EUROPÄISCHER RECHNUNGSHOF

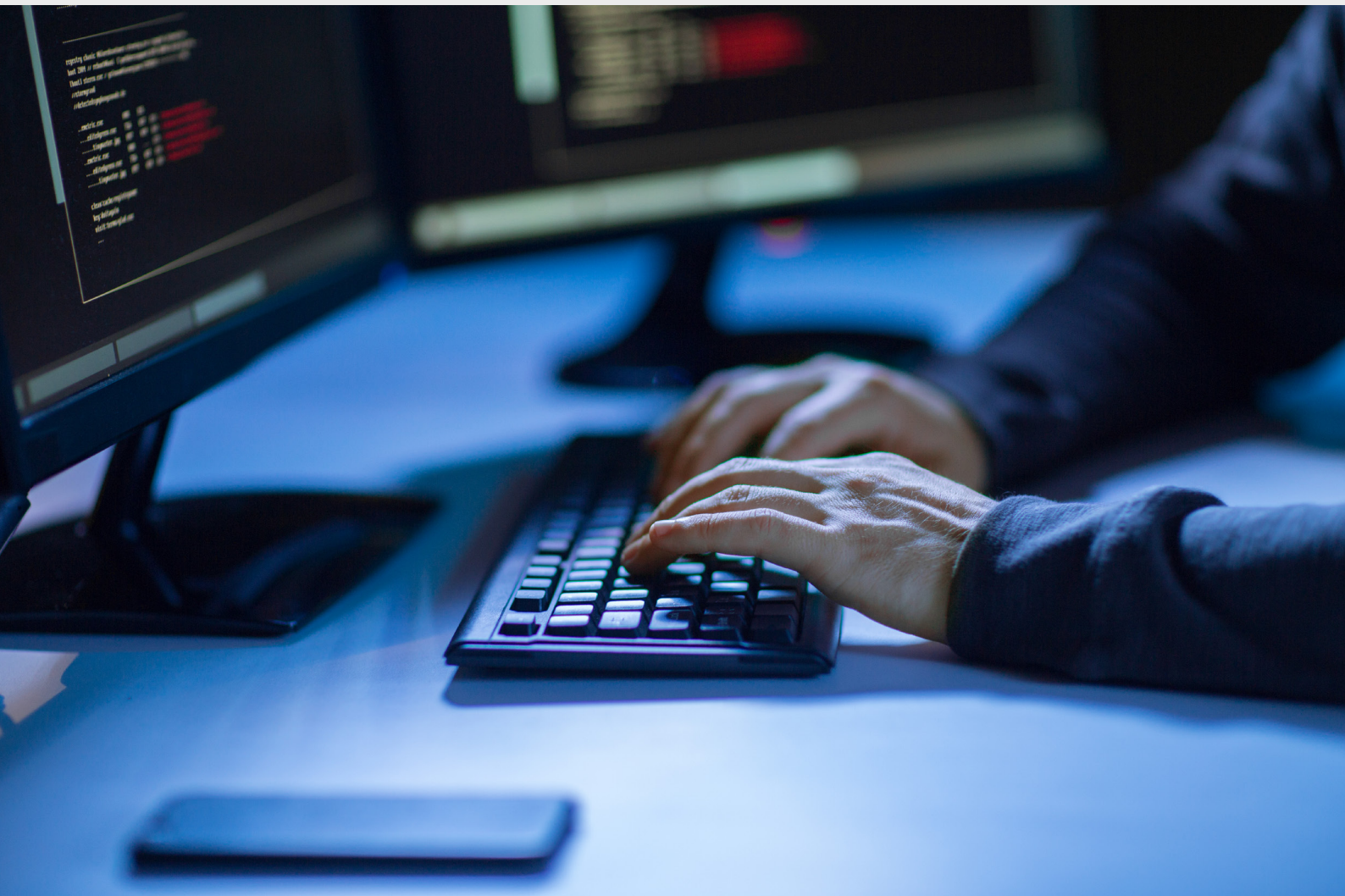
DE

2019

Herausforderungen für eine wirksame Cybersicherheitspolitik der EU

Themenpapier

März 2019



Über das Themenpapier:

Dieses Themenpapier stellt keinen Prüfungsbericht dar. Es soll vielmehr einen Überblick über die komplexe Politik der EU im Bereich der Cybersicherheit bieten und aufzeigen, wo die größten Herausforderungen für die wirksame Umsetzung der Politik liegen. Betrachtet werden Netz- und Informationssicherheit, Cyberkriminalität, Cyberabwehr und Desinformation. Das Themenpapier wird auch die Grundlage für künftige Prüfungen in diesem Bereich bilden.

Unsere Analyse basiert auf der Untersuchung von Informationen, die in amtlichen Dokumenten, Positionspapieren und Studien von Dritten öffentlich zugänglich sind. Die Bestandsaufnahme fand zwischen April und September 2018 statt, wobei die bis Dezember 2018 eingetretenen Entwicklungen berücksichtigt wurden. Zusätzlich wurde eine Erhebung bei den Rechnungskontrollbehörden der Mitgliedstaaten durchgeführt und es wurden wichtige Akteure aus den EU-Organen und Vertreter des Privatsektors befragt.

Die von uns ermittelten Herausforderungen lassen sich in vier große Gruppen einteilen: i) die politischen Rahmenbedingungen, ii) Finanzierung und Ausgaben, iii) Stärkung der Cyber-Resilienz und iv) wirksame Reaktion auf Cybervorfälle. Die Cybersicherheit in der EU zu erhöhen, bleibt eine absolute Notwendigkeit. Daher mündet jedes Kapitel in eine Reihe von Denkanstößen für die politischen Entscheidungsträger, Gesetzgeber und Fachleute aus der Praxis.

Unser Dank gilt den Kommissionsdienststellen, dem Europäischen Auswärtigen Dienst, dem Rat der Europäischen Union, der ENISA, Europol, der Europäischen Cybersicherheitsorganisation und den Rechnungskontrollbehörden der Mitgliedstaaten für ihr konstruktives Feedback.

Inhalt

Zusammenfassung

I Technologie eröffnet unendlich viele neue Möglichkeiten mit neuen Produkten und Diensten, die Teil unseres Alltags werden. Im Gegenzug erhöht sich aber auch die Gefahr, Opfer von Cyberkriminalität oder Cyberangriffen zu werden, und die gesellschaftlichen und wirtschaftlichen Auswirkungen dieser Phänomene steigen stetig. Die jüngsten Bemühungen der EU seit 2017, die Maßnahmen zur Verbesserung der Cybersicherheit und Stärkung der digitalen Autonomie voranzutreiben, fallen daher in eine entscheidende Phase.

II Dieses Themenpapier stellt keinen Prüfungsbericht dar. Es beruht auf öffentlich zugänglichen Informationen und soll einen Überblick über ein komplexes und uneinheitliches Gefüge politischer Maßnahmen geben und aufzeigen, wo die größten Herausforderungen für die wirksame Umsetzung der Politik liegen. Gegenstand unseres Themenpapiers sind die Cybersicherheitspolitik der EU sowie die Cyberkriminalität und Cyberabwehr und die zur Bekämpfung von Desinformation ergriffenen Maßnahmen. Die von uns ermittelten Herausforderungen lassen sich in vier große Gruppen einteilen: i) die politischen und rechtlichen Rahmenbedingungen, ii) Finanzierung und Ausgaben, iii) Stärkung der Cyber-Resilienz und iv) wirksame Reaktion auf Cybervorfälle. Jedes Kapitel umfasst einige Denkanstöße zu den genannten Herausforderungen.

Die politischen und rechtlichen Rahmenbedingungen

III Maßnahmen zu entwickeln, die am weitgefassten Ziel der EU-Cybersicherheitsstrategie – das weltweit sicherste digitale Umfeld zu schaffen – ausgerichtet sind, stellt in Ermangelung messbarer Ziele und spärlicher verlässlicher Daten ein schwieriges Unterfangen dar. Ergebnisse werden selten gemessen, und es wurden nur einige wenige Politikbereiche evaluiert. Eine wesentliche Herausforderung besteht also darin, durch den Übergang zu einer Leistungskultur mit integrierten Evaluierungsverfahren eine **angemessene Rechenschaftspflicht und aussagekräftige Evaluierung zu gewährleisten**.

IV Der Rechtsrahmen ist nach wie vor nicht vollendet. **Lücken und Inkohärenzen bei der Umsetzung von EU-Recht in nationales Recht** können dazu führen, dass Rechtsvorschriften nicht voll und ganz greifen.

Finanzierung und Ausgaben

V **Investitionsniveau und Ziele in Einklang zu bringen** ist schwierig: Dazu müssen nicht nur die Gesamtinvestitionen in die Cybersicherheit – die in der EU bisher niedrig waren und nach dem Gießkannenprinzip erfolgten – aufgestockt werden, sondern es muss auch die Wirkung erhöht werden, insbesondere durch bessere Nutzung der mit Forschungsausgaben erzielten Ergebnisse und Sicherstellung einer gezielten Ausrichtung auf und Förderung von Start-up-Unternehmen.

VI **Die Ausgaben der EU klar im Blick zu haben** ist entscheidend für die Union und die Mitgliedstaaten, denn nur so ist ersichtlich, wo es Lücken zu schließen gilt, um die gesetzten Ziele zu erreichen. Da es kein spezielles EU-Budget für die Finanzierung der Cybersicherheitsstrategie gibt, ist nicht klar, welche Mittel wohin fließen.

VII In Zeiten, in denen die politischen Prioritäten mehr und mehr von Sicherheitserwägungen bestimmt werden, könnte **Ressourcenknappheit in den für Cyberfragen zuständigen EU-Agenturen** dazu führen, dass die Union ihre ehrgeizigen Ziele nicht verwirklichen kann. Hierbei gilt es auch, Wege für die dauerhafte Anwerbung von Talenten zu erschließen.

Stärkung der Cyber-Resilienz

VIII In der EU und auf internationaler Ebene bestehen im öffentlichen wie im privaten Sektor zahlreiche Schwachstellen im Bereich der Cybersicherheits-Governance. Dadurch kann die internationale Gemeinschaft nur eingeschränkt auf Cyberangriffe reagieren und solche Angriffe eindämmen. Außerdem erschwert dies eine EU-weit kohärente Herangehensweise. Die Herausforderung besteht damit in der **Stärkung der Cybersicherheits-Governance**.

IX **Kompetenzsteigerung und größeres Problembewusstsein** in allen Sektoren und auf allen Ebenen der Gesellschaft sind in Anbetracht des zunehmenden weltweiten Kompetenzdefizits im Bereich der Cybersicherheit von größter Bedeutung. Es gibt derzeit nur wenige EU-weite Standards für Aus- und Fortbildung, Zertifizierung oder Risikobewertung im Cyberbereich.

X Vertrauen ist Voraussetzung für die Stärkung der allgemeinen Cyber-Resilienz. Die Kommission gelangte zu der Einschätzung, dass die Koordinierung generell noch unzureichend ist. **Ein besserer Informationsaustausch und eine bessere Abstimmung** zwischen öffentlichem und privatem Sektor bleiben weiterhin eine Herausforderung.

Wirksame Reaktion auf Cybervorfälle

XI Die digitalen Systeme sind mittlerweile so komplex, dass es schlicht unmöglich ist, alle Angriffe zu verhindern. Die Antwort auf diese Herausforderung lautet **schnelle Erkennung und Reaktion**. Die Cybersicherheit ist jedoch noch nicht vollständig in die auf EU-Ebene vorhandenen Koordinierungsmechanismen zur Krisenreaktion integriert, wodurch die Union möglicherweise weniger gut in der Lage ist, auf große grenzüberschreitende Cybervorfälle zu reagieren.

XII Der **Schutz kritischer Infrastrukturen und gesellschaftlicher Funktionen** ist von entscheidender Bedeutung. Die potenzielle Einmischung in Wahlverfahren und Desinformationskampagnen stellen eine große Herausforderung dar.

XIII Die derzeitige Bedrohungslage durch Cyberangriffe, mit denen die EU und das breitere internationale Umfeld konfrontiert sind, erfordert unentwegtes Engagement und ein unverbrüchliches Bekenntnis zu den Grundwerten der EU.

Einleitung

01 Technologie eröffnet unendlich viele neue Möglichkeiten. Wenn neue Produkte und Dienste aufkommen, werden sie zu einem Bestandteil unseres täglichen Lebens. Allerdings steigt mit jeder neuen Entwicklung auch unsere technologische Abhängigkeit – und in gleichem Maße die Bedeutung der Cybersicherheit. Je mehr personenbezogene Daten wir ins Internet stellen und je weiter die Vernetzung voranschreitet, desto höher ist die Wahrscheinlichkeit, Opfer von Cyberkriminalität oder Cyberangriffen zu werden.

Was ist unter Cybersicherheit zu verstehen?

02 Es gibt keine einheitliche allgemein anerkannte Definition der Cybersicherheit[1]. Grob gesprochen handelt es sich um alle Vorkehrungen und Maßnahmen zum Schutz von Informationssystemen und deren Nutzern vor unbefugten Zugriffen, vor Angriffen und vor Schaden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

03 Cybersicherheit bedeutet, Cybervorfälle zu verhüten oder sie zu erkennen, darauf zu reagieren und sich davon zu erholen. Vorfälle können vorsätzlich ausgelöst werden oder nicht und reichen von der unbeabsichtigten Preisgabe von Informationen bis zu Angriffen auf Unternehmen und kritische Infrastrukturen, zum Diebstahl personenbezogener Daten und sogar zur Einmischung in demokratische Prozesse. Alle Formen können weitreichende negative Auswirkungen auf Einzelpersonen, Organisationen und Gemeinschaften haben.

04 In den politischen Kreisen der EU impliziert der Begriff Cybersicherheit mehr als Netz- und Informationssicherheit. Er umfasst alle rechtswidrigen Aktivitäten, bei denen digitale Technologien im Cyberraum eingesetzt werden. Dazu gehören folglich Akte der Cyberkriminalität wie Angriffe mithilfe von Computerviren und Betrug mit unbaren Zahlungsmitteln und auch die Überbrückung der Kluft zwischen Systemen und Inhalt, wie bei der Verbreitung kinderpornografischen Materials im Netz. Ferner fallen darunter Desinformationskampagnen zur Beeinflussung von Online-Debatten und mutmaßliche Einmischung in Wahlen. Darüber hinaus gehen laut Europol Cyberkriminalität und Terrorismus ineinander über[2].

05 Unterschiedliche Akteure (u. a. Staaten, kriminelle Vereinigungen und Hacktivisten) lösen – aus unterschiedlichen Motiven – Cybervorfälle aus. Die Folgen

dieser Vorfälle sind auf nationaler, europäischer und sogar globaler Ebene spürbar. Das Internet ist nicht fassbar und weitgehend grenzenlos. Diese Eigenschaften und die verwendeten Instrumente und Taktiken machen es oftmals schwer, den Urheber eines Angriffs zu ermitteln (das sogenannte "Zuordnungsproblem").

06 Die zahlreichen Arten von Bedrohungen im Bereich der Cybersicherheit lassen sich nach ihren Auswirkungen auf die Daten – Preisgabe, Veränderung, Zerstörung oder Zugangsverweigerung – oder den verletzten zentralen Grundsätzen der Informationssicherheit einteilen, wie in ***Abbildung 1*** dargestellt. ***Kasten 1*** enthält einige Beispiele für Angriffe. Da die Angriffe auf Informationssysteme immer raffinierter werden, sind unsere Abwehrmechanismen zunehmend zahnloser[3].

Abbildung 1 – Arten von Bedrohungen und welche Sicherheitsgrundsätze sie gefährden

Quelle: Europäischer Rechnungshof in Anlehnung an eine Studie des Europäischen Parlaments[4].
Vorhängeschloss = Sicherheit ist gewährleistet; Ausrufezeichen = Sicherheit ist gefährdet.

Kasten 1

Arten von Cyberangriffen

Mit jedem neuen Gerät, das online genutzt wird oder das sich mit anderen Geräten verbindet, vergrößert sich, was im Jargon der Cybersicherheit als "Angriffsfläche" bezeichnet wird. Das exponentielle Wachstum beim Internet der Dinge, der Cloud, bei Big Data und der Digitalisierung der Industrie geht einher mit einer Zunahme bei der Aufdeckung von Schwachstellen, sodass böswillige Akteure immer mehr Opfer ins Visier nehmen können. Durch die Vielzahl der Angriffsarten und ihre zunehmende Komplexität ist es wirklich schwierig, mit dieser Entwicklung Schritt zu halten[5].

