SWP

SWP-Studie

Annegret Bendiek / Matthias Schulze

Attribution als Herausforderung für EU-Cybersanktionen

Eine Analyse von WannaCry, NotPetya, Cloud Hopper, Bundestag-Hack, OVCW

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

SWP-Studie 17
Oktober 2021, Berlin

- Die Attribution von Cyberangriffen ist ein souveräner Akt der EU-Mitgliedstaaten. Diese haben jedoch unterschiedliche technische und geheimdienstliche Fähigkeiten. Das führt zu Inkohärenzen in der europäischen Cyberdiplomatie, etwa bei der Verhängung von Cybersanktionen.
- Die Analyse der politischen Reaktionen auf die Cybervorfälle WannaCry, Not-Petya, Cloud Hopper, OVCW und Bundestag-Hack offenbart folgende Probleme: Die Attribution dauert lange und ist auf Erkenntnisse von Nato-Partnern angewiesen; die technischen Realitäten und die rechtlichen Tatbestandsmerkmale zur Klassifikation und Verfolgung von Cyberangriffen passen nicht immer zusammen; die Gewichtung der Tatbestandsmerkmale ist unklar.
- Cybersanktionen sollen gezielte Maßnahmen und vor allem in ihrer Intensität verhältnismäßig sein: Destruktive Angriffe wie WannaCry oder NotPetya sollten härtere Konsequenzen nach sich ziehen als alltägliche Fälle von Cyberspionage wie Cloud Hopper oder Bundestag-Hack. Hier muss die EU ihre Werkzeuge genauer konfigurieren.
- Die EU sollte die rechtlichen Tatbestandsmerkmale schärfen und Beweisstandards zur Attribution vereinheitlichen. Die Gemeinsame Cyber-Stelle der EU und EU INTCEN im Europäischen Auswärtigen Dienst sollten gestärkt werden, um den Austausch forensischer Informationen zu verbessern und die Politik der Attribution effektiver koordinieren zu können.
- Die EU-Mitgliedstaaten und ihre alliierten Partner müssen Angreifer häufiger gemeinsam verurteilen, damit die davon ausgehende politische Botschaft wirklich deutlich wird. Dazu wäre es sinnvoll, für den Erlass von Cybersanktionen qualifizierte Mehrheitsentscheidungen zuzulassen.

SWP-Studie

Annegret Bendiek / Matthias Schulze

Attribution als Herausforderung für EU-Cybersanktionen

Eine Analyse von WannaCry, NotPetya, Cloud Hopper, Bundestag-Hack, OVCW

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

SWP-Studie 17
Oktober 2021, Berlin

SWP-Studien unterliegen einem Verfahren der Begutachtung durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*, sie werden zudem einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/. SWP-Studien geben die Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6372
ISSN (Online) 2747-5115
doi: 10.18449/2021S17v02
Die erste Version mit der doi 10.18449/2021S17 ist nicht mehr verfügbar.

Am 2.12.2021 korrigierte Version.

Inhalt

Dr. Annegret Bendiek ist Stellvertretende Leiterin der Forschungsgruppe EU/Europa.
Dr. Matthias Schulze ist Stellvertretender Leiter der Forschungsgruppe Sicherheitspolitik.

Attribution als Herausforderung für EU-Cybersanktionen. Eine Analyse von WannaCry, NotPetya, Cloud Hopper, Bundestag-Hack, OVCW

Die Europäische Union hat im Juli 2020 erstmals sogenannte Cybersanktionen gegenüber Einzelpersonen verhängt, die mit dem russischen, nordkoreanischen oder chinesischen Staat in Verbindung gebracht werden. Die Maßnahmen umfassen Einreiseverbote und das Einfrieren von Vermögenswerten. Sie gelten in der EU-27 und sind als diplomatische bzw. politische Antwort auf zahlreiche schwerwiegende und bösartige Cyberoperationen gegen die EU beschlossen worden. Cybersanktionen sind nur *ein* Instrument aus dem »gemeinsamen diplomatischen Werkzeugkasten« (Cyber Diplomacy Toolbox) und sie liegen unterhalb der Schwelle eines bewaffneten Konfliktaustrags. Seit 2017 versuchen die EU-Mitgliedstaaten mit dieser Toolbox, im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU (GASP) auf schwerwiegende Cyberoperationen koordiniert zu antworten. Eine verhältnismäßige, kohärente und vor allem rechtssichere Erwiderung der EU auf solche Cyberangriffe zu zeigen, ist allerdings in der Umsetzung höchst anspruchsvoll. Die diplomatische Reaktion muss in ihrer rechtlichen, technischen und politischen Dimension konsistent sein, für den Fall, dass gelistete Personen die restriktiven Maßnahmen der EU, also gegen sie individuell verhängte Finanzsanktionen oder Reisebeschränkungen, gerichtlich anfechten. Denn über das Mittel der Nichtigkeitsklage nach Artikel 263 IV des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) genießen die Adressaten derartiger Strafmaßnahmen uneingeschränkten Rechtsschutz vor dem Europäischen Gerichtshof.

Will die EU rechtmäßige Cybersanktionen verhängen, ist zunächst eine sorgfältige und nachvollziehbare Ermittlung der Urheberschaft (Attribution) von Cyberangriffen erforderlich. Allerdings ist das Verfahren der Attribution, das heißt die technische, rechtliche und politische Zuordnung von Cyberattacken zu verantwortlichen Personen, auf EU-Ebene inkohärent und teilweise widersprüchlich. Die Gründe dafür sind vielfältig: Attribution ist ein souveräner Akt der Mitgliedstaaten, die zugleich recht unterschiedliche technische und geheimdienstliche Fähigkeiten haben. Die

EU soll zunächst koordinieren, forensische Beweise sammeln und Erkenntnisse austauschen. Der Prozess der Attribution bis hin zur Verhängung von Cybersanktionen ist für die EU ein Novum. Ihn sorgfältig durchzuführen ist angesichts der gestiegenen Anzahl und Intensität von Angriffen im Cyber- und Informationsraum (CIR) dringend geboten.

Die zentrale Fragestellung dieser Studie lautet daher: Wie funktioniert die Attribution von Cyberangriffen auf der rechtlichen, technischen und politischen Ebene innerhalb der EU? Welche Defizite, Inkohärenzen und Widersprüche gibt es in diesem Prozess? Welche Folgen hat dies für den Erlass von Cybersanktionen durch die EU? Und wie können die identifizierten Defizite überwunden werden?

Die Untersuchung von fünf großen Cyberattacken (WannaCry 2017, NotPetya 2017, Operation Cloud Hopper 2016, des Bundestag-Hacks 2015 sowie des verhinderten Angriffs auf die Organisation für das Verbot chemischer Waffen 2018) kommt zu folgenden Ergebnissen:

Erstens ist festzustellen, dass die Attributionsfähigkeit der EU hochgradig auf den Informationsaustausch (»intelligence sharing«) mit den USA und Großbritannien angewiesen ist. Während die Five-Eyes-Nachrichtendienstallianz (bestehend aus den USA, Großbritannien, Kanada, Australien und Neuseeland) ihre Attribution und ihr öffentliches »naming and shaming« medienwirksam koordinieren, laufen die Abstimmungsprozesse in der EU-27 naturgemäß langsamer ab: Zwischen einem Cybervorfall und dem Erlass von Sanktionen vergehen Monate, wenn nicht Jahre. Damit die Signalwirkung restriktiver Maßnahmen künftig schneller ausgelöst wird und die Angreifer früher zur Rechenschaft gezogen werden können, ist es erforderlich, dass die EU die Verantwortungszuschreibung möglichst rasch vornimmt.

Zweitens entspricht der Rechtsrahmen, der für EU-Cybersanktionen entwickelt wurde, nicht immer den technischen Realitäten von Cyberoperationen. Die Tatbestandsmerkmale, die ein Cybervorfall erfüllen muss, damit angemessene Sanktionen als Rechtsfolge begründet werden können, sind zu schärfen. Es sollte stärker zwischen erfolgreichen Attacken und intendierten Angriffsversuchen differenziert werden. Die Definition der Angriffsmotivation lässt sich mitunter nicht rechtssicher aus technischen Indikatoren ableiten. Gleichwohl ist sie zentral für die rechtliche Bewertung eines Angriffs und die daran anschließende Begründung eines Sanktionsbeschlusses.

Drittens sollte bei Cybervorfällen stärker nach der Intensität und nach technischen Merkmalen differenziert werden, um die diplomatischen Reaktionen der EU und auch die Sanktionen proportional darauf abstimmen zu können: WannaCry und NotPetya verursachten weltweit Milliardenschäden und hätten weitaus härtere Strafmaßnahmen als Kontensperrungen nach sich ziehen können.

Viertens wären die EU-Staaten gut beraten, die für eine Attribution erforderlichen Beweisstandards zu vereinheitlichen und für eine weitgehend transparente Attributionsevidenz Sorge zu tragen, ohne dabei nachrichtendienstliche Zugänge aufs Spiel zu setzen. Alle Mitgliedstaaten sollten ein vergleichbares standardisiertes System (Probability Yardstick) verwenden, um bei Aussagen zur Verantwortlichkeit, die nicht zum Beispiel forensisch bewiesen sind, eine Einordnung zu ermöglichen.

Schließlich müssen Informationen über Indicators of Compromise (IoCs), also Merkmale und Daten, die auf die Kompromittierung eines Systems oder Netzwerks hindeuten, durch die Gemeinsame Cyber-Stelle in der EU-Kommission (Joint Cyber Unit) und das EU INTCEN beim Europäischen Auswärtigen Dienst (EAD) allen Beteiligten zur Verfügung gestellt werden, damit jeder an den angebotenen Lösungen teilhaben kann. Beide Institutionen sollten kompetenzrechtlich gestärkt werden, um die Cyberlagebilderfassung zu verbessern.

Vor diesem Hintergrund wäre der Bundesregierung zu empfehlen, die Initiative der französischen Ratspräsidentschaft zur Reform des »EU-Instrumentariums für die Cyberdiplomatie« tatkräftig zu unterstützen, damit Angriffe auf die kritische Infrastruktur, auf Versorgungsketten und demokratische Institutionen der EU künftig wirkungsvoller abgewehrt werden können. Dies deckt sich mit den Anforderungen für die Umsetzung der Cybersicherheitsstrategie vom Dezember 2020.

Zur Genese der Cyber-diplomatie und der Attributionsproblematik

Seit 2013 erarbeitet die Europäische Union als Rechtsgemeinschaft politische und regulative Maßnahmen, um auf »böswillige« Cyberoperationen reagieren zu können, die sich von Drittstaaten aus gegen die EU richten.[1] Sie tritt im Rahmen ihrer Cyberdiplomatie für eine friedliche Lösung internationaler Streitigkeiten ein und betont die Bedeutung eines »globalen, offenen, freien, stabilen und sicheren Cyberraums«.[2] Diese Grundhaltung prägte schon die erste Cybersicherheitsstrategie 2013 und wurde zuletzt im Dezember 2020 mit der aktuell gültigen Strategie bestätigt.[3] Erklärtes Ziel ist es, die Stabilität, die Sicherheit und die Vorteile des Internets zu erhalten und die Nutzung von Informations- und Kommunikationstechnologien zu gewährleisten.[4] Die EU-Mitgliedstaaten wirken seither in multilateralen Foren wie der Governmental Group of Experts und der Open Ended Working Group auf Ebene der Vereinten Nationen (UN) maßgeblich daran mit, Cyber-Normen im geltenden Völkerrecht zu verankern und eine regelbasierte internationale Ordnung im Cyber- und Informationsraum (CIR) zu etablieren und durchzusetzen.[5] Die Staatengemeinschaft einigte sich 2015 darauf, dass eine Reaktion auf Cyberangriffe proportional sein sollte bzw. dass Gegenreaktionen erst dann völkerrechtlich legitimiert sind, wenn die Attacken einen bestimmten Umfang haben und bestimmte Effekte hervorrufen, also in ihrer Intensität einem bewaffneten Angriff ähneln. Unter das Gebot der Verhältnismäßigkeit fällt zum Beispiel der Verzicht auf Cyber-

1 Wesentliche Ergebnisse dieser Studie verdanken wir den tiefgründigen Recherchen von Anna Sophia Tiedeke, Kerstin Zettl und Andreas Schmidt. Die Genannten haben durch ihre Analysen im Rahmen des Pilotprojekts zur Machbarkeit eines Repositoriums über Cybervorfälle in Europa in Kooperation mit dem Cyberaußenpolitikstab in den Jahren 2020/21 maßgeblich zur Erarbeitung der SWP-Studie beigetragen. Ein besonderer Dank gilt auch Veronika Datzer für ihre Korrekturen.

Die Angriffe werden benannt als »WannaCry«, »NotPetya«, »Operation Cloud Hopper«, »Bundestag-Hack« und »versuchter Angriff auf die Organisation für das Verbot chemischer Waffen (OVCW)«. Die EU hat diese Attacken als böswillige Cyberangriffe und versuchte Cyberangriffe mit potentiell erheblichen Auswirkungen eingestuft, »die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen«.

2 Rat der Europäischen Union, *Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten – Billigung*, Brüssel, 16.4.2018, <https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/de/pdf>.

3 Annegret Bendiek / Matthias C. Kettemann, *EU-Strategie zur Cybersicherheit: Desiderat Cyberdiplomatie*, Berlin: Stiftung Wissenschaft und Politik, Februar 2021 (SWP-Aktuell 12/2021), <https://www.swp-berlin.org/publikation/eu-strategie-zur-cybersicherheit-desiderat-cyberdiplomatie>; Annegret Bendiek / Raphael Bossong / Matthias Schulze, *Die erneuerte Strategie der EU zur Cybersicherheit. Halbherziger Fortschritt angesichts weitreichender Herausforderungen*, Berlin: Stiftung Wissenschaft und Politik, Oktober 2017 (SWP-Aktuell 72/2017), <https://www.swp-berlin.org/publikation/die-erneuerte-strategie-der-eu-zur-cybersicherheit>; Annegret Bendiek, *Umstrittene Partnerschaft: Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit*, Berlin: Stiftung Wissenschaft und Politik, Dezember 2013 (SWP-Studie 26/2013), <https://www.swp-berlin.org/publikation/cyber politik-transatlantische-zusammenarbeit>.

4 Rat der Europäischen Union, *Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten* [wie Fn. 2], S. 2.

5 Vgl. Matthias Schulze, *Konflikte im Cyberspace*, Berlin: Deutsche Gesellschaft für die Vereinten Nationen, 2020 (UN-Basis-Informationen 61), <https://dgvn.de/veroeffentlichungen/publikation/einzel/konflikte-im-cyberspace/> (Zugriff am 6.5.2021); Alex Grigsby, »The End of Cyber Norms«, in: *Survival*, 59 (2017) 6, S. 109–122.

operationen gegen kritische Infrastrukturen. Eine aktive Cyberabwehr ist erlaubt, wenn Staaten ihre Sorgfaltspflichten vernachlässigen.[6] Diese Normen sind für die EU handlungsleitend.

Mit den spektakulären Cyberoperationen WannaCry und NotPetya (beide im Frühjahr 2017) ist der politische Handlungsdruck gestiegen, gegen diese Form des Angriffs aktiv vorzugehen.[7] WannaCry gilt bis dato als die umfänglichste Cyberattacke mit »Opfern« in über 150 Ländern, NotPetya als einer der bislang kostspieligsten und destruktivsten Angriffe.[8] Wenige Monate später, im Juni 2017, einigte sich der Rat der EU in einem GASP-Beschluss darauf, einen »diplomatischen Reaktionsrahmen« (bekannt als Cyber Diplomacy Toolbox) zu erarbeiten, um die Union in den Stand zu versetzen, eine gemeinsame, koordinierte diplomatische Gegenreaktion auf schwerwiegende Cybervorfälle unterhalb der Schwelle eines bewaffneten Konflikts zu zeigen. Angreifer sollen durch Androhung von Vergeltungsmaßnahmen (»naming and shaming«) dazu bewegt werden, Angriffe gegen die EU zu unterlassen. Der Rat verkündete folgerichtig im April 2018, dass er den Missbrauch von Informations- und Kommunikationstechnologie (IKT) für »böswillige« Zwecke nicht mehr länger hinnehmen werde.[9] Am 17. Mai 2019 wurde das Cybersanktionsregime mit der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe komplettiert und sozusagen scharfgeschaltet.[10]

6 Vgl. Annegret Bendiek, *Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen und Sicherheitspolitik*, Berlin: Stiftung Wissenschaft und Politik, März 2016 (SWP-Studie 3/2016) <https://www.swp-berlin.org/publikation/sorgfaltsverantwortung-im-cyberraum>; dies., *European Digital Sovereignty: Combining Self-interest with Due Diligence*, Ottawa: Centre for European Studies, Carleton University, Dezember 2020 (EU Policy Brief 5), <https://carleton.ca/ces/wp-content/uploads/Bendiek-EU-Policy-Brief-Digital-Sovereignty-2.pdf> (Zugriff am 4.6.2021).

7 Weitere sicherheitspolitische Initiativen der EU sind unter anderem der Politikrahmen für die Cyberabwehr (Cyber Defence Policy Framework, 2018), der Rechtsakt zur Cybersicherheit und die 5G-Toolbox (beide 2019), die Strategie für die Sicherheitsunion und die EU-Verordnung zum Screening von (Digital-)Investitionen (2020).

8 Andy Greenberg, »White House Blames Russia for NotPetya, the ›Most Costly Cyberattack in History‹«, *Wired* (online), 15.2.2018, <https://www.wired.com/story/white-house-russia-notpetya-attribution/> (Zugriff am 18.5.2021).

9 Rat der Europäischen Union, *Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten* [wie Fn. 2].

10 Ebd.

Im Juli 2020, also erst Jahre nach den Vorfällen, verhängte der Rat der EU Cybersanktionen gegen nordkoreanische, chinesische und russische Angreifer, denen er unter anderem die Verantwortung für die Cybervorfälle WannaCry, Cloud Hopper und NotPetya zuschreibt.[11] Die Verzögerung erklärt sich unter anderem daraus, dass eine Ermittlung der Urheberschaft von Cyberangriffen, konkret die technische, rechtliche und politische Attribution, anspruchsvoll ist und IT-forensische und nachrichtendienstliche Fähigkeiten voraussetzt. Nur wenige Mitgliedstaaten, unter anderem Schweden, die Niederlande, Estland, Österreich, Frankreich oder Deutschland, verfügen über diese Attributionsfähigkeiten und bringen die (nicht bei allen gleichmäßig ausgeprägte) Bereitschaft mit, Informationen über EU INTCEN, die geheimdienstliche Analyseabteilung des Europäischen Auswärtigen Dienstes (EAD), mit anderen Mitgliedstaaten zu teilen. Voraussetzung für einen Brüsseler Sanktionserlass als Reaktion auf schwerwiegende Cyberangriffe ist, dass die EU Urheber und »böswillige« Absicht plausibel machen kann. Dies gestaltet sich nicht nur wegen der genuin dezentralen Struktur des Cyber- und Informationsraums, sondern auch wegen der unterschiedlichen mitgliedstaatlichen Ausgangsbedingungen und mangelnden Analysefähigkeiten im EAD bzw. auf EU-Ebene als ein recht komplexes Unterfangen.

Ein kollektiver, gemeinsamer Prozess der Attribution findet innerhalb der EU nur punktuell statt.

Die Attribution ist ein zentrales Problem in der Cyberkonfliktforschung und stellt eine besondere Herausforderung für die Cyberdiplomatie und das Cybersanktionsregime der EU dar.[12] Sicherheitspolitik und die Attribution von Cyberangriffen sind Prärogative der EU-Mitgliedstaaten. Diese sind zurückhal-

11 Rat der Europäischen Union, *Beschluss (GASP) 2020/1127 des Rates vom 30. Juli 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen*, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020D1127&from=DE> (Zugriff am 2.6.2021). Auf der rechtlichen Grundlage von Artikel 13 Absatz 1 VO (EU) 2019/796 wurde in Anhang I der VO (EU) 2019/796 die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen gemäß Artikel 3 VO (EU) 2019/796 geändert.

12 Vgl. Florian J. Egloff / Max Smeets, »Publicly Attributing Cyber Attacks: A Framework«, in: *Journal of Strategic Studies*, (2021), S. 1—32.

tend, wenn es darum geht, sensible Informationen zu Cyberangriffen auf EU-Ebene zu teilen, da sie Rückschlüsse auf einzelstaatliche Cyberabwehrfähigkeiten ermöglichen. Die Weitergabe von Erkenntnissen könnte staatliche Quellen und geheime Zugänge kompromittieren. Ein kollektiver, gemeinsamer Prozess der Attribution findet innerhalb der EU nur punktuell statt: In der Regel attribuiert jeder Mitgliedstaat autonom für sich. Die EU versucht lediglich die relevanten Informationen zu bündeln und die politische Reaktion auf Cyberangriffe zu koordinieren. Dieser Umstand erschwert auch ein gemeinsames Auftreten der Mitgliedstaaten beim »naming and shaming« von Angreifern in der EU-Cyberdiplomatie. Ungeachtet dessen ist eine zwischen den Mitgliedstaaten und den EU-Institutionen koordinierte Attribution eine notwendige Vorbedingung für die Aktivierung des diplomatischen Reaktionsrahmens und für Sanktionen der EU.

Ein fragmentierter Attributionsprozess schwächt die Glaubwürdigkeit, Legitimität und Effektivität der EU-Cyberdiplomatie. Inkohärentes Handeln ist eine Folge davon: Die russischen Geheimdienstmitarbeiter, gegen die 2020 Cybersanktionen in Form von Einreiseverboten und Kontensperrungen verhängt wurden, waren bereits wenige Jahre zuvor mit den gleichen restriktiven Maßnahmen durch ein anderes EU-Sanktionsregime belegt worden. Die Maßnahmen duplizierten sich also und hatten keinen zusätzlichen Effekt.[13] Abgesehen von der Redundanz dieses Schrittes ist außerdem zu fragen, inwiefern Reisebeschränkungen und eingefrorene Konten wirklich eine abschreckende Wirkung auf Angreifer haben oder letztlich nur Symbolpolitik sind.[14] Zudem leiden die Effektivität und die Legitimität von Cybersanktionen, wenn das öffentliche »naming and shaming« der Urheber von Cyberangriffen nicht durch die mitgliedstaatlichen Regierungen unterstützend mitgetragen wird.

Es obliegt jeder Regierung zu entscheiden, ob sie sich den veröffentlichten Attributionen anderer EU-Staaten anschließt.

Es obliegt jeder Regierung zu entscheiden, ob sie sich den veröffentlichten Attributionen anderer EU-Staaten diplomatisch und/oder medial anschließt. Nur 6 der 27 EU-Staaten haben beispielsweise die Sanktionen von 2020 gegen Russland durch Regierungserklärungen oder diplomatische Statements bekräftigt.[15] Obwohl Deutschland die Cybersanktionen nach dem Bundestag-Hack im Jahr 2015 auf EU-Ebene mit auf den Weg gebracht hatte, konnte sich die Bundesregierung nur zögernd zu einer öffentlichen Verurteilung der Täter durchringen. Durch diese Halbherzigkeit werden die Signalwirkung und die politische Schlagkraft der Cybersanktionen unnötig gemindert. Ist die politische Botschaft inkohärent, also das »signaling« der EU-Staaten, bei gleichzeitigem Einstimmigkeitserfordernis im Rat, verliert die Androhung von Strafmaßnahmen an Stringenz. Dies hat zur Folge, dass Cyberangreifer derzeit nicht in ausreichendem Maße davon abgehalten werden, Attacken zu verüben.[16] Das Vetorecht und die Vielstimmigkeit der Mitgliedstaaten schaden der außenpolitischen Glaubwürdigkeit der Europäer auch in der internationalen Cyberdiplomatie. Und nicht nur das: Die EU-Staaten unterlaufen mit diesem Verhalten die im Rahmen der Vereinten Nationen beschlossene und auch für sie verbindliche Sorgfaltspflicht.

