentrum für Europäische Integrationsforschung (ZEI)** ist ein interdisziplinäres Forschungs- und Weiterbildungsinstitut der Universität Bonn. *ZEI – DISCUSSION PAPER* richten sich mit ihren von Wissenschaftlern und politischen Akteuren verfassten Beiträgen an Wissenschaft, Politik und Publizistik. Sie geben die persönliche Meinung der Autoren wieder. Die Beiträge fassen häufig Ergebnisse aus laufenden Forschungsprojekten des ZEI zusammen.

The **Center for European Integration Studies (ZEI)** is an interdisciplinary research and further education institute at the University of Bonn. *ZEI – DISCUSSION PAPER* are intended to stimulate discussion among researchers, practitioners and policy makers on current and emerging issues of European integration and Europe´s global role. They express the personal opinion of the authors. The papers often reflect on-going research projects at ZEI.

Die neuesten ZEI Discussion Paper / Most recent ZEI Discussion Paper:

C 247 (2018) Wolfgang Reinhard
Die Expansivität Europas und ihre Folgen

C 248 (2018) Joseph M. Hughes
“Sleeping Beauty” Unleashed: Harmonizing a Consolidated European Security and Defence Union

C 249 (2018) Rahel Hutgens/Stephan Conermann
Macron’s Idea of European Universities. From Vision to Reality

C 250 (2018) Javier González López
Bosnia and Herzegovina: a Case Study for the Unfinished EU Agenda in the Western Balkans

C 251 (2019) Günther H. Oettinger
Europäische Integration aus historischer Erfahrung. Ein Zeitzeugengespräch mit Michael Gehler

C 252 (2019) Chiara Ristuccia
Industry 4.0: SMEs Challenges and Opportunities in the Era of Digitalization

C 253 (2019) Agnes Kasper/Alexander Antonov
Towards Conceptualizing EU Cybersecurity Law

C 254 (2019) Susanne Baier-Allen
Europe and America

C 255 (2019) Ludger Kühnhardt
The European Archipelago. Rebranding the Strategic Significance of EU Overseas Countries and Territories

C 256 (2019) Henri de Waele / Ellen Mastenbroek (eds.)
Perspectives on Better Regulation in the EU

C 257 (2020) Ludger Kühnhardt
Richard von Weizsäcker (1920-2015). Momentaufnahmen und Denkwege eines europäischen Staatsmannes

C 258 (2020) Ermir I. Hajdini, Nikola Jokić, Teodora Lađić, Ksenija Milenković, Denis Preshova, Flandra Syla (eds.)
Western Balkans and the European Union

C 259 (2020) Christos Stylianides
European Emergency Coordination

C 260 (2020) Cillian O’Gara
European Energy Security

C 261 (2020) Johannes Wiggen
Chancen und Grenzen europäischer Cybersicherheitspolitik

Die vollständige Liste seit 1998 und alle Discussion Paper zum Download finden Sie auf unserer Homepage: http://www.zei.de. For a complete list since 1998 and all Discussion Paper for download, see the center‘s homepage: http://www.zei.de.

Rheinische
Friedrich-Wilhelms-
Universität Bonn

Center for European
Integration Studies

Genscherallee 3
D-53113 Bonn
Germany

Tel.: +49-228-73-1810
Fax: +49-228-73-1818
http://www.zei.de

ISSN 1435-3288 **ISBN 978-3-946195-05-4**