Malware (Schadsoftware) soll Geräte oder Netze beschädigen. Malware ist ein Sammelbegriff für Viren, Trojaner, Ransomware, Würmer, Adware und Spyware. **Ransomware** verschlüsselt Daten, sodass die Nutzer auf ihre Dateien erst wieder Zugriff haben, nachdem sie (i. d. Regel in einer Kryptowährung) Lösegeld gezahlt haben oder eine Aktion ausgeführt wurde. Laut Europol sind Ransomware-Angriffe insgesamt am häufigsten und die Zahl der Ransomware-Varianten ist in den letzten Jahren geradezu explosionsartig angestiegen. **Distributed Denial of Service** bzw. DDoS-Angriffe, die den Ausfall von Diensten oder Ressourcen herbeiführen, indem sie diese mit Anfragen überlasten, nehmen ebenfalls zu. Ein Drittel der Organisationen hatte 2017 mit solchen Angriffen zu tun[6].

Nutzer können so manipuliert werden, dass sie unwissentlich eine Aktion ausführen oder vertrauliche Informationen preisgeben. Mithilfe dieses Tricks kann Datendiebstahl oder Cyberspionage begangen werden. Er wird **Social Engineering** genannt. Erreichen lässt sich dies auf unterschiedlichen Wegen, eine gängige Methode ist jedoch das sogenannte **Phishing**. Dabei werden Nutzer durch E-Mails, die aus vertrauenswürdigen Quellen zu stammen scheinen, zur Preisgabe von Informationen oder zum Anklicken von Links verleitet, durch die Geräte mit Schadsoftware infiziert werden. Mehr als die Hälfte der Mitgliedstaaten berichtete über Untersuchungen im Zusammenhang mit Netzangriffen[7].

Die vielleicht folgenschwerste Art von Bedrohungen sind die fortgeschrittenen, andauernden Bedrohungen, die sognannten "**Advanced Persistent Threats**" (ATP). Dahinter stehen raffinierte Angreifer, deren Ziel das langfristige Ausspähen und Stehlen von Daten und mitunter auch die Zerstörung von Daten ist. Es geht primär darum, so lange wie möglich unentdeckt zu bleiben. ATP sind oftmals staatlich gelenkt und auf besonders sensible Sektoren wie Technologie, Verteidigung und kritische Infrastrukturen ausgerichtet. Mindestens ein Viertel aller Cybervorfälle und der größte Teil der Kosten soll auf Cyberspionage zurückzuführen sein[8].

Wie ernst ist das Problem?

07 Die Auswirkungen einer unzureichenden Vorbereitung auf einen Cyberangriff lassen sich wegen des Mangels an zuverlässigen Daten schwer erfassen. Der durch Cyberkriminalität verursachte wirtschaftliche Schaden ist zwischen 2013 und 2017 um das Fünffache gestiegen[9]. Betroffen waren Staaten und Unternehmen, große ebenso wie kleine. Die prognostizierte Zunahme bei den Prämien für Cyber-Versicherungen von 3 Milliarden Euro im Jahr 2018 auf 8,9 Milliarden Euro im Jahr 2020 ist Ausdruck dieser Entwicklung.

08 Der durch Cyberangriffe verursachte finanzielle Schaden nimmt immer weiter zu. Gleichzeitig besteht eine alarmierende Diskrepanz zwischen den Kosten eines Angriffs und den Kosten für Verhütung, Ermittlung und Schadensbehebung. Die Durchführung eines DDoS-Angriffs kann beispielsweise mit nicht mehr als 15 Euro/Monat zu Buche schlagen. Die Verluste – auch der Imageschaden – für das angegriffene Unternehmen sind hingegen deutlich höher[10].

09 Obwohl 80 % der EU-Unternehmen im Jahr 2016 mindestens einen Cybersicherheitsvorfall verzeichneten[11], ist das Risikobewusstsein immer noch erschreckend niedrig. 69 % der Unternehmen in der EU haben keine oder nur eine grobe Vorstellung von ihrem Gefährdungspotenzial durch Cyberkriminalität[12], 60 % haben noch nie eine Schätzung der potenziellen finanziellen Verluste vorgenommen[13]. Einer internationalen Erhebung zufolge würde außerdem ein Drittel der Unternehmen den Hackern eher Lösegeld zahlen als in Informationssicherheit zu investieren[14].

10 Von den Angriffen mit der Ransomware *Wannacry* und der Wiper-Malware *NotPetya* waren im Jahr 2017 weltweit mehr als 320 000 Nutzer in rund 150 Ländern betroffen[15]. Diese Vorfälle wirkten international wie ein Weckruf für die Gefahr durch Cyberangriffe und brachten die Cybersicherheit wieder zurück ins Zentrum des politischen Denkens. Außerdem sind 86 % der EU-Bürger inzwischen der Ansicht, dass die Gefahr, Opfer von Cyberkriminalität zu werden, zunimmt[16].

Maßnahmen der EU im Bereich der Cybersicherheit

11 Die EU hat seit 2001 Beobachterstatus im Ausschuss für das Übereinkommen über Computerkriminalität des Europarates[17] (Übereinkommen von Budapest). Seitdem hat die EU politische, rechtliche und finanzielle Maßnahmen ergriffen, um ihre Cyber-Resilienz zu verbessern. Angesichts der Zunahme groß angelegter Cyberangriffe und schwerwiegender Cybervorfälle wurden die Bemühungen seit 2013 intensiviert

(siehe ***Abbildung 2***). Außerdem haben die Mitgliedstaaten ihre ersten nationalen Cybersicherheitsstrategien angenommen (und in einigen Fällen bereits aktualisiert).

12 Die wichtigsten EU-Akteure auf dem Gebiet der Cybersicherheit sind in ***Kasten 2*** und ***Anhang I*** beschrieben.

Kasten 2

Die Beteiligten

Ziel der **Europäischen Kommission** ist es, die Kapazitäten und die Zusammenarbeit im Bereich der Cybersicherheit auszubauen, der EU als Akteur im Bereich der Cybersicherheit mehr Gewicht zu verleihen und die Cybersicherheit in andere Politikbereiche der EU zu integrieren. Für die Cybersicherheitspolitik sind in erster Linie die Generaldirektionen **CNECT** (Cybersicherheit) und **HOME** (Cyberkriminalität) zuständig, deren Agenden der digitale Binnenmarkt bzw. die Sicherheitsunion sind. Die GD **DIGIT** ist für die IT-Sicherheit der Systeme der Kommission zuständig.

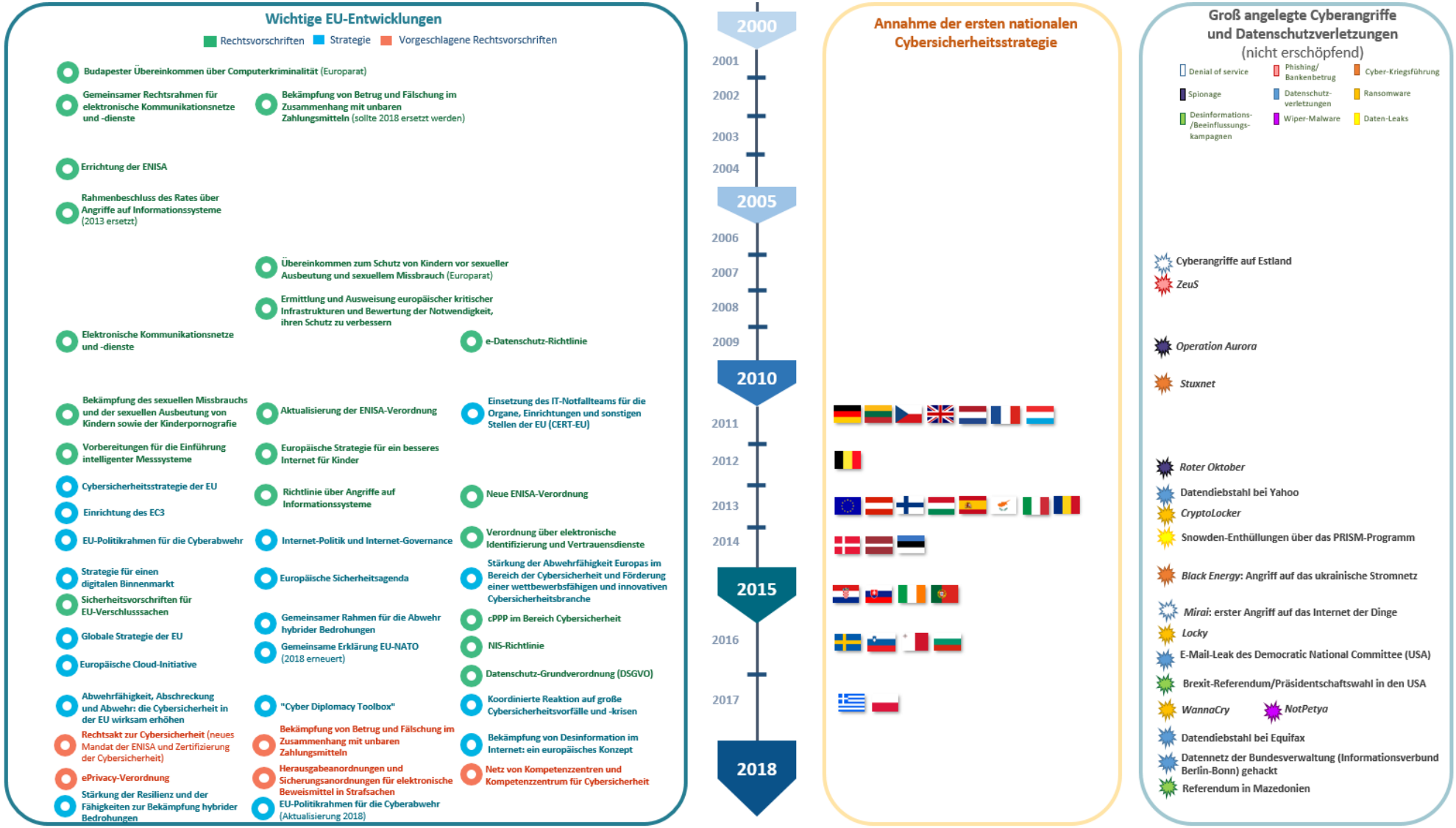
Die Kommission wird von einer Reihe von EU-Agenturen unterstützt, insbesondere der **ENISA** (Agentur der Europäischen Union für Netz- und Informationssicherheit), die in der EU für Cybersicherheit zuständig ist. Die ENISA hat in erster Linie beratende Funktion und unterstützt die Gestaltung der Politik, den Kapazitätsaufbau und Sensibilisierungsmaßnahmen. Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (**EC3**) von Europol wurde geschaffen, um die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU zu verstärken. Bei der Kommission ist zudem ein IT-Notfallteam (**CERT-EU**) angesiedelt, das alle Organe, Einrichtungen und Agenturen der EU unterstützt.

Der **Europäische Auswärtige Dienst** (EAD) ist federführend bei der Cyberabwehr, der Cyberdiplomatie und strategischen Kommunikation. Er beherbergt Zentren für Informationsgewinnung und -analyse. Ziel der **Europäischen Verteidigungsagentur** (EDA) ist der Ausbau der Cyberabwehrfähigkeit.

Die **Mitgliedstaaten** sind in erster Linie für ihre eigene Cybersicherheit zuständig. Auf EU-Ebene arbeiten sie im **Rat** zusammen, der zahlreiche Gremien für Koordinierung und Informationsaustausch (darunter die Horizontale Gruppe "Fragen des Cyberraums") eingerichtet hat. Das **Europäische Parlament** ist Teil der Rechtsetzungsbehörde.

Organisationen des Privatsektors, einschließlich Industrie, Netzverwaltungsstellen und Hochschulen, tragen als Partner zur Gestaltung und Umsetzung der Politik bei – auch im Wege einer vertraglichen öffentlich-privaten Partnerschaft (**cPPP**).

Abbildung 2 – Beschleunigte Politikgestaltung und Rechtsetzung (Stand: 31. Dezember 2018)



Quelle: Europäischer Rechnungshof.

Politik

13 Das Cyberökosystem der EU ist komplex und vielschichtig und betrifft eine ganze Reihe interner Politikbereiche wie Justiz und Inneres, den digitalen Binnenmarkt und die Forschung. In den Außenbeziehungen ist die Cybersicherheit ein Thema in der Diplomatie und zunehmend Teil der neu entstehenden Verteidigungspolitik der EU.

14 Eckpfeiler der EU-Politik ist die **Cybersicherheitsstrategie 2013**[18], die das digitale Umfeld in der EU – bei gleichzeitiger Wahrung der Grundwerte und Grundfreiheiten – zum sichersten weltweit machen soll. Die Strategie verfolgt fünf Kernziele: i) Erhöhung der Widerstandsfähigkeit gegenüber Cyberangriffen, ii) Eindämmung der Cyberkriminalität, iii) Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten, iv) Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit und v) Entwicklung einer internationalen Cyberraumstrategie im Einklang mit den Grundwerten der EU.

15 Die Cybersicherheitsstrategie hängt mit drei später angenommenen Strategien zusammen:

— Ziel der **Europäischen Sicherheitsagenda** (2015) ist es, die Strafverfolgung und das Vorgehen der Justiz im Fall von Cyberkriminalität zu verbessern, in erster Linie durch die Aktualisierung bestehender Strategien und Rechtsvorschriften[19]. Ferner geht es darum, Hindernisse zu ermitteln, die strafrechtlichen Untersuchungen über Cyberstraftaten im Wege stehen und Maßnahmen zur Verbesserung der Cyberkapazität zu fördern.

— Die **Strategie für einen digitalen Binnenmarkt**[20] (2015) soll – durch Schaffung der richtigen Bedingungen für die bestmögliche Ausschöpfung des Wachstumspotenzials der digitalen Wirtschaft – den Zugang zu digitalen Waren und Dienstleistungen verbessern. Dazu muss es gelingen, Sicherheit, Vertrauen und Inklusion im Online-Bereich zu stärken.

— Die **Globale Strategie**[21] von 2016 soll die Rolle der EU in der Welt stärken. Durch das erneuerte Engagement für Fragen des Cyberraums, die Zusammenarbeit mit wichtigen Partnern und die dezidierte Berücksichtigung von Cyberaspekten in allen Politikbereichen einschließlich der Widerlegung von Desinformation durch strategische Kommunikation bildet die Cybersicherheit einen Grundpfeiler.

16 In den letzten Jahren, seit der Cyberraum zunehmend für militärische Zwecke[22] und als Waffe[23] genutzt wird, gilt er als die fünfte Dimension der Kriegsführung[24]. Die Cyberabwehr schützt Cybersysteme, Netze und kritische Infrastrukturen vor Angriffen mit militärischen und sonstigen Mitteln. Der 2014 angenommene **Politikrahmen für die Cyberabwehr** wurde 2018 aktualisiert[25]. Zu den sechs Prioritäten in der aktualisierten Fassung von 2018 zählen die Entwicklung von Fähigkeiten im Bereich der Cyberabwehr sowie der Schutz der Kommunikations- und Informationsnetze der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU. Die Cyberabwehr ist auch Teil des Rahmens für die Ständige Strukturierte Zusammenarbeit (SSZ) und der Zusammenarbeit zwischen der EU und der NATO.

17 Im **Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen** (2016) geht die EU auf Cyberbedrohungen für kritische Infrastrukturen und für private Nutzer ein und betont, dass Cyberangriffe auch als Desinformationskampagnen in sozialen Medien durchgeführt werden können[26]. Sie verweist außerdem darauf, dass das Bewusstsein für hybride Bedrohungen verbessert und die Zusammenarbeit zwischen der EU und der NATO verstärkt werden muss, was in den Gemeinsamen Erklärungen der EU und der NATO der Jahre 2016 und 2018 konkretisiert wurde[27].

18 2017 legte die Kommission in Anbetracht der zunehmenden Dringlichkeit des Schutzes im digitalen Bereich ein neues Cybersicherheitspaket vor. Zu diesem Paket gehörte eine neue Mitteilung der Kommission zur Aktualisierung der Cybersicherheitsstrategie von 2013[28], ein Konzeptentwurf für eine schnelle und koordinierte Reaktion auf einen größeren Angriff und für die rasche Umsetzung der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie)[29]. Darüber hinaus umfasste das Paket eine Reihe von Legislativvorschlägen (siehe Ziffer ***22***).

Rechtsvorschriften

19 Seit 2002 wurden Rechtsvorschriften mit mehr oder weniger engem Bezug zur Cybersicherheit verabschiedet.

20 Wichtigste Säule der Cybersicherheitsstrategie von 2013 und rechtliches Kernstück ist die **Richtlinie zur Netz- und Informationssicherheit (NIS)**[30] aus dem Jahr 2016, mit der erstmals EU-weit geltende Rechtsvorschriften zur Cybersicherheit festgelegt wurden. Gemäß dieser Richtlinie, die bis Mai 2018 in nationales Recht umzusetzen war, müssen die Mitgliedstaaten nationale Strategien für die Sicherheit von Netz- und Informationssystemen annehmen sowie zentrale Anlaufstellen und Computer-Notfallteams (CSIRTs)[31] einrichten. Ziel ist es, ein Mindestmaß an

Harmonisierung bei den einschlägigen Fähigkeiten der Mitgliedstaaten herbeizuführen. Außerdem werden in der Richtlinie Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste in kritischen Sektoren und für Anbieter digitaler Dienste festgelegt.