Im Wissen um diese Defizite haben die EU und die französische Regierung mit Blick auf ihre anstehende Ratspräsidentschaft angekündigt, die Cyber Diplomacy Toolbox zu evaluieren, inklusive der darin katalogisierten Cybersanktionen. Wenn die EU Sanktionen erlässt, muss sie rechtsstaatliche Mindeststandards gegenüber den betroffenen Personen einhalten. Da-

13 Stefan Soesanto, »Europe Has No Strategy on Cyber Sanctions«, *Lawfare*, 20.11.2020, <www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions> (Zugriff am 6.5.2020).

14 Annegret Bendiek / Minna Ålander / Paul Bochtler, *GASP: Von der Ergebnis- zur Symbolpolitik. Eine datengestützte Analyse*, Berlin: Stiftung Wissenschaft und Politik, November 2020 (SWP-Aktuell 86/2020), <https://www.swp-berlin.org/publikation/gasp-von-der-ergebnis-zur-symbolpolitik>; vgl. auch Francesco Giumelli / Fabian Hoffmann / Anna Książczaková, »The When, What, Where and Why of European Union Sanctions«, in: *European Security*, 30 (2021) 1, S. 1–23; Niklas Helwig / Juha Jokela / Clara Portela (Hg.), *Sharpening EU Sanctions Policy for a Geopolitical Era,* Helsinki: Prime Minister's Office, 2020, <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162257/VNTEAS_2020_31.pdf> (Zugriff am 4.6.2021); Clara Portela et al., »Consensus against All Odds: Explaining the Persistence of Sanctions on Russia«, in: *Journal of European Integration*, 43 (2020) 6, S. 1–17.

15 Soesanto, »Europe Has No Strategy on Cyber Sanctions« [wie Fn. 13]

16 Erica D. Borghard / Shawn W. Lonergan, »The Logic of Coercion in Cyberspace«, in: *Security Studies*, 26 (2017) 3, S. 452–481 (463).

mit einher gehen qualitative Anforderungen an die Attribution. Die vorliegende Studie wird im Folgenden die Dringlichkeit einer Reform des diplomatischen Reaktionsrahmens darlegen und Ansatzpunkte für dessen Neugestaltung aufzeigen. Dafür werden zunächst die Cybervorfälle, die das Cyber-Sanktionsregime auf EU-Ebene im Jahr 2020 erstmals auslösten, namentlich der Bundestag-Hack 2015, WannaCry, NotPetya (beide 2017), der Angriff auf die Organisation für das Verbot chemischer Waffen (OVCW) und die Operation Cloud Hopper im Hinblick darauf untersucht, wie kohärent die EU diese Attacken technisch, rechtlich und politisch eingeordnet hat. Nicht analysiert werden indes die operativen Verfahren der Attribution, die zwischen den Sicherheitsbehörden praktiziert werden, ihr Informations- und Wissensaustausch und die Effektivität des Sanktionsregimes im Sinne ihrer Wirkung auf die Adressaten.

Die Politik der Attribution

Attribution beschreibt den Prozess, in dessen Verlauf die Verantwortung für einen Cyberangriff einem Akteur zugeschrieben wird. Es geht also um die Frage: Wer war es?[17] Die Verlässlichkeit der Attribution verändert sich im Zuge der Zeit, da sich das Wissen über einen Cybervorfall nach und nach mehrt und die Unsicherheit über die Verantwortlichkeit potentiell abnimmt. Je mehr Zeit und analytische Fähigkeiten zur Verfügung stehen, desto größer ist in der Regel die Gewissheit der Attribution. Der Prozess hat drei Ebenen: eine technische, eine rechtliche und eine politische (siehe Grafik 1, S. 12). Sie bauen aufeinander auf, doch bisweilen gibt es Zielkonflikte zwischen ihnen:

Die Kombination dieser drei Ebenen lässt sich als *Politik der Attribution* definieren. Gemeint ist damit also der Prozess der technischen und rechtlichen Aufklärung und öffentlichen (Nicht-)Benennung von Urhebern eines Cyberangriffs sowie das Initiieren von Gegenmaßnahmen.

Nach einem Cybervorfall erfolgt zunächst die *technische Attribution*. Dabei werden mit Mitteln der IT-Forensik technische Artefakte und Indizien wie Netzwerklogs oder Malware-Spuren (sogenannte Indicators of Compromise, IoCs) in den Computern ausgewertet, die von dem Angriff betroffen sind. Diese werden mit den Tools, Techniques/Tactics & Procedures (TTP) vergangener Vorfälle verglichen und in Beziehung zueinander gesetzt. Daraus lassen sich, ähnlich wie bei kriminalistischen Ermittlungen, konkurrierende Hypothesen über Angreifer generieren und oft direkt Indizien für die Urheberschaft ableiten. Plakativ formuliert ist das Ziel der technischen Attribution, Wissen über das Vorgehen des Angreifers zu sammeln (»den Angreifer kennen«). Dieser Vorgang ist taktischer Natur, denn aus simplen Netzwerkartefakten lässt sich nur schwer auf die strategische oder politische Motivation eines Cybervorfalls schließen.[18] Auch die »soziopolitische Frage«, welcher Akteur sich hinter einem angreifenden Computer verbarg und in wessen Auftrag er handelte, lässt sich basierend auf TTPs nur schwer abschließend beantworten. Es kommt immer wieder vor, dass gleiche oder ähnliche Malware von verschiedenen Hackergruppen genutzt wird. Daher kann mittels der technischen Analyse nicht unmittelbar beantwortet werden, wer einen Angriff verursacht hat. Technische Indizien wie Spracheinstellungen von Systemen können Hinweise liefern, aber genauso gut auch absichtlich platzierte falsche Fährten sein (»false flag«).[19]

Im Zuge der rechtlichen und politischen Attribution, die nicht immer trennscharf unterscheidbar sind, versucht der angegriffene Staat eher akteursbezogene Fragen zu beantworten: Welche Person bzw. welche Organisation ist für den Hack verantwortlich? Wer gab den Befehl dafür? Welche strategische oder politische Motivation war maßgebend für eine Operation? Hier geht es also nicht mehr nur um rein technische Indikatoren, sondern auch um politische Faktoren wie nationale Sicherheitsstrategien und geopolitische Kontexte.[20] Das Kernelement der *politischen Attribution* ist das »naming and shaming« des Angreifers, entweder bilateral über nichtöffentliche, diplomatische Kanäle oder medial, mit dem Ziel, einen Urheber öffentlich bloßzustellen. Leitend für die politische Attribution ist die Hoffnung, dass der Verursacher sein Verhalten überdenkt und von zukünftigen Angriffen ablässt. Politische Attribution kann also *öffentliche Attribution* sein, etwa im Verbund mit Alliierten und Partnern, um die Legitimität einer

17 Thomas Rid / Ben Buchanan, »Attributing Cyber Attacks«, in: *Journal of Strategic Studies*, 38 (2014) 1–2, S. 4–37 (4).

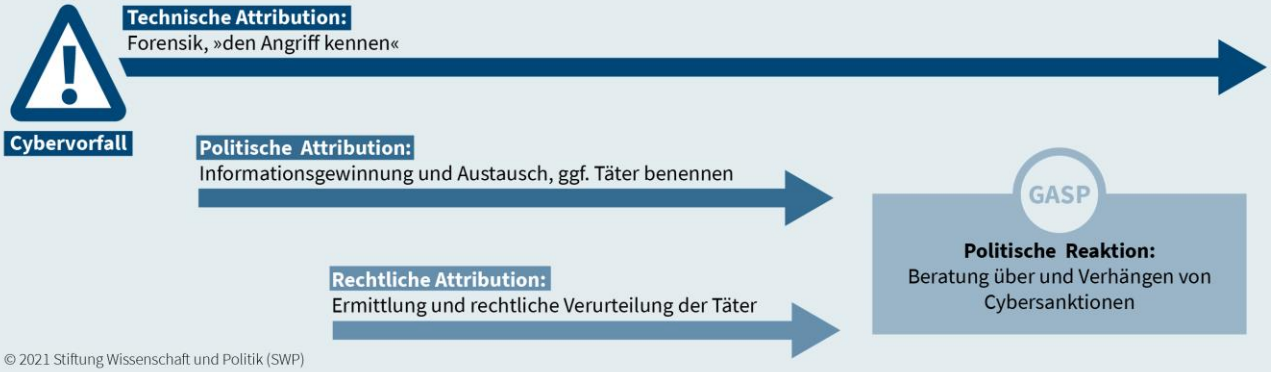
18 Ryan Stillions, »The Detection Maturity Level Model«, *Ryan Stillions Blogspot*, 22.4.2014, <http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html> (Zugriff am 1.1.2020).

19 Erik Gartzke / Jon R. Lindsay, »Weaving Tangled Webs. Offense, Defense, and Deception in Cyberspace«, in: *Security Studies*, 24 (2015) 2, S. 316–348.

20 Jason Healey, *Beyond Attribution: Seeking National Responsibility in Cyberspace*, Washington, D.C.: Atlantic Council, 22.12.2012 (Issue Brief), <https://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace> (Zugriff am 15.9.2021).

Grafik 1

Drei Dimensionen der Attribution
Die Feststellung der Urheberschaft und der Verantwortlichkeit



Verurteilung vor der internationalen Öffentlichkeit zu stärken. Ein Staat kann aber auch auf öffentliche Attribution bewusst verzichten, wenn die politische Situation für ein »naming and shaming« nicht opportun erscheint, etwa während einer politischen Krise, wenn die Beweislage dünn ist oder wenn eigene Quellen nicht kompromittiert werden sollen.[21] Zudem muss ein öffentlich attribuierender Staat unter Umständen mit Gegenmaßnahmen wie Sanktionen rechnen. Politische Attribution findet also immer im Kontext der internationalen Beziehungen und Mächtedynamik statt. Oft erfordert politische Attribution eine Ermessensentscheidung, einen »judgement call«, weil die technischen Indikatoren nicht eindeutig sind. Politische Attribution zielt also darauf ab, den Urheber nicht nur zu kennen, sondern auch zu benennen.

Die *rechtliche Attribution* ist dann wesentlich und unerlässlich, wenn eine rechtmäßige politische Reaktion auf Cybervorfälle erfolgen soll. Rechtliche Attribution beschreibt die strafrechtliche Schuldzuweisung bzw. Anklage. Die politische Attribution und die rechtliche Verantwortlichkeitszuweisung sind nach dem Völkerrecht formal voneinander zu unterscheidende staatliche Handlungen.[22] Wichtig bei der rechtlichen Attribution ist die Unterscheidung zwischen individueller und staatlicher Verantwortlichkeit.[23] Notwendige Vorbedingung jeder rechtlichen Verantwortungszuweisung ist die rechtliche Klassifikation des Vorfalls: Cyberkriminalität ist nach anderen Rechtsstatuten zu behandeln als eine völkerrechtliche Straftat. Sie lässt individuelle Sanktionen zu, während eine Handlung gegen das Völkerrecht unter genau definierten Umständen auch kollektiv wirkende Maßnahmen legitimieren kann. Cyberkriminalität ist wiederum von der Cyberspionage zu unterscheiden, die international nicht verboten ist, strafrechtlich jedoch individuell geahndet werden kann. Und diese ist wiederum von Cyberattacken mit der Eigenschaft eines bewaffneten Angriffs abzugrenzen, die nach Artikel 2.4 der UN-Charta völkerrechtswidrig sind. Letztere können sogar das Recht auf Selbstverteidigung nach Artikel 51 UN-Charta begründen und den Einsatz militärischer Maßnahmen rechtfertigen.

Eine angemessene und verhältnismäßige rechtliche Gegenreaktion auf Cyberangriffe setzt detaillierte technische und politische Kompetenzen zur Charakterisierung von Vorfällen voraus. Staaten können denselben Cybervorfall, je nach ihren Detektions- und Ermittlungsfähigkeiten, rechtlich unterschiedlich bewerten — und ihn entweder dem Deliktfeld der Cyberkriminalität zuordnen oder als eine verborgene Spionageaktion einstufen. Zudem gibt es je nach Klassifikation auch unterschiedliche Erfordernisse an Beweisstandards. Rechtliche Attribution zielt auch

21 Egloff/Smeets, »Publicly Attributing Cyber Attacks« [wie Fn. 12].

22 Siehe zur deutschen Interpretation des Völkerrechts: The Federal Government, *On the Application of International Law in Cyberspace. Position Paper*, Berlin, März 2021, S. 12, <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf> (Zugriff am 6.5.2021).

23 International Law Commission (ILC), *Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARS)*, August 2001, <https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf> (Zugriff am 15.6.2021).

darauf ab, einzelne Individuen, also den Menschen hinter der Maschine, mit den Mechanismen der Strafverfolgung zur Rechenschaft zu ziehen. Dabei gelten höhere Beweisstandards als bei dem politischen Prozess des »naming und shaming«. Beweise müssen gerichtsfest sein, nachrichtendienstliche Quellen sind nur bedingt verwertbar. Politische und rechtliche Attribution laufen dementsprechend nicht zwingend synchron und sind bisweilen inkohärent. Es kann zum Beispiel vorkommen, dass in der Frühphase nach einem Cyberangriff, wenn die Unsicherheit groß und die Beweislage noch dünn ist, fälschlicherweise ein Akteur öffentlich verantwortlich gemacht wird, um dann später im Zuge der rechtlichen Attribution festzustellen, dass es sich um eine False-Flag-Operation handelte. Ein Beispiel hierfür ist der Cyberangriff auf den französischen Sender *TV5 Monde* im Jahr 2015, der im Kontext der Terrorangriffe zunächst dem »Islamischen Staat« (IS) zugeschrieben worden ist, später aber als russische Operation unter falscher Flagge klassifiziert wurde.[24]

Attributionsentscheidungen können bei staatlichen Organisationen, etwa bei Judikative und Exekutive, unterschiedlich und inkohärent ausfallen, etwa wenn die Ermittlungsergebnisse die politischen Annahmen nicht decken. Ein Akteur kann verantwortlich erklärt werden, weil es politisch zwar opportun erscheint, die technische und rechtliche Beweislage aber eine andere Sprache spricht. In Anbetracht all dieser Imponderabilien wird deutlich, wie essentiell es für die kollektive Attribution innerhalb der EU-Cyberdiplomatie ist, ein gemeinsames Verständnis davon zu entwickeln, was unter einem schwerwiegenden Cyberangriff zu verstehen ist. Genauso wichtig ist eine enge Abstimmung attribuierender Organisationen auf staatlicher Ebene (Nachrichtendienste, Strafverfolgungsbehörden) sowie auf supra- bzw. interstaatlicher Ebene.

Was ist ein schwerwiegender Cyberangriff auf die EU?

Unter einer schwerwiegenden Cyberattacke versteht die EU laut ihrer Verordnung vom 17. Mai 2019 (Art. 1 Abs. 1 VO) eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten durch einen tatsächlichen oder versuchten Cyberangriff, der erhebliche oder potentiell erhebliche Auswirkungen hat.[25] Eine äußere Bedrohung der Mitgliedstaaten liegt vor, wenn Cyberangriffe gegen kritische Infrastrukturen, Dienstleistungen oder staatliche Institutionen und Prozesse ausgeführt werden, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder der Gesundheit, Sicherheit und des Wohlergehens der Bevölkerung sind, insbesondere in den Bereichen Energie, Verkehr, Banken, Gesundheitswesen, Trinkwasserversorgung oder digitale Infrastruktur (Art. 1 Abs. 4 VO). Ein Cyberangriff (oder ein versuchter Cyberangriff) ist jede Handlung, die den Zugang bzw. Eingriff in Informations- und Kommunikationssysteme umfasst. Als Informationssysteme gelten Systeme zur automatischen Verarbeitung digitaler Daten; in ein solches System wird eingegriffen, wenn sein Betrieb durch Beschädigung, Löschung, Veränderung, Unterdrückung oder die Übermittlung digitaler Daten behindert oder gestört wird. Cyberangriffe liegen aber auch dann vor, wenn in Daten eingegriffen wird oder diese abgefangen werden. Es reicht also auch schon beispielsweise der Diebstahl von Daten, Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum (Art. 1 Abs. 3 und 7 VO). Ob ein Cyberangriff (potentiell) erhebliche Auswirkungen hat, bemisst sich unter anderem nach dem Umfang, dem Ausmaß, der Wirkung oder der Schwere der (versuchten) Störung für wirtschaftliche und gesellschaftliche Tätigkeiten, nach der Höhe des materiellen Schadens und des vom Täter erlangten wirtschaftlichen Nutzens sowie nach der Menge und Art der gestohlenen Daten, auf die zugegriffen wurde (Art. 2 VO).

Tabelle 1 bietet eine Übersicht über die rechtlichen Merkmale, mit denen Cyberangriffe klassifiziert werden. Mit diesen Tatbestandsmerkmalen definiert die EU verbotene Verhaltensweisen und bestimmt, welche Charakteristika ein Cybervorfall gemäß EU-Recht haben muss, um eine bestimmte rechtliche Konsequenz auszulösen, die sogenannte Rechtsfolge.

24 Gordon Corera, »How France's TV5 Was Almost Destroyed by ›Russian Hackers‹«, *BBC News* (online), 10.10.2016, <https://www.bbc.com/news/technology-37590375> (Zugriff am 14.7.2021).

25 Rat der Europäischen Union, »Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen«, in: *Amtsblatt der Europäischen Union*, (17.5.2019) L 129 I/1, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0796&from=EN> (Zugriff am 2.6.2021).

Tabelle 1

Kriterien für die rechtliche Attribution von Cybervorfällen

Kriterium	Erforderliche Merkmale
Cyberangriff (Art. 1 Abs. 3 und 7 Verordnung [EU] 2019/796)	**Handlungen, die** **a. den Zugang zu Informationssystemen** **b. den Eingriff in Informationssysteme** **c. den Eingriff in Daten oder** **d. das Abfangen von Daten** umfassen, wenn diese Handlungen vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder der Daten oder eines Teils des Systems oder der Daten nicht ordnungsgemäß gestattet wurden oder nach dem Recht der Union oder des betreffenden Mitgliedstaats nicht zulässig sind. Einschließlich **versuchter** Cyberangriffe
Angreiferbestimmung (Art. 1 Abs. 2 und 4 Verordnung [EU] 2019/796)	**Angreifer** a. sind außerhalb der EU ansässig (natürliche/juristische Personen, Organisationen oder Einrichtungen) oder operieren von außerhalb b. nutzen außerhalb der EU gelegene Infrastrukturen. **Opfer** innerhalb der EU (kritische Infrastrukturen, inkl. Seekabel und Weltraum-Objekte mit Kritis-Funktion)
Schäden und Umfang (Art. 2 Verordnung [EU] 2019/796)	Feststellung der »erheblichen Auswirkung« bemisst sich nach a. **Umfang, Ausmaß, Wirkung oder Schwere der verursachten Störung** für wirtschaftliche und gesellschaftliche Tätigkeiten, wesentliche Dienste, kritische staatliche Funktionen, die öffentliche Ordnung oder die öffentliche Sicherheit; b. der Zahl der betroffenen natürlichen oder juristischen Personen, Organisationen oder Einrichtungen; c. der Zahl der betroffenen **Mitgliedstaaten**; d. der **Höhe des wirtschaftlichen Schadens**, der zum Beispiel durch einen groß angelegten Diebstahl von Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum verursacht wurde; e. dem vom Täter für sich selbst oder für andere erlangten **wirtschaftlichen Nutzen**; f. der **Menge oder Art der gestohlenen Daten** oder dem Ausmaß der Datenschutzverstöße oder g. der Art der wirtschaftlich sensiblen Daten, auf die zugegriffen wurde.

Tabelle 1 (Forts.)

Kriterien für die rechtliche Attribution von Cybervorfällen

Kriterium	Erforderliche Merkmale
Operationsziel bzw. Opfer (Art. 1 Abs. 4 Verordnung [EU] 2019/796)	a. **kritische Infrastrukturen**, einschließlich **Seekabel** und in den **Weltraum** gestartete Gegenstände, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind; b. **Dienstleistungen**, die für die Aufrechterhaltung wesentlicher sozialer und/oder wirtschaftlicher Tätigkeiten erforderlich sind, insbesondere in den Sektoren 1. Energie (Elektrizität, Öl und Gas) 2. Verkehr (Luft, Schiene, Wasser und Straße) 3. Bankenwesen, Finanzmarktinfrastrukturen 4. Gesundheitswesen (Gesundheitsdienstleister, Krankenhäuser und Privatkliniken) 5. Trinkwasserlieferung und -versorgung 6. digitale Infrastruktur 7. und in anderen Sektoren, die für den betreffenden Mitgliedstaat von wesentlicher Bedeutung sind; c. **kritische staatliche Funktionen**, insbesondere in den Bereichen 1. Verteidigung 2. Staatsführung und 3. Institutionen, die für das Funktionieren des Staates wesentlich sind, zum Beispiel Wahlen 4. Institutionen, die für das Funktionieren der wirtschaftlichen und der zivilen Infrastruktur wesentlich sind 5. innere Sicherheit 6. Außenbeziehungen, einschließlich diplomatische Missionen; d. Vorrichtungen zur Speicherung oder Verarbeitung von Verschlusssachen; e. Katastrophenstäbe der Regierungen.

Quelle: Eigene Darstellung

Welche Institutionen und Verfahren bestimmen die Attribution?

Für die Attribution wird auf den allgemeinen Rechtsgrundsatz (General Principle, Art. 38 Abs. 1c IGH-Statut) verwiesen, dass jeder Staat die Verpflichtung hat, nicht wissentlich zuzulassen, dass sein Hoheitsgebiet für Handlungen genutzt wird, die die Rechte anderer Staaten verletzen.[26] Nach diesen Prinzipien ist es jedem Mitgliedstaat freigestellt, welche Methode und welches Verfahren er zur Attribution wählt. Die politische Attribution bleibt zwar ein souveräner Akt der Mitgliedstaaten, zugleich hat die EU aber eine wesentliche Koordinierungsfunktion.[27] Eine klare Hierarchie in der »Befehlskette« existiert nicht. Der Attributionsprozess läuft somit institutionell parallel zwischen Kommission, Rat und Europol sowie in Abstimmung mit den 27 Mitgliedstaaten ab (siehe Grafik 2, S. 17).

Die Kommission hat die Prinzipien des EU-Handelns festgelegt, die auch für die anderen EU-Institutionen maßgebend sind. Im September 2017 hat sie einen Entwurf für eine koordinierte Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle großen Ausmaßes ausgearbeitet (kurz: *Blueprint*).[28] Leitprinzipien sind die Beachtung der Verhältnismäßigkeit, der Subsidiarität, der Komplementarität und der Vertraulichkeit von Informationen bei der politischen Reaktion auf Cyberangriffe.[29] Zahllose Angriffe sind nur möglich, weil die Basissoftware (das Betriebssystem, Browser-Anwendungen, VPN etc.) fehlerhaft ist. In ihrem Entwurf legte die EU-Kommission den Schwerpunkt auf den Aufbau einer resilienten IKT-Struktur, auf den Schutz des Binnenmarkts und auf die Umsetzung eines Cyberkrisen-Reaktionsprozesses. Dieser sogenannte Blueprint-Mechanismus läuft parallel zum Krisenmanagement der GASP. Divergierende institutionelle Interessen können vorhandene Widersprüche und Inkohärenzen durchaus verschärfen, doch zeichnet sich schon jetzt ab, dass der EAD mit seiner neu eingerichteten Analyseeinheit für hybride Bedrohungen, der Hybrid Fusion Cell, in seine Rolle hineingewachsen ist und der Informationsaustausch über Cybervorfälle einen kollektiven Mehrwert bietet. Der EAD übernimmt mittlerweile auch die Funktion, über die Informationskriegsdoktrin von Drittstaaten aufzuklären.