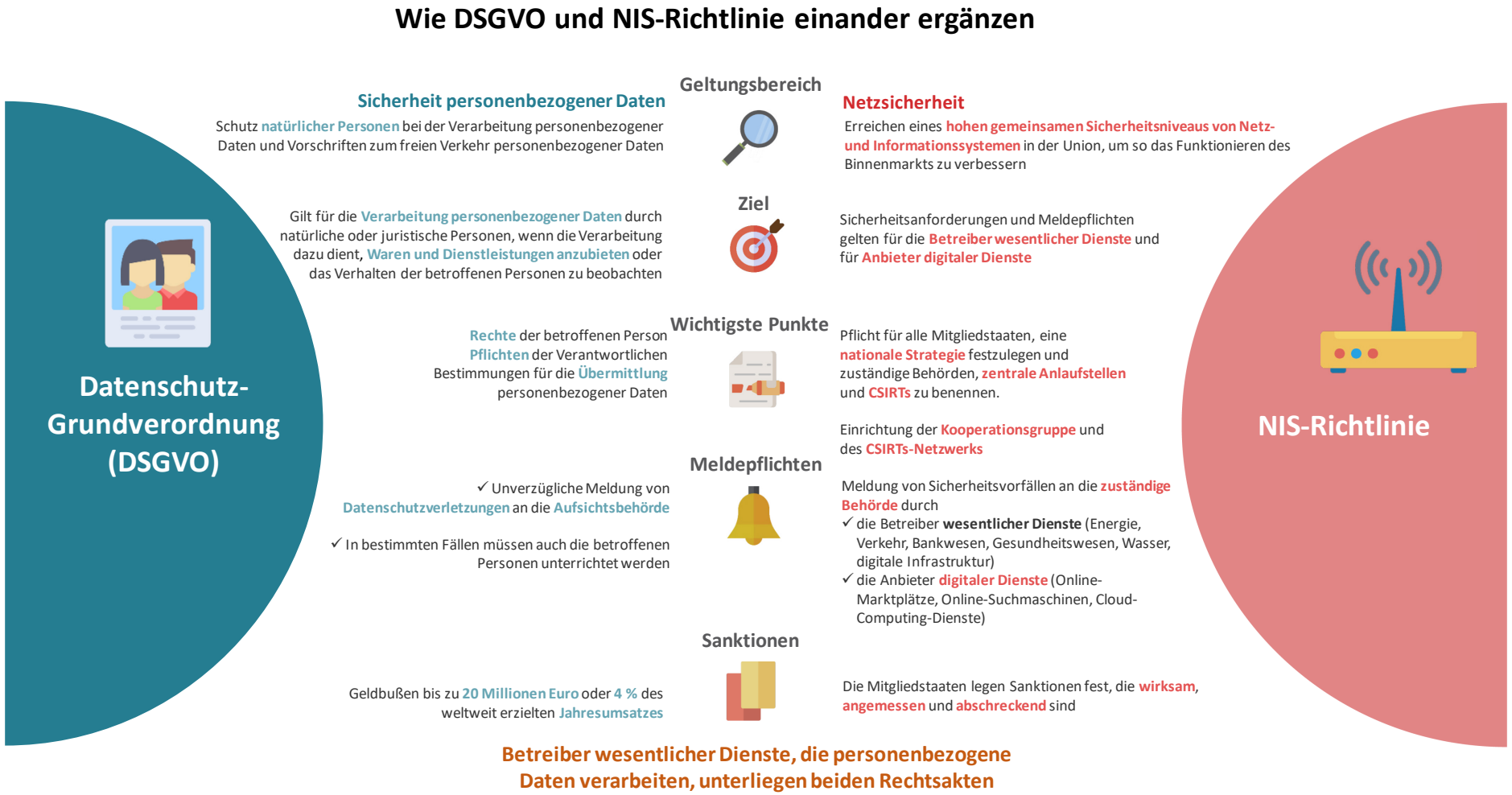
21 Daneben trat 2016 die **Datenschutz-Grundverordnung**[32] (DSGVO) in Kraft, die seit Mai 2018 anzuwenden ist. Diese Verordnung soll die personenbezogenen Daten der EU-Bürger durch die Aufstellung von Regeln für ihre Verarbeitung und Verbreitung schützen. Darin werden bestimmte Rechte für die betroffenen Personen und Pflichten für die Verantwortlichen (Anbieter digitaler Dienste) bei der Verwendung und Übermittlung von Informationen festgelegt. Ferner gibt die Verordnung vor, dass Verstöße zu melden sind und in bestimmten Fällen Geldbußen verhängt werden können. ***Abbildung 3*** veranschaulicht, wie die NIS-Richtlinie und die DSGVO einander in ihren Zielsetzungen, die Cybersicherheit zu verbessern und den Datenschutz zu sichern, ergänzen.

22 Die derzeit erörterten Vorschläge für Rechtsvorschriften umfassen den Rechtsakt zur Cybersicherheit zur Stärkung der ENISA und Einführung eines EU-weiten Zertifizierungsverfahrens[33], die Verordnung über Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel[34] und die Richtlinie über elektronische Beweismittel[35]. Der 2018 vorgelegte Vorschlag zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren (nachstehend "Netz von Cybersicherheitskompetenzzentren und Forschungskompetenzzentrum") ist Teil des Cybersicherheitspakets von 2017[36].

23 Es ist nicht ganz einfach, die politischen und rechtlichen Rahmenbedingungen für die Cybersicherheit und ihren Einfluss auf unser tägliches Leben im vollen Umfang zu erfassen.

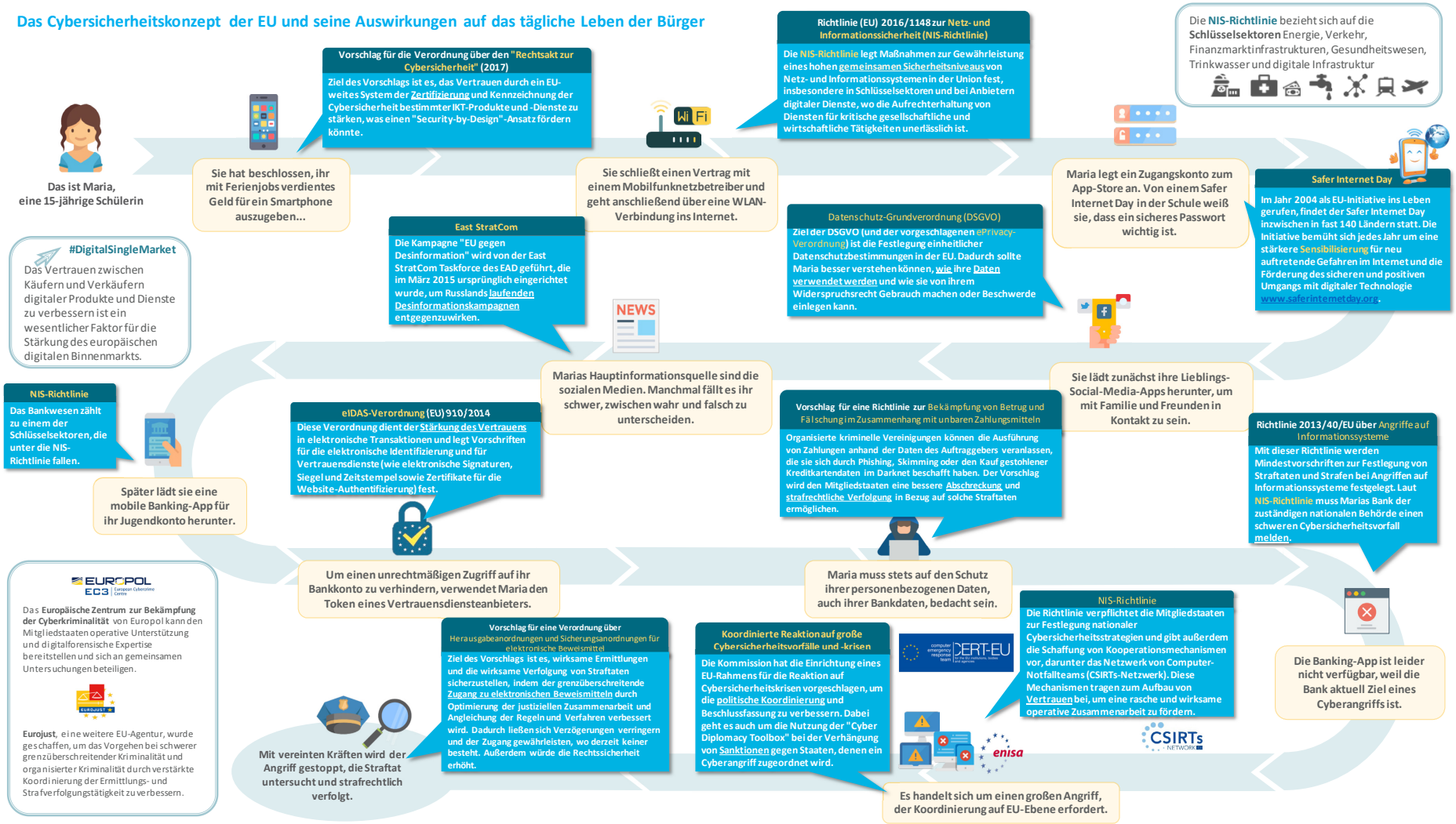
24 ***Abbildung 4*** ist der Versuch einer grafischen Darstellung der Schnittpunkte verschiedener Rechtsakte und anderer Maßnahmen mit dem Leben eines fiktiven EU-Bürgers.

Abbildung 3 – Wie DSGVO und NIS-Richtlinie einander ergänzen



Quelle: Europäischer Rechnungshof.

Abbildung 4 – Das Cybersicherheitskonzept der EU und seine Auswirkungen auf das tägliche Leben der Bürger



Quelle: Europäischer Rechnungshof.

Politische und rechtliche Rahmenbedingungen schaffen

25 Das Cyberökosystem der EU ist komplex und vielschichtig – viele Akteure sind daran beteiligt (siehe ***Anhang I***). Die einzelnen Bausteine des Systems zusammenzuführen ist ein schwieriges Unterfangen. Seit 2013 gibt es konzertierte Bemühungen um ein stimmiges Vorgehen der EU im Bereich der Cybersicherheit[37].

Herausforderung 1: aussagekräftige Evaluierung und Rechenschaftspflicht

26 Wie die Kommission festgestellt hat, lässt sich ein Kausalzusammenhang zwischen der Strategie von 2013 und eingetretenen Änderungen nur schwer herstellen. In der Strategie von 2013 waren die Ziele sehr allgemein formuliert, sie brachten eher eine Vision als messbare Vorgaben zum Ausdruck[38]. Die Ausgestaltung von Maßnahmen, die sich in diese weitgefassten Ziele einfügen, stellt in Ermangelung messbarer Vorgaben ein Problem dar. Der aktualisierte Politikrahmen für die Cyberabwehr (2018) zielt ab auf die Entwicklung von Zielen zwecks Festlegung des zu erreichenden Mindestmaßes an Cybersicherheit und Vertrauen. Dies gilt jedoch nur für die Cyberabwehr. Für das angestrebte Maß an Resilienz der EU insgesamt wurden keine Ziele vorgegeben.

27 Ergebnisse werden selten gemessen, und es wurden nur einige wenige Politikbereiche evaluiert[39]. Dies ist teilweise darauf zurückzuführen, dass viele (legislative oder sonstige) Maßnahmen erst kürzlich eingeführt wurden, sodass ihre Auswirkungen noch nicht umfassend evaluiert werden können. Die Herausforderung besteht darin, aussagekräftige Bewertungskriterien festzulegen, die eine Messung der Auswirkungen ermöglichen. Außerdem ist eine konsequente Bewertung im Bereich der Cybersicherheit ganz allgemein noch nicht die Norm. Es ist daher erforderlich, zu einer Leistungskultur mit integrierten Evaluierungsverfahren und einer standardisierten Berichterstattung überzugehen. Das derzeitige Mandat der ENISA erstreckt sich nicht darauf, den Stand der Cybersicherheit und -abwehrbereitschaft der EU zu bewerten und zu überwachen.

28 Politik kann nur dann auf der Grundlage von Fakten gestaltet werden, wenn ausreichende zuverlässige Daten und Statistiken vorliegen, mit denen sich Trends und Bedürfnisse überwachen und analysieren lassen. Da es kein obligatorisch anzuwendendes gemeinsames Überwachungssystem gibt, sind kaum zuverlässige

Daten vorhanden. Indikatoren sind nur selten ohne Weiteres verfügbar und schwer zu bestimmen[40]. Dennoch wurden für einige Bereiche wie etwa den EU-Politikzyklus zur Bekämpfung der schweren und organisierten Kriminalität spezifische Parameter entwickelt.

29 Nur wenige Mitgliedstaaten erheben regelmäßig amtliche Daten zu cyberbezogenen Fragen, sodass Vergleiche erschwert sind. Die EU hat sich bislang kaum zu einer notwendigen Konsolidierung der Statistiken auf europäischer Ebene geäußert[41]. Auch zu Kernthemen[42] wie den wirtschaftlichen Aspekten der Cybersicherheit, einschließlich verhaltensbezogener Aspekte (falsch gesetzte Anreize, Informationsasymmetrien), dem Verstehen der Auswirkungen des Versagens der Cybersicherheit und von Cyberkriminalität, Makrodaten zu Cybertrends und erwarteten Herausforderungen sowie den besten Lösungen im Umgang mit Bedrohungen gibt es nur wenige unabhängige Analysen auf EU-Ebene.

30 Da keine konkreten Ziele festgelegt wurden und zuverlässige Daten sowie zweckmäßige Indikatoren fehlen, wurden die Erfolge der Strategie bislang weitgehend aus qualitativer Sicht beurteilt. In Fortschrittsberichten werden oftmals die durchgeführten Tätigkeiten oder erreichten Etappenziele beschrieben, ohne ausführliche Messung der Ergebnisse. Für die Beurteilung der Resilienz der Systeme wurden zudem noch keine Ausgangswerte festgelegt. Überdies ist es in Ermangelung einer kodifizierten Definition von Cyberkriminalität nahezu unmöglich, auf europäischer Ebene einschlägige Indikatoren zu bestimmen, die bei Überwachung und Evaluierung hilfreich wären.

31 Die unabhängige Aufsicht über die Umsetzung der Cybersicherheitspolitik ist in den Mitgliedstaaten nicht gleich geregelt. Der Hof führte bei den nationalen Rechnungskontrollbehörden eine Umfrage zu ihren Erfahrungen mit der Prüfung dieses Bereichs durch. Die Hälfte der Umfrageteilnehmer[43] hatte diesen Bereich nie geprüft. Bei denjenigen, die Prüfungen durchgeführt hatten, lag deren Schwerpunkt auf der IT-Governance, dem Schutz kritischer Infrastrukturen, dem Informationsaustausch und der Abstimmung zwischen wichtigen Akteuren und der Lage bei Abwehrbereitschaft, Meldung und Reaktion auf Vorfälle. Zu den seltener behandelten Themen zählten Sensibilisierungsmaßnahmen und das Kompetenzdefizit im digitalen Bereich. Die Ergebnisse dieser Prüfungen oder Bewertungen wurden aus Gründen der nationalen Sicherheit nicht immer veröffentlicht. Eine Liste der von nationalen Rechnungskontrollbehörden veröffentlichten Prüfungsberichte ist ***Anhang III*** zu entnehmen.

32 Defizite bei den cyberbezogenen Kompetenzen (siehe auch Ziffern ***82-94***) und Probleme bei der Bewertung der Fortschritte im Bereich der Cybersicherheit wurden als die größten Herausforderungen bei der Prüfung der staatlichen Maßnahmen in diesem Bereich empfunden.

Herausforderung 2: Schließung von Lücken im EU-Recht und Behebung seiner uneinheitlichen Umsetzung

33 Konzeption und Umsetzung von EU-Rechtsvorschriften können nicht ansatzweise mit dem Tempo mithalten, mit dem neue Technologien und Bedrohungen aufkommen. Die Verfahren der Union wurden nicht mit dem digitalen Zeitalter vor Augen konzipiert. Die Entwicklung innovativer und flexibler Verfahren, die einen zweckmäßigen politischen und rechtlichen Rahmen gewährleisten[44], um die Zukunft besser vorwegnehmen und gestalten zu können, hat daher absolute Priorität[45].

34 Trotz der Bemühungen um mehr Kohärenz ist der rechtliche Rahmen für die Cybersicherheit nach wie vor unvollständig (Beispiele sind ***Tabelle 1*** zu entnehmen). Fragmentierung und Lücken erschweren die Erreichung der allgemeinen politischen Ziele und führen zu Ineffizienz. Zu den von der Kommission bei der Bewertung der Strategien aufgezeigten Lücken gehörten das Internet der Dinge, das Gleichgewicht der Verantwortung zwischen Nutzern und Anbietern digitaler Produkte sowie bestimmte in der NIS-Richtlinie nicht behandelte Aspekte. Der vorgeschlagene Rechtsakt zur Cybersicherheit soll hier – durch Einführung einer "eingebauten Sicherheit" (*security by design*) im Rahmen eines EU-weiten Zertifizierungssystems – zum Teil Abhilfe schaffen. Einige Akteure sind der Ansicht, dass eine klar definierte Industriepolitik für den Cyberbereich und ein gemeinsamer Ansatz für Cyberspionage nach wie vor eindeutig fehlen[46].

Tabelle 1 - Lücken und uneinheitliche Umsetzung des Rechtsrahmens (ohne Anspruch auf Vollständigkeit)

Politikbereich	Beispiele
Digitaler Binnenmarkt	o Die geltende Richtlinie über den Verbrauchsgüterkauf geht auf Cybersicherheit nicht ein. Mit den Richtlinienvorschlägen über digitale Inhalte[47] und Online-Handel[48] soll diese Lücke geschlossen werden. o Die Rechtsvorschriften für die Sorgfaltspflichten sind begrenzt und je nach EU-Mitgliedstaat unterschiedlich, was zu Rechtsunsicherheit und Problemen bei der Durchsetzung von Rechtsbehelfen führt[49]. o Die Entwicklung der Strategien im Bereich der Offenlegung von Software-Schwachstellen geht in den Mitgliedstaaten in unterschiedlichem Tempo voran. Ein übergeordneter Rechtsrahmen auf EU-Ebene, der einen koordinierten Ansatz ermöglichen würde, besteht nicht[50].
Verbesserung der Netz- und Informationssicherheit	o Es steht den Mitgliedstaaten frei, Sektoren einzubeziehen, die in der NIS-Richtlinie nicht berücksichtigt wurden[51]. Die – nicht abgedeckten – Beherbergungsindustrien können Einfallstor für andere Verbrechen, u. a. Menschen- und Drogenhandel sowie illegale Einwanderung, sein[52].
Bekämpfung der Cyberkriminalität	o Viele Mitgliedstaaten haben elektronische Beweismittel in ihren nationalen Rechtsvorschriften nicht definiert[53] (siehe auch Ziffer ***22***). o Im geltenden Rahmenbeschluss über Betrug mit unbaren Zahlungsmitteln sind weder nichtmaterielle Zahlungsinstrumente wie virtuelle Währungen, E-Geld und mobile Bezahlsysteme noch Handlungen wie Phishing, Skimming und Besitz und Weitergabe von Informationen über den Zahlungsleistenden ausdrücklich berücksichtigt[54]. o Die Richtlinie über Angriffe auf Informationssysteme geht nicht unmittelbar auf das illegale Abgreifen von Daten von innen heraus (z. B. Cyberspionage) ein, was Herausforderungen für die Strafverfolgung nach sich zieht[55]. o Nach dem Urteil des Gerichtshofs der Europäischen Union über die Vorratsdatenspeicherung[56] behinderte die unterschiedliche Rechtspraxis in den Mitgliedstaaten die Strafverfolgung mit der möglichen Folge, dass Ermittlungshinweisen nicht lückenlos nachgegangen werden konnte und die wirksame Verfolgung von Cyberstraftaten beeinträchtigt wurde[57].

Quelle: Europäischer Rechnungshof.

35 Die Anwendung einiger Aspekte der Rechtsvorschriften bleibt weiterhin den nationalen Behörden und privaten Betreibern überlassen. Im Rahmen der Kooperationsgruppe beispielsweise erfolgt die Bewertung der nationalen Strategien für die Sicherheit der Netz- und Informationssysteme und die Wirksamkeit der CSIRTs freiwillig. Auch die Zertifizierung von IKT-Produkten und -Diensten im Rahmen des im Rechtsakt zur Cybersicherheit vorgeschlagenen Zertifizierungssystems wird auf Freiwilligkeit beruhen.

36 In der EU ist die Regelung der Cybersicherheit den Mitgliedstaaten vorbehalten. Dessen ungeachtet kommt der EU eine entscheidende Rolle dabei zu, die Bedingungen zu schaffen, unter denen die Mitgliedstaaten ihre Kapazitäten verbessern sowie zusammenarbeiten und Vertrauen aufbauen können. In Anbetracht der großen Unterschiede, die zwischen den Mitgliedstaaten in Bezug auf Kapazitäten und Engagement bestehen[58], wird die Bereitstellung sensibler Informationen (die die nationale Sicherheit betreffen) jedoch weiterhin auf freiwilliger Basis erfolgen.

37 Durch die uneinheitliche Umsetzung von EU-Rechtsvorschriften in den Mitgliedstaaten kann es zu Inkohärenzen bei der Rechtsauslegung und -anwendung kommen, wodurch die Vorschriften nicht ihre volle Rechtskraft entfalten können. So legen die Mitgliedstaaten beispielsweise unterschiedlich aus, wie die Ausfuhrkontrollen von Gütern mit doppeltem Verwendungszweck anzuwenden sind[59], wodurch bestimmte in der EU niedergelassene Unternehmen Technologien und Dienste ausführen könnten, die für digitale Überwachung und Menschenrechtsverletzungen durch Zensur oder Abhören genutzt werden könnten. Das Europäische Parlament hat diesbezüglich Bedenken geäußert[60].

38 Der Schutz der Privatsphäre und der freien Meinungsäußerung erfordert zudem maßgeschneiderte Maßnahmen vonseiten des Gesetzgebers, um das notwendige Gleichgewicht zwischen dem Schutz der Grundwerte und den Sicherheitserfordernissen der EU zu erreichen. Wie soll beispielsweise die Ende-zu-Ende-Verschlüsselung gewährleistet und zugleich die Strafverfolgung optimal unterstützt werden? Wie lassen sich die Vorgaben der DSGVO erfüllen, wenn klar ist, welche Auswirkungen sie auf öffentlich zugängliche Informationen über Registranten von Domänennamen und Inhaber von IP-Adressenblöcken hat? Und welche negativen Folgen das für strafrechtliche Ermittlungen haben kann[61]?

39 Durch Rechtsvorschriften allein ist die Resilienz nicht gewährleistet. Das Ziel der NIS-Richtlinie besteht zwar darin, in der EU ein hohes Sicherheitsniveau zu erreichen, sie strebt aber ausdrücklich keine maximale, sondern eine minimale Harmonisierung an[62]. Mit der Weiterentwicklung der digitalen Umgebung werden sich immer wieder neue Lücken auftun.

Denkanstöße – politischer Rahmen

- Welcher entscheidenden Schritte bedarf es, damit sich politische Entscheidungsträger und Gesetzgeber gleichermaßen veranlasst sehen, zu einer stärkeren Leistungskultur im Bereich der Cybersicherheit überzugehen, wozu auch die Definition gehört, was unter allgemeiner Resilienz zu verstehen ist?
- Wie kann die Forschung besser zur Generierung der erforderlichen Daten und Statistiken beitragen, um aussagekräftige Evaluierungen zu ermöglichen?
- Wie lassen sich die Gesetzgebungsverfahren der EU so anpassen, dass auf das Tempo der Entwicklungen bei Technologien und Bedrohungen flexibler reagiert und besser eingegangen werden kann?
- Wie lässt sich die im EU-Politikzyklus gängige Praxis der Aufstellung von Parametern (Indikatoren, Zielwerte) so anpassen, verstärken und reproduzieren, dass sie den gesamten Cybersicherheitsbereich erfasst?
- Was können die nationalen Rechnungskontrollbehörden aus den von ihren Fachkollegen angewandten Ansätzen für die Prüfung von Cybersicherheitsstrategien und -maßnahmen lernen?
- Welche Inkohärenzen bei der Umsetzung und Anwendung des EU-Rechtsrahmens verhindern eine wirksamere Reaktion auf Lücken im Bereich der Cybersicherheit und auf Cyberkriminalität und wie könnten die Mitgliedstaaten und die EU-Organe hier am besten gegensteuern?
- Wie wirksam erweisen sich die EU-Ausfuhrkontrollen von digitalen Waren und Dienstleistungen bei der Verhinderung von Menschenrechtsverletzungen außerhalb der EU?

Finanzierung und Ausgaben

40 Die EU will zum weltweit sichersten Online-Umfeld werden. Damit dieses ehrgeizige Ziel erreicht werden kann, sind erhebliche Anstrengungen aller Beteiligten, einschließlich einer soliden und angemessen verwalteten Finanzgrundlage erforderlich.

Herausforderung 3: Anpassung der Investitionshöhe an die Ziele

Aufstockung der Investitionen

41 Auf die Cybersicherheit entfallen insgesamt schätzungsweise rund 0,1 % des BIP. In den Vereinigten Staaten[63] liegt dieser Prozentsatz (einschließlich der Privatwirtschaft) mit 0,35 % höher. Für das Jahr 2019 sind – in % des BIP – rund 0,1 % bzw. 21 Milliarden USD an Ausgaben der US-Bundesregierung veranschlagt[64].

42 In der EU waren die Ausgaben vergleichsweise gering, aufgesplittert und wurden häufig nicht durch konzertierte staatlich geführte Programme gestützt. Zahlenmaterial gibt es kaum. Schätzungen zufolge belaufen sich die öffentlichen Ausgaben der EU für Cybersicherheit auf 1 bis 2 Milliarden Euro jährlich[65]. Einige Mitgliedstaaten geben in Prozent des BIP ein Zehntel oder sogar weniger aus als die Vereinigten Staaten[66]. Die EU und ihre Mitgliedstaaten müssen wissen, wie viel sie alle gemeinsam investieren, um erkennen zu können, welche Lücken geschlossen werden müssen.

43 Ein vollständiges Bild zu gewinnen ist schwierig, da bedingt durch den übergreifenden Charakter der Cybersicherheit und den vielfach nicht nach Cybersicherheit und allgemeinen IT-Ausgaben trennbaren Ausgaben keine eindeutigen Daten vorliegen[67]. Die Umfrage des Hofes hat bestätigt, dass zuverlässige Statistiken über die Ausgaben im öffentlichen und im privaten Sektor kaum zu erlangen sind. 75 % der nationalen Rechnungskontrollbehörden gaben an, dass sie keinen Gesamtüberblick über die staatlichen Ausgaben für Cybersicherheit haben, und in keinem einzigen Mitgliedstaat sind öffentliche Stellen verpflichtet, die Ausgaben für Cybersicherheit in ihren Finanzplänen gesondert auszuweisen.

44 Die Aufstockung der öffentlichen und privaten Investitionen in Europas Cybersicherheitsunternehmen stellt eine besondere Herausforderung dar. Öffentliches Kapital ist vielfach in der Startphase verfügbar, in der Wachstums- und der Expansionsphase ist dies jedoch seltener der Fall[68]. Die zahlreichen Fördermaßnahmen

der EU werden – vor allem wegen des bürokratischen Aufwands – nicht in Anspruch genommen[69]. Insgesamt schneiden die Cybersicherheitsunternehmen im Vergleich zur internationalen Konkurrenz schlechter ab: Sie sind zahlenmäßig unterlegen und können im Durchschnitt deutlich geringere Finanzierungsbeiträge einwerben[70]. Damit die EU ihre Ziele im Bereich der Digitalpolitik erreichen kann, muss sichergestellt werden, dass Start-up-Unternehmen gezielt angesprochen und gefördert werden.

Verstärkung der Auswirkungen

45 Die Schließung der Investitionslücke im Cyberbereich muss zu nützlichen Ergebnissen führen. So werden trotz der Stärke des Forschungs- und Innovationssektors der EU Ergebnisse nicht ausreichend patentiert, vermarktet oder ausgebaut, um zur Stärkung von Resilienz, Wettbewerbsfähigkeit und digitaler Autonomie beizutragen[71]. Die gilt insbesondere im Vergleich zu den internationalen Wettbewerbern der EU. Dass die Ergebnisse nicht richtig genutzt werden, hat eine Reihe von Ursachen[72], darunter

- das Fehlen einer kohärenten transnationalen Strategie zum Ausbau des Ansatzes, sodass er den weiterreichenden digitalen Bedarf der EU in Bezug auf Wettbewerbsfähigkeit und größere Autonomie erfüllt;
- die Länge der Wertschöpfungskette, die bewirkt, dass Tools schon bald veraltet sind;
- die fehlende Nachhaltigkeit, weil bei Projektende in der Regel die Projektteams aufgelöst und der Support (einschließlich Updates und Patches) eingestellt wird.

46 Die von der Kommission vorgeschlagene Einrichtung eines Netzes von Cybersicherheitskompetenzzentren und eines Forschungskompetenzzentrums ist ein Versuch, die Zersplitterung auf dem Gebiet der Cybersicherheitsforschung zu überwinden und in großem Umfang Investitionen anzukurbeln[73]. In der EU gibt es insgesamt rund 665 Kompetenzzentren.

Herausforderung 4: ein klarer Überblick über die Ausgaben der EU

47 Ein Gesamtüberblick über die Ausgaben ist wichtig für Transparenz und bessere Koordinierung. Fehlt er, ist für die politischen Entscheidungsträger schwer zu erkennen, wie Ausgaben und Bedarf aufeinander abgestimmt werden müssen, um die vorrangigen Ziele zu erreichen.

48 Für die Finanzierung der Cybersicherheitsstrategie sind keine spezifischen Haushaltsmittel vorgesehen. Auf EU-Ebene werden die Ausgaben für Cybersicherheit vielmehr aus dem Gesamthaushaltsplan der EU und aus Kofinanzierungsmitteln der Mitgliedstaaten gedeckt. Die Analyse des Hofes zeigt einen komplexen Aufbau mit mindestens zehn verschiedenen Instrumenten aus dem EU-Gesamthaushaltsplan, wobei nicht klar ersichtlich ist, welche Mittel wohin fließen (siehe ***Anhang II***).

49 Sich einen klaren Überblick über die Ausgaben für ein Thema zu verschaffen, das viele Politikbereiche betrifft, stellt daher eine beträchtliche Herausforderung dar. Ausgabenprogramme werden von verschiedenen Dienststellen der Kommission verwaltet, die ihre eigenen Ziele, Vorschriften und Zeitpläne haben. Die Lage wird noch komplizierter bei Berücksichtigung der Kofinanzierung durch die Mitgliedstaaten, wie beim Fonds für die innere Sicherheit (Polizei)[74].

Identifizierbare Ausgaben für die Cybersicherheit

50 Im Zeitraum 2014-2018 wendete die Kommission mindestens 1,4 Milliarden Euro für die Umsetzung der Strategie auf[75], wobei der Löwenanteil über das Programm "Horizont 2020" bereitgestellt wurde[76]. Die Horizont-2020-Mittel werden vor allem über das Programm im Bereich der Herausforderung "Sichere Gesellschaften" und über Projekte des Einzelziels "Führende Rolle bei grundlegenden und industriellen Technologien" mobilisiert[77]. Der Hof stellte fest, dass bis September 2018 insgesamt 786 Millionen Euro für Projekte mit Bezug zur Cybersicherheit vertraglich gebunden wurden[78]. In ***Abbildung 5*** ist auf der Grundlage dieser Analyse aufbereitet, um welche Art von Projekten es sich handelt.

Abbildung 5 – Horizont-2020-Forschungsprojekte mit Bezug zur Cybersicherheit, für die Aufträge vergeben wurden (Millionen Euro)

Quelle: Europäischer Rechnungshof.

51 Im Jahr 2016 wurde eine vertragliche öffentlich-private Partnerschaft auf den Weg gebracht, um die europäische Cybersicherheitsbranche zu stimulieren. Aus dem Programm Horizont 2020 sollten 450 Millionen Euro für diese vertragliche öffentlich-private Partnerschaft bereitgestellt werden, und vom privaten Sektor sollten bis 2020 weitere 1,8 Milliarden Euro eingeworben werden. In den 18 Monaten bis 31. Dezember 2017 wurden 67,5 Millionen Euro an Horizont-2020-Mitteln bereitgestellt, der Privatsektor investierte 1 Milliarde Euro[79].

52 Die Bekämpfung der Cyberkriminalität wird auch mit Mitteln des Fonds für die innere Sicherheit – Polizei (ISF-P) unterstützt. Der ISF-P unterstützt Studien, Expertentreffen und Kommunikationsmaßnahmen; diese beliefen sich im Zeitraum 2014-2017 auf nahezu 62 Millionen Euro. Außerdem können die Mitgliedstaaten im Rahmen der geteilten Mittelverwaltung Zuschüsse für Ausrüstung, Schulung, Forschung und Datenerhebung erhalten. 19 Mitgliedstaaten haben solche Zuschüsse in Höhe von insgesamt 42 Millionen Euro in Anspruch genommen.