Der Rahmen für eine gemeinsame diplomatische Antwort auf böswillige Cyberaktivitäten, der sogenannte diplomatische Reaktionsrahmen, greift dann, wenn der Rat sich darüber verständigt hat, dass eine äußere Bedrohung vorliegt (siehe Grafik 2, S. 17). Jeder Mitgliedstaat kann einen Vorschlag unterbreiten, um eine bestimmte Maßnahme aus dem Repertoire der Cyber Diplomacy Toolbox zu aktivieren. Die vorbereitenden Absprachen zum Ratsbeschluss treffen das Politische und Sicherheitspolitische Komitee (PSK), die Horizontale Arbeitsgruppe »Cyberangelegenheiten« (Horizontal Working Party on Cyber Issues, HWPCI, kurz HWP Cyber), die Kommissionspräsidentin und deren Stellvertreter sowie der Hohe Vertreter für Außen- und Sicherheitspolitik (siehe Grafik 2, Mitte).

Cyberangriffe werden in der Horizontalen Arbeitsgruppe besprochen, dem fachlich zuständigen Gremium innerhalb der EU, und dort auch abschließend behandelt. Die HWP ERCHT koordiniert das Vorgehen der EU-Mitgliedstaaten. Ihr werden Beweise vorgelegt, die durch die Strafverfolgungsbehörden und Geheimdienste der Mitgliedstaaten ermittelt und überprüft

26 »Island of Palmas Case (Netherlands, USA), 4 April 1928«, in: United Nations (Hg.), *Reports of International Arbitral Awards*, Bd. II, Lake Success 1949, S. 829—871 (839); International Court of Justice (ICJ), *The Corfu Channel Case. Judgment of 9 April 1949*, Den Haag, Februar 1949 (ICJ Reports 1949), S. 22, und ICJ, *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay). Judgment of 20 April 2010*, Den Haag 2010 (ICJ Reports 2010), S. 69, para. 197: gebotene Sorgfaltspflicht in Bezug auf »all activities which simply take place under the jurisdiction and control of each party«, <https://www.icj-cij.org/public/files/case-related/135/135-20100420-JUD-01-00-EN.pdf> (Zugriff am 14.9.2021); siehe außerdem Michael N. Schmitt (Hg.), *Tallinn Manual on the International Law Applicable to Cyberwarfare*, Cambridge: Cambridge University Press, 2013, S. 27—28, para. 8.

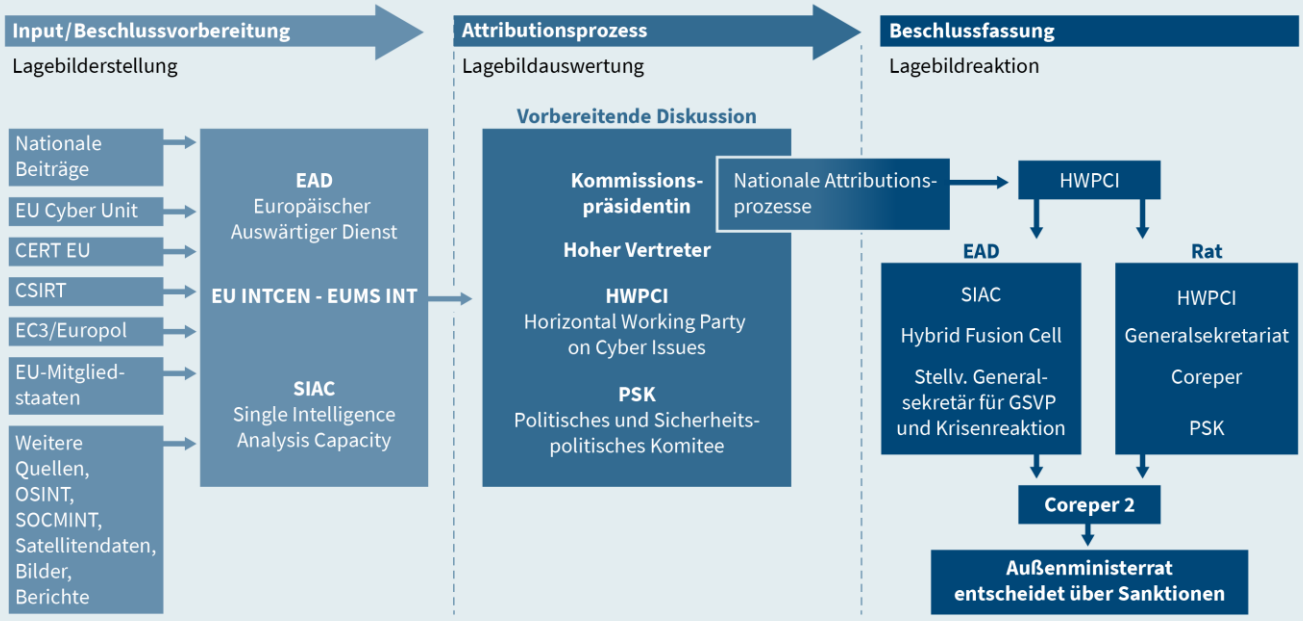
27 Rat der Europäischen Union, »Verordnung (EU) 2019/796« [wie Fn. 25].

28 Europäische Kommission, »Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen«, in: *Amtsblatt der Europäischen Union*, (19.9.2017) L 239, S. 36—58, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017H1584&from=EN>; Council of the European Union, *EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, Brüssel, 26.6.2018, <https://data.consilium.europa.eu/doc/document/ST-10086-2018-INIT/en/pdf> (Zugriff am 2.6.2021).

29 Mit der Gemeinsamen Cyber-Einheit in der Kommission sollen die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU-Mitgliedstaaten über eine europäische Plattform zusammenarbeiten. Gemäß der Richtlinie zur Netz- und Informationssicherheit (NIS) sollen schon jetzt die Computer Security Incident Response Teams (CSIRTs) ihre technischen Lösungen miteinander austauschen.

Grafik 2

Cyber Diplomacy Toolbox
Cyberdiplomatischer Reaktionsrahmen der EU



werden, in Zusammenarbeit mit den Computer Security Incident Response Teams (CSIRT), dem European Cybercrime Centre (EC3), der European Union Agency for Cybersecurity (ENISA) oder dem Computer Emergency Response Team der EU (CERT-EU) (siehe Grafik 2, oben rechts).

Im EAD werden die Informationen gebündelt (Grafik 2, links). Hier liegt die Zuständigkeit beim stellvertretenden Generalsekretär für Krisenreaktion, bei der Single Intelligence Analysis Capacity (SIAC, die wiederum aus Vertretern von EU INTCEN und der Abteilung Aufklärung des Militärstabs der EU, EUMS INT, besteht) und bei der Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell). Außerdem sind weitere EU-Einrichtungen wie die ENISA, Europol/EC3 und das CERT-EU zu informieren.[30] Die zentrale Stelle für eine koordinierte Reaktion ist das Europäische Zentrum für Cyberkriminalität (EC3) von Europol. Schwerwiegende Cybervorfälle sollen Europol gemeldet werden. Die oberste Polizeibehörde der EU identifiziert, bewertet und klassifiziert abschließend die Cybervorfälle nach einer Bedrohungsmatrix.[31] Informationen für die Beurteilung des Gefahren- und Schadenpotentials werden über die Mitgliedstaaten zusammengetragen.

Im Rat beschäftigt sich der Ratsvorsitz (der zugleich Vorsitzender der Horizontalen Gruppe »Fragen des Cyberraums« [HWPCI] ist) oder der Ausschuss der Ständigen Vertreter (AStV) mit Cybersicherheitsvorfällen. Unterstützt wird er dabei durch das Generalsekretariat des Rates oder das Politische und Sicherheitspolitische Komitee (PSK, Grafik 2, rechts Mitte). Auf der Arbeitsebene ist die HWP Cyber die zentrale Instanz für die Attribution.[32] Hier wird insbesondere

30 Die Ermittlungen in Strafverfahren bei Fällen von Cyberangriffen werden von den nationalen Strafverfolgungsbehörden durchgeführt. Dabei werden diese von Europol und der Joint Cybercrime Action Taskforce (JCAT) beim European Cybercrime Centre (EC3) unterstützt.

31 Seit 2018 greift die EU auf das EU Law Enforcement Emergency Response Protocol (EU LE ERP) in Federführung von Europol zurück.

32 Rat der Europäischen Union, »Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die Integrierte EU-Regelung für die politische Reaktion auf Krisen«, in: *Amtsblatt der Europäischen Union*, (17.12.2018) L 320/28, <https://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=CELEX:32018D1993&from=EN> (Zugriff am 2.6.2021). Cybersicherheit soll zudem in die »Integrierte Regelung für die politische Reaktion auf Krisen« (IPCR) auf Ratsebene einbezogen werden.

mit Hilfe der Rechtsabteilung der faktische juristische Gehalt und die Verlässlichkeit der Information hinterfragt. Letzteres erfordert stets eine Rückfrage an INTCEN/SIAC. Die Einstufung des Cybervorfalls folgt einem sprachlich festgelegten Codex (Probability Yardstick). Die Mitgliedstaaten verwenden ein vergleichbares standardisiertes System, um Aussagen, die forensisch nicht bewiesen sind, überhaupt einordnen zu können. Für die HWP Cyber ist das Ziel der politischen Attribution, zu einem gemeinsamen Lagebild zu gelangen. Die Bereitschaft der Mitgliedstaaten, an dieser Arbeit mitzuwirken, ist mit der Vielzahl öffentlich zugänglicher forensischer Fakten über die Indicators of Compromise (IoC) gestiegen. Diese werden oftmals von privaten Sicherheitsanalysefirmen dokumentiert und sind allgemein verfügbar.

Als Beweise zum Erlass von Cybersanktionen kommen umfassende nachrichtendienstliche Erkenntnisse, öffentlich zugängliche Informationen, auch solche über die möglichen Interessen des Angreifers, aber ebenso technische Daten in Frage. Die Beweise können aber durchaus auch für Ermittlungen in Strafverfahren fundamental sein.[33] Auf EU-Ebene folgt eine Beratung im Ausschuss der Ständigen Vertreter (AStV II). Dort wird entschieden, ob weitere Ermittlungen für notwendig erachtet werden oder ob der Rat Sanktionen erlassen kann. Gemäß Artikel 31 Absatz 1 EU-Vertrag (EUV) muss der Rat die Beschlüsse einstimmig fassen. Die verantwortlichen natürlichen oder juristischen Personen, Organisationen oder Einrichtungen können dann in die Durchführungsverordnung aufgenommen, sprich auf die Sanktionsliste gesetzt werden.[34] Bei einem Ratsbeschluss zur GASP handelt es um einen Rechtsakt ohne Gesetzescharakter, jedoch sind die Umsetzungsbeschlüsse und Verordnungen des Rates nach Artikel 28 Absatz 2 EUV über Cybersanktionen bindend.[35]

Die Cyber Diplomacy Toolbox als Stufenplan

Der Europäische Rat bzw. der Rat für auswärtige Angelegenheiten stimmt der Attribution zu und ist für die Gegenreaktion auf Cyberangriffe zuständig. Das Maßnahmenrepertoire der Cyber Diplomacy Toolbox deckt sich weitgehend mit dem klassischen GASP-Instrumentarium. Allerdings ist die Toolbox als konkreter Stufenplan mit steigendem Eskalationspotential konzipiert. Die Zuordnung eines Cyberangriffs zu einem Urheber ist hierfür eine notwendige Vorbedingung. Jede einzelne Eskalationsstufe mit der entsprechenden diplomatischen, politischen bzw. völkerrechtskonformen Reaktion setzt einen einstimmigen Ratsbeschluss voraus (siehe Tabelle 2, S. 20).

In der Cyberdiplomatie kann ein breites Spektrum an GASP-Instrumenten eingesetzt werden.

Die GASP-Instrumente, die in der Cyberdiplomatie zum Einsatz kommen können, erstrecken sich über ein Spektrum, das von präventiven, kooperativen, stabilisierenden, restriktiven Maßnahmen bis hin zu völkerrechtskonformen Strafmaßnahmen zur Selbstverteidigung reicht. Intensität und Tragweite möglicher Reaktionen auf Cyberangriffe nehmen entsprechend dem Stufenplan zu.[36] Die EU-Cyber-Diplomacy-Toolbox und die darin katalogisierten Cybersanktionen erfüllen eine »signaling«-Funktion. Die EU macht damit für jede Konflikteskalationsstufe ihre zu erwartende diplomatische Gegenreaktion transparent.[37] Potentielle Angreifer sollen durch die Androhung rechtlicher, wirtschaftlicher und militärischer Sanktionen von böswilligen Handlungen abgehalten werden: »Sanktionen sind als eine der Optionen, die der EU-Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (die sogenannte *Cyber Diplomacy Toolbox*) zur Verfügung

33 Council of the European Union, *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*, 9.10.2017, <https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf> (Zugriff am 2.6.2021).

34 Matthias Monroy, »EU beschließt System für Cyber-Sanktionen«, *Telepolis*, 20.5.2019, <https://www.heise.de/tp/features/EU-beschliesst-System-fuer-Cyber-Sanktionen-4426777.html> (Zugriff am 7.6.2021). Umgesetzt werden die Sanktionen durch die Mitgliedstaaten entlang der Leitlinien im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU (Dok. 15579/03) in der Fassung von 2017.

35 Vgl. Art. 24 Abs. 1 Satz 3 EUV in Verbindung mit (i.V.m.) Art. 31 Abs. 1 Unterabsatz 1 Satz 2.

36 Annegret Bendiek, *Die EU als Friedensmacht in der internationalen Cyberdiplomatie*, Berlin: Stiftung Wissenschaft und Politik, März 2018 (SWP-Aktuell 22/2018), <https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2018A22_bdk.pdf>.

37 Vgl. James D. Fearon, »Signaling Foreign Policy Interests«, in: *Journal of Conflict Resolution*, 41 (1997) 1, S. 68–90; Florian J. Egloff/Myriam Dunn Cavelty, »Attribution and Knowledge Creation Assemblages in Cybersecurity Politics«, in: *Journal of Cybersecurity*, 7 (2021) 1, doi: 10.1093/cybsec/tyab002.

stellt, darauf ausgerichtet, *fortgesetzte und zunehmende böswillige Handlungen im Cyberraum* zu *verhindern*, von ihnen *abzuschrecken* und auf sie zu *reagieren*.«[38]

So kann der Toolbox je nach Schwere eines Cybervorfalls eine passgenaue diplomatische und/oder angemessene völkerrechtskonforme Reaktion entnommen werden. Während die präventiven und kooperativen Maßnahmen weitgehend den klassischen Instrumenten der diplomatischen Vermittlung ähneln, zielen die stabilisierenden und restriktiven Maßnahmen auf die konkrete Gefahrenabwehr. Die völkerrechtskonforme Reaktion wird autonom von den Staats- und Regierungschefs der EU beschlossen.

Diese Einstufung trägt dazu bei, dass das Handeln der EU für Dritte erwartbar und damit verlässlicher erscheint.

Präventive Maßnahmen haben eine geringe Intensität und erfordern nicht unbedingt eine Attribution. Unter diese Kategorie fallen Formate für politische Dialoge mit Drittstaaten, die mit der Hoffnung verbunden sind, durch Informationsaustausch und eine Vertiefung der Zusammenarbeit auf das Verhalten und die Position der Partner Einfluss nehmen zu können.

Kooperative Maßnahmen umfassen zum Beispiel EU-Demarchen, also diplomatische Protestnoten, die auf Weisung des Hohen Vertreters (HR) von der EU-Delegation im jeweiligen Gastland übergeben werden können. Demarchen können auch gemeinsam mit Drittstaaten vorgetragen werden.

Stabilisierende Maßnahmen: Hierbei einigt sich der Rat einstimmig auf eine Aktion oder einen Gemeinsamen Standpunkt der EU. Umsetzungsakte setzen einen einstimmigen Beschluss voraus. Artikel 31 Absatz 2 EUV lässt aber zu, dass Durchführungsbeschlüsse mit qualifizierter Mehrheit gefasst werden, es sei denn, sie hätten militärische oder verteidigungspolitische Bezüge. Dies könnte entsprechenden Entscheidungen im Bereich der Cyberdiplomatie die Tür öffnen. Bisher wurde von dieser Möglichkeit nicht Gebrauch gemacht. Ein schwächeres Signal kann der Hohe Vertreter im Namen der EU aussenden, indem er eine Erklärung abgibt, zu der der Rat zuvor seine Einwilligung geben muss. Eine Erklärung des HR »im Namen der EU« ergeht zumeist in denjenigen Fällen, in denen ein EU-Standpunkt angesichts einer neuen Situation erst erarbeitet oder eine bestehende Position angepasst werden muss. Der HR kann aber durchaus auch eine Erklärung in eigener Verantwortung abgeben, wenn eine schnelle Reaktion erforderlich und eine Abstimmung im Kreis der EU-27 nicht möglich ist. Allerdings wird in der internationalen Diplomatie registriert, ob alle EU-Staaten dieser Erklärung zugestimmt haben oder eben nicht. Entsprechend ist ihre Wirkung einzustufen.

Restriktive Maßnahmen: Die EU kann zur Durchsetzung politischer Ziele infolge von schwerwiegenden Cyberangriffen restriktive Maßnahmen verhängen. Solche Sanktionen stellen aktuell die höchste Eskalationsstufe vor den völkerrechtskonformen Reaktionen dar. Sie sind sozusagen der »Hammer« im EU-Werkzeugkasten (und werden auch als solche bezeichnet), da sie schmerzhafte ökonomische Effekte bei Drittakteuren auslösen sollen. Restriktive Maßnahmen richten sich in der Regel gegen Vertreter von Regierungen bestimmter Drittstaaten, aber auch gegen Staatsfirmen oder andere juristische und natürliche Personen. Sie müssen vom Rat einstimmig beschlossen werden und im Einklang mit den in Artikel 24 EUV genannten Zielen der GASP stehen.

In der EU gilt das Gebot, dass Sanktionen immer gezielt sein sollten (targeted sanctions).[39] Nachdem sich Handelsembargos in der Vergangenheit als wenig wirksam erwiesen haben, verhängt die EU als Reaktion auf böswillige Aktivitäten im Cyber- und Informationsraum in der Regel gezielte Maßnahmen wie Kontensperrungen sowie Einreise- und Investitionsverbote.[40] Listungen von Personen und Unternehmen, Kontensperrungen oder Einreisebeschränkungen gelten in allen Mitgliedstaaten. Die Betroffenen haben grundsätzlich die Möglichkeit, gegen den Erlass von Sanktionen mit rechtsstaatlichen Mitteln vorzugehen. Gegen die Listung im Wege einer Durchführungsverordnung besteht Rechtsschutz über die Nichtig-

38 Rat der Europäischen Union, »Böswillige Cyberangriffe: EU-Sanktionen gegen zwei Personen und eine Einrichtung wegen Hackerangriff auf den Bundestag 2015«, Pressemitteilung«, 22.10.2020 (Hervorhebungen im Original), <https://www.consilium.europa.eu/de/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/> (Zugriff am 14.9.2021).

39 Rat der Europäischen Union, *Sanktionen: Wann und wie die EU restriktive Maßnahmen verhängt*, 13.7.2021, <https://www.consilium.europa.eu/de/policies/sanctions/> (Zugriff am 13.7.2021).

40 Patryk Pawlak / Thomas Biersteker, *Guardian of the Galaxy. EU Cyber Sanctions and Norms in Cyberspace*, Paris: European Institute for Security Studies, Oktober 2019 (Chaillot Paper 155), S. 9, <https://www.iss.europa.eu/content/guardian-galaxy-eu-cyber-sanctions-and-norms-cyberspace> (Zugriff am 6.5.2021).

Tabelle 2

Cyberdiplomatischer Reaktionsrahmen der EU (Cyber Diplomacy Toolbox), extrahiert aus: siehe Quelle

Präventive Maßnahmen	Kooperative Maßnahmen	Stabilisierende Maßnahmen	Restriktive Maßnahmen	Völkerrechtskonforme Maßnahmen
■ Vertrauens- und sicherheitsbildende Dialoge ■ Kapazitätsaufbau in Drittstaaten ■ *awareness raising*	■ EU-Demarchen (ggf. in Kooperation mit Drittstaaten) ■ Diplomatische Protestnoten	■ Gemeinsamer Standpunkt des Europäischen Rates ■ GASP-Beschluss ■ Erklärungen des HR im Namen des Rates ■ Erklärung des HR	■ Maßnahmen nach Art. 215 AEUV/ GASP-Beschluss Titel V Kapitel 2 EUV ■ Kontensperrungen ■ Reisebeschränkungen	■ Solidaritätsklausel (Art. 222 AEUV) ■ Beistandsklausel (Art. 42 (7) EUV) im Einklang mit Artikel 51 UN-Charta (Recht auf Selbstverteidigung)
Resilienz (Resilience)		**Abwehr (Denial)**		**Vergeltung (Retaliation)**
	Beispiele: ■ (Non public) Demarche »on the need to respect the rules-based order in cyberspace« (April 2019) ■ (Non public) Demarche »on the need to respect the rules-based order in cyberspace« (November 2019)	**Beispiele:** ■ Ratsschlussfolgerungen zu WannaCry und NotPetya (April 2018) ■ »Common messages« (2018) ■ Erklärung HR/VP, Präsidenten von Europäischem Rat und EU-Kommission zum OVCW-Angriff (Oktober 2018) ■ Erklärung des HR im Namen der EU »to respect the rules-based order in cyberspace« (April 2019)	**Beispiele:** ■ Horizontales Cybersanktionsregime (Mai 2019) ■ »Koordinierte Attribution auf EU-Ebene« (Annex zu den Umsetzungsrichtlinien, Juni 2019) ■ Ratsverordnungen (Juli 2020)	

Quellen: Rat der Europäischen Union, *Entwurf von Schlussfolgerungen des Rates über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (»Cyber Diplomacy Toolbox«) – Annahme*, Brüssel, 7.6.2017, und Council of the European Union, *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*, Brüssel, 9.10.2017.

keitsklage nach Artikel 263 IV AEUV vor dem Europäischen Gerichtshof (EuGH).

Restriktive Maßnahmen im Rahmen der GASP sind das invasivste Instrument, das die Cyber Diplomacy Toolbox unterhalb der Schwelle eines bewaffneten Konflikts vorsieht. Allerdings klafft im Werkzeugkasten eine große Lücke zwischen den Mitteln, die für den zivilen, und denen, die für den militärischen

Konfliktaustrag als höchste Eskalationsstufe zur Verfügung stehen.

Völkerrechtskonforme Reaktion: Die Anwendung der Solidaritäts- und Beistandsklauseln, die erst mit dem Vertrag von Lissabon Teil des EU-Acquis geworden sind, ist ebenfalls eine Option im Falle eines schwerwiegenden Cyberangriffs gegen einen Mitgliedstaat oder die EU als Ganze. Die Solidaritätsklausel nach Artikel 222 AEUV sieht vor, dass sich die EU-Staaten gegenseitig unterstützen, wenn einer oder mehrere von ihnen Opfer von Terroranschlägen, Naturkatastrophen oder von Menschen verursachten Katastrophen — und damit auch von schwerwiegenden Cybervorfällen — geworden ist bzw. sind.