53 Zur Unterstützung der justiziellen Zusammenarbeit und der Umsetzung von Rechtshilfeabkommen mit besonderem Schwerpunkt auf dem Austausch von elektronischen Daten und Finanzinformationen wurden im Rahmen des von der

Generaldirektion Justiz und Verbraucher (GD JUST) verwalteten Programms "Justiz" Mittel in Höhe von 9 Millionen Euro bereitgestellt.

54 In der NIS-Richtlinie heißt es ausdrücklich, dass die CSIRTs mit angemessenen Mitteln ausgestattet sind, damit sie ihre Aufgaben wirksam erfüllen können[80]. Im Zeitraum 2016-2018 standen im Rahmen der Fazilität "Connecting Europe" jährlich 13 Millionen Euro bereit, für die Mitgliedstaaten im Hinblick auf die Umsetzung der Anforderungen der Richtlinie Anträge stellen konnten. Es gibt keine Studie, in der bestimmt wurde, wie hoch der tatsächliche Finanzbedarf des CSIRTs-Netzwerks und der Kooperationsgruppe ist, um Wirkung zu entfalten.

55 Ein Teil der operativen Kosten der Agenturen ist speziell für Cybersicherheit oder die Bekämpfung von Cyberkriminalität vorgesehen. Genaue Zahlen lassen sich aus den öffentlich zugänglichen Informationen allerdings nur schwer ableiten.

56 Das Übereinkommen von Budapest (siehe Ziffer ***11***) bildet die Grundlage für die Ausgaben der EU für Cybersicherheit im Ausland. Die Union wendete im Zeitraum 2014-2018 rund 50 Millionen Euro für die Verbesserung der Cybersicherheit außerhalb ihrer Grenzen auf. Knapp die Hälfte dieses Betrags stammte aus dem Stabilitäts- und Friedensinstrument. Es gab ein Hauptprojekt – das mit 13,5 Millionen Euro dotierte GLACY+ –, mit dem weltweit die Kapazitäten zur Entwicklung und Umsetzung von Rechtsvorschriften im Bereich der Cyberkriminalität und die internationale Zusammenarbeit gestärkt werden sollte[81]. Ansonsten lag der Schwerpunkt der Ausgaben aus anderen EU-Finanzinstrumenten weitgehend auf den Staaten des Westlichen Balkans[82] sowie den Ländern der Europäischen Nachbarschaftspolitik. Hier lässt sich als Beispiel das Projekt "Cybercrime@EAP" mit den Ländern der Östlichen Partnerschaft anführen, mit dem die Internationale Zusammenarbeit auf dem Gebiet der Cyberkriminalität und der elektronischen Beweismittel verbessert werden soll.

Sonstige Ausgaben für die Cybersicherheit

57 Es ist nicht immer möglich, konkrete Ausgaben für die Cybersicherheit innerhalb von EU-Programmen festzumachen:

- Horizont-2020-Fördermittel für cyber-physische Systeme wurden auch über das Gemeinsame Unternehmen "Elektronikkomponenten und -systeme für eine Führungsrolle Europas" (ECSEL) bereitgestellt. Der Hof konnte jedoch nicht

feststellen, welche Teile der 27 Projekte im Gesamtwert von 437 Millionen Euro aus den Jahren 2015 und 2016 sich konkret auf Cybersicherheit bezogen.

- Im Rahmen der europäischen Struktur- und Investitionsfonds sind bis zu 400 Millionen Euro an Ausgaben für Cybersicherheit und Vertrauensdienste vorgesehen. Darunter fallen Investitionen in Sicherheit und Datenschutz zur Verbesserung der Interoperabilität und Vernetzung der digitalen Infrastruktur, elektronische Identifizierung sowie Dienste zum Schutz der Privatsphäre und Vertrauensdienste.

58 In ihrem operativen Gesamtplan 2018 bekundete die Europäische Investitionsbank ihre Absicht, die Finanzierungen von Technologien mit doppeltem Verwendungszweck, Cybersicherheit und zivile Sicherheit in einem Dreijahreszeitraum auf bis zu 6 Milliarden Euro auszuweiten[83].

Ausblick

59 Der Teilbereich Cybersicherheit, für den im Rahmen des für den Zeitraum 2021-2027 vorgeschlagenen Programms "Digitales Europa" (DEP)[84] 2 Milliarden Euro vorgesehen sind, soll die Cybersicherheitsbranche der EU sowie den Schutz der Gesellschaft insgesamt stärken, u. a. durch Unterstützung der Umsetzung der NIS-Richtlinie. Das vorgeschlagene Netz von Cybersicherheitskompetenzzentren und eines Forschungskompetenzzentrums, mit dem auf einen strafferen Ansatz abgezielt wird, soll einer der Hauptumsetzungsmechanismen für EU-Ausgaben im Rahmen des Programms "Digitales Europa" werden.

60 Die Verteidigungsausgaben aus dem EU-Haushalt wurden kürzlich durch das Europäische Programm zur industriellen Entwicklung im Verteidigungsbereich aufgestockt, für das in den Jahren 2019 und 2020 500 Millionen Euro vorgesehen sind[85]. Im Mittelpunkt steht die Verbesserung von Koordinierung und Effizienz bei den Verteidigungsausgaben der Mitgliedstaaten durch Anreize für gemeinsame Entwicklungen. Angestrebt wird ein Investitionsvolumen von insgesamt 13 Milliarden Euro für die Verteidigungsfähigkeit nach 2020 durch den Europäischen Verteidigungsfonds, wovon ein Teil auf Cyberabwehr entfällt[86].

Herausforderung 5: Angemessene Ressourcen für die EU-Agenturen

61 Die drei wichtigsten Einrichtungen, auf die sich die Cybersicherheitspolitik der EU stützt – ENISA, EC3 von Europol und CERT-EU (siehe ***Kasten 2***) –, sind in Zeiten, in denen die politischen Prioritäten mehr und mehr von Sicherheitserwägungen bestimmt werden, mit Herausforderungen im Zusammenhang mit ihren Ressourcen konfrontiert. Mit ihren derzeitigen personellen und finanziellen Ressourcen können die EU-Agenturen den an sie gestellten Erwartungen kaum gerecht werden[87].

62 Den Anträgen der Agenturen auf zusätzliche Ressourcen zur Deckung der steigenden Nachfrage wurde nicht vollständig entsprochen, was die (fristgerechte) Verwirklichung der politischen Ziele gefährden könnte. Zum Beispiel:

- Unter anderem aufgrund von Ressourcenengpässen konnte die ENISA ihre Ziele im Jahr 2017 nicht voll und ganz erreichen[88]. Im Paket von 2017 wurden in Anbetracht des neuen Auftrags der ENISA zusätzliche Ressourcen vorgeschlagen.

- Die Ausstattung mit Analysten und die Investitionen in IKT-Kapazitäten haben beim EC3 von Europol nicht mit den Anforderungen Schritt gehalten[89]. Auch bei der Gemeinsamen Taskforce gegen die Cyberkriminalität (J-CAT) des EC3 von Europol sind Experten aus den Mitgliedstaaten und Drittländern tätig, um erkenntnisgestützte Ermittlungen zu unterstützen. Die Kosten werden weitgehend von den Entsendestaaten getragen, was diese davon abhält, mehr Experten zu entsenden. Eine befristete einzelfallbezogene Entsendung mit einer Finanzierung aus Mitteln von Europol oder dem EU-Politikzyklus wurde konzipiert, um mehr Ländern die Beteiligung zu ermöglichen.

63 Einige Engpässe sind selbst verschuldet. Viele Mitarbeiter des CERT-EU und der ENISA sind Vertragsbedienstete, und die Einstellungsverfahren für diese Kategorie von Arbeitskräften sind in der Regel langsam. Andere Probleme, wie die dauerhafte Anwerbung von Talenten, sind darauf zurückzuführen, dass die Agenturen nicht mit den im Privatsektor gezahlten Gehältern mithalten können oder die Karriereaussichten schlecht sind. Die ENISA hat deshalb im Zeitraum 2014-2016 einen Großteil ihrer Tätigkeit outgesourct[90].

64 Knappheit beim Personal und den erforderlichen Tools kann erhebliche Risiken bergen, insbesondere im Zusammenhang mit der Sammlung von Informationen über Bedrohungen. Die Datenmengen aus offenen und geschlossenen Quellen wachsen weiter und könnten es den Analysten unmöglich machen, ordentliche

Bedrohungsanalysen vorzunehmen. Fehlen die richtigen Kapazitäten und Tools zur erfolgreichen Integration und Verknüpfung dieser Daten, ist keine effektive Übertragung in verwertbare Informationen über Bedrohungen möglich, die in der ganzen EU ausgetauscht und analysiert werden können[91].

Denkanstöße – Finanzierung und Ausgaben

- Wie können Kommission und Gesetzgeber die Ausgaben der EU für Cybersicherheit straffen und expliziter auf klar definierte Ziele abstimmen?
- Wie können die Engpässe bei der Bereitstellung von Ressourcen für die EU-Agenturen übergreifend gelöst und dabei der Bedarf und die Ziele der EU berücksichtigt werden?
- Durch welche Maßnahmen auf Ebene der EU und der Mitgliedstaaten können Hindernisse abgebaut werden, die KMU davon abhalten, Investitionskapital zur Ausweitung ihrer Tätigkeiten in Anspruch zu nehmen?
- Welche konkreten und nachhaltigen Ergebnisse werden mit Horizont-2020-Fördermitteln erreicht, wenn es um Cybersicherheitslösungen geht?
- Wie werden mit den EU-Maßnahmen zum Kapazitätsaufbau außerhalb ihrer Grenzen Kapazitäten im Einklang mit den EU-Werten ausgebaut?

Aufbau einer cyber-resilienten Gesellschaft

65 Cybersicherheits-Governance betrifft den Umgang mit Bedrohungen und Risiken, den Kapazitätsaufbau und die Sensibilisierung sowie die Koordinierung und den Informationsaustausch basierend auf Vertrauen.

Herausforderung 6: Stärkung von Governance und Standards

Governance im Bereich der Informationssicherheit

66 Governance im Bereich der Informationssicherheit bedeutet die Schaffung von Strukturen und Strategien zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Sie ist mehr als nur eine Frage der Technik und erfordert effektive Führung, stabile Prozesse und auf die Ziele der Organisation abgestimmte Strategien[92]. Ein Teilbereich ist die Cybersicherheits-Governance, die alle Arten von Cyberbedrohungen betrifft, einschließlich gezielter, raffinierter Angriffe, Sicherheitsverletzungen oder Vorfälle, die schwer zu erkennen oder in den Griff zu bekommen sind.

67 Die Mitgliedstaaten wenden im Bereich der Cybersicherheits-Governance unterschiedliche Modelle an, und in den einzelnen Mitgliedstaaten ist die Zuständigkeit für Cybersicherheit oft auf mehrere Stellen verteilt. Diese Unterschiede könnten die Zusammenarbeit behindern, die notwendig ist, um auf groß angelegte, grenzübergreifende Sicherheitsvorfälle zu reagieren und Informationen über Bedrohungen auf nationaler Ebene – oder gar EU-Ebene – auszutauschen. Die Umfrage des Hofes bei den nationalen Rechnungskontrollbehörden ergab, dass Schwachstellen in den Governance-Regelungen und im Risikomanagement öffentlicher Behörden als größte Gefahrenquellen wahrgenommen wurden.

68 Obwohl die Folgen für Organisationen des Privatsektors schwerwiegend sein können, bestehen zahlreiche Schwachstellen im Bereich der Cybersicherheits-Governance. Fast neun von zehn Organisationen geben an, dass ihre für Cybersicherheit zuständige Stelle ihrem Bedarf nicht voll und ganz gerecht wird[93], und in vielen Fällen stehen die für die Cybersicherheit zuständigen Mitarbeiter zumindest zwei Stufen unter dem Vorstand[94].

69 Die Richtlinien der EU zum Gesellschaftsrecht enthalten keine spezifischen Anforderungen hinsichtlich der Offenlegung von Cyberrisiken. Die US-amerikanische Börsenaufsichtsbehörde (*Securities and Exchange Commission*) gab unlängst unverbindliche Leitlinien heraus, um öffentliche Unternehmen bei ihren Angaben zu Cybersicherheitsrisiken und -vorfällen zu unterstützen[95]. Der Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden[96] warnte vor den steigenden Cyberrisiken und forderte Finanzinstitute zur Absicherung anfälliger IT-Systeme und zur Auslotung inhärenter Risiken bei Informationssicherheit, Konnektivität und Outsourcing auf[97].

70 Die Stärkung der Governance im Bereich der Informationssicherheit von KMU erweist sich als besonders schwierig, da diese zumeist nicht in der Lage sind, angemessene Systeme zu implementieren. Den KMU fehlen zweckmäßige Leitlinien zur Umsetzung der Anforderungen an Informationssicherheit und Datenschutz und zur Verringerung von Technologierisiken[98]. Zu den zentralen Herausforderungen zählt daher ein besseres Verständnis ihres Bedarfs und die Bereitstellung der erforderlichen Anreize und Unterstützung.

71 Die Fähigkeit der Weltgemeinschaft, auf Cyberangriffe zu reagieren und sie einzuhegen, wird dadurch beeinträchtigt, dass auf internationaler Ebene ein kohärenter Rahmen für Cybersicherheits-Governance fehlt. Es ist deshalb wichtig, einen Konsens über einen solchen Governance-Rahmen zu erzielen, der die Interessen der EU und ihre Werte am besten widerspiegelt[99]. Versuche zur Festlegung verbindlicher internationaler Normen für den Cyberraum gestalten sich zunehmend schwieriger, was sich daran zeigt, dass sich die von den UN eingesetzte Gruppe von Regierungssachverständigen im Jahr 2017 nicht darauf einigen konnte, wie das Völkerrecht bei staatlichen Reaktionen auf Vorfälle anzuwenden ist.

72 Um ihrer Agenda für Cyberraum-Governance Nachdruck zu verleihen, hat die EU außerdem sechs förmliche Cyber-Partnerschaften mit dem Ziel geschlossen, in einen regelmäßigen politischen Dialog einzutreten, um Vertrauen aufzubauen und gemeinsame Bereiche der Zusammenarbeit zu entwickeln[100]. Die Ergebnisse sind gemischt, doch insgesamt kann die EU auf internationaler Ebene noch nicht als wichtiger Akteur im Bereich der Cybersicherheit gelten, auch wenn sie mittlerweile stärker in Erscheinung tritt[101].

Informationssicherheit bei den EU-Organen

73 Jedes EU-Organ verfügt über eigene Regeln für die Governance im Bereich der Informationssicherheit. Laut einer interinstitutionellen Vereinbarung leistet die Kommission den anderen Organen und Agenturen Unterstützung in Sachen

Informationssicherheit. Die Organe und Einrichtungen der EU haben erkannt, dass sie sich bei der Entwicklung ihrer Cyber-Kapazitäten und Risikomanagementkonzepte abstimmen müssen. Kommission, Rat und EAD sollen 2020 der Horizontalen Gruppe "Fragen des Cyberraums" einen Bericht über Governance und die Klarstellung und Harmonisierung der Cybersicherheits-Governance bei den Organen und Agenturen der EU vorlegen[102].

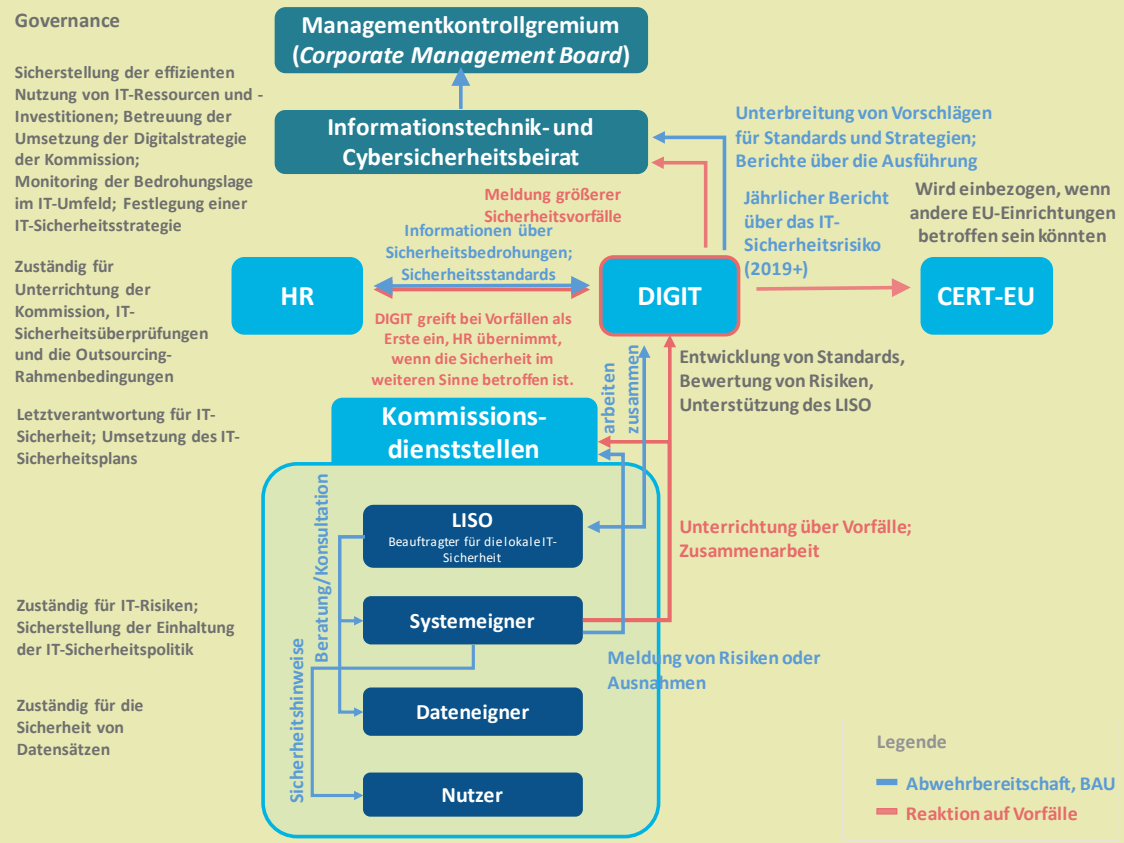
74 Bei der Kommission ist die Generaldirektion Informatik (DIGIT) für die Sicherheit der IT-Infrastruktur und IT-Dienste zuständig (siehe ***Kasten 3***). Die wichtigsten IT-Sicherheitsziele der Digitalstrategie der Kommission sind die Einbeziehung der IT-Sicherheit in die Verwaltungspraxis, die Bereitstellung einer (kosteneffizienten) und wirksamen Infrastruktur und Erhöhung der Widerstandsfähigkeit, die Ausweitung des Umfangs der Erkennung und Abwehr von Sicherheitsvorfällen und die Verschmelzung der Lenkung und Leitung in IT- und Sicherheitsfragen[103]. Gemäß Dienstleistungsvertrag stellt die Kommission sicher, dass praktisch die gesamte Software aktiv gepflegt wird und nur herstellergestützte Software zum Einsatz kommt[104].

75 Dass die Organe geschützt werden müssen, gilt auch für die GSVP-Missionen und -Strukturen der EU weltweit. Eine der Prioritäten des EU-Politikrahmens für die Cyberabwehr (Aktualisierung 2018) ist die Verbesserung des Schutzes der von EU-Stellen genutzten Kommunikationsnetze der GSVP. Es wurde ein EAD-interner Lenkungsausschuss für Cybersicherheit (*Cyber Governance Board*) eingesetzt, der im Juni 2017 erstmals zusammentrat[105].

Kasten 3

Schutz der Informationssysteme der Kommission

Die rund 1 300 Systeme und 50 000 Geräte der Kommission sind ständig Ziel von Cyberangriffen. Die Zuständigkeit für IT ist dezentral organisiert (siehe Abbildung unten). Informations- und IT-Sicherheit beruhen auf einem von der GD DIGIT festgelegten gemeinsamen IT-Sicherheitsplan. Der Informationstechnik- und Cybersicherheitsbeirat (*Information Technology and Cybersecurity Board*) der Kommission fungiert als Oberster IT-Sicherheitsbeauftragter der Kommission und ist das Bindeglied zwischen der operativen Seite der IT-Sicherheit und der höchsten Management-Ebene der Kommission in Form des Managementkontrollgremiums (*Corporate Management Board*).



Quelle: Europäischer Rechnungshof auf der Grundlage von Kommissionsbeschlüssen[106].

Hauptaufgabe der GD Humanressourcen und Sicherheit (DG HR) ist es, Mitarbeiter, Informationen und Vermögenswerte der Kommission zu schützen. Die GD HR untersucht außerdem Vorfälle, deren Dimension über die reine IT-Sicherheit hinausgeht und die somit Informationen für ihre Maßnahmen im Bereich der Spionageabwehr und Terrorismusbekämpfung liefern.

Die GD DIGIT, bei der das IT-Notfallteam (CERT-EU) angesiedelt ist, ist für die IT-Sicherheit zuständig. Das 2011 eingerichtete CERT-EU verfügt über jährlich rund 2,5 Millionen Euro sowie etwa 30 Mitarbeiter. Es greift bei IT-Sicherheitsvorfällen, die mehrere Organe betreffen, als Erster ein, arbeitet jedoch nicht rund um die Uhr. Das CERT-EU betreut eine Plattform für den Informationsaustausch. Im Jahr 2018 schloss es eine unverbindliche Vereinbarung mit der ENISA, dem EC3 und der Europäischen Verteidigungsagentur, um die Zusammenarbeit und Koordinierung zu verbessern. Außerdem besteht zwischen dem CERT-EU und der *Computer Incident Response Capability* (NCIRC) der NATO eine technische Vereinbarung.

Bewertungen der Bedrohungslage und der Risiken

76 Fundierte und fortlaufende Bedrohungs- und Risikobewertungen sind wichtige Instrumente, und zwar für öffentliche und private Organisationen gleichermaßen. Es gibt jedoch keinen einheitlichen Ansatz für die Klassifizierung und Erfassung von Cyberbedrohungen oder für Risikobewertungen, sodass der Inhalt der Bewertungen

sehr unterschiedlich ausfällt, was ein EU-weit kohärentes Vorgehen in Bezug auf die Cybersicherheit erschwert[107]. Außerdem beruhen diese häufig auf denselben Quellen oder sogar anderen Bedrohungsbewertungen, sodass gebetsmühlenartig dieselben Feststellungen vorgetragen[108] und andere Bedrohungen womöglich zu wenig beachtet werden. Diese Situation wird dadurch verschärft, dass Information nach wie vor ungern weitergegeben und nicht alle Vorfälle gemeldet werden.

77 Die beim EAD angesiedelte Analyseeinheit für hybride Bedrohungen[109] wurde geschaffen, um die Lagebeurteilung zu verbessern und die Entscheidungsfindung durch Weitergabe von Analyseergebnissen zu unterstützen. Sie muss ihre Fachkompetenz, auch im Bereich der Cybersicherheit, noch erweitern. Daneben versorgt das CERT-EU die Organe, Einrichtungen und Agenturen der EU mit Berichten und Briefings über Cyberbedrohungen, deren Ziel sie sind.

78 Die ENISA hat in der Vergangenheit festgestellt, dass viele Mitgliedstaaten ein qualitatives Bedrohungsverständnis haben und Bedarf an mehr Modellierung im Bereich Cyberbedrohungen besteht[110]. Die Überwachung der Kapazitäten für die strategische Analyse wird das Gesamtverständnis verbessern. Bedrohungsbewertungen könnten aber nicht nur technologische, sondern auch sozialpolitische und wirtschaftliche Bedrohungen erfassen, damit ein umfassenderes Bild der Bedrohungsauslöser sowie der Motive der Akteure entsteht.

Anreize

79 Noch gibt es zu wenig rechtliche und wirtschaftliche Anreize für Organisationen, um Vorfälle zu melden und Informationen darüber weiterzugeben. Aus Angst vor Imageschäden ziehen viele Organisationen es immer noch vor, Cyberangriffe diskret zu behandeln oder die Täter zu bezahlen. Inwieweit sich die Zahl der Meldungen durch die NIS-Richtlinie tatsächlich erhöht, bleibt abzuwarten. Die Kommission rechnet in erster Linie auf nationaler Ebene mit Verbesserungen, durch den Rechtsakt zur Cybersicherheit kommt jedoch die europäische Dimension hinzu[111].

80 Durch Aufnahme bestimmter Standards in ihre Ausschreibungen haben öffentliche Auftraggeber als Käufer digitaler Produkte und Dienste maßgeblichen Einfluss auf Anbieter. Auch die Forschungs- und Programmförderung lässt sich so steuern (etwa durch Verlangen bestimmter technischer Standards wie Internet-Protokoll IPv6 zur Unterstützung der Bekämpfung von Cyberkriminalität). Derzeit gibt es allerdings keinen gemeinsamen Rahmen für die Beschaffung von Cybersicherheitsinfrastrukturen[112]. Diesbezüglich kann die Kommission viel tun. Mit

dem für den nächsten Mehrjährigen Finanzrahmen vorgeschlagenen Programm "Digitales Europa" soll Abhilfe geschaffen werden bei den bislang begrenzten Investitionen des öffentlichen Sektors in den Erwerb der neuesten Cybersicherheitstechnologie.

81 Durch Nutzung ihrer Regulierungsbefugnis kann die Kommission dafür sorgen, dass die richtigen Standards entwickelt und flächendeckend eingeführt werden, um die Sicherheit zu verbessern. Die Zusammenarbeit von Kommission und Europol mit Netzverwaltungsstellen wie ICANN (siehe Ziffer ***38***) und RIPE-NCC[113] ist eine Voraussetzung dafür, dass die geeignete Architektur zur Bekämpfung der Cyberkriminalität eingerichtet werden kann, um die Strafverfolgungs- und die Justizbehörden zu unterstützen.

Herausforderung 7: Kompetenzsteigerung und größeres Problembewusstsein

82 Die ENISA hat darauf hingewiesen, dass die Nutzer eine entscheidende Rolle im Kampf gegen Cyberangriffe haben und daher Kompetenzen, Ausbildung und Problembewusstsein für den Aufbau einer gegen Cyberangriffe gewappneten Gesellschaft unabdingbar sind[114]. Personen, die am Arbeitsplatz oder zu Hause Warnsignale sehr versiert erkennen und über die richtigen Techniken verfügen, können Angriffe verzögern und verhindern.

83 Besonders bedenklich ist das wachsende Missverhältnis zwischen dem Wissen, das notwendig ist, um eine Straftat im Internet zu begehen oder einen Cyberangriff zu starten, und der zur Abwehr erforderlichen Kompetenz. Das Modell "Verbrechen als Dienstleistung" hat die Hürden für den Zugang zum Markt für Cyberkriminalität verringert: Wem das technische Wissen für den Bau von Botnets, Exploit-Kits und Ransomware-Paketen fehlt, kann sie jetzt mieten.

Schulung, Aufbau von Kompetenzen und Kapazitäten

84 Die Welt steht vor dem Problem eines wachsenden Kompetenzdefizits im Bereich der Cybersicherheit; der Mangel an Fachkräften hat sich mit 20 % mehr offenen Stellen seit 2015 verschärft[115]. Mit den klassischen Rekrutierungsmethoden lässt sich der Bedarf, Management- und interdisziplinäre Positionen inbegriffen, nicht decken[116]. Fast 90 % der Arbeitskräfte im Bereich Cybersicherheit sind Männer; durch den anhaltenden Mangel an Geschlechterdiversität verkleinert sich der Talentpool

weiter[117]. Außerdem sind cyberbezogene Fächer in den nichttechnischen Studienprogrammen an den Hochschulen unterrepräsentiert.

85 Aus- und Fortbildung ist überall nötig – in der Beamtenschaft, bei Strafverfolgungs- und Justizbehörden, den Streitkräften und im Ausbildungswesen. So müssen beispielweise Gerichte in der Lage sein, mit den sich rasch wandelnden technischen Besonderheiten der Cyberkriminalität und den davon betroffenen Opfern umzugehen[118]; für Aus- und Fortbildung und Zertifizierung gelten derzeit keine EU-weiten Standards[119]. Auch die EU-Organe müssen über den richtigen Kompetenzmix verfügen. Wenn der richtige Kompetenzmix fehlt, sind die Organe möglicherweise nicht in der Lage, den Umfang entsprechend einzugrenzen, die richtigen Partner und den Bedarf im Bereich der Sicherheit zu ermitteln oder Programme zu verwalten. Dies kann wiederum die Wirksamkeit der Programme oder der Politikentwicklung der EU beeinträchtigen.

86 Obwohl die Bildungspolitik in der EU Sache der Mitgliedstaaten ist, finden bereits zahlreiche Schulungen (siehe ***Tabelle 2***) und Übungen (siehe ***Kasten 4***) statt. Die EU kann dazu beitragen, dass in die Lehrpläne aller relevanten Fachbereiche EU-weite Standards aufgenommen werden[120]. Im Bereich der digitalen Forensik beispielsweise sind gemeinsame Ausbildungsstandards erforderlich, um den Weg zur Zulässigkeit von Beweismitteln in den Mitgliedstaaten zu ebnen. Wegen des grenzüberschreitenden Charakters der Cyberkriminalität können mehrere Rechtssysteme beteiligt sein, weshalb Schulungen auf EU-Ebene erforderlich sind. Und doch hat die Agentur der EU für Aus- und Fortbildung auf dem Gebiet der Strafverfolgung darauf hingewiesen, dass mehr als zwei Drittel der Mitgliedstaaten den Bediensteten von Strafverfolgungsbehörden nicht regelmäßig Schulungen im Cyberbereich anbieten[121]. Die EU kann potenziell auch Wege aufzeigen, wie sich bei Aus- und Fortbildung Synergien zwischen dem zivilen und militärischen Bereich nutzen lassen[122]. Allerdings hat die ENISA festgestellt, dass derzeit zwar umfassende Fortbildungsmöglichkeiten in kritischen Sektoren angeboten werden, die Resilienz kritischer Infrastrukturen aber nicht ausreichend behandelt wird[123].

Tabelle 2 – Beispiele für Schulungsinitiativen der EU im Cyberbereich

Projekte der Europäischen Verteidigungsagentur, z. B. Unterstützung bei Übungen durch den Privatsektor und das Cyber-Ranges-Projekt	Netzwerk des Europäischen Sicherheits- und Verteidigungskollegs (bietet zivil-militärische Schulungen an), einschließlich einer Plattform zur Aus- und Fortbildung, Evaluierung und Übung bezüglich Cyberfragen	Aus- und Fortbildungsmaßnahmen der ENISA – dabei handelt es sich um Schulungsprogramme in Bereichen, in denen es auf dem Markt keine entsprechenden Angebote gibt
Schulungsprogramme von Europol, CEPOL, ECTEG[124] – einschließlich des *Training Governance Model* und *Training Competency Framework* (mit Zertifizierung)	Netz von Kompetenzzentren und Forschungskompetenzzentrum (vorgeschlagen)	Die im elften Fortschrittsbericht zur Sicherheitsunion vorgeschlagenen Maßnahmen zu Verschlüsselungstechniken
Zusammenarbeit zwischen der EU und der NATO bei Aus- und Weiterbildung im Bereich der Cyberabwehr	Militärisches Erasmus-Programm	Europäisches Netz für die Aus- und Fortbildung von Richtern und Staatsanwälten

Quelle: Europäischer Rechnungshof.

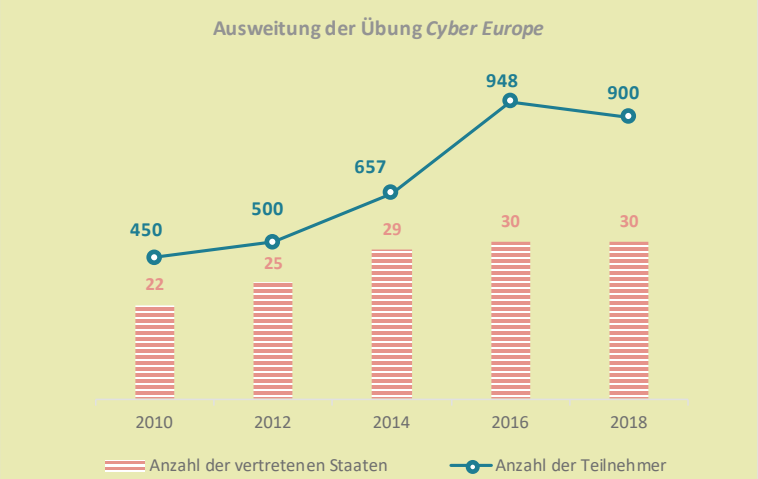
87 Die EU hat Experten für Terrorismusbekämpfung/Sicherheit an 17 Delegationen entsandt, um die Verbindung zwischen der inneren und der äußeren Sicherheit der EU zu verstärken[125]. Trotz der knappen Ressourcen könnte größeres Fachwissen im Cyberbereich dabei helfen, die richtigen Projekte auf den Weg zu bringen und Synergien mit anderen Programmen und Finanzierungsquellen zu ermitteln[126]. Es könnte der Cybersicherheit auch zu mehr Beachtung im politischen Dialog verhelfen, obwohl sie mit zahlreichen anderen Prioritäten wie Migration, organisierter Kriminalität oder aus dem Ausland zurückkehrenden Kämpfern konkurrieren müsste.

Kasten 4

Übungen

Übungen sind ein wichtiger Bestandteil der Aus- und Fortbildung im Cyberbereich. Sie bieten eine erstklassige Gelegenheit zur Förderung der Abwehrbereitschaft durch Testmöglichkeiten in lebensnahen Szenarien und dienen dem Aufbau von Netzwerken für Arbeitsbeziehungen. Seit 2010 finden sie viel häufiger statt.