Das schärfste Reaktionsmittel wäre die Aktivierung der Beistandsklausel nach Artikel 42 Absatz 7 EUV. Die Bestimmung entspricht in etwa Artikel 5 des Nato-Vertrags, verhält sich jedoch für Nato-Mitglieder hierzu subsidiär. Konkret heißt dies, dass »im Falle eines bewaffneten Angriffs auf das Hoheitsgebiet eines Mitgliedstaats« die anderen Mitgliedstaaten im Einklang mit Artikel 51 der UN-Charta (Recht zur Selbstverteidigung) Hilfe leisten müssen.[41] Beide Klauseln können nur bei Cyberangriffen angewandt werden, die einen Verstoß gegen das Gewaltverbot (Art. 2.4 UN-Charta) als *jus cogens* darstellen.

Das Recht auf eine militärische Selbstverteidigung gegen Cyberattacken geht allerdings mit hohen Anforderungen einher: Zum einen muss eine Cyberoperation hinsichtlich Umfang und Wirkung mit dem Einsatz von Waffengewalt vergleichbar sein, um entsprechend eingestuft werden zu können. Außerdem muss die Operation entweder direkt oder indirekt einem Staat zurechenbar sein bzw. muss sich dessen Verantwortlichkeit (gerichtsfest) nachweisen lassen.

Nur wenige Mitgliedstaaten sind technisch zu reaktiven defensiven Cyber-Gegenschlägen oder eigenen Cyberoperationen in der Lage.

Cybersanktionen müssen nicht notwendigerweise auf die oben beschriebenen klassischen Instrumente der Gemeinsamen Außen und Sicherheitspolitik oder der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU beschränkt bleiben. Sie können von den Mitgliedstaaten auch digital im Cyber- und Informationsraum beantwortet werden.[42] So haben die Staats- und Regierungschefs im Rat die Möglichkeit, als letztes Mittel der Toolbox eine »aktive« Cyberverteidigung in Form eines digitalen Vergeltungsschlags (»hack back«) zu beschließen, wie er auch von anderen Cybermächten, zum Beispiel den USA oder Israel, durchgeführt wird. Reaktive defensive Cyber-Gegenschläge bzw. eigene Cyberoperationen in Drittstaaten sind unter bestimmten Voraussetzungen möglich, etwa zur Gefahrenabwehr. Aktuell sind aber nur einige wenige Mitgliedstaaten technisch dazu in der Lage.

Solche Gegenschläge zielen auf IT-Sicherheitsschwachstellen, deren Ausnutzung die EU im Einklang mit ihrer Cybersicherheitsstrategie grundsätzlich vermeiden will. Cyberoperationen in fremden Netzen in Friedenszeiten können eine Souveränitätsverletzung darstellen.[43] Das Risiko, statt des Täters ein anderes Opfer auszuschalten oder erhebliche Kollateralschäden bei Unbeteiligten zu erzeugen, ist schwer zu bemessen. Auch dies steht im Widerspruch zur EU-Cyberstrategie, die auf Konfliktprävention statt Eskalation, auf das Mitigieren statt Ausnutzen von IT-Unsicherheiten sowie auf vertrauens- und sicherheitsbildende Maßnahmen und eine rechtsstaatlich und völkerrechtlich legitimierte Cyberdiplomatie setzt.

41 Europäische Union, *EU-Vertrag* (Vertrag über die Europäische Union), 1.12.2009, <https://dejure.org/gesetze/EU> (Zugriff am 2.6.2021).

42 Rat der Europäischen Union, *Sanktionen* [wie Fn. 39].

43 Jack Goldsmith / Alex Loomis, *»Defend Forward« and Sovereignty*, Stanford, CA: Hoover Institution, April 2021 (Aegis Series Paper Nr. 2102), <https://www.hoover.org/sites/default/files/research/docs/goldsmith-loomis_webreadypdf.pdf>; Jason Healey, »Memo to POTUS: Responding to Cyber Attacks and PPD-20«, *The Cipher Brief*, 24.5.2018, <https://www.thecipherbrief.com/column_article/memo-potus-responding-cyber-attacks-ppd-20>.

Fallstudien: EU-Cybersanktionen und ihre Attributionen

Die im Folgenden dargestellten Cyberangriffe WannaCry 2017, NotPetya 2017, Operation Cloud Hopper 2017, Bundestag-Hack 2015 und der versuchte Angriff auf die Organisation für das Verbot chemischer Waffen (OVCW) 2018 bildeten die Grundlage für die Verhängung der ersten EU-Cybersanktionen durch den Rat der Europäischen Union im Juli 2020. Bereits im Mai 2019 hatte der Rat sie als böswillige Cyberangriffe mit erheblichen Auswirkungen auf die Sicherheit der Union und ihrer Mitgliedstaaten eingestuft.[44] Die Europäische Kommission und die Hohe Vertreterin haben den Erlass von Cybersanktionen mit einer hybriden Bedrohung der Union begründet.[45] Die genannten Fälle werden im Folgenden untersucht, um das Verfahren der Attribution der EU auf der technischen, politischen und rechtlichen Ebene nachzuvollziehen. Die Analyse erfolgt entlang der in der Ratsverordnung (EU) 2019/796 und im Ratsbeschluss (GASP) 2019/797 definierten Tatbestandsmerkmale (vgl. oben, Tabelle 1, S. 14f).[46] Im Folgenden werden anhand des ersten Cybersanktionsregimes und der Cybervorfälle, die ihm zugrunde liegen, die Diskrepanzen verdeutlicht zwischen einer rechtlich notwendigen und einer politisch hinreichenden Attribution.

WannaCry 2017

Der WannaCry-Cyberangriff begann am 12. Mai 2017 und dauerte nur einige Tage an. WannaCry war eine Erpressersoftware (Ransomware). Bei Angriffen dieser Art findet ein Eingriff in Informationssysteme statt, auf das Zielsystem wird eine Schadsoftware aufgespielt, die Daten werden verschlüsselt. Diese sind für die Nutzerin und den Nutzer so lange nicht verfügbar, bis sie durch Lösegeldzahlungen meist in Bitcoin wieder freigekauft werden.[47] Die Schadsoftware verbreitete sich selbständig, genauer gesagt wurmartig auf verwundbaren Zielsystemen.[48] Diese Verbreitungstechnik basierte auf einem zuvor von der US-amerikanischen National Security Agency (NSA) entwendeten Exploit namens Eternalblue, der auch in der NotPetya-Attacke und in chinesischen APT-

44 Rat der Europäischen Union, »Verordnung (EU) 2019/796« [wie Fn. 25], Art. 2.

45 Europäische Kommission / Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, *Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union*, Brüssel, 6.4.2016 (JOIN/2016/18 final), <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52016JC0018> (Zugriff am 2.6.2021).

46 Rat der Europäischen Union, »Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen«, in: *Amtsblatt der Europäischen Union*, (17.5.2019) L 129 I/13, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019D0797&rid=11> (Zugriff am 2.6.2021); ders., »Verordnung (EU) 2019/796« [wie Fn. 25].

47 Berichte, ob in diesem Fall die Daten nach Zahlung des Lösegelds wieder freigegeben wurden, sind widersprüchlich; Brian Krebs, »Global ›Wana‹ Ransomware Outbreak Earned Perpetrators $26,000 so Far«, *Krebs on Security*, 13.5.2017, <https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/> (Zugriff am 2.6.2021).

48 Zammis Clark, »The Worm That Spreads WanaCrypt0r«, *Malwarebytes*, 12.5.2017, <https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/>; Austin McBride, »The Hours of WannaCry«, *Cisco Umbrella* (online), 16.5.2017, <https://umbrella.cisco.com/blog/the-hours-of-wannacry> (Zugriff jeweils am 2.6.2021).

(Advanced Persistent Threat)-Kampagnen entdeckt wurde.[49] Eternalblue nutzte dabei eine fehlerhafte Implementierung des SMB-Protokolls von Microsoft, um auf Dateien und Drucker anderer Rechner desselben Netzwerks zuzugreifen. Dadurch konnte sich die Schadsoftware ohne eine vorangegangene Nutzerinteraktion von Rechner zu Rechner schlängeln, solange Microsoft die Sicherheitslücken in seinem Windows-Betriebssystem durch neueste Patches nicht schließen konnte.[50]

Opfer, Schäden und Operationsziel

Nach Medienberichten waren etwa 230.000 Computer in rund 150 Ländern von dem WannaCry-Angriff betroffen, darunter auch EU-Mitgliedstaaten. Die sogenannte Wurmfähigkeit der Software ermöglichte WannaCry eine unkontrollierbare Verbreitung und löste zahlreiche Kollateraleffekte aus. Zur Entschlüsselung von Daten wurden Lösegeldzahlungen in Höhe von circa 35.000 US-Dollar geleistet. Der Gesamtschaden wurde auf rund vier Milliarden US-Dollar geschätzt.[51] Opfer der Attacke waren Unternehmen wie Télefonica und O_2 (Spanien und EU), DB Schenker (eine Tochterfirma der Deutschen Bahn), FedEX (USA), Renault (Frankreich), Nissan in Großbritannien, Sony Pictures (USA), die Telekommunikationsunternehmen Vivo (Brasilien) und MegaFon (Russland), Sandvik (Schweden), PetroChina und chinesische Tankstellen. Ferner waren der Banco Bilbao Vizcaya Argentaria (Spanien), die Bangladesh-Bank, die Tien Phong Bank (Vietnam),[52] das russische Innen- und Katastrophenschutzministerium, das rumänische Außenministerium und die polnische Finanzaufsichtsbehörde betroffen.[53] Die UK National Health Services und zahlreiche britische Krankenhäuser mussten ihre Arbeit einstellen.[54] Der Schaden in Großbritannien wurde auf circa 92 Millionen Pfund beziffert. Mehr als 19.000 Behandlungen konnten nicht durchgeführt werden. Auswirkungen auf die Gesundheit und das Leben von Patienten nahmen die Hacker in Kauf.[55] Die Ticketautomaten der Deutschen Bahn fielen aus, Erpressernachrichten erschienen auf zahlreichen Anzeigetafeln.[56]

Das strategische Ziel der Operation ist vergleichsweise schwer zu bestimmen. Der Wurm-Charakter, die Verwendung eines NSA-Exploits, der eingebaute »Notausschalter«, ein sogenannter Kill-Switch (über einen im Schadcode oder im Firewall-Log nachlesbaren Domainnamen), und die Notwendigkeit einer manuellen Entschlüsselung infizierter Rechner sprechen dafür, dass WannaCry auf eine kleinere Disruption und einen Konflikt mit der NSA ausgerichtet war. Gegen kriminelle Motive spricht ein gewisser Dilettantismus, der nicht mit einer professionellen Ransomwarekampagne zu vereinbaren ist: »Hoher Schaden, hohe Publicity, sehr hohe Sichtbarkeit für Strafverfolgungsbehörden und vermutlich die geringste Profitmarge, die wir bisher von moderaten oder gar kleinen Ransomwarekampagnen gesehen haben«, so der Cybersecurity-Forscher Craig Williams.[57] Vermutet wurde auch, dass es sich um ein Ablenkungsmanöver gehandelt haben könnte, um andere Spionageoperationen zu verdecken oder die NSA-Machen-

49 Andy Greenberg, »The Strange Journey of an NSA Zero-Day — Into Multiple Enemies' Hands«, *Wired* (online), 7.5.2019, <https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/> (Zugriff am 2.6.2021).

50 Alex Berry / Josh Homan / Randy Eitzman, »WannaCry Malware Profile«, *FireEye*, 23.5.2017, <https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html> (Zugriff am 2.6.2021).

51 Christof Windeck, »WannaCry: Gewaltiger Schaden, geringer Erlös«, *Heise Online*, 14.5.2017, <https://www.heise.de/security/meldung/WannaCry-Gewaltiger-Schaden-geringer-Erloes-3713689.html> (Zugriff am 2.6.2021).

52 Volker Briegleb, »Ransomware WannaCry befällt Rechner der Deutschen Bahn«, *Heise Online*, 13.5.2017, <https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html>; Stefan Betschon, »Wanna Cry: Bilanz des Hackerangriffs in 150 Ländern«, in: *Neue Zürcher Zeitung* (online), 15.5.2017, <https://www.nzz.ch/international/computersicherheit-cyberangriff-gefaehrdet-windows-pc-rund-um-die-welt-ld.1293201> (Zugriff jeweils am 2.6.2021).

53 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017*, Wiesbaden, Juli 2018, <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html> (Zugriff am 2.6.2021).

54 »NHS Services Still Facing Cyber Threat«, *BBC News* (online), 15.5.2017, <https://www.bbc.com/news/uk-39921479> (Zugriff am 2.6.2021).

55 Saira Ghafur et al., »A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS«, in: *npj Digital Medicine*, 2 (2019).

56 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* [wie Fn. 53], S. 12.

57 Andy Greenberg, »The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes«, *Wired* (online), 15.5.2017, <https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/> (Zugriff am 2.6.2021).

schaften bloßzustellen. WannaCry könnte schließlich auch ein »last resort effort« gewesen sein, also eine Maßnahme, mit der noch politisches Kapital aus einer zuvor aufgeflogenen Geheimdienstoperation geschlagen werden sollte.[58]

Attribution der Angreifer

Im Juni 2017, nur zwei Monate später, trugen die NSA und der britische Nachrichtendienst GCHQ (Government Communications Headquarters) mit »moderater Gewissheit« vor, dass Nordkoreas »Generalbüro für Aufklärung« mit dem Cyberangriff »WannaCry« in Verbindung stehe.[59] Die öffentliche politische Attribution an Nordkorea durch die Regierungen Großbritanniens und der USA erfolgte ein halbes Jahr später am 18. Dezember 2017. Sanktionen haben die USA nicht umgehend verhängt.[60] Das UK National Cyber Security Centre (NCSC) erklärte, mit einer »hohen Wahrscheinlichkeit« sei die nordkoreanische Gruppe »Lazarus« bzw. »APT 38« für die Angriffe verantwortlich. Die Five Eyes (Großbritannien, USA, Australien, Neuseeland, Kanada) und Japan stellten sich hinter diese Verurteilung. Konkrete Beweise legten die Regierungen nicht vor. Umso bemerkenswerter ist es, dass die Symantec-Mitarbeiterin Amy L. Johnson bereits einige Monate zuvor, Ende Mai 2017, eine Verbindung zur APT-Gruppe Lazarus gezogen hatte.[61] Die Security-Researcher Rafael Amado und Pasquale Stirparo vermuteten den Ursprung von WannaCry hingegen nicht in Nordkorea.[62] Ebenfalls im Mai 2017 hatte die Sicherheitsfirma Symantec aufgedeckt, dass frühere, im Internet kursierende Versionen von WannaCry, die vermutlich auf Malware-Testläufe zurückzuführen sind, Ähnlichkeiten mit den TTPs (Tools, Techniques/Tactics & Procedures) der Lazarus-Gruppe aufwiesen.[63] Komponenten von WannaCry seien als eine Weiterentwicklung der Cyberoperation gegen Sony Pictures aus dem Jahr 2014 identifiziert worden. Dass bei WannaCry und Sony-Hack dieselben Passwörter für Zip-Dateien verwendet wurden, wird als Indiz dafür gesehen, dass die Malware von derselben Gruppe geschrieben wurde.[64] Zudem glichen sich die Bitcoin-Konten der Kampagnen, was auf einen identischen Urheber hindeutet.[65] Dafür, dass es sich um die gleiche Akteursgruppe handelt, sprechen außerdem die IP-Adressen der Command & Control-Server (C2) und die Verwendung ähnlicher Verschlüsselungstechniken zur sicheren Kommunikation. Die US-Regierung hat etwa ein Jahr später, im September 2018, die Softwareentwickler Park Jin Hyok, Jon Chang Hyok und Kim Il als Mitarbeiter der E-Commerce-Firma Chosun Expo angeklagt. Die Firma gehört dem nordkoreanischen Staat.[66] In den TTPs von Lazarus fanden sich Rückbezüge auf Nutzerinnenaccounts, gefälschte Online-Identitäten (Fake Online Personas), Passwörter, mehrfach verwendeter Software-Code und IP-Adressen, die der Firma Chosun Expo gehörten bzw. zugeordnet werden können.[67]

58 Rafael Amado, »WannaCry: An Analysis of Competing Hypotheses«, *Digital Shadows* (online), 18.5.2017, <https://www.digitalshadows.com/blog-and-research/wannacry-an-analysis-of-competing-hypotheses/> (Zugriff am 2.6.2021).

59 Ellen Nakashima, »The NSA Has Linked the WannaCry Computer Worm to North Korea«, in: *The Washington Post* (online), 14.6.2017, <https://wapo.st/3EnCyoP> (Zugriff am 2.6.2021).

60 »Cyber-attack: US and UK Blame North Korea for WannaCry«, *BBC News* (online), 19.12.2017, <https://www.bbc.com/news/world-us-canada-42407488> (Zugriff am 2.6.2021).

61 Amy L. Johnson, »WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group«, *Broadcom*, 22.5.2017, <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269> (Zugriff am 2.6.2021).

62 Amado, »WannaCry. An Analysis« [wie Fn. 58]; Pasquale Stirparo, »Analysis of Competing Hypotheses, WCry and Lazarus (ACH part 2)«, *Internet Storm Center*, 31.5.2017, <https://isc.sans.edu/forums/diary/Analysis+of+Competing+Hypotheses+WCry+and+Lazarus+ACH+part+2/22470/> (Zugriff am 2.6.2021).

63 Johnson, »WannaCry« [wie Fn. 61].

64 Joseph Menn, »Symantec Says ›Highly Likely‹ North Korea Group behind Ransomware Attacks«, *Reuters*, 23.5.2017, <https://www.reuters.com/article/us-cyber-attack-northkorea-idUSKBN18I2SH> (Zugriff am 2.6.2021).

65 Details dazu auch in der Anklageschrift der US-Justiz: United States District Court for the Central District of California, *United States of America v. Park Jin Hyok*, Juni 2018, <https://www.justice.gov/opa/press-release/file/1092091/download> (Zugriff am 14.9.2021).

66 Ebd.

67 Catalin Cimpanu, »How US Authorities Tracked Down the North Korean Hacker behind WannaCry«, *ZDNet* (online), 6.9.2018, <https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/> (Zugriff am 13.5.2021).

EU-Reaktion auf WannaCry

Am 16. April 2018 veröffentlichte der Rat Schlussfolgerungen, in denen er die böswillige Nutzung von Informations- und Kommunikationstechnologien in Form der WannaCry- und NotPetya-Attacke verurteilte. Erst zwei Jahre später aber, Ende Juli 2020, verhängte er mit der Durchführungsverordnung 2020/1125[68] wirtschaftliche Strafmaßnahmen gegen das Unternehmen Chosun Expo.[69] Es handelt sich um gezielte Sanktionen (»Smart Sanctions«). Dabei wurden sämtliche Gelder und wirtschaftlichen Ressourcen eingefroren, die Eigentum oder Besitz der natürlichen oder juristischen Personen, Organisationen oder Einrichtungen sind oder von diesen gehalten oder kontrolliert werden. Den sanktionierten Personen, Organisationen oder Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden.

Der Verantwortungszuschreibung an Lazarus/APT38 gingen aufwendige diplomatische Bemühungen voraus.

Der Verantwortungszuschreibung an Lazarus/APT38 gingen aufwendige diplomatische Bemühungen voraus. Die Attribution stützte sich vorwiegend auf Informationen von US-Sicherheitsdiensten. Die Anklage gegen Park Jin Hyok — laut US-Justiz[70] ein Mitarbeiter einer Strohfirma im Dienst der nordkoreanischen Regierung — beruhte auf rund 1.000 beschlagnahmten E-Mail- und Social-Media-Konten, 85 internationalen Rechtshilfeersuchen und profitierte von der Zuarbeit der Firmen Mandiant und FireEye.[71] Die Klageschrift (»Criminal Complaint«) gegen Park Jin Hyok zeigt auf, wie Person, E-Mail-Adressen, die IT-Infrastruktur für den Angriff, Opfer und Malware-Familien zusammenhängen.[72]

Estland,[73] die Niederlande,[74] Frankreich,[75] Großbritannien,[76] Australien[77] und die USA[78] begrüßten ebenfalls die restriktiven Maßnahmen der EU, um die Signalwirkung gegen die Verantwortlichen zu verstärken. Die USA attribuierten den Angriff im Juni 2017 an Nordkorea,[79] Großbritannien[80] folgte im Oktober 2017.[81] Das UN-Büro für Drogen- und Verbrechensbekämpfung, namentlich dessen Chef Neil Walsh, verurteilte zwar die WannaCry-Attacke als kriminellen Akt, völkerrechtliche Maßnahmen wurden aber nicht ergriffen.[82]

68 Rechtliche Grundlage ist Artikel 13 VO (EU) 2019/796 (i.V.m. Art. 215 AEUV und Art. 21 EUV).
69 Artikel 3 Absatz 1 und 2 VO (EU) 2019/796.
70 US Department of Justice, *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*, Washington, D.C., 6.9.2018, <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and> (Zugriff am 2.6.2021).
71 US District Court for the Central District of California, *United States of America v. Park Jin Hyok* [wie Fn. 65], S. 2.
72 Ebd., S. 175.
73 Republic of Estonia, Ministry of Foreign Affairs, »The EU Implements Its Cyber Sanctions Regime for the First Time«, Tallinn, 30.7.2020, <https://vm.ee/en/news/eu-implements-its-cyber-sanctions-regime-first-time> (Zugriff am 1.10.2021).
74 Government of the Netherlands, »Blok: ›EU Condemns Malicious Behaviour in Cyberspace‹«, 30.7.2020, <https://www.government.nl/latest/news/2020/07/30/eu-condemns-malicious-behaviour-cyberspace> (Zugriff am 1.10.2021).
75 France Diplomacy, *EU – Cyberattacks – Q&A from the Press Briefing*, 30.7.2020, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20> (Zugriff am 1.10.2021).
76 »UK and Allies Reveal Global Scale of Chinese Cyber Campaign«, Press Release, *GOV.UK*, 20.12.2018, <https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign> (Zugriff am 1.10.2021).
77 Australian Government, Department of Foreign Affairs and Trade, *European Union Cyber Sanctions Listings*, 1.8.2020, <https://www.dfat.gov.au/news/media-release/european-union-cyber-sanctions-listings> (Zugriff am 1.10.2021).
78 U.S. Department of State, »The United States Applauds the EU's Action on Cyber Sanctions«, Press Statement of Michael R. Pompeo, Secretary of State, 30.7.2020, <https://2017-2021.state.gov/the-united-states-applauds-the-eus-action-on-cyber-sanctions/index.html> (Zugriff am 1.10.2021).
79 Jack Goldsmith, »The Strange WannaCry Attribution«, *Lawfare*, 21.12.2017, <https://www.lawfareblog.com/strange-wannacry-attribution> (Zugriff am 1.10.2021).
80 »UK and Allies Reveal Global Scale of Chinese Cyber Campaign« [wie Fn. 76].
81 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), »NotPetya and WannaCry Call for a Joint Response from International Community«, Tallinn, 30.6.2017, <https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/> (Zugriff am 1.10.2021).
82 Kolja Brockmann, »European Union Sanctions on North Korea: Balancing Non-proliferation with the Humanitarian Impact«, Solna: Stockholm International Peace Research Institute (SIPRI), 11.12.2020, <https://www.sipri.org/commentary/topical-background/2020/european-union-

NotPetya 2017

Am 27. Juni 2017, dem Vorabend des ukrainischen »Tags der Verfassung«, setzte eine Wiper-Malware zahlreiche Rechner weltweit, vor allem aber in der Ukraine außer Betrieb, indem sie Festplatten löschte.[83] Die Malware NotPetya gelangte über einen Supply-Chain-Angriff auf den Update-Mechanismus der ukrainischen Steuerverwaltungssoftware M.E.Doc in ein lokales Netz.[84] Die Malware breitete sich selbständig wurmartig auf Unternehmen aus, die die genannte Software nutzten. Unternehmen in zahlreichen Staaten wurden mit NotPetya infiziert.[85]

Wie ging NotPetya vor? Ist der Brückenkopf gebildet, versucht ein Modul im Arbeitsspeicher mit Hilfe des Tools Mimikatz User-Anmeldeinformationen (»credentials«) auszulesen, auch solche von Usern mit administrativen Rechten. Unter Verwendung dieser Daten wird die Schadsoftware auf andere Rechner kopiert. Der neu infizierte Rechner startet diesen Verteilungsmechanismus seinerseits. Alternativ erfolgt die Streuung in Unternehmensnetzwerken über dieselbe Komponente Eternalblue, die auch WannaCry zugrunde lag.[86] Analysen von Ende Juni 2017 klassifizierten die Schadsoftware aufgrund von Ähnlichkeiten im Code zunächst als eine Variante der Petya-Ransomware-Familie, die von Cyber-Kriminellen seit 2016 genutzt wird.[87] Das Vorgehen der Malware ähnelte Petya: Die Festplatte wird verschlüsselt, der Microsoft-Bootloader durch eine Zahlungsaufforderung ersetzt. Die Angreifer verlangten 300 US-Dollar in Bitcoin. Um Informationen zur Wiederherstellung der Daten zu erlangen, sollten die Betroffenen eine E-Mail an eine Adresse beim Berliner Provider Posteo senden. Der Anbieter sperrte das E-Mail-Konto umgehend.[88]

Opfer, Schäden und Operationsziel

Die Cyberangriffe NotPetya und EternalPetya haben weltweit 65 Länder und rund 49.000 Systeme geschädigt. Unter den Opfern waren zahlreiche Unternehmen in der EU.[89] Die eingeschleuste Ransomware blockierte den Zugriff auf Daten. Betroffene Konzerne waren unter anderem Maersk (Dänemark), Rosneft (Russland), Merck Sharp & Dohme (USA), Mondelez (USA), FedEx/TNT (USA/Niederlande), Reckitt Benckiser (UK), Saint-Gobain (Frankreich) und Beiersdorf (Deutschland). In den USA legte die Malware die Datenverarbeitungsstrukturen von 80 Krankenhäusern und medizinischen Einrichtungen des US Heritage Valley Health System lahm.[90] Den Angreifern gelang es, die ukrainischen IT-Netze, Systeme der Zentralbank, den internationalen Flughafen Kiew-Borispyl, die U-Bahn der Hauptstadt und die Agentur für die Verwaltung der Sperrzone um das havarierte Kernkraftwerk in Tschernobyl zu infiltrieren.[91] Viele

sanctions-north-korea-balancing-non-proliferation-humanitarian-impact>, und EU Sanctions Map, aktualisiert am 21.12.2020, <https://bit.ly/2Y8oYWg> (Zugriff jeweils am 1.10.2021).