Die Teilnahme erfolgt vor Ort oder aus der Ferne. Nach den Übungen werden Bewertungen zur Feststellung der gewonnenen Erkenntnisse vorgenommen, die möglicherweise jedoch noch nicht vollständig bei den strategisch/politischen, operativen und technischen Ebenen ankommen[127].



Quelle: Europäischer Rechnungshof auf der Grundlage von ENISA-Dokumenten.

Die wichtigsten Übungen von EU und NATO – die alle zwei Jahre stattfindende *Cyber Europe* (operativ) und die einmal jährlich stattfindende *Locked Shields* (technisch) – ziehen mehr als 1 000 Teilnehmer aus rund 30 teilnehmenden Staaten an. Schwerpunkt bei beiden Übungen ist der Schutz und die Aufrechterhaltung kritischer Infrastrukturen unter simulierten Angriffsszenarien. Die Übungen wurden erheblich ausgeweitet, und umfassen nun mediale, rechtliche und finanzpolitische Aspekte, um die Lagebeurteilung durch die Fachleute aus der Praxis zu verbessern. Die parallelen und koordinierten Übungen (PACE) sind strategischer Art und dienen der Erprobung der Zusammenarbeit von EU und NATO in einem hybriden Krisenszenario.

Dies sind nicht die einzigen internationalen Übungen. Die ENISA organisiert die jährliche Cyber-Challenge, bei der Teams gegeneinander antreten, um sich sicherheitsbezogenen Aufgaben wie Internet- und mobile Sicherheit, Cryptopuzzles, Reverse Engineering, Ethik und Forensik zu stellen. Die erste Übung auf ministerieller Ebene – EU CYBRID – fand im September 2017 statt. Im Fokus stand die strategische Entscheidungsfindung. Im Jahr 2018 wurde gemeinsam mit der NATO die *Crossed-Swords*-Übung gestartet mit dem Ziel, die offensiven Komponenten der *Locked-Shields*-Übung zu verbessern. Die NATO organisiert auch die Cyber-Coalition-Übungen.

Ganz wesentlich ist dabei, dass sich alle wichtigen Akteure aktiv einbringen und alle Übungen abgestimmt werden, damit Doppelarbeit vermieden wird und ein effizienter Austausch der gesammelten Erfahrungen stattfindet.

Problembewusstsein

88 Oftmals sind Bürgerinnen und Bürger Angriffsvektoren und verbreiten Desinformation, da sie durch Schwachstellen in billigen und weithin genutzten Geräten und Softwarelösungen unwissentlich gefährdet sind oder Opfer von *Social Engineering* werden. Nur durch Sensibilisierung kann daher eine wirksame Cyber-Resilienz entstehen, was jedoch keineswegs eine leichte Aufgabe ist, da die Komplexität der Cybersicherheit und die damit verbundenen Risiken für Nichtfachleute schwer zu verstehen sind.

89 Beispiele für Sensibilisierungsmaßnahmen sind der jährliche Europäische Monat der Cybersicherheit (*European Cyber Security Month*, ECSM) und der Tag des sichereren Internets (*Safer Internet Day*). Am Europäischen Monat der Cybersicherheit beteiligen sich inzwischen sieben Drittstaaten[128]. Die Europol-Kampagne *Say No!* hat zum Ziel, Kinder besser vor sexueller Nötigung und Erpressung im Internet zu schützen. Dieser Gefahr vorzubeugen ist deshalb wichtig, weil derzeit nur wenige Opfer solche Straftaten der Polizei melden[129]. Die Kommission räumt ein, dass die Cybersicherheitsstrategie bei der Sensibilisierung von Bürgern und Unternehmen bisher nur "bedingt wirksam" war[130]. Gründe hierfür sind das Ausmaß der Aufgabe, begrenzte Ressourcen, unterschiedliches Engagement der Mitgliedstaaten und fehlende wissenschaftliche Grundlagen dafür, wie Sensibilisierung erreicht und gemessen werden kann.

90 Die Herausforderung für die Kommission und die einschlägigen Agenturen besteht darin, dafür zu sorgen, dass die Sensibilisierungsmaßnahmen das jeweilige Zielpublikum erreichen, niemanden ausschließen, an der Bedrohungslandschaft ausgerichtet sind und keine ungewollten Effekte wie "Sicherheitsüberdruss"[131]

auslösen. Außerdem müssen Evaluierungsmethoden und Parameter zur Bewertung der Wirksamkeit entwickelt werden. Dies sollte gleichermaßen in den EU-Organen selbst stattfinden, wo das Problembewusstsein ebenfalls verbessert werden muss[132].

Herausforderung 8: Informationsaustausch und Koordinierung verbessern

91 Cybersicherheit erfordert die Zusammenarbeit des öffentlichen und des privaten Sektors, in erster Linie beim Austausch von Informationen und bewährten Verfahren. Nur durch Vertrauen auf allen Ebenen lassen sich günstige Rahmenbedingungen für den grenzübergreifenden Austausch sensibler Informationen schaffen. Durch unzulängliche Koordinierung kommt es zu Fragmentierung, Doppelarbeit und einer Aufsplitterung des Fachwissens. Eine wirksame Koordinierung kann hingegen zu greifbaren Erfolgen wie der Abschaltung von Marktplätzen im Darknet führen[133]. Trotz der in den letzten Jahren erzielten Fortschritte, ist das Maß an Vertrauen auf EU-Ebene und in einigen Mitgliedstaaten[134] nach wie vor ungenügend[135].

Koordinierung zwischen den EU-Organen und mit den Mitgliedstaaten

92 Eine der Zielsetzungen der Cybersicherheitsstrategie und der durch die NIS-Richtlinie eingeführten Kooperationsstrukturen war es, das Vertrauen zwischen den Interessenträgern zu stärken. In der Bewertung der Strategie wird anerkannt, dass der Grundstein für eine strategische und operative Zusammenarbeit auf EU-Ebene gelegt wurde[136]. Dennoch ist die Koordinierung im Allgemeinen unzulänglich[137]. Die Herausforderung besteht darin, dafür zu sorgen, dass der Informationsaustausch nicht nur sachdienlich ist, sondern auch ein umfassendes Bild der Gesamtsituation ermöglicht. Wichtig ist dabei, auf der Grundlage einer anerkannten Terminologie ein gemeinsames Verständnis zu erreichen (siehe ***Kasten 5***).

93 Die ENISA merkte in ihrer Evaluierung jedoch an, der Ansatz der EU im Hinblick auf die Cybersicherheit sei nicht ausreichend koordiniert, was zu einem Mangel an Synergien zwischen den Tätigkeiten der ENISA und denen anderer Interessenträger führe. Die Kooperationsmechanismen sind noch recht unausgereift[138]. Der Rechtsakt zur Cybersicherheit will hier durch Stärkung der Koordinierungsfunktion der ENISA Abhilfe schaffen. Die 2018 zwischen der ENISA, der Europäischen Verteidigungsagentur, dem EC3 von Europol und CERT-EU geschlossene Vereinbarung wurde von dem Wunsch getragen, die Zusammenarbeit zu verbessern[139]. Eine Priorität der Kommission in den kommenden Jahren wird sein, für eine angemessene

Abstimmung von politischen Initiativen, Bedarf und Investitionen zu sorgen, um die Aufsplitterung zu überwinden und Synergien zu schaffen[140].

94 Koordinierungsfunktionen sind in mehrere institutionelle Gremien integriert. Die Taskforce für die Sicherheitsunion sollte eine wesentliche Rolle bei der Koordinierung der verschiedenen Generaldirektionen der Kommission im Hinblick auf die Ausgestaltung der Sicherheitsunion übernehmen[141]. Die GD CNECT führt den Vorsitz in der Unterarbeitsgruppe "Cybersicherheit" der Taskforce.

95 Beim Rat ist die Horizontale Gruppe "Fragen des Cyberraums" für die Cybersicherheit zuständig. Sie koordiniert strategische und horizontale Fragen des Cyberraums, hilft bei der Vorbereitung von Übungen und der Evaluierung ihrer Ergebnisse. Die Gruppe arbeitet eng mit dem Politischen und Sicherheitspolitischen Komitee zusammen, das eine zentrale Rolle bei der Entscheidungsfindung bei allen cyberbezogenen diplomatischen Maßnahmen hat (siehe ***Kasten 6*** im folgenden Kapitel). Da Cybersicherheit ein Querschnittsthema ist, gestaltet sich die Abstimmung aller einschlägigen Interessen schwierig: Nicht weniger als 24 Arbeitsgruppen und Vorbereitungsgremien waren zuletzt mit Fragen zum Cyberbereich befasst[142].

96 Die beiden zuletzt vorgelegten Legislativvorschläge – zur Stärkung der ENISA (2017) und zur Einrichtung eines Netzes von Cybersicherheitskompetenzzentren und eines Forschungskompetenzzentrums (2018) – sind speziell auf das Problem der Fragmentierung und der Doppelarbeit ausgelegt. Ein wichtiger Grund für die Einrichtung des Netzes von Cybersicherheitskompetenzzentren und eines Forschungskompetenzzentrums war die Notwendigkeit, die Lücke zu füllen, die bei den in der NIS-Richtlinie vorgesehenen Kooperationsstrukturen besteht, da diese nicht auf die Entwicklung von zukunftsweisenden Lösungen ausgelegt sind.

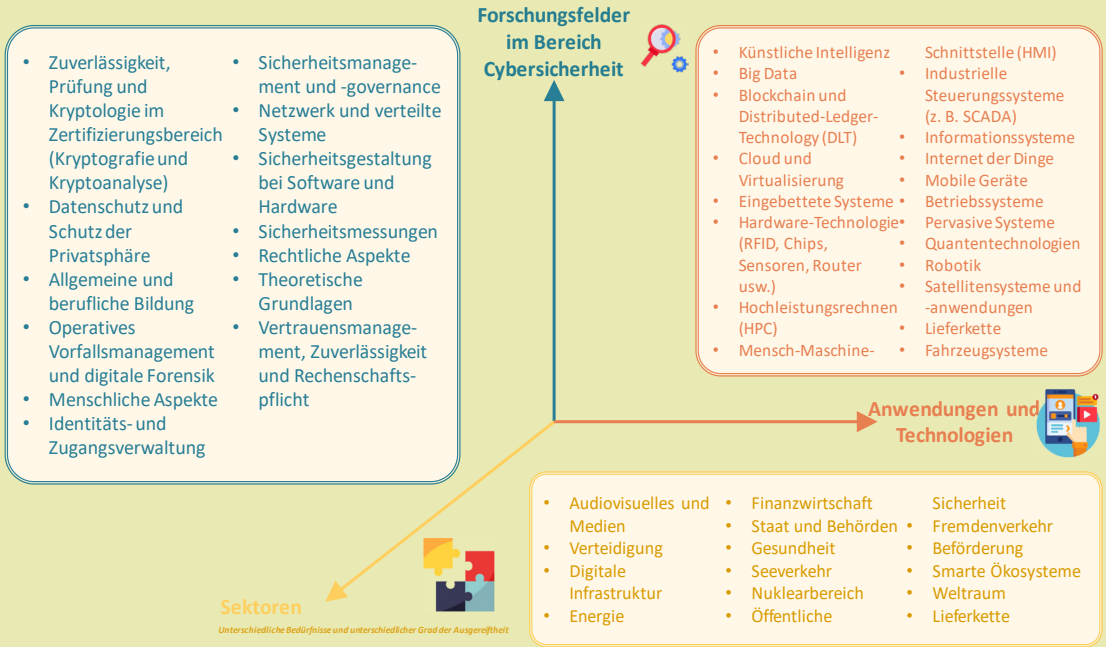
Kasten 5

Bemühungen um einen gemeinsamen Netzjargon: *Technologische Kohärenz*

Begriffliche Klarheit verbessert die Lagebeurteilung und Koordinierung[143] und ermöglicht es, präzise festzulegen, was eine Bedrohung und was ein Risiko ist.

Die Gemeinsame Forschungsstelle (JRC) der Kommission hat auf der Grundlage unterschiedlicher internationaler Normen jüngst eine überarbeitete Forschungssystematik entwickelt[144]. Sie soll Forschungseinrichtungen in ganz Europa als Index dienen.

Cybersicherheits-Systematik



Quelle: Europäischer Rechnungshof auf der Grundlage von Daten der Europäischen Kommission.

Bis vor Kurzem verwendeten die Organe und Agenturen der EU keine gemeinsamen Definitionen. Das ändert sich gerade. Die Kooperationsgruppe gestaltete im Rahmen ihres Konzeptentwurfs eine Systematik für Sicherheitsvorfälle, um eine effiziente grenzüberschreitende Zusammenarbeit zu erleichtern.

Zusammenarbeit und Informationsaustausch mit dem Privatsektor

97 Die Zusammenarbeit zwischen Behörden und dem Privatsektor ist unerlässlich, um die Cybersicherheit insgesamt zu verbessern. Dessen ungeachtet stellte die Kommission in ihrer Bewertung der Cybersicherheitsstrategie aus dem Jahr 2017 fest, dass der Informationsaustausch zwischen privaten Interessenträgern sowie zwischen dem öffentlichen und dem privaten Sektor noch nicht optimal sei, weil vertrauenswürdige Meldeverfahren und Anreize für den Austausch von Informationen fehle[145], was das Erreichen strategischer Ziele erschwere. Sie wies außerdem darauf hin, dass ein effizienter Kooperationsmechanismus fehlt, anhand dessen die Mitgliedstaaten zusammenarbeiten, um beim Ausbau dauerhafter industrieller Fähigkeiten strategisch vorzugehen[146].

98 Informationsaustausch- und Analysezentren sollen als Plattformen dienen und Ressourcen bereitstellen, die den Informationsaustausch zwischen dem öffentlichen und dem privaten Sektor sowie das Sammeln von Informationen über Cyberbedrohungen erleichtern. Dabei geht es darum, durch den Austausch von Erfahrungen, Wissen und Analysen, insbesondere über Ursachen, Vorfälle und Bedrohungen Vertrauen aufzubauen. Nationale und sektorbezogene Informationsaustausch- und Analysezentren gibt es bereits in vielen Mitgliedstaaten, auf europäische Ebene sind es jedoch noch recht wenige[147]. Hier bestehen jedoch zahlreiche Herausforderungen (Ressourcenknappheit, schwierige Erfolgsmessung, Erschließung der richtigen Strukturen, um den öffentlichen und den privaten Sektor zu gewinnen, Einbeziehung der Strafverfolgungsbehörden), die bewältigt werden müssen, wenn die Zentren zur Umsetzung der NIS-Richtlinie und auf gesamteuropäischer Ebene zum Aufbau von Fähigkeiten im Sicherheitsbereich beitragen sollen[148].

99 Der Cyberkriminalität in ihrer Komplexität ist nur durch enge Zusammenarbeit mit dem privaten Sektor beizukommen, die Effizienz dieser Zusammenarbeit variiert jedoch von Mitgliedstaat zu Mitgliedstaat und hängt davon ab, wie groß das Vertrauen ist[149]. Das EC3 von Europol hat jedenfalls eine Reihe von Beratungsgruppen eingerichtet, in denen Akteure des Privatsektors, die Organe und Agenturen der EU und andere internationale Organisationen vertreten sind, um die Zusammenarbeit durch Vernetzung, den strategischen Austausch nachrichtendienstlicher Erkenntnisse und Kooperation zu verbessern. Die Arbeitsgruppen richten ihre Tätigkeit an Plänen aus, die auf die Ziele des EU-Politikzyklus abgestimmt sind[150]. Der kriminelle Missbrauch der Verschlüsselung ist ein weiterer Bereich voller Herausforderungen, die eine engere Zusammenarbeit mit dem Privatsektor erfordern. Das EC3 von Europol prüft derzeit, welche Möglichkeiten es für die einzelfallbezogene kurzfristige

Entsendung von Experten aus dem Privatsektor und von Hochschulen zur Gemeinsamen Taskforce gegen die Cyberkriminalität gibt (siehe Ziffer ***62***).

100 Das Fehlen effizienter Kooperationsmechanismen ist ein Problem für die zivilen und die militärischen Fachkreise – im öffentlichen wie im privaten Sektor. Eine gemeinsame Herausforderung besteht in folgenden Bereichen: Kryptographie, eingebettete IKT-Systeme, Erkennung von Malware, Simulationstechniken, Schutz für Netze und Kommunikationssysteme sowie Authentifizierungstechnologien. Die Förderung der zivil-militärischen Zusammenarbeit sowie von Forschung und Technologie (insbesondere durch die Unterstützung von KMU) sind zwei der Prioritäten des EU-Politikrahmens für die Cyberabwehr (Aktualisierung 2018).