83 Andy Greenberg, »The Untold Story of NotPetya, the Most Devastating Cyberattack in History«, *Wired* (online), August 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (Zugriff am 26.5.2020).

84 Jürgen Schmidt, »Petya/NotPetya: Kein Erpressungstrojaner, sondern ein ›Wiper‹«, *Heise Online*, 29.6.2017, <https://www.heise.de/security/meldung/Petya-NotPetya-Kein-Erpressungstrojaner-sondern-ein-Wiper-3759293.html> (Zugriff am 2.6.2021).

85 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* [wie Fn. 53], S. 14.

86 Für eine detaillierte Beschreibung des Bugs und der Exploitation siehe Nadav Grossman, »EternalBlue — Everything There Is to Know«, *Check Point Research*, 29.9.2017, <https://research.checkpoint.com/2017/eternalblue-everything-know/>; zur Schwachstellle CVE-2017-0144 siehe *Microsoft-Sicherheitsbulletin MS17-010*, 11.10.2017, <https://docs.microsoft.com/de-de/security-updates/securitybulletins/2017/ms17-010> (Zugriff jeweils am 14.9.2021).

87 Iain Thomson, »Everything You Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide«, *The Register* (online), 28.6.2017, <https://www.theregister.com/2017/06/28/petya_notpetya_ransomware/> (Zugriff am 2.6.2021).

88 Schmidt, »Petya/NotPetya« [wie Fn. 84].

89 Jai Vijayan, »3 Years after NotPetya, Many Organizations Still in Danger of Similar Attacks«, *Dark Reading* (online), 30.6.2020, <https://www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks/d/d-id/1338200> (Zugriff am 2.6.2021).

90 US Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, 19.10.2020, <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and> (Zugriff am 2.6.2021).

91 Jonas Jansen / Alexander Armbruster, »Hacker legen Zentralbank und Flughafen in Kiew lahm«, in: *Frankfurter Allgemeine Zeitung* (online), 27.6.2017, <https://www.faz.net/aktuell/wirtschaft/ransomware-attacke-legt-viele-unternehmen-lahm-15079944.html> (Zugriff am 2.6.2021).

der betroffenen Unternehmen sind für die Aufrechterhaltung wesentlicher Dienstleistungen der Daseinsvorsorge — teilweise in den EU-Staaten — erforderlich.[92] Weltweit verursachte der Cyberangriff einen wirtschaftlichen Gesamtschaden von circa 10 Milliarden US-Dollar.[93] Einzelne Firmen konnten ihre IT-Infrastrukturen über mehrere Wochen nicht wiederherstellen. Die dänische Reederei Maersk und der Frachtdienstleister TNT Express bezifferten ihren Schaden jeweils auf über 300 Millionen US-Dollar. NotPetya wird als eine der schwerwiegendsten und kostspieligsten Cybervorfälle angesehen.

Das Operationsziel lässt sich recht klar bestimmen: Bestimmte technische Indikatoren, wie die einzige Kontakt-E-Mail-Adresse, die einen »single point of failure« darstellt, der den Erpressungsvorgang durch simple Gegenmaßnahmen abwenden lässt, sind untypisch für kriminelles Vorgehen. Die unprofessionelle Vorgehensweise bei der Lösegeldabwicklung ließ Zweifel aufkommen, ob ein staatlicher Akteur in Frage käme. Erst später entdeckte man die Wiper-Funktionalität des Virus, also dessen Fähigkeit, einen möglichst großen Datenverlust bei den Betroffenen zu verursachen. NotPetya tarnte sich als Standard-Petya-Ransomware. Ausgerichtet war die Malware aber auf eine professionell durchgeführte politische Sabotageaktion. Im Laufe der Attribution verfestigte sich die These, dass es sich bei der NotPetya-Attacke sogar um eine großflächige Zerstörungs- und Zersetzungskampagne handelte, die gegen die Ukraine gerichtet war. Der Angriffsvektor über eine Software in der Ukraine spricht jedenfalls für eine derartige Zielfokussierung. Ob die erheblichen weltweiten Kollateralschäden intendiert waren, ist bis heute unklar; immerhin waren auch russische Unternehmen betroffen. Es ist also auch denkbar, dass NotPetya aufgrund seiner hohen Sichtbarkeit im Sinne eines »signaling« bzw. »tacit bargaining« als diplomatisches Druckmittel gegen die Ukraine eingesetzt wurde.[94]

Attribution der Angreifer

Die technische Attribution ist im Fall NotPetya kaum rekapitulierbar. Die Schadsoftware wird mit Advanced Persistent Threats in Verbindung gebracht, Angriffskampagnen, die in der IT-Sicherheitsindustrie unter Codenamen wie »Sandworm«, »BlackEnergy Group«, »Voodoo Bear«, »Iron Viking«, »Quedagh«, »Olympic Destroyer« und »Telebots« bekannt sind. Wie sich diese APT-Gruppen zueinander verhalten, ob sie identisch sind oder nur punktuell zusammenarbeiten bzw. in welcher Beziehung sie zu staatlichen Stellen in Russland stehen, war zum Zeitpunkt des Cybervorfalls nicht bekannt.

NotPetya reiht sich ein in eine mehrjährige Folge von zahlreichen Cyberangriffen dieser Akteure gegen ukrainische Unternehmen, Behörden und Energieversorger.[95] Der slowakischen IT-Sicherheitsfirma ESET zufolge nutzte die APT-Gruppe Telebots ab April 2018 eine neue Backdoor-Komponente, die Ähnlichkeiten mit Industroyer-Malware-Frameworks aufwies. Mit dem Schadprogramm Industroyer war im Dezember 2016 bereits das ukrainische Stromnetz angegriffen worden.[96] Code, Angriffsinfrastruktur, IoCs und Operationsziel ließen zu dem Zeitpunkt noch keine eindeutige politische und rechtliche Attribution an einen Akteur zu.[97] Gemeinsamkeiten und Verwandtschaften in der Schadsoftware verschiedener Angriffskampagnen sind nur ein unsicheres Indiz, denn diese weisen lediglich auf ähnliche Entwickler, nicht aber zwangsläufig auf dieselben operativen Angreifer hin.[98] Die Cyberkriminalität ist nämlich arbeitsteilig organisiert und funktionell differenziert, verschiedene Gruppen kopieren zudem TTPs untereinander.[99] Die Entwicklung und Durchführung von Attacken kann in unterschiedlichen Händen liegen. FireEye führte

92 Eric Auchard / Jack Stubbs / Alessandra Prentice, »New Computer Virus Spreads from Ukraine to Disrupt World Business«, *Reuters*, 27.6.2017, <https://www.reuters.com/article/us-cyber-attack-idUSKBN19I1TD> (Zugriff am 2.6.2021).

93 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* [wie Fn. 53], S. 14.

94 CCDCOE, »NotPetya and WannaCry Call for a Joint Response from International Community« [wie Fn. 81].

95 Greenberg, »The Untold Story of NotPetya« [wie Fn. 83].

96 Anton Cherepanov / Robert Lipovsky, »New TeleBots Backdoor: First Evidence Linking Industroyer to NotPetya«, *WeLiveSecurity* 11.10.2018, <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/> (Zugriff am 2.6.2021). ESET zufolge ist es unwahrscheinlich, dass ein dritter Akteur die Anpassungen vorgenommen hat.

97 Vgl. Andy Greenberg, *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, New York: Doubleday, 2019, Kap. 36.

98 Vgl. ebd., S. 277.

99 Rolf S. van Wegberg, *Outsourcing Cybercrime*, Delft: Delft University of Technology, 2020, <https://doi.org/10.4233/uuid:f02096b5-174c-4888-a0a7-dafd29454450>.

bei der Attribution an Russland recht vage Argumente an, dass nämlich russischsprachige Dokumente auf einem C2-Server der APT-Gruppe gefunden wurden und dass die Gruppe in einigen Cyberoperationen eine Zero-Day-Lücke verwendete, die zuvor auf einer russischen Hackerkonferenz präsentiert worden war.[100]

Die CIA geht davon aus, dass das russische Militär hinter NotPetya gestanden habe. Beweise wurden aber nicht präsentiert.

Die politische und rechtliche Attribution gestaltete sich holprig. Das Bundeskriminalamt (BKA) hatte 2017 Ermittlungen aufgenommen, ohne aber eine Anklage oder einen Haftbefehl zu erlassen. Dieser Umstand lässt jedenfalls die Vermutung zu, dass weder für einen »hinreichenden« noch für einen »dringenden Tatverdacht« genügend Beweise ermittelt werden konnten. Die CIA ging einem Bericht der *Washington Post* im Januar 2018 zufolge mit »hoher Gewissheit« davon aus, dass das russische Militär (genauer: der Militärnachrichtendienst GRU, und dort das Hauptzentrum für Spezialtechnologien; GTsST) hinter NotPetya gestanden habe. Beweise wurden aber nicht präsentiert.[101] Die öffentliche politische Attribution erfolgte Mitte Februar 2018, indem die Five Eyes die Angriffe der russischen Regierung zurechneten.[102] Dänemark, Lettland, Schweden und Finnland erklärten ihre Unterstützung für diese Zuschreibung. Damit wurde der Akt zu einer der öffentlichen Attributionen mit dem breitesten Rückhalt.[103] Wenige Monate später, Anfang Oktober 2018, sorgte das britische NCSC für mehr Klarheit bei der Frage, welche APT-Gruppen mit dem GRU in Verbindung zu bringen sind. Dazu zählt demnach etwa die APT 28, die auch unter den Namen Fancy Bear und Sofacy operierte. Die ebenfalls GRU-nahe Gruppe Sandworm ist auch unter den Namen Voodoo Bear und BlackEnergy bekannt.[104] Zur formalen rechtlichen Attribution schritten das US-Außenministerium und das britische NCSC erst im Februar 2020. Gemeinsam stellten sie Bezüge zu einer vergleichbaren Cyberoperation in Georgien her, für die die erwähnte GRU-Abteilung GTsST bzw. eine Unit »74455« verantwortlich erklärt wurde. Das britische Außenministerium ergänzte apodiktisch: »Diese GRU-Einheit [GTsST, 74455] war verantwortlich für […] NotPetya«.[105] Die USA erhoben schließlich Mitte Oktober 2020 formell Anklage gegen sechs russische Staatsbürger.[106] Ihnen wird vorgeworfen, als Offiziere des russischen Militärgeheimdienstes GRU in der Militäreinheit 74455 an mehreren bösartigen Cyberangriffen beteiligt gewesen zu sein (u.a. die Attacken mit Stromausfällen in der Ukraine 2015 und 2016, NotPetya, der Cyberangriff auf die OVCW und der Hack von Emmanuel Macrons Wahlkampfteam während der französischen Präsidentschaftswahlen 2017).

EU-Reaktion auf NotPetya

Der Rat der Europäischen Union hatte am 16. April 2018 die böswillige Nutzung von Informations- und Kommunikationstechnologien verurteilt, einschließlich jener Fälle, die unter dem Namen WannaCry und NotPetya bekannt sind.[107] Aber erst zwei Jahre später,

100 Andy Greenberg, »Your Guide to Russia's Infrastructure Hacking Teams«, *Wired* (online), 12.7.2017, <https://www.wired.com/story/russian-hacking-teams-infrastructure/> (Zugriff am 2.6.2021).

101 Ellen Nakashima, »Russian Military Was behind ›NotPetya‹ Cyberattack in Ukraine, CIA Concludes«, in: *The Washington Post* (online), 13.1.2018, <https://wapo.st/3khtQAq> (Zugriff am 2.6.2021).

102 Paul Ivan, *Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox*, Brüssel: European Policy Centre, März 2019, S. 5, <https://www.epc.eu/content/PDF/2019/pub_9081_responding_cyberattacks.pdf>; Francesco Bussoletti, »All Five Eyes Countries Have Blamed Russia for the NotPetya Cyber Attack«, *Difesa & Sicurezza* (online), Februar 2018, <https://www.difesaesicurezza.com/en/cyber-en/all-five-eyes-countries-have-blamed-russia-for-the-notpetya-cyber-attack/> (Zugriff jeweils am 15.9.2021).

103 Ivan, *Responding to Cyberattacks* [wie Fn. 102], S. 5.

104 National Cyber Security Centre, »Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed«, London, Oktober 2018, <https://www.ncsc.gov.uk/pdfs/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.pdf> (Zugriff am 2.6.2021).

105 Foreign & Commonwealth Office, »UK Condemns Russia's GRU over Georgia Cyber-attacks«, Press release, 20.2.2020, <https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks> (Zugriff am 2.6.2021).

106 United States District Court for the Western District of Pennsylvania, *United States of America v. Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko and Petr Nikolayevich Pliskin*, 15.10.2020, <https://www.justice.gov/opa/press-release/file/1328521/download> (Zugriff am 15.9.2021).

107 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1125 des Rates vom 30. Juli 2020 zur Durch-

am 30. Juli 2020, erließ er mit der Durchführungsverordnung (EU) 2020/1125[108] wirtschaftliche Sanktionen,[109] also gezielte Sanktionen gegen Einzelpersonen.[110] Im *Amtsblatt der Europäischen Union* wurden die beschuldigten Akteure benannt: »Das Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), auch unter seiner Feldpostnummer 74455 bekannt, ist verantwortlich für Cyberangriffe mit erheblichen Auswirkungen, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen[,] und für Cyberangriffe mit erheblichen Auswirkungen auf Drittstaaten; dazu zählen die als ›NotPetya‹ oder ›EternalPetya‹ bekannten Cyberangriffe vom Juni 2017 und die im Winter 2015 und 2016 gegen das ukrainische Stromnetz gerichteten Cyberangriffe.«[111] Die Five Eyes und einige wenige EU-Mitgliedstaaten hatten, wie gesehen, die russische Regierung schon wesentlich früher, im Februar 2018, für verantwortlich erklärt. Zu ihrer kollektiven Reaktion gelangte die EU somit erst über zwei Jahre später.

Operation Cloud Hopper 2016

Die Aktion Cloud Hopper gilt als Fall von Wirtschaftsspionage.[112] Der Angriff, der im Jahr 2016 begann, wird als Supply-Chain-Attacke klassifiziert. Er richtete sich gegen sogenannte »Managed Service Provider« (MSP). Das sind Firmen, die wie Hewlett Packard Enterprise (HPE) und IBM unter anderem über Cloud-Dienste, Applikationen und Infrastruktur wie Server und Netzwerke IT-Dienstleistungen für Drittunternehmen bzw. Regierungsstellen weltweit übernehmen. Die Hacker drangen in die Cloud-Management-Infrastruktur dieser MSP mit Hilfe von »spear phishing«-E-Mails ein, die als Nachrichten von Klienten der Serviceanbieter getarnt waren. Laut einer technischen Analyse der Firma Trend Micro hatten die Angreifer einen modifizierten Remote-Access-Trojaner (RAT) aus der PlugX-, Poison-Ivy-, ChChes- und Graftor-Malware-Familie in Word-Dokumente implementiert, die den E-Mails anhingen.[113]

Die Angreifer »hüpften« (Hopper) sozusagen über verschiedene Cloud-Instanzen und erlangten so Zugriff auf die Systeme.

Einmal ausgeführt, etablierte der Trojaner einen Brückenkopf auf den MSP-Systemen und kommunizierte mit C2-Servern in Tianjin. Zudem wurden Keylogger installiert, die Namen und Passwörter zur Infrastruktur der Klienten protokollierten und ausleiteten. Diese Zugangsdaten nutzten die Hacker, um lateral über die MSP-Cloud-Infrastruktur auf die Systeme ebenjener Klienten zuzugreifen. Aus diesem Modus Operandi erklärt sich der Name Cloud Hopper: Die Angreifer »hüpften« sozusagen über verschiedene Cloud-Instanzen und erlangten so Zugriff auf die Systeme. Der Angriff wird allseits als technisch versiert bewertet. Der verwendete Code nutzte Zertifikate großer IT-Unternehmen, um authentisch zu erscheinen. Eine Abwehr solcher Supply-Chain-Angriffsvektoren gilt grundsätzlich als schwierig.[114]

Opfer, Schäden, Operationsziel

Neben IBM und HPE waren laut der Nachrichtenagentur *Reuters* weitere Unternehmen im Visier der Angreifer: Ericsson, SKF (beide Schweden), Valmet (Finnland), Tata Consultancy Services (Indien), Fujitsu, NTT Data (beide Japan), Dimension Data (Südafrika), Computer Sciences Corporation, DXC Technology

führung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen«, in: *Amtsblatt der Europäischen Union*, (30.7.2020) L 246/4, <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32020R1125&from=DE> (Zugriff am 2.6.2021).

108 Ebd., 3. Erwägungsgrund.

109 Rechtliche Grundlage dafür ist Artikel 13 VO (EU) 2019/796 (i.V.m. Art. 215 AEUV).

110 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1125« [wie Fn. 107], Anhang.

111 Ebd.

112 Lucian Constantin, »›Five Eyes‹ Countries Attribute APT10 Attacks to Chinese Intelligence Service«, *Security Boulevard*, 21.12.2018, <https://securityboulevard.com/2018/12/five-eyes-countries-attribute-apt10-attacks-to-chinese-intelligence-service/> (Zugriff am 2.6.2021).

113 »Operation Cloud Hopper: What You Need to Know«, *Trend Micro*, 10.4.2017, <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know> (Zugriff am 20.5.2021).

114 Jack Stubbs / Joseph Menn / Christopher Bing, »Special Report: Inside the West's Failed Fight against China's ›Cloud Hopper‹ Hackers«, *Reuters*, 26.6.2019, <https://www.reuters.com/article/us-china-cyber-cloudhopper-special-repor-idUSKCN1TR1DK> (Zugriff am 20.5.2021).

sowie die NASA (alle USA).[115] Das deutsche Bundesamt für die Sicherheit in der Informationstechnik (BSI) warnte im Dezember 2018, dass auch hiesige Unternehmen Opfer der Angriffskampagne sein könnten, ohne dies jedoch näher zu spezifizieren.[116] Außer den genannten waren noch weitere US-amerikanische Ziele betroffen: die Sabre Corp (US), ein weltweit agierender Anbieter für Flug- und Hotelbuchungen, sowie die Huntington Ingalls Industries, die größte Werft der USA, die auch Atom-U-Boote für die US Navy baut. 40 Computer der US Navy waren ebenfalls kompromittiert. Persönliche Informationen von 100.000 Navy-Mitarbeitern und -Mitarbeiterinnen wurden gestohlen.[117] In einer US-Anklageschrift gegen die Urheber ist von mindestens 25 US-Entitäten und 14 weiteren Opfern in 12 Bundesstaaten die Rede.[118] Berichte über das Ausmaß des Schadens sind widersprüchlich.[119] Verglichen mit anderen Vorfällen ist die Informationslage dünn. Die MSP und HPE hielten wegen Haftungsfragen und möglichen rechtlichen Konsequenzen Informationen über ihre Klienten zurück. Einige Unternehmen bestätigten erfolgreiche Intrusionen, konnten aber nicht feststellen, ob Daten entwendet wurden. Zu den Kosten gibt es keine Schätzungen.[120]

Es gibt Hinweise, dass mehrere Angriffsteams mit unterschiedlichen Fähigkeiten arbeitsteilig vorgingen.

Auffällig ist, dass die angegriffenen Systeme vorwiegend zum Bereich der Schwerindustrie gehörten, zur Luft- und Seefahrt, zur Telekommunikation und Satellitentechnik. Operationsziel waren in erster Linie Wirtschaftsspionage bzw. im Fall von Sabre Kundendaten und im Fall der Navy politisch motivierte Nachrichtengewinnung.[121] Die Attacke war schwer zu detektieren und hinterließ kaum Spuren. Es gibt zudem Hinweise, dass mehrere Angriffsteams mit unterschiedlichen Fähigkeiten arbeitsteilig vorgingen, ein Zeichen für die Komplexität der Kampagne. Die TTP sprechen gegen den typischen Modus Operandi von Cyberkriminellen und für eine staatliche Organisation mit ausreichend finanziellen Ressourcen.

Attribution der Angreifer

Im Dezember 2018 rechnete die US-Regierung den Angriff öffentlich der Gruppe APT 10 zu (alias MenuPass, POTASSIUM, Stone Panda, Red Apollo und CVNX), die mit dem chinesischen Ministerium für Staatssicherheit in Verbindung gebracht wird. Das US-Justizministerium veröffentlichte die Anklagen gegen zwei chinesische Staatsbürger: Zhu Hua und Zhang Shilong.[122] Die Beschuldigten arbeiteten für die Huaying Haitai Science and Technology Development Company in Tianjin, China. Beide seien Teil der APT-Gruppe, die sich seit 2006 auf den Diebstahl geistigen Eigentums von Industrien im strategischen Interesse Chinas spezialisiert habe. Als technische Beweise gelten die Kommunikation der Malware mit IP-Adressen in Tianjin, die Registrierung von über 1.300 DNS-Servern in den USA und die Kongruenz der Angriffsaktivitäten mit den Büroarbeitszeiten in der chinesischen Zeitzone. Die Verantwortungszuweisung stützte sich auf Informationen von InfraGard und Trend Micro.[123] Die Five Eyes schlossen sich der politischen Attribution an. Das britische NCSC konstatierte, es sei »äußerst wahrscheinlich« (»highly likely«), dass APT 10 dauerhafte Beziehungen zum chinesischen Ministerium für Staatssicherheit unterhalte und nach dessen Vorgaben operiere.[124] Japan, das ebenfalls betroffen war, erklärte seine Zustimmung zu der

115 Ebd.

116 »German Security Office Warned German Firms about Chinese Hacking — Report«, *Reuters*, 19.12.2018, <https://www.reuters.com/article/uk-germany-security-idUKKBN1OI0HS> (Zugriff am 20.5.2021).

117 US Department of Justice, »Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information«, Press release 18-1673, Dezember 2018, <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion> (Zugriff am 20.5.2021).

118 United States District Court for the Southern District of New York, *United States of America v. Zhu Hua and Zhang Shilong*, Indictment, 20.12.2018, S. 13ff.

119 Ebd., S. 4. Die DoJ-Anklage spricht von Hunderten von Gigabyte an gestohlenem geistigem Eigentum.

120 IBM Security / Ponemon Institute, *Cost of a Data Breach Report 2019*, Traverse City, MI, 2019, <https://www.ibm.com/downloads/cas/ZBZLY7KL> (Zugriff am 21.5.2021).

121 Stubbs / Menn / Bing, »Special Report« [wie Fn. 114].

122 US Department of Justice, »Two Chinese Hackers« [wie Fn. 117].

123 Ebd.

124 Foreign and Commonwealth Office/NCSC, »UK and Allies Reveal Global Scale of Chinese Cyber Campaign«, 20.12.2018, <https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign> (Zugriff am 2.6.2021).

öffentlichen Attribution.[125] Deutschland unterstützte das Vorgehen einen Tag später ebenfalls.[126]

EU-Reaktion auf Cloud Hopper

Im Laufe des Jahres 2019 entschloss sich die EU im Rahmen der GASP zu einer politischen Reaktion auf die Cloud-Hopper-Attacke. Die damalige Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, Federica Mogherini, erklärte am 12. April 2019, dass böswillige Cyberaktivitäten, die die Integrität, Sicherheit und wirtschaftliche Wettbewerbsfähigkeit der Union durch Diebstahl geistigen Eigentums untergraben, zu unterlassen seien. Die Botschaft richtete sich an die Gruppe APT 10.[127] Aber erst ein Jahr später, Ende Juli 2020, ging der Rat mit den Durchführungsverordnungen 2020/1125[128] und 2020/1744[129] einen Schritt weiter und verhängte im November 2020 Sanktionen. Die unter anderem damit in Kraft getretenen Einreisebeschränkungen gründen sich auf Artikel 4 Beschluss (GASP) 2019/797.[130] Sanktioniert wurden die chinesischen Staatsbürger Gao Qiang und Zhang Shilong sowie das Unternehmen Huaying Haitai, die für die Cyberangriffe in den Jahren von 2014 bis 2017 verantwortlich erklärt werden.[131] Zhang Shilong sei der Urheber der Schadsoftware. Zhang sei bei der Firma Huaying Haitai beschäftigt gewesen, die die Operation Cloud Hopper ermöglicht habe. Die Uhrzeiten der Angriffe und die Ziele würden nahelegen, dass die verantwortlichen Hacker aus China heraus agiert und mit der Regierung in Verbindung gestanden hätten.[132]

Bundestag-Hack 2015

Es wird vermutet, dass eine Mitarbeiterin der Fraktion Die Linke im Bundestag am 30. April 2015 einen Link in einer E-Mail öffnete, die vermeintlich von der UNO gesendet worden war und Informationen über den Ukraine-Konflikt versprach.[133] Der Link führte zu einer kompromittierten Website, die einen Trojaner installierte. Der damalige BSI-Präsident Michael Hange bestätigte später im Bundestagsausschuss, dass sich die Täter am 5. Mai 2015 auf dem Domaincontroller und der Admin-Workstation anmelden konnten. Mit dem Tool Mimikatz ermittelten sie Passwörter weiterer Nutzerkonten. Mit Hilfe extrahierter Passwörter und diverser Fernsteuerungsprogramme seien die Angreifer am 6. Mai 2015 auf bis zu 50 weitere Systeme gelangt.[134] Die Eindringlinge erlangten Administrationsrechte für die Microsoft-Umgebung von Parlament und Fraktionen.

Im Auftrag der Linksfraktion erhielt der IT-Sicherheitsforscher Claudio Guarnieri früh Zugriff auf Angriffsartefakte.[135] Als Mittel zur Erstinfektion vermutete er Phishing, alternativ auch einen Bug in Windows oder im Flash Player. Unklar war zu diesem

125 Constantin, »›Five Eyes‹ Countries« [wie Fn. 112].
126 »Regierungspressekonferenz vom 21. Dezember 2018«, *Bundesregierung* (online), 20.5.2021, <https://www.bundesregierung.de/breg-de/aktuelles/regierungspressekonferenz-vom-21-dezember-2018-1563932> (Zugriff am 20.5.2021).
127 Rat der Europäischen Union, »Erklärung der Hohen Vertreterin im Namen der EU zur Wahrung der regelbasierten Ordnung im Cyberraum«, Pressemitteilung, Brüssel, 12.4.2019, <https://www.consilium.europa.eu/de/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/> (Zugriff am 14.9.2021).
128 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1125« [wie Fn. 107].
129 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1744 des Rates vom 20. November 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen«, in: *Amtsblatt der Europäischen Union*, (23.11.2020) L 393/1, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020R1744&from=DE> (Zugriff am 2.6.2021).
130 Rat der Europäischen Union, »Beschluss (GASP) 2019/797« [wie Fn. 46], Art. 4.
131 Stubbs / Menn / Bing, »Special Report« [wie Fn. 114].
132 Federal Bureau of Investigation, »Chinese Hackers Indicted«, 20.12.2018, <https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018> (Zugriff am 2.6.2021).
133 Dem geleakten Protokoll der Sitzung des zuständigen Bundestagssauschusses zufolge sagte der Präsident des BSI, dass die Erstinfektion durch einen sogenannten Watering-Hole-Angriff erfolgte; Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und -medien [= IuK-Kommission], *Kurzprotokolle der 6., 7. und 8. Sitzung der IuK-Kommission des Deutschen Bundestages*, Berlin, Mai bis Juli 2015 (nichtöffentliche und nichtoffizielle Version), <https://pastebin.com/raw/LZzpN3Lb> (Zugriff am 2.1.2021).
134 »Kurzprotokoll der 7. Sitzung der IuK-Kommission«, 11.6.2015, in: IuK-Kommission, *Kurzprotokolle* [wie Fn. 133].
135 Claudio Guarnieri, »Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag«, *Netzpolitik.org*, 19.6.2015, <https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag> (Zugriff am 15.9.2021).

Zeitpunkt, ob der Angriff auf den Rechner der Linksfraktion Teil des Bundestag-Hacks oder eine eigenständige Attacke war. Das Krisennotfallmanagement stellte sich als eine Belastungsprobe für die Gewaltenteilung heraus, weil die IT-Sicherheit der Legislative durch das BSI bzw. das Bundesamt für Verfassungsschutz als exekutive Instanzen unterstützt werden musste.

Opfer, Schäden und Operationsziel

Durch den Trojanerangriff wurden der zentrale Server der Bundestagsverwaltung und Rechner von Abgeordneten kompromittiert, sogar das Büro von Bundeskanzlerin Angela Merkel. Es wird angenommen, dass eine beachtliche Anzahl von E-Mail-Unterhaltungen aus den Jahren 2012 bis 2015 entwendet wurden.[136] Rund 50 IT-Systeme waren betroffen[137] und größere Datenmengen aus dem Bundestag ausgeleitet: »Nachweislich« wurden mindestens 16 Gigabyte (ggf. mit Duplikaten) »an etwa neun bekannte, weltweit verteilte, verdächtige Server« gesendet.[138] Das genaue Datenvolumen und der Inhalt der abgeflossenen Daten (Verschlusssachen) sind nicht bekannt.[139] Bis September 2015 wendete die Bundestags-IT-Abteilung für »die Abwehr und das Wiederaufsetzen Mittel in Höhe von ca. 1 Mio.« auf. Für das Folgejahr wurden fünf neue Stellen beantragt. Das BSI hat für die Behebung der Schäden der Cyberattacke 350 Werktage in Rechnung stellen müssen.[140]

Mit dem Angriff auf das höchste Verfassungsorgan der Bundesrepublik Deutschland wurde die Funktionsfähigkeit der Demokratie in Gefahr gebracht. Gleichwohl war das Ziel der Operation in erster Linie politische Spionage. Im Januar 2017 ließen Unbekannte die Domain »btleaks.com« registrieren, vermutlich in der Absicht, analog zum Hack der Parteizentrale der Demokratischen Partei (DNC Hack) in den USA im Jahr 2016 und der Website dcleaks.com die gestohlenen Daten bei passender Gelegenheit, beispielsweise vor den Bundestagswahlen, zu veröffentlichen.[141] »Zwietracht säen oder Unsicherheit schüren« waren zum damaligen Zeitpunkt als Erklärungen plausibel, obwohl das gestohlene Material, wie bei klassischen Spionageoperationen üblich, nicht veröffentlicht wurde.[142] Der politische Kontext ist aber für die rechtliche und politische Bewertung eines Angriffs zentral.

Attribution der Angreifer

Zwar kann man aus öffentlichen Quellen durchaus etwas über die technischen Merkmale des Angriffs erfahren, doch hielt die Bundesregierung diese attributionsrelevanten Details geheim. Entsprechend sind die Berichte des BSI und der Nachrichtendienste als vertraulich eingestuft. Das BKA und die deutschen Strafverfolger griffen bei ihren Ermittlungen auch auf belastende Informationen zurück, die US-Behörden im Zuge ihrer Untersuchung zum DNC-Hack gesammelt hatten.[143] Die IT-Sicherheitsfirma ThreatConnect beschrieb in einem Blog-Eintrag, wie es ihr gelang, zu rekonstruieren, dass beim Angriff auf die US-Demokraten im Wahlkampf 2016 dasselbe Zertifikat verwendet wurde wie beim Bundestag-Hack 2015.[144]

136 Jörg Diehl / Marcel Rosenbach / Fidelius Schmid, »Rekonstruktion eines Cyberangriffs: Wie russische Hacker Angela Merkels Mailkonten knackten«, in: *Der Spiegel* (online), 8.5.2020, <https://www.spiegel.de/netzwelt/web/angela-merkel-wie-russische-hacker-die-mailkonten-der-bundeskanzlerin-knackten-a-00000000-0002-0001-0000-000170816296> (Zugriff am 2.6.2021).

137 »Kurzprotokoll der 7. Sitzung« [wie Fn. 134].

138 Ebd.

139 Ebd.

140 Anna Biselli, »Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ«, *Netzpolitik.org*, 7.3.2016, <https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/> (Zugriff am 21.5.2021).

141 »Diese 4 Webseiten deuten auf ein Bundestagsleak hin und hier steht warum«, *Buzzfeed*, 8.8.2017, <https://www.buzzfeed.de/recherchen/diese-webseiten-deuten-auf-ein-bundestagsleak-hin-und-hier-steht-warum-90134843.html> (Zugriff am 21.5.2021).

142 Diehl / Rosenbach / Schmid, »Rekonstruktion eines Cyberangriffs« [wie Fn. 136].

143 Florian Flade / Hakan Tanriverdi, »Der Mann in Merkels Rechner — Jagd auf Putins Hacker« (BR Podcast), Folge 4: Der Mann in Merkels Rechner, *BR Bayern 2*, 22.4.2021, <https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/853> (Zugriff am 21.5.2021).

144 »Finding Nemo(hosts)«, *Threatconnect Research*, 21.7.2017, <https://threatconnect.com/blog/finding-nemohost-fancy-bear-infrastructure/> (Zugriff am 2.6.2021). Timo Steffens hat diesen eingängig in einem Buch beschrieben: *Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt*, Berlin: Springer Vieweg, 2018, S. 66ff.

Die Entwicklung des Schadprogramms setzte eine solide Finanzierung und die Unterstützung durch eine etablierte Organisation und warscheinlich einen Staat voraus.

Claudio Guarnieri benannte entsprechend früh im Juni 2015 die in Russland operierende Gruppe APT 28 als möglichen Urheber. Dabei stützte er sich auch auf einen Bericht des IT-Sicherheitsunternehmens FireEye (2014), das behauptete, dass APT 28 vom russischen Staat finanziert würde. FireEye schließt dies aus vergangenen Operationen, bei denen ähnliche Malware-Artefakte und TTPs bzw. deren Weiterentwicklungen identifiziert wurden. Die Angriffstools wurden auf Systemen mit russischen Spracheinstellungen zu den in Moskau und St. Petersburg üblichen Bürozeiten kompiliert. Die jahrelange, professionelle Entwicklung des Schadprogramms setzte eine solide Finanzierung und darüber hinausgehende Unterstützung durch eine etablierte Organisation und »most likely« einen Staat voraus. Die Cyberoperationsziele seien konsistent mit den gegenwärtigen außenpolitischen Interessen und Methoden Russlands.[145] Guarnieris Argumente für die Attribution an APT 28 wurden durch eine Dokumentation des Wirtschaftsberatungsunternehmens PricewaterhouseCoopers (PwC) erhärtet. Bestimmte IPs und SSL-Zertifikate, die beim Bundestag-Hack eine Rolle spielten, wurden dem PwC-Report zufolge bereits zuvor für einen Angriff verwendet, der der Gruppe Sofacy/APT 28 zuzuschreiben ist.[146]

Im Juni 2015 vermutete der Präsident des Bundesamts für Verfassungsschutz Hans-Georg Maaßen, dass ein ausländischer Geheimdienst für den Angriff verantwortlich sei, ohne aber technische Details zu nennen.[147] Ein Jahr später offenbarte Maaßen, dass der russische Staat hinter den Angreifern stecke.[148] Die Beweise dafür würden nicht nur aus der technischen Analyse stammen, sondern auch aus nachrichtendienstlichen Erkenntnissen.[149]

Anfang 2018 machte der niederländische In- und Auslandsgeheimdienst AIVD (Algemene Inlichtingen en Veiligheidsdienst) Informationen über die Hackergruppe APT 29, auch Cozy Bear genannt, publik.[150] Medienberichten zufolge hatten sich die Niederländer 2014 in die Netze der APT-Gruppe gehackt, Zugriff auf Überwachungskameras des Gebäudes erlangt, in dem die Hacker ihre Büros hatten, und Mitglieder der APT als Geheimdienstmitarbeiter identifiziert. Erhärtet wurde dieser Befund wiederum durch die Untersuchungen des US-Sonderermittlers Robert Mueller. In dessen Bericht von April 2019 und in einer früheren Anklageschrift vom Juli 2018 werden zwölf Geheimdienstmitarbeiter der Einheiten 26165 und 74455 des russischen Militärnachrichtendienstes GRU als Urheber benannt. Der Mueller-Report untermauert die These, dass die Angreifer des GRU über verschiedene Operationen wie NotPetya, den OVCW-Hack und den Bundestag-Hack hinweg ähnliche TTPs verwendet haben.[151]

Ab 2018 erklärten weitere Staaten öffentlich die russische Regierung für mehrere Cyberoperationen verantwortlich. Im Herbst 2018 schloss sich die Bundesregierung dieser Sichtweise an: »Auch die Bundesregierung geht mit an Sicherheit grenzender Wahrscheinlichkeit davon aus, dass hinter der Kampagne APT 28 der russische Militärgeheimdienst GRU steckt […] Diese Einschätzung beruht auf einer insgesamt sehr guten eigenen Fakten- und Quellenlage.«[152] Im

145 FireEye, *APT28: A Window into Russian Espionage Operations?*, Milpitas, CA, 2014, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> (Zugriff am 2.6.2021).

146 Guarnieri, »Digital Attack on German Parliament« [wie Fn. 135].

147 Patrick Beuth, »Hackerangriff im Bundestag: ›Das ist kein allzu großer Fall‹«, in: *Zeit Online*, 12.6.2015, <https://www.zeit.de/digital/datenschutz/2015-06/bundestag-hack-karlsruher-firma-aufklaerung> (Zugriff am 2.6.2021).

148 »Russia ›Was behind German Parliament Hack‹«, *BBC News* (online), 13.5.2016, <https://www.bbc.com/news/technology-36284447> (Zugriff am 2.6.2021).

149 »Hacker im Staatsauftrag — Netzwerk Recherche #nr17«, *YouTube*, 9.6.2021, Min. 6:50, <https://www.youtube.com/watch?v=OfRb6hssfu8> (Zugriff am 9.6.2021).

150 Huib Modderkolk, »Dutch Agencies Provide Crucial Intel about Russia's Interference in US-Elections«, in: *De Volkskrant*, 25.1.2018, <https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/> (Zugriff am 2.6.2021).

151 US Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Vol. I, Washington, D.C., März 2019, S. 36ff, <https://www.justice.gov/archives/sco/file/1373816/download> (Zugriff am 21.5.2021); US District Court for the District of Columbia, *United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin and Others*, Indictment, CR 18-215, 13.7.2018, <https://www.justice.gov/file/1080281/download> (Zugriff am 9.1.2021).

152 »Auch Bundesregierung macht Russland verantwortlich für Cyberangriffe«, *Spiegel Online*, 5.10.2018, <https://www.spiegel.de/netzwelt/netzpolitik/apt28-bundesregierung-

November 2019 informierte der Generalbundesanwalt über erstmalige Ermittlungen gegen die Gruppe APT28/Fancy Bear.[153] Nach deren Abschluss sprach Bundeskanzlerin Merkel im Mai 2020 »von ›harten Evidenzen‹ für eine russische Beteiligung und von einem ›ungeheuerlichen‹ Vorgang.«[154]

EU-Reaktion auf den Bundestag-Hack

Am 22. Oktober 2020 erließ der Rat der Europäischen Union mit der Durchführungsverordnung (EU) 2020/1536 Sanktionen gegen das 85. Hauptzentrum für Spezialdienste (GTsSS) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) und dessen Militärgeheimdienstbeamte Dmitry Badin und Igor Kostyukov.[155] Bei den gezielten Strafmaßnahmen handelt es sich um wirtschaftliche Sanktionen gemäß Artikel 3 der VO (EU) 2019/796 und Einreisebeschränkungen nach Artikel 4 Beschluss (GASP) 2019/797.[156] In der Begründung heißt es, dass Dmitry Badin als Agent des GTsST an der Cyberattacke mit erheblichen Auswirkungen gegen den Deutschen Bundestag im April und Mai 2015 beteiligt gewesen sei**.** Igor Kostyukov habe als Leiter der Hauptdirektion der »Militäreinheit 26165« — in Fachkreisen bekannt unter den Beinamen »APT28«, »Fancy Bear«, »Sofacy Group«, »Pawn Storm« und »Strontium« — den Hack durchgeführt. Beide GRU-Mitarbeiter wurden nicht nur für die Attacke gegen den Deutschen Bundestag, sondern auch für den versuchte Cyberangriff im April 2018 auf die Organisation für das Verbot chemischer Waffen (OVCW) für verantwortlich erklärt.[157]

Versuchter Angriff auf die OVCW 2018

Am 13. April 2018 bereiteten vier russische Geheimdienstagenten einen sogenannten WiFi-Spoofing-Angriff[158] auf die Organisation für das Verbot chemischer Waffen (OVCW/engl. OPCW) in Den Haag vor. Sie stellten auf dem Parkplatz des Marriott-Hotels neben dem OVCW-Gebäude einen Mietwagen ab, der mit einem gefälschten WiFi-Hotspot (einem sogenannten WiFi-Pineapple) präpariert war. Der manipulierte Pineapple-Router sollte das Original-WLAN der OVCW imitieren und auf diese Weise die Daten der Nutzerinnen und Nutzer abgreifen. Ein solches Vorgehen wird als Man-in-the-Middle-Angriff bezeichnet.[159] WiFi-Spoofing funktioniert nur, wenn das Fake-WLAN in direkter physischer Nähe zum Original platziert wird. Die Täter müssen dafür unmittelbar vor Ort sein (»close access operation«). In diesem Fall wurden sie dabei bereits vom niederländischen Militärgeheimdienst (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) observiert und festgenommen. Der Tageszeitung *Guardian* zufolge hatten die Niederländer rechtzeitig einen Hinweis von britischen Nachrichtendiensten erhalten.[160] Die vier GRU-Mitarbeiter waren am 10. April 2018 über den Amsterdamer Flughafen Schiphol eingereist und seitdem überwacht worden.[161] Die niederländischen Sicherheitsbehörden intervenierten frühzeitig, um eine erfolgreiche Kompromittierung der OVCW zu verhindern. Sie beschlag-

beschuldigt-offiziell-russland-der-cyberangriffe-a-1231744.html> (Zugriff am 6.10.2021).

153 Jörg Diehl / Fidelius Schmid, »Deutschland ermittelt gegen russische Hacker«, in: *Der Spiegel*, 16.11.2019.

154 »Hackerangriff auf Bundestag: Angela Merkel erhebt schwere Vorwürfe gegen Moskau«, in: *Der Spiegel* (online), 13.5.2020, <http://www.spiegel.de/politik/deutschland/hackerangriff-angela-merkel-erhebt-schwere-vorwuerfe-gegen-moskau-a-36fc72c7-7f66-47e6-997d-fbd5a08ae4d5> (Zugriff am 9.1.2021).

155 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1536 des Rates vom 22. Oktober 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen«, in: *Amtsblatt der Europäischen Union*, (22.10.2020) L 351 I/1, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32020R1536> (Zugriff am 2.6.2021).

156 Ebd., Anhang.

157 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1125« [wie Fn. 107].

158 WiFi-Spoofing basiert darauf, dass Nutzer sich irrtümlich bei einem Hotspot mit ihren regulären Nutzerinnen- bzw. Nutzerdaten anmelden.

159 Andy Greenberg, »How Russian Spies Infiltrated Hotel Wi-Fi to Hack Their Victims up Close«, *Wired* (online), 4.10.2018, <https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/> (Zugriff am 25.5.2021).

160 Luke Harding, »How Russian Spies Bungled Cyber-attack on Weapons Watchdog«, in: *The Guardian* (online), 4.10.2018, <https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog> (Zugriff am 25.5.2021).

161 US Department of Justice, *US v. Aleksei Sergeyevich Morenets*, Oktober 2018, <https://www.justice.gov/usao-wdpa/vw/us-v-Aleksei-Sergeyevich-Morenets> (Zugriff am 2.6.2021).

nahmten diplomatische Visa, eine größere Summe Bargeld, das technische Equipment, Smartphones, Laptops, Pässe und Reisequittungen.[162] Der Angriff blieb damit erfolg- und folgenlos.[163]

Attribution der Angreifer

Durch die frühzeitige Festnahme der Angreifer gestaltete sich die Attribution in diesem Fall recht unkompliziert. Die forensische Analyse des beschlagnahmten Equipments ließ Rückschlüsse nicht nur auf das Operationsziel, sondern sogar auch auf vergangene und geplante Operationen zu. Die Ermittler gewannen Informationen zu dem Giftanschlag auf den ehemaligen GRU-Agenten Sergei Skripal in Salisbury (UK). Der Angriff mit einem Nervenkampfstoff hatte einen Monat zuvor stattgefunden, die OVCW war mit der Analyse beauftragt. Reisebuchungen zeigten, dass das nächste Ziel der Täter ein OVCW-Labor in der Schweiz war. Die WiFi-Logs des Equipments offenbarten zudem, dass die Gruppe zuvor in Malaysia und in Brasilien unterwegs gewesen war. Zeitliche und räumliche Übereinstimmungen mit den niederländischen Ermittlungen zur Urheberschaft des Abschusses des Airliners MH17 in Malaysia sowie zu den Olympischen Spielen 2016 in Brasilien wurden evident.[164]

Die Logs der beschlagnahmten Mobiltelefone führten direkt ins GRU-Hauptquartier.

Nach Untersuchungen der Welt-Anti-Doping-Agentur (WADA) waren die russischen Leichtathleten im Juli 2016 wegen Dopingvorwürfen von den Olympischen Spielen in Rio de Janeiro ausgeschlossen worden. Im September 2016 war die WADA ebenfalls Opfer eines Cyberangriffs des gleichen Teams geworden. Die Logs der beschlagnahmten Mobiltelefone führten direkt ins GRU-Hauptquartier. Visa und Taxiquittungen, die ein staatlicher Nachrichtendienst für die Abbuchung von Dienstreisen benötigt, bestätigten die Beteiligung der GRU-Einheit 26165, die auch schon in die NotPetya-Attacke und den Bundestag-Hack involviert war.

Die politische Attribution erfolgte am 4. Oktober 2018 durch die niederländische Regierung in einer langen Pressekonferenz, in der alle Ermittlungsdetails erörtert wurden. Die Niederländer konstatierten, dass jeder Vorfall, der die Integrität internationaler Organisationen unterminiere, »unakzeptabel« sei. Die Regierung in Den Haag bestellte den russischen Botschafter ein, die niederländische Verteidigungsministerin und der britische Botschafter verurteilten den GRU bzw. indirekt die russische Regierung für diese Angriffe.[165] In den USA wurde am gleichen Tag der Pressekonferenz Anklage gegen sieben russische Geheimdienstoffiziere erhoben. Sie seien Mitarbeiter der GRU-Einheit 26165,[166] die neben dem Angriff auf die OVCW auch Angriffe gegen die Antidopingagenturen USADA, WADA und Canadian Centre for Ethics in Sport (CCED) durchgeführt hätten.[167] Zwei Monate zuvor, im August 2018, hatten die USA die Niederlande um Rechtshilfe bei der Verfolgung russischer Cyberoperationen gegen amerikanische und internationale Organisationen gebeten. Die Anschuldigungen und Indizien, die in der Anklage CR 18-263 zum Fall des versuchten OVCW-Angriffs zusammengetragen wurden,[168] decken sich mit den Hinweisen des niederländischen Verteidigungsministeriums. Die Logdaten des WiFi-Angriffsequipments bezeugten, dass die Angreifer zur selben Zeit im selben Hotel waren, als der Laptop eines Vertreters der kanadischen Anti-Dopingbehörde CCED infiltriert wurde.

Bemerkenswert ist das Ausbleiben einer rechtlichen Attribution. Die Niederländer verzichteten auf eine Anklage und setzten die überführten Spione nur kurzfristig fest. Am Tag nach ihrer Festnahme wurden sie in ein Flugzeug nach Russland gesetzt und des Landes verwiesen. Die GRU-Mitarbeiter verfügten über offizielle Diplomatenpässe, was sie vor Strafverfolgung schützte. Ein Offizier des niederländischen Nachrichtendienstes begründete den Sachverhalt so: »Hacken ist illegal. Der Versuch zu hacken ist es eben-

162 Onno Eichelsheim, »GRU Close Access Cyber Operation against OPCW«, *Netherlands Ministry of Defence*, 4.10.2018, <https://english.defensie.nl/binaries/defence/documents/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw/ppt+pressconference+ENGLISH+DEF.pdf>.

163 US Department of Justice, *US v. Aleksei Sergeyevich Morenets* [wie Fn. 161].

164 Government of the Netherlands, »Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW«, 25.5.2021, <https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw> (Zugriff am 25.5.2021).

165 Ebd.

166 US Department of Justice, *US v. Aleksei Sergeyevich Morenets* [wie Fn. 161].

167 Ebd.

168 Ebd.

falls. Die Vorbereitung eines Versuchs ist es allerdings nicht.«[169] Der OVCW-Hack ist einzigartig, weil es sich nicht um einen klassischen Cyberangriff handelte. Der Angriff konnte rechtzeitig unterbunden werden und wurde umgehend durch die niederländische Regierung bekannt gemacht, wobei sie der EU in einem Umfang Details zur Attribution vorlegte, wie sie kaum in einem anderen Fall des Cybersanktionsregimes zur Verfügung standen. Die Transparenz über die technische, rechtliche und politische Attribution gilt als beispielhaft und lässt wenig Raum für Fehlschlüsse.

EU-Reaktion auf den versuchten Angriff auf die OVCW

Die Präsidenten des Europäischen Rates und der Europäischen Kommission sowie die Hohe Vertreterin für Außen- und Sicherheitspolitik äußerten sich erstmals am 4. Oktober 2018 in einer gemeinsamen Erklärung zu dem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen. Sie beschrieben den Vorfall als »einen aggressiven Akt, in dem Verachtung für das hohe Ziel der OVCW zum Ausdruck gebracht wurde«.[170] In diesem Fall funktionierte das Timing der politischen Attribution: Sie erfolgte zumindest stringent und im Konzert mit den Verbündeten, und die Signalwirkung war deutlich. Ende Juli 2020 wurden die EU-Sanktionen erlassen, mit den Durchführungsverordnungen 2020/1125[171] und deren Ergänzung 2020/1744[172] von Ende November 2020. Die restriktiven Maßnahmen richten sich gegen das 85. Hauptzentrum für Spezialdienste (GTsSS) innerhalb des GRU und gegen dessen Mitarbeiter Alexey Minin, Aleksei Morenets, Evgenii Serebriakov und Oleg Sotnikov.[173]

169 Flade/Tanriverdi, »Der Mann in Merkels Rechner — Jagd auf Putins Hacker« (BR Podcast) [wie Fn. 143], Folge 3: Ganz nah dran, <https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/3-ganz-nah-dran/1823410> (Zugriff am 21.5.2021).

170 European Council, »Joint Statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian Cyber Attacks«, Pressemitteilung, Brüssel, 4.10.2018, <https://www.consilium.europa.eu/de/press/press-releases/2018/10/04/joint-statement-by-presidents-tusk-and-juncker-and-high-representative-mogherini/> (Zugriff am 30.9.2021).

171 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1125« [wie Fn. 107].

172 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1744« [wie Fn. 129].

173 Rat der Europäischen Union, »Durchführungsverordnung (EU) 2020/1125« [wie Fn. 107], Anhang.

Defizite der Politik der Attribution

Die Analyse zeigt, dass die Attributionskompetenz der EU defizitär ist. Sie deckt die Schwachstellen auf, unter denen die technische, politische und rechtliche Identifikation von Verantwortlichen für Cyberangriffe gegenwärtig leidet, und macht deutlich, welch hohe Hürden auf dem langen Weg zu einer effektiven und legitimen »Politik der Attribution« sowohl auf EU- als auch auf intergouvernementaler Ebene noch zu überwinden sind.

Erstens ist die EU maßgeblich auf Hinweise und Expertise verbündeter Drittstaaten wie den Five Eyes und IT-Firmen aus den USA abhängig. Eigene Beweise, die die Sicherheitsdienste von EU-Mitgliedstaaten zutage fördern, sind in der Regel mangel- und lückenhaft. Der OCVW-Angriff wäre ohne den Hinweis der britischen Behörden nicht rechtzeitig aufgedeckt und verhindert worden. Die deutschen Ermittlungen zum Bundestag-Hack basierten auf öffentlich zugänglichen Anklageschriften und einem nichtöffentlichen Austausch mit dem US-amerikanischen FBI. Fraglich ist, ob der für die Attribution notwendige Informationsaustausch mit dem Five-Eyes-Mitglied Großbritannien aufrechterhalten wird.

Zweitens ist evident, dass die EU in fast allen beschriebenen Fällen zeitlich verzögert reagiert hat. Die Abstimmungsprozesse und die für Cybersanktionen im Rahmen der GASP erforderliche Einstimmigkeit zwingen zu einer langwierigen Attribution, die zum Teil erst Jahre später nach den Verurteilungen durch die Partner der Five Eyes stattfand. Das mag auf die komplexe technische Forensik zurückzuführen sein, die typisch für Cybervorfälle ist, sicherlich aber auch auf die parallel durchgeführten Verfahren zum Informationsaustausch auf EU- und mitgliedstaatlicher Ebene. Die Zuständigkeiten für die Cyber-Kriminalitätsbekämpfung, für Cyberspionage und Spionageabwehr sowie für die militärische Cyberverteidigung liegen zuvorderst bei den Mitgliedstaaten und müssen auf EU-Ebene über Europol, im EAD durch EU INTCEN und künftig auch über die Gemeinsame Cyber-Stelle in der EU-Kommission koordiniert werden.

Mit dem Brexit hat sich die Attributionskompetenz der EU erheblich vermindert.

Drittens zeigt sich, dass die Five Eyes die zur politischen Attribution notwendige Vertraulichkeit beachten: Sie stimmen sich zügig ab und veröffentlichen zeitgleich Verlautbarungen, die auf umfangreichen Erkenntnissen beruhen. Damit steht die Legitimität der Attribution beinahe außer Frage. Mit dem Brexit hat sich die Attributionskompetenz der EU erheblich vermindert, da das Vereinigte Königreich geheimdienstliche Erkenntnisse nicht mehr über EU INTCEN teilt, sehr wohl aber noch auf bilateraler Ebene Informationen mit ausgewählten EU-Staaten austauscht. Im Vergleich zu den Five Eyes erfolgt die politische Attribution unterstützend zu den EU-Cybersanktionen nur vereinzelt und sporadisch. Eine glaubwürdige Politik der Attribution setzt voraus, dass alle Mitgliedstaaten gegenüber Dritten mit einer Stimme sprechen. Die politische Attribution ist nach wie vor die Prärogative der Mitgliedstaaten. Die Wirkung einer einzelstaatlichen Attribution ist jedoch limitiert. Die Bündelung von Attributionsreports auf EU-Ebene kann die Legitimität und Effektivität eines Sanktionsbeschlusses erheblich steigern. Dies gilt in besonderem Maße, wenn die Verantwortlichkeitszuschreibung zeitgleich in Abstimmung mit internationalen Partnern erfolgt. Die sogenannte »naming and shaming«-Kampagne von Verbündeten kann nur gelingen, wenn die jeweiligen Außenministerien koordiniert handeln.

Viertens: Cybersanktionen sollen bei Angriffen mit »erheblichen Auswirkungen« verhängt werden bzw. dann, wenn die entsprechenden Tatbestandsmerkmale erfüllt sind. Allerdings zeigt die Analyse, dass sich aus technischen Indikatoren und IoCs nur schwer bestim-

men lässt, ob ein Tatbestandsmerkmal tatsächlich erfüllt ist, was wiederum der Fall sein muss, um eine Rechtsfolge wie Sanktionen legitimieren zu können. Die bekannten Tatbestandsmerkmale der analysierten Cybervorfälle sind recht uneindeutig, berücksichtigen technische Details nicht in angemessenem Maße, ihre Gewichtung ist zudem unklar. So stellt sich etwa die Frage, ob ein Angriff gegen Wahlsysteme schwerwiegender ist als ein Angriff gegen kritische Infrastruktur. Wiegt ein Angriff gegen zahlreiche weniger kritische Systeme schwerer als ein Angriff auf ein Krankenhaus?[174] Die Problematik, eine böswillige Absicht nachzuweisen, die von Drittstaaten ausgeht, zeigt sich an den folgenden Tatbestandsmerkmalen:

a) Das Tatbestandsmerkmal der »*böswilligen* Nutzung von IKT« lässt sich nicht in allen Fällen eindeutig bestimmen. Bei WannaCry und NotPetya ist tatsächlich ein hinreichender Grad der Böswilligkeit feststellbar: aufgrund der willkürlichen Zielauswahl, der Inkaufnahme von Betriebsstörungen kritischer Infrastrukturen wie Krankenhäusern und der Schäden in Milliardenhöhe, die Staaten und Unternehmen entstanden sind. In anderen Fällen ist die Böswilligkeit kaum unzweifelhaft nachzuweisen.

b) Die Tatbestandsmerkmale, die einen *Cyberangriff definieren* sollen (Zugang zu-, Eingriff in Informationssysteme und Eingriff in Daten oder das Abfangen von Daten), sind aus technischer Sicht nicht eindeutig voneinander zu trennen. Ein Eingriff in Informationssysteme ist immer gleichbedeutend mit dem Eingriff in Daten, da Abwehrsysteme umgangen und Schadsoftware eingebracht wird, also nahezu zwangsläufig Daten auf ein Dateisystem geschrieben werden. Gleiches zeigt sich auch bei der Differenzierung zwischen *Angriffen* und *Angriffsversuchen*: Organisationen mit guten Detektionssystemen erhalten täglich Tausende Security-Alerts. Diese sind a priori oft nicht als Angriffsversuche zu erkennen, da sich die Wirkung eines Angriffs erst nach Ausführung von Schadcodes erkennen lässt. Erst wenn durch die Analyse derartiger Malware unter Rückgriff auf Threat-Intelligence-Techniken Informationen zu Angriffsinfrastrukturen oder Tools bekannter APT-Gruppen ermittelt worden sind, können betroffene Organisationen den Vorfall als bedrohlichen Akt interpretieren.

Das strategische Operationsziel lässt sich aus meist rein taktischen IoCs nur schwer bestimmen.

c) Auch lässt sich das strategische *Operationsziel bzw. die Angriffsmotivation* aus meist rein taktischen IoCs nur schwer bestimmen. Bei WannaCry ist die Angriffsmotivation zum Beispiel nicht eindeutig. Die Deutung des Bundestag-Hacks als Versuch der Beeinflussung lässt sich ebenfalls nur schwer aus den IoCs schließen. Sie speist sich aus der gängigen Vorstellung einer hybriden Bedrohung, die erst Jahre später, nach dem DNC-Hack, im transatlantischen Diskurs vorherrschend wurde.

d) Die *Auswahl der Fälle*, die die EU zu Cybersanktionen veranlassten, weist Inkonsistenzen auf. Warum zum Beispiel Fälle klassischer Spionage (Bundestag-Hack und Cloud Hopper) in das Cybersanktionsregime einbezogen wurden, konkrete Versuche der Wahlbeeinflussung (Macron-Leaks) aber nicht, ist nicht plausibel und wird in der Begründung der einzelnen Sanktionen auch nicht plausibel gemacht. Spionage gehört seit Jahrzehnten zur Staatenpraxis. Sie ist zwar in so gut wie allen nationalen Rechtsordnungen strafbewehrt, nicht aber nach internationalem Recht rechtswidrig.[175] Beim Hack der E-Mails von Emmanuel Macrons Wahlkampfteam im Jahr 2017 wurden Kommunikationsinhalte gestohlen und analog zum DNC-Hack auch geleakt, und dies zwei Tage vor dem Stichwahltag.[176] Anders als beim Bundestag-Hack liegt hier eindeutig das Tatbestandsmerkmal der Beeinflussung eines Wahlprozesses vor, was über politische Spionage hinausgeht und als Verletzung staatlicher Souveränität betrachtet werden kann.

174 Julia Grauvogel / Christian von Soest, *Cybersanktionen: Zunehmende Anwendung eines neuen Instruments*, Hamburg: German Institute of Global and Area Studies (GIGA), April 2021 (GIGA Focus — Global, Nr. 3), <https://pure.giga-hamburg.de/ws/files/24469713/gf_web_global_2021_03_D.pdf> (Zugriff am 14.9.2021).

175 Wären die abgeflossenen Informationen im Rahmen des Bundestagswahlkampfs 2017 instrumentalisiert worden, wie zuvor die internen E-Mails des Democratic National Committees in den USA 2016, so hätte das rechtliche Konzept der »illegal intervention« oder »self-determination« Anwendung finden können.

176 Jean-Baptiste Jeangène Vilmer, *The »Macron Leaks« Operation: A Post-mortem*, Washington, D.C.: Atlantic Council, Juni 2019, <https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf> (Zugriff am 1.3.2021).

Wenn man ein starkes politisches Signal hätte aussenden wollen, hätte dieser Vorfall in das Cybersanktionsregime von 2020 aufgenommen werden müssen. Die US-Strafverfolgungsbehörden hatten im Kontext der NotPetya-Anklage hinsichtlich der Macron-Leaks im Rahmen einer rechtlichen Attribution den russischen GRU verantwortlich gemacht.[177]

Bürozeiten und IP-Adressen im Kontext einer Cyberattacke sind lediglich Indizien für die Urheberschaft eines Akteurs.

e) Zudem ist fraglich, inwiefern die *technische Attribution einen plausiblen Nachweis der rechtlichen Verantwortlichkeit* erlaubt. Aus der Analyse der bisherigen Cyberangriffe in der EU wird nicht immer deutlich, welche technischen IoCs eine angemessene Grundlage für eine rechtlich-normative Attribution von Cyberangriffen nach europarechtlicher (oder auch völkerrechtlicher) Bewertung darstellen. Bürozeiten und IP-Adressen im Kontext einer Cyberattacke sind lediglich Indizien, aber keine Belege für die Urheberschaft eines im staatlichen Auftrag agierenden Akteurs. Taxiquittungen, Mobilfunklogs und gehackte Überwachungskameras im GRU-Hauptquartier haben dagegen eine größere Beweiskraft. Die Diskrepanz zwischen den technischen Indikatoren und den rechtlich erforderlichen Tatbestandsmerkmalen ist evident: In den Fällen Bundestag-Hhack und Cloud Hopper sind die Informationen spärlich, die die EU bzw. die Bundesregierung veröffentlichte, verglichen mit den öffentlich einsehbaren Erkenntnissen der IT-Sicherheitsunternehmen, den technischen Details in US-amerikanischen Anklageschriften in ähnlich gelagerten Fällen und der Transparenzoffensive der niederländischen Regierung nach dem OVCW-Vorfall.

f) Die Uneinheitlichkeit der Beweislage und *die mangelnde Transparenz* der rechtlichen Beweisführung beeinträchtigen die Legitimität der Sanktionen. Eine möglichst breite und von der Öffentlichkeit nachvollziehbare Fundierung der Forensik würde dazu beitragen, die Sanktionen plausibler zu machen. Die US-Anklageschriften in den hier diskutierten Fällen leisten dies in weit größerem Umfang, als die EU dies mit ihren im Amtsblatt veröffentlichten Begründungen vermag, und sie tragen die Belege auch offensiver vor. Die Mitgliedstaaten sollten für eine technisch versierte und rechtlich fundierte Legitimierung von Cybersanktionen eintreten, im wohlverstandenen Eigeninteresse übrigens, denn EU-Sanktionsentscheidungen können vor dem Europäischen Gerichtshof juristisch angefochten werden.[178]

g) Eine weitere Uneinheitlichkeit zeigt sich bei den Beweisstandards, insbesondere im Fall des Bundestag-Hacks. Die diesbezüglich vorgenommene Attribution beruht laut Bundesregierung auf einer »insgesamt sehr guten eigenen Fakten- und Quellenlage«.[179] In den anderen Fällen sind sich die europäischen, US-amerikanischen und britischen Sicherheitsbehörden mal »mit an Sicherheit grenzender Wahrscheinlichkeit«, mal nur »mit hoher Gewissheit« sicher bei ihrer Attribution. Eine europaweite, besser noch transatlantisch vereinheitlichte Terminologie und Methodik wäre allein schon bei Rechtshilfeersuchen hilfreich. Wenn dann noch die Informationen zur Beweislage künftig systematischer aufgearbeitet, kategorisiert und in enger Absprache mit verbündeten Staaten veröffentlicht werden, könnten Cybersanktionen auf EU-Ebene deutlich plausibler gemacht werden als bisher.

Diskussionswürdig ist letztlich auch die *Qualität der Gegenreaktionen*, also der Sanktionen selber. In allen Fällen wurden Reisebeschränkungen verhängt und Konten eingefroren. Für die Cyberangriffe Cloud Hopper, Bundestag-Hack und den OVCW-Vorfall mag dies adäquat und proportional sein. WannaCry und NotPetya dagegen sind viel schwerwiegendere Fälle. Sie erfüllen weitaus mehr und vor allem gewichtigere Tatbestandsmerkmale wie große finanzielle Schäden und die Sabotage kritischer Infrastrukturen. NotPetya ist nach Rechtsauffassung einiger Beobachter sogar unmittelbar an der Schwelle zu einem bewaffneten Angriff zu verorten.[180] Die Intensität der Sanktionen

177 United States District Court Western District of Pennsylvania, *United States of America v. Yuri Sergeyevich Andrienko* [wie Fn. 106].

178 Ivan, *Responding to Cyberattacks* [wie Fn. 102].

179 »Cyberattacken: Regierung beschuldigt Russland offiziell«, in: *Süddeutsche Zeitung* (online), 5.10.2018, <https://www.sueddeutsche.de/service/internet-cyberattacken-regierung-beschuldigt-russland-offiziell-dpa.urn-newsml-dpa-com-20090101-181005-99-250924> (Zugriff am 2.6.2021).

180 Piret Pernik, »Responding to ›the Most Destructive and Costly Cyberattack in History‹«, Tallinn: International Centre for Defence and Security (ICDS), 23.2.2018, <https://icds.ee/

erscheint hier nicht in einem angemessenen Verhältnis zur Intensität der Angriffe. Es ließe sich durchaus argumentieren, dass in beiden Fällen deutliche Souveränitätsverletzungen begangen wurden, die völkerrechtliche Gegenmaßnahmen erlaubt hätten.[181]
Schnelle und differenzierte EU-Sanktionen als Reaktion auf Cyberangriffe werden auf absehbare Zeit die Ausnahme bleiben. Die Kohärenz des Sanktionsvorgangs sollte durch einen reformierten Blueprint der Kommission (siehe oben, S. 16) verbessert werden. Die neu geschaffene Gemeinsame Cyber-Stelle (Joint Cyber Unit) der Kommission wird künftig eine wichtige Rolle in der europäischen Cybersicherheit spielen, neben Europol, ENISA und dem EU-CERT. Die von der EU betriebene Politik der Attribution wird aber künftig sicherlich nicht allein von der EU-Kommission gesteuert werden können. Die Kommission wird gerade in dieser Frage auf eine enge Absprache mit der Ratsarbeitsgruppe HWP Cyber angewiesen sein.

en/responding-to-the-most-destructive-and-costly-cyberattack-in-history/> (Zugriff am 2.6.2021).

181 Alex Hern, »›NotPetya‹ Malware Attacks Could Warrant Retaliation, Says Nato Affiliated-Researcher«, in: *The Guardian* (online), 3.7.2017, <https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik> (Zugriff am 2.6.2021).

Schlussfolgerungen

In der Attributionspolitik der EU zeigt sich, dass die vertikale, horizontale und institutionelle Kohärenz im auswärtigen Handeln der EU und zwischen den EU-Mitgliedstaaten zu wünschen übrig lässt. Der Zwang, im Rat einstimmig zu entscheiden, und die mangelnde rechtliche und finanzielle Ausstattung des EAD machen es der EU schwer, sich in der internationalen Cyberdiplomatie zu profilieren. Die Bundesregierung sollte die französische Ratspräsidentschaft dabei unterstützen, für den Erlass von EU-Cybersanktionen qualifizierte Mehrheitsentscheidungen als Regelfall einzuführen. Im Interesse der Sicherheit der Union und ihres Binnenmarkts ist es geboten, restriktive Maßnahmen der GASP, wie EU-Cybersanktionen, schneller als bisher zu initiieren und zuverlässig zu verhängen, um Täter und Angreifer umgehend zur Rechenschaft zu ziehen.

Die rechtlichen Begriffe in den EU-Verordnungen sollten geschärft und mit der technischen Forensik stärker in Beziehung gesetzt werden. Bei der praktischen Umsetzung dieser Aufgabe muss eine Reihe von Voraussetzungen erfüllt werden. Denn für eine eindeutige technische Attribution, die Aufschlüsse über die Angriffsmotivation zulässt, sind hohe rechtliche Hürden zu überwinden, wenn die in der einschlägigen Verordnung dargelegten Kriterien erfüllt werden sollen, die für die Bestimmung der Urheberschaft unabdingbar sind. Idealerweise müsste die Politik der Attribution hinsichtlich der rechtlichen Vorgaben angepasst werden. Gelingt dies nicht, wäre gegebenenfalls das Recht anzupassen. Die Einführung einer Unterscheidung zwischen notwendigen und hinreichenden Attributionsstandards gemäß einem einheitlichen Bewertungssystem (Propability Yardstick) wäre mit den rechtsstaatlichen Erfordernissen des Unionsrechts und den gegenwärtigen Möglichkeiten der technischen Forensik zumindest abzugleichen. Auch Erfahrungen aus anderen internationalen Cyberattacken können herangezogen werden. So gab es zum Beispiel schon vor der Operation Cloud Hopper vergleichbare Supply-Chain-Angriffe. Cloud Hopper hat böswilligen Hackern die Attraktivität eines derartigen Angriffs auf den Binnenmarkt bestätigt, frei nach dem Motto »hacke einmal, ernte vielmals«. Die Reaktion auf Versorgungskettenangriffe sollte daher — entsprechend den Empfehlungen der Kommission in dem Blueprint-Dokument — durch Cyberabwehrübungen der ENISA eingeübt werden.

Laut der neuen EU-Cybersicherheitsstrategie von 2020 sollen private Unternehmen, öffentliche Einrichtungen und nationale Behörden ihre Informationen über Cybervorfälle systematisch und umfassend austauschen. Dies wird als Voraussetzung für eine gemeinsame Reaktion der EU angesehen. Die Gemeinsame Cyber-Stelle bei der EU-Kommission soll als »virtuelle und physische Plattform für die Zusammenarbeit der verschiedenen Cybersicherheitskreise in der EU dienen«. Ihr Schwerpunkt soll dabei auf »der operativen und technischen Koordinierung bei schwerwiegenden grenzüberschreitenden Cybervorfällen und Bedrohungen« liegen. Diese operative Zusammenarbeit im Dienste der Cybersicherheit soll gemäß der Sorgfaltsverantwortung der Cyberdiplomatie intensiviert werden. Die Cyber-Stelle soll auch eine Drehscheibe für die Kommunikation mit den Five Eyes sein, damit über die Grenzen der EU hinaus gemeinsame, öffentliche Attributionen möglich werden.

Inzwischen gibt es auch eine Debatte darüber, inwieweit EU-Regierungen und die EU sich dafür rüsten sollten, Gegenschläge auszuführen. Auch die Cybersicherheitsstrategie enthält darauf bereits einen Hinweis. Fälle wie WannaCry und NotPetya unterstreichen die Dringlichkeit. Demnach will die EU einen »Vorschlag zur näheren Definition der EU-Cyberabschreckung« erarbeiten. Aktive Cyberabwehrmaßnahmen wären nach der Cyber Diplomacy Toolbox die höchste Eskalationsstufe nach vorausgehender Aktivierung der vertraglich verankerten Solidaritäts- bzw. Beistandsklausel. Sie können nur ergriffen werden, soweit sie im Einklang mit dem humanitären Völkerrecht sind. Die letzte Stufe des Krisenmanagements bestünde darin, einen laufenden Angriff durch aktive Gegenwehr zu stoppen. Ultima Ratio wäre ein sogenannter Hackback, also das gezielte Ausschalten eines Servers, von dem ein Angriff ausgeht. Im Sinne der Sorgfaltsverantwortung wäre dies nur dann zu

rechtfertigen, wenn ein laufender Angriff schwere, existenzbedrohende Folgen hat und alle anderen Mittel ausgereizt sind. Die dafür notwendigen rechtlichen Rahmenbedingungen und die Kompetenzverteilung sind noch nicht festgelegt, selbst auf nationaler Ebene nicht, geschweige denn, dass das hierfür erforderliche Attributionsverfahren auf EU-Ebene bereits rechtlich formalisiert wäre. Ein Krisenmanagement, bei dem alle 27 Mitgliedstaaten zustimmen müssten, eine digitale Cyberabwehr zu aktivieren, dürfte sich nach derzeitigem Stand im Notfall als zu komplex und zu langsam erweisen.

Umso mehr gilt es, die Attributionskompetenz der EU und die IT-Sicherheit im Binnenmarkt zu stärken. Ungeachtet der sicherlich richtigen Erkenntnis, dass für eine solide Attribution viele Voraussetzungen erfüllt sein müssen, ist es ein Erfordernis für die Durchsetzung des Rechtsstaatsprinzips, dass Täter und Angreifer zur Rechenschaft gezogen werden. Deshalb ist die Schaffung von Analysefähigkeiten eine notwendige Bedingung, in die es zu investieren lohnt. Ebenso muss ein verbindlicher IT-Grundschutz in der EU gewahrt sein. Neue gesetzliche Vorschriften, wie sie im Zuge der Reform der geltenden Netzwerk- und Informationssicherheitsrichtlinie und durch das von Binnenmarktkommissar Thierry Breton im September 2021 angekündigte Cyberresilienzgesetz zu erwarten sind, werden sich zu Recht auf die Absicherung von Infrastrukturen, Cloud-Diensten und Lieferketten im weiteren Sinne konzentrieren. Die Vorgabe für Kapitalgesellschaften, gegen Cybersicherheitsbedrohungen Vorsorge zu treffen, führt derzeit aber nicht dazu, dass die nötigen finanziellen Mittel in den Aufbau widerstandsfähiger IT-Systeme investiert werden; Mittel fließen stattdessen in den Abschluss von Versicherungspolicen. Die Ursachen für zahlreiche Angriffe und deren Erfolg liegen in der unzureichenden Absicherung der Basissoftware, die oft aus den USA stammt, wo Firmen nicht für deren Sicherheitsmängel zur Verantwortung zu ziehen sind. Auch an diesem Punkt ist folglich eine enge transatlantische Abstimmung notwendig, will man vermeiden, dass sich die Rechtsvorschriften auf beiden Seiten des Atlantiks nicht konterkarieren.

Die wichtigsten und dauerhaft wirksamsten Maßnahmen der operativen Zusammenarbeit innerhalb der Union und mit den Partnern der Five Eyes sind Prävention und Detektion. Wie anhand der Diskrepanz zwischen der Detektion der technischen IoCs und der politischen bzw. rechtlichen Attribution gezeigt wurde, spielt die politische Bewertung eines Vorfalls im Rahmen eines strategischen Lagebilds durch die Hybrid Fusion Cell im EAD eine besondere Rolle. Sie muss das Gesamtbild der Vorfälle im Cyberraum berücksichtigen, weil auch mit militärisch relevanten hybriden Bedrohungen zu rechnen ist. Dazu wäre es sinnvoll, vergangene und aktuelle Angriffskampagnen, vermutete Urheber, Ziele, die Zahl der betroffenen Mitgliedstaaten, aufgetretene Schäden und deren rechtliche Einordnung in einer Art Cyber-Konfliktdatenbank zu sammeln und diese Informationen den Mitgliedstaaten zur Verfügung zu stellen. Das führt mit größerer Wahrscheinlichkeit zu einem gemeinsamen Verständnis der Vorfälle und im Idealfall zu einer kohärenten Reaktion. Dafür wäre der EAD mit mehr technisch versiertem und rechtlich qualifiziertem wissenschaftlichem Personal zu besetzen. Erst eine fundierte Forensik ermöglicht eine strategisch substanzielle Lagebilderstellung.

Für einen vergleichbaren Austausch zum Schutz kritischer Infrastruktur ist das bisherige CSIRT-Netz in der EU mit seinen technischen Kompetenzen zwar hilfreich; für ein verbessertes Attributionsmanagement der EU gilt es aber, die Joint Cyber Unit in der EU-Kommission auszubauen. Cyberdiplomatie setzt eine kontinuierliche Kommunikation zwischen den nationalen Sicherheitsbehörden, der Wirtschaft und Wissenschaft voraus. Diese Aufgabe obliegt der Gemeinsamen Cyber-Stelle, die sie wiederum nur in enger Absprache mit dem EAD in der Single Intelligence Analysis Capacity erfüllen kann. Öffentliche und private CERT-Verbünde und Zusammenschlüsse in der Industrie sind ebenfalls unverzichtbar, wenn es darum geht, Expertenwissen zur Cyberdiplomatie zu bündeln. Es könnte, wie erwähnt, erwogen werden, zwischen hinreichenden und notwendigen Attributionsstandards zu unterscheiden. Damit bei dieser Thematik die Schnittstellen zwischen dem Rat und der Kommission künftig reibungsloser funktionieren, können neben EU INTCEN auch die Joint Cyber Unit der Kommission und Europol (EC3) diese Knotenpunkte gemeinsam managen. Als Institution wäre Europol in besonderem Maße prädestiniert, die Kompetenzgrenzen zwischen dem GASP-Verfahren des EAD und dem Krisenmanagementverfahren der Kommission aufzuweichen. Ultima Ratio wäre die Schaffung eines Doppelhuts auf höchster Ebene in der Funktion des Präsidenten des Europäischen Rates und der Kommissionspräsidentin. Im Falle der Fusion läge dann die strategische Lagebilderstellung zum Schutz des Binnenmarkts und zur EU-Sicherheitsunion in supranationaler Kompetenz.

Anhang

Glossar

Advanced Persistent Threat (APT)
Ein Advanced Persistent Threat liegt dann vor, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter Angreifender zu Zwecken der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt.html>

Backdoor
Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (»Hintertür«) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt, die sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen richten.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132796>

Bootloader
Ein Bootloader ist ein Startprogramm, das durch die Firmware eines Rechners von einem startfähigen Medium geladen und anschließend ausgeführt wird. Der Bootloader lädt dann weitere Teile des Betriebssystems, gewöhnlich einen Kernel.
<https://de.wikipedia.org/wiki/Bootloader>

Bug / Schwachstelle / Sicherheitslücke
Mit Bugs werden Fehler in Programmen bezeichnet. Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam und eine Institution oder ein System geschädigt wird. Existiert eine Schwachstelle, ist ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132814>

Command & Control Server (C2)
Die meisten Schadprogramme nehmen nach der Infektion eines Systems Kontakt zu einem Kontrollserver (C&C-Server) der Angreifer im Internet auf, um von dort weiteren Schadcode nachzuladen, Instruktionen zu empfangen oder auf dem infizierten System ausgespähte Informationen (wie Benutzernamen und Passwörter) an diesen Server zu übermitteln. Die Kontaktaufnahme erfolgt häufig unter Verwendung von Domainnamen, die von den Tätern speziell für diesen Zweck registriert wurden.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132798>

DNS
Das Domain Name System (DNS) ordnet den im Internet genutzten Adressen und Namen, wie beispielsweise www.bsi.bund.de, die zugehörige IP-Adresse zu.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132772>

Domaincontroller
Der Domain- oder Domänencontroller ist ein Server, der eine Domäne und seine verschiedenen Objekte zentral verwaltet und kontrolliert. Anwender, die sich an einer Netzwerkdomäne anmelden möchten, wenden sich zuerst an den für ihre Domäne zuständigen Domänencontroller.
<https://www.ip-insider.de/was-ist-ein-domaenen controller-a-626094/>

Eternalblue
Eternalblue ist ein → Exploit, der Programmierfehler in der → SMB-Implementierung (auch NetBIOS bzw. Common Internet File System) des Betriebssystems Windows ausnutzt. Die Lücke wird als CVE-2017-0144 (SMB Remote Windows Kernel Pool Corruption) bezeichnet.
<https://de.wikipedia.org/wiki/EternalBlue>

Exploit
Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle lässt sich mit Hilfe eines Exploits zum Beispiel ein Programm zum Absturz bringen, lassen sich Benutzerrechte ausweiten oder beliebiger Programmcode ausführen.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfeh lungen/Glossar-der-Cyber-Sicherheit/Functions/glossar. html?nn=522504&cms_lv2=132800>

Five Eyes
Nachrichtendienstallianz, bestehend aus den USA, Großbritannien, Kanada, Australien und Neuseeland.
<https://en.wikipedia.org/wiki/Five_Eyes>

Indicators of Compromise
Indicators of Compromise (IoCs) sind technische Informationen, die zur Detektion einer Infektion mit Schadsoftware oder einer anderweitigen Kompromittierung verwendet werden können. Häufig handelt es sich dabei um netzwerkbasierte Signaturen wie Domainnamen von Kontrollservern oder um hostbasierte Signaturen, die auf den Endgeräten gesucht werden (wie Hashsummen von Schadprogrammen, Einträge in der Windows-Registry o.Ä.).
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfeh lungen/Glossar-der-Cyber-Sicherheit/Functions/glossar. html?nn=522504&cms_lv2=132764>

Industroyer
Industroyer ist eine Malware, von der angenommen wird, dass sie bei dem Cyberangriff auf das ukrainische Stromnetz am 17. Dezember 2016 verwendet wurde. Der Angriff schnitt ein Fünftel der Hauptstadt Kiew für eine Stunde vom Strom ab. Es ist die erste bekannte Malware, die speziell für den Angriff auf Stromnetze entwickelt wurde.
<https://malpedia.caad.fkie.fraunhofer.de/details/win. industroyer>

IP-Adresse
Eine Adresse, unter der ein Rechner innerhalb eines Netzwerks nach dem Internetprotokoll (IP) erreichbar ist.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfeh lungen/Glossar-der-Cyber-Sicherheit/Functions/glossar. html?nn=522504&cms_lv2=132764>

Keylogger
Ein Keylogger (dt. »Tasten-Protokollierer«) ist eine Hard- oder Software, die dazu verwendet wird, die Eingaben des Benutzers an der Tastatur eines Computers zu protokollieren und damit zu überwachen oder zu rekonstruieren.
<https://de.wikipedia.org/wiki/Keylogger>

Mimikatz
Mimikatz ist ein freies und quelloffenes Programm für Microsoft Windows, mit dem, unter Ausnutzung von Schwachstellen, zwischengespeicherte Anmeldeinformationen (Credentials) angezeigt werden können.
<https://de.wikipedia.org/wiki/Mimikatz>

MSP
Ein Managed Services Provider (MSP) (engl. für Betreibermodellanbieter oder Betreiberlösungsanbieter) ist ein Informationstechnologie-Dienstleister, der die Verantwortung für die Bereitstellung einer definierten Reihe von Dienstleistungen für seine Kunden übernimmt und verwaltet.
<https://de.wikipedia.org/wiki/Managed_Services_ Provider>

Patch
Ein Patch (»Flicken«) ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Die Einspielung dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als Patch-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132810>

Phishing
Das Wort setzt sich aus »Password« und »Fishing« zusammen, zu Deutsch »nach Passwörtern angeln«. Beim Phishing wird zum Beispiel mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten unter Umständen selbst unwissentlich in die Hände Unberechtigter.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132810>

Ransomware
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch »ransom«) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.
<https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?cms_lv2=132812>

RAT (Remote Access Trojan)
Ein Remote-Access-Trojaner (RAT) ist eine Art von Malware, die dem Angreifer die vollständige Fernkontrolle über ein System ermöglicht. Wenn ein RAT auf einen Computer gelangt, ermöglicht er dem Hacker den einfachen Zugriff auf die lokalen Dateien, die sichere Anmeldeautorisierung und andere sensible Informationen, oder er nutzt diese Verbindung, um Viren herunterzuladen, die unbeabsichtigt an andere weitergegeben werden könnten.
<https://heimdalsecurity.com/blog/what-is-a-remote-access-trojan-rat/>

Single Point of Failure
Unter einem Single Point of Failure (kurz SPOF bzw. dt.: einzelner Ausfallpunkt) versteht man einen Bestandteil eines technischen Systems, dessen Ausfall den Ausfall des gesamten Systems nach sich zieht.
<https://de.wikipedia.org/wiki/Single_Point_of_Failure>

SMB
Server Message Block (SMB), in einer Ur-Version auch als Common Internet File System (CIFS) bezeichnet, ist ein Netzprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen. Es ist ein zentraler Teil der Netzdienste der Windows-Produktfamilie und erlaubt den Zugriff auf Dateien und Verzeichnisse, die sich auf einem anderen Computer befinden.
<https://de.wikipedia.org/wiki/Server_Message_Block>

SSL-Zertifikat
Ein SSL-Zertifikat ist eine kleine Datei, die einen kryptografischen Schlüssel digital an die Details einer Organisation bindet. Wenn es auf einem Webserver installiert ist, aktiviert es das https-Protokoll und ermöglicht sichere Verbindungen von einem Webserver zu einem Browser. Typischerweise wird SSL verwendet, um Kreditkarten-Transaktionen, Datentransfers und Logins zu sichern. SSL wird in jüngerer Zeit immer mehr zur Norm bei der Sicherung des Browsens.
<https://www.globalsign.com/de-de/ssl-information-center/was-ist-ein-ssl-zertifikat>

TTP (Tools, Tactics & Procedures)
Das Gesamtbild des Angriffsverhaltens, das sich aus den verwendeten Mitteln, den eingesetzten Taktiken und Techniken und den bevorzugten Abläufen eines Akteurs ergibt. Eine Taktik ist die Beschreibung des Verhaltens auf höchster Ebene; Techniken bieten eine detailliertere Beschreibung des Verhaltens im Kontext einer Taktik; und Prozeduren bieten eine untergeordnete, sehr detaillierte Beschreibung des Verhaltens im Kontext einer Technik.
<https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures>

Wiper
Ein Wiper ist eine Klasse von Malware, deren Ziel es ist, die Festplatte des von ihr infizierten Computers zu löschen.
<https://en.wikipedia.org/wiki/Wiper_(malware)>

Zero Day
Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, bezeichnet man als Zero-Day-Exploit. Die Öffentlichkeit und insbesondere der Hersteller des betroffenen Produkts erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die sich diese Schwachstelle zunutze machen. Der Begriff Zero Day leitet sich also davon ab, dass ein entsprechender → Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch den Hersteller existierte — also an einem fiktiven »Tag null«. Der Hersteller hat folglich keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132776>

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AIVD	Algemene Inlichtingen- en Veiligheidsdienst (niederländischer In- und Auslandsgeheimdienst)
APT	Advanced Persistent Threat
AStV/Coreper	Ausschuss der Ständigen Vertreter
BBC	British Broadcasting Corporation
BKA	Bundeskriminalamt
BSI	Bundesamt für die Sicherheit in der Informationstechnik (Bonn)
C2	Command & Control (Server)
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CCED	Canadian Centre for Ethics in Sport (Ottawa)
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency (USA)
CIR	Cyber- und Informationsraum
CSIRT	Computer Security Incident Response Team
DNC	US Democratic National Committee
DNS	Domain Name System
EAD	Europäischer Auswärtiger Dienst
EC3	European Cybercrime Centre (bei Europol)
ENISA	European Union Agency for Cybersecurity
EuGH	Europäischer Gerichtshof
EU INTCEN	European Union Intelligence and Situation Centre
EU LE ERP	EU Law Enforcement Emergency Response Protocol
EUMS	European Union Military Staff
EUV	Vertrag über die Europäische Union
FBI	Federal Bureau of Investigation (USA)
GASP	Gemeinsame Außen- und Sicherheitspolitik (der EU)
GCHQ	Government Communications Headquarters (UK)
GIGA	German Institute of Global and Area Studies (Hamburg)
GRU	Glawnoje Raswedywatelnoje Uprawlenije (Russischer Militärnachrichtendienst)
GTsSS	Glawnii Zentr Spezial'noj Sluschbi (85. Hauptzentrum für Spezialdienste der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation)
GTsST	Glawnii Zentr Spezial'nych Technologii (Hauptzentrum für Spezialtechnologien der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation)
HR	High Representative (High Representative of the Union for Foreign Affairs and Security Policy)
HWPCI	Horizontal Working Party on Cyber Issues (auch: HWP Cyber)
HWP ERCHT	Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats
ICDS	International Centre for Defence and Security (Tallinn)
ICJ	International Court of Justice
IGH	Internationaler Gerichtshof
IKT	Informations- und Kommunikationstechnologie
ILC	International Law Commission

INTCEN	siehe EU INTCEN
IoC	Indicator of Compromise (Kompromittierungs-indikator)
IP	Internet Protocol
IPCR	Integrated Political Crisis Response (EU)
IS	»Islamischer Staat«
i.V.m.	in Verbindung mit
JCAT	Joint Cybercrime Action Taskforce (bei Europol)
KRITIS	Kritische Infrastrukturen
MIVD	Militaire Inlichtingen- en Veiligheidsdienst (niederländischer Militärgeheimdienst)
MSP	Managed Service Provider
NCSC	National Cyber Security Centre (UK)
NIS	Network and Information Security (Directive, EU)
NSA	National Security Agency (USA)
OSINT	Open Source Intelligence
OVCW	Organisation für das Verbot chemischer Waffen (Den Haag)
PSK	Politisches und Sicherheitspolitisches Komitee (der EU)
RAT	Remote-Access-Trojaner
SIAC	Single Intelligence Analysis Capacity
SMB	Server Message Block
SOCMINT	Social Media Intelligence
SPOF	Single Point of Failure
TTP	Tools, Techniques/Tactics & Procedures
UN	United Nations/Vereinte Nationen
USADA	United States Anti-Doping Agency
VO	Verordnung
VP	Vizepräsident der EU-Kommission
VPN	Virtual Private Network
WADA	World Anti-Doping Agency (Montreal)

Vergleichstabelle der Fälle (nur online)

Siehe die Tabelle unter https://bit.ly/SWP21S17Anhg

Weitere SWP-Publikationen zum Thema

Matthias Schulze
Ransomware. Technische, nationale und multilaterale Gegenmaßnahmen
SWP-Aktuell 56/2021, 31.8.2021, 8 Seiten

Annegret Bendiek / Matthias C. Kettemann
EU-Strategie zur Cybersicherheit: Desiderat Cyberdiplomatie
SWP-Aktuell 12/2021, 9.2.2021, 8 Seiten

Annegret Bendiek / Matthias Schulze
Schwachstellen der deutschen Cybersicherheitsstrategie 2021
SWP-Kurz gesagt, 20.9.2021