Denkanstöße – Stärkung der Resilienz

- Wie lässt sich auf EU-Ebene ein ausgewogenes Verhältnis herstellen zwischen der notwendigen Straffung der Cybersicherheitspolitik und einer effizienten Koordinierung zwischen den verschiedenen Akteuren und der Zersplitterung der Zuständigkeiten?
- Wie gut sind die Organe und Agenturen der EU auf den nächsten großen Angriff vorbereitet, der unmittelbar gegen sie gerichtet ist?
- Was kann getan werden, um die für den Cyberbereich zuständigen Agenturen der EU für Talente attraktiver zu machen?
- Welche weiteren Maßnahmen müssen ergriffen werden, damit sichergestellt ist, dass alle Organe und Agenturen der EU über angemessene Kapazitäten verfügen, die eine kohärente Risiko- und Bedrohungsbewertung ermöglichen?
- Was unternehmen die Europäischen Aufsichtsbehörden (Europäische Bankenaufsichtsbehörde, Europäische Wertpapier- und Marktaufsichtsbehörde und Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), um den für den Finanzsektor typischen Cyberschwachstellen zu begegnen und was lässt sich davon für andere Sektoren übernehmen?
- Wie kann – in Anbetracht des generellen Wissensdefizits – die technische Hilfe der EU für Behörden optimal genutzt werden, um bei der Verbesserung der Cyber-Resilienz die größtmögliche Wirkung zu erzielen?
- Wie können die EU und die Mitgliedstaaten ihre Teilnahme an internationalen Gesprächen so nutzen, dass sie Governance und Normen für den Cyberraum mitgestalten und den Werten der EU Gewicht verleihen?
- Welche Sensibilisierungsmaßnahmen (einschließlich Prävention) greifen auf EU- und auf mitgliedstaatlicher Ebene tatsächlich, und wie kann die EU diese Maßnahmen ausweiten?
- Wie kann sich die EU einbringen, damit die Geschlechterdiversität im Bereich der Cybersicherheit Einzug hält?
- Wie können die EU und die Mitgliedstaaten die Synergien zwischen den zivilen und militärischen Fachkreisen – im Einklang mit dem Politikrahmen für die Cyberabwehr (Aktualisierung 2018) – verstärken?

Wirksame Reaktion auf Cybervorfälle

101 Die Konzeption einer wirksamen Reaktion auf Cyberangriffe ist entscheidend, um sie schnellstmöglich im Keim zu ersticken. Besonders wichtig ist, dass kritische Sektoren, die Mitgliedstaaten und die EU-Organe schnell und koordiniert reagieren können. Dies setzt voraus, dass die Angriffe frühzeitig erkannt werden.

Herausforderung 9: wirksame Erkennung und Reaktion

Erkennung und Meldung

102 Mit herkömmlichen Erkennungstools lassen sich die allermeisten Angriffe im Alltagsgeschehen abwehren[151]. Allerdings sind die digitalen Systeme mittlerweile so komplex, dass es unmöglich ist, jeden einzelnen Angriff zu verhindern. Da die Angriffe sehr raffiniert ausgeführt werden, bleiben sie oft lange Zeit unentdeckt. Laut Expertenmeinung sollte der Schwerpunkt daher auf rascher Erkennung und Abwehr liegen[152]. Manche Erkennungstools – wie Automatisierung, maschinelles Lernen und Verhaltensanalysen, die auf Risikominderung sowie darauf abstellen, das Systemverhalten zu analysieren und daraus zu lernen – werden jedoch von den Unternehmen nur schlecht angenommen[153]. Dies liegt zum Teil an vermeintlichen positiven Treffern, bei denen harmlose Handlungen fälschlicherweise als böswillig eingestuft werden.

103 Nach Aufdeckung und Analyse einer Sicherheitsverletzung ist eine zügige Meldung und Berichterstattung erforderlich, damit andere öffentliche und private Einrichtungen Vorbeugungsmaßnahmen ergreifen und die zuständigen Behörden die Betroffenen unterstützen können. Vielen Organisationen widerstrebt es, Cybervorfälle einzuräumen und zu melden[154]. Die frühzeitige Einbeziehung von Strafverfolgungsbehörden in die Erstreaktion auf mutmaßliche Fälle von Cyberkriminalität und ein proaktiver Informationsaustausch mit den CSIRTs sind ebenfalls von grundlegender Bedeutung.

104 Da es früher auf EU-Ebene keine gemeinsamen Vorgaben für die Meldung von Sicherheitsvorfällen gab, bestand das Risiko, dass sich die Mitteilung von Sicherheitsverletzungen verzögerte und keine Abwehrmaßnahmen ergriffen werden konnten. Hier sollte mit der Einführung der NIS-Richtlinie Abhilfe geschaffen werden (siehe Ziffer ***20***). Nach dem *WannaCry*-Angriff von 2017 kam die Kommission zu dem Schluss, das CSIRT-Netz sei "noch nicht voll einsatzfähig"[155]. Im Zuge der Umsetzung

der Richtlinie wird sich zeigen, ob die von der Kooperationsgruppe erstellten Leitlinien wirksam dazu beitragen, die Zurückhaltung bei der Meldung von Vorfällen aufzuweichen[156].

105 Betreiber wesentlicher Dienste in bestimmten Sektoren haben im Rahmen der geltenden EU-Vorschriften mehrfache Meldepflichten (einschließlich gegenüber den Verbrauchern), was die Effizienz des Verfahrens beeinträchtigen kann. Für Wirtschaftsteilnehmer im Finanz- und im Bankensektor etwa gelten – im Rahmen der DSGVO, der NIS-Richtlinie, der Zahlungsdiensterichtlinie, EZB/SSM, Target 2 und der eIDAS-Verordnung[157] – unterschiedliche Meldekriterien, Standards, Schwellenwerte und Fristen. Diese Pflichten müssen unbedingt gestrafft werden, denn abgesehen vom unnötigen Verwaltungsaufwand kann diese Heterogenität zu einer bruchstückhaften Berichterstattung führen.

Koordinierte Reaktion

106 Die Entwicklung eines europäischen Rahmens für die Zusammenarbeit bei Cybersicherheitskrisen ist noch im Gange. Der diesbezügliche "Konzeptentwurf"[158] (siehe Ziffer ***18***) wurde daher eingeführt, um der integrierten Regelung für die politische Reaktion auf Krisen einen Bezug zum Cyberbereich zu geben, die Lagebeurteilung zu verbessern und für eine stärkere Verknüpfung mit anderen Krisenmanagementmechanismen der EU zu sorgen[159]. In dieses Konzept einbezogen sind die Organe und Agenturen der EU und die Mitgliedstaaten. Ein nahtloses Ineinandergreifen all dieser Krisenreaktionsmechanismen ist ein schwieriges Unterfangen[160]. Dass derzeit ein gemeinsames sicheres Kommunikationsnetz zwischen allen EU-Organen fehlt, ist ebenfalls ein entscheidender Schwachpunkt[161].

107 Die Fähigkeit der EU, im Fall eines großen, grenzüberschreitenden Vorfalls auf operativer und politischer Ebene auf Cyberangriffe zu reagieren, wurde als "begrenzt" bezeichnet. Dies liegt u.a. daran, dass die Cybersicherheit noch nicht in die auf EU-Ebene vorhandenen Mechanismen für die Koordinierung der Krisenreaktion integriert ist[162]. Die NIS-Richtlinie ist auf diese Problematik nicht eingegangen.

108 Die kürzlich vorgeschlagene Reform der ENISA, wonach der Agentur eine größere operative Rolle bei der Bewältigung großer Cybersicherheitsvorfälle zukommen sollte, wurde von den Mitgliedstaaten nicht mitgetragen, denen zufolge die Aufgabe der Agentur vorzugsweise darin bestehen sollte, die operativen Maßnahmen der Mitgliedstaaten zu unterstützen und zu ergänzen[163]. Auf Ebene der Mitgliedstaaten gibt es zahlreiche CERTs/CSIRTs, deren Kapazitäten allerdings sehr

unterschiedlich sind, was einer wirksamen grenzüberschreitenden Zusammenarbeit, wie sie bei der Reaktion auf große Vorfälle notwendig ist, im Wege steht[164].

109 Der Hof versuchte, die den einzelnen Akteuren im Konzeptentwurf zugewiesenen unterschiedlichen Rollen in ein Gesamtbild zu setzen, stieß aber auf Lücken, die im Zuge der Umsetzung gefüllt werden müssen. Ein ursprünglich zu wenig beachteter Bereich war die Strafverfolgung, obwohl das EU-Notfallprotokoll für die Strafverfolgungsbehörden im Dezember 2018 in Kraft trat[165]. Der Konzeptentwurf wird nur Erfolg haben, wenn er praktisch umsetzbar ist und alle Beteiligten ihre Aufgaben kennen – dies muss in den kommenden Jahren umfassend erprobt werden.

110 Wirksame Reaktion geht über reine Schadensbegrenzung hinaus. Es ist ebenfalls von zentraler Bedeutung, die für die Angriffe Verantwortlichen ausfindig zu machen. Die Täter zu ermitteln und zu identifizieren kann sich insbesondere bei einem hybriden Angriff wegen des zunehmenden Missbrauchs von Anonymisierungsprogrammen, Kryptowährungen und Verschlüsselung als sehr schwierig erweisen. Dies wird als das Zuordnungsproblem bezeichnet. Die Lösung dieses Problems ist nicht nur eine technische Frage, sie hat auch eine strafrechtliche Seite. Rechtliche und verfahrenstechnische Unterschiede zwischen den Ländern können strafrechtliche Ermittlungen und die strafrechtliche Verfolgung von Verdächtigen erschweren. Zur Lösung des Zuordnungsproblems muss der Austausch operativer Informationen durch klarere Verfahren etwa mit Europol oder dem Europäischen Justiziellen Netz gegen Cyberkriminalität von Eurojust stärker formalisiert werden.

111 Auf politischer Ebene wurde das Instrumentarium für die Cyberdiplomatie, die sogenannte "Cyber Diplomacy Toolbox" (siehe ***Kasten 6***) entwickelt, um internationale Streitigkeiten im Cyberraum auf friedlichem Wege beizulegen. Die Schaffung der Teams für die rasche Reaktion auf Cybervorfälle und einer Initiative für die gegenseitige Unterstützung im Bereich der Cybersicherheit sind zwei Projekte zur Förderung eines stärkeren Informationsaustauschs, die derzeit im Rahmen der Ständigen Strukturierten Zusammenarbeit entwickelt werden[166].

Kasten 6

Die "Cyber Diplomacy Toolbox"

Die gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten[167] (*Cyber Diplomacy Toolbox*) beruht auf den 2015 vom Rat angenommenen Schlussfolgerungen zur Cyberdiplomatie[168]. Ziel der Cyberdiplomatie ist die Entwicklung und Umsetzung eines gemeinsamen umfassenden Ansatzes im Umgang mit dem Cyberraum, der auf den Werten der EU, dem Rechtsstaatsprinzip, Kapazitätsaufbau und Partnerschaften, der Förderung des Multi-Stakeholder-Modells für die Internet-Governance, der Eindämmung von Cyberbedrohungen und einer größeren Stabilität in den internationalen Beziehungen basiert.

Die Toolbox ermöglicht es der EU und den Mitgliedstaaten, eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten vorzubereiten, und dazu alle im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik zu Gebote stehenden Maßnahmen zu nutzen. Das können Präventivmaßnahmen (z. B. Sensibilisierung, Kapazitätsaufbau), Kooperationsmaßnahmen, Stabilisierungsmaßnahmen und restriktive Maßnahmen (z. B. Reisebeschränkungen, Waffenembargos, Einfrieren von Geldern) oder Unterstützung der Reaktion der Mitgliedstaaten sein[169]. Dahinter steht der Gedanke, dass verstärkte Zusammenarbeit bei der Eindämmung von Gefahren und klares Aufzeigen der voraussichtlichen Folgen einer gemeinsamen Reaktion (potenziell) von aggressivem Verhalten abhalten können.

Eine gemeinsame Reaktion der EU auf böswillige Cyberaktivitäten würde in einem angemessenen Verhältnis zur Tragweite, Größenordnung, Dauer, Intensität, Komplexität, Raffiniertheit und Wirkung der Cyberaktivität stehen.

Der Erfolg der Toolbox wird ganz wesentlich davon abhängen, wie eng sie mit dem Konzeptentwurf und der integrierten Regelung für die politische Reaktion auf Krisen (siehe Ziffer ***106***) verwoben ist, wie gut die Lagebeurteilung durch schnellen und kontinuierlichen Austausch von Informationen funktioniert (was auch die Zuordnung umfasst)[170] und schließlich davon, wie effektiv die Zusammenarbeit ist. Eine weitere Voraussetzung für die erfolgreiche Einführung der Toolbox ist die wirksame und koordinierte Kommunikation. Bislang kam die Toolbox zweimal zum Einsatz: Zur Anknüpfung eines Dialogs mit den Vereinigten Staaten nach dem *WannaCry*-Angriff[171] und zur Ausarbeitung der Schlussfolgerungen des Rates zur Verurteilung der böswilligen Nutzung von Informations- und Kommunikationstechnologien[172]. Die operative Umsetzung der Toolbox ist im Gange - inwieweit sie ihre Ziele erreicht, bleibt abzuwarten.

Herausforderung 10: Schutz kritischer Infrastrukturen und gesellschaftlicher Funktionen

Schutz der Infrastruktur

112 Ein großer Teil der kritischen Infrastrukturen in der EU wird über industrielle Steuerungssysteme betrieben[173]. Viele davon wurden als eigenständige Systeme mit begrenzter Konnektivität zur Außenwelt konzipiert. Da Komponenten der industriellen Steuerungssysteme an das Internet angeschlossen wurden, sind sie nun anfälliger für Einflussnahme von außen. Pflege und Instandhaltung vorhandener Systeme sind unter Umständen nicht mehr möglich, doch ein Upgrade der Systeme ist weder schnell noch kostengünstig zu haben. Maßnahmen zur Verbesserung der Sicherheit kritischer Infrastrukturen müssen daher Upgrades der industriellen Steuerungssysteme umfassen.

113 Mit fortschreitender Digitalisierung der Industrie (gemeinhin als "Industrie 4.0" bezeichnet) können die Auswirkungen eines großen Vorfalls in einer Branche Folgewirkungen in anderen Bereichen haben. Die ENISA hat darauf hingewiesen, dass die wechselseitige Abhängigkeit von kritischen Sektoren erfasst werden muss[174]. Nur so kann man sich ein Bild von der potenziellen Ausbreitung eines Vorfalls machen. Außerdem wird dadurch eine Grundlage für gut koordinierte Reaktionen geschaffen.

114 Die NIS-Richtlinie zielt auf eine Verbesserung der Abwehrbereitschaft in für kritische Infrastrukturen zuständigen Schlüsselsektoren ab. Sie erstreckt sich allerdings nicht auf alle relevanten Sektoren (siehe ***Tabelle 1***)[175], was die Wirksamkeit der Strategie[176] schmälert: In dieser Hinsicht besonders problematisch ist der Schutz der demokratischen Integrität von Wahlen vor der Einflussnahme auf die Wahlinfrastruktur und vor Desinformation (siehe ***Kasten 7***). Eine zentrale Herausforderung – neben der Überarbeitung der geltenden Rechtsvorschriften – wird daher die Frage sein, wie diese Sektoren in eine wirksame Reaktion auf große Sicherheitsvorfälle eingebunden werden können.

115 Schwachstellen bei kritischen Infrastrukturen machen nicht an Europas Grenzen halt. Eine besondere Herausforderung für die Kommission besteht darin, die EU-Bewerberländer dazu anzuhalten, die gleichen Standards anzunehmen wie die Mitgliedstaaten, beispielsweise in Bereichen wie cyberbezogene Rechtsvorschriften oder Schutz kritischer Infrastrukturen.

Kasten 7

Schutz kritischer gesellschaftlicher Funktionen: *Bekämpfung der Wahleinmischung*

Im Mai 2019 sind rund 400 Millionen Wählerinnen und Wähler zur Stimmabgabe bei den Wahlen zum Europäischen Parlament aufgerufen, der ersten seit Inkrafttreten der Datenschutz-Grundverordnung. Diese Wahlen finden im Kielwasser von Skandalen rund um den Missbrauch personenbezogener Daten für politische Mikrotargeting-Kampagnen und beispielloser konzertierter Desinformationskampagnen ("Fake News") statt. Die Kommission hat darauf hingewiesen, dass mit einer Einmischung in diese Wahlen mit Mitteln des Internets zu rechnen ist[177]. Dagegenzuhalten erfordert ein Vorgehen, das alle Behördenebenen und die gesamte Gesellschaft einbezieht.

Wahlinfrastruktur

Die Abhaltung von Wahlen ist ein komplexer Vorgang. Die Mitgliedstaaten haben für den Schutz und die Integrität der Wahlen zu sorgen. Wahleinmischung und Einflussnahme auf die Wahlinfrastruktur kann ein Versuch sein, die Wählergunst, den Ausgang der Wahlen oder den Wahlvorgang an sich zu beeinflussen, einschließlich der eigentlichen Stimmabgabe, der Stimmenauszählung und der Kommunikation. Bei den Wahlen zum Europäischen Parlament ist der Schutz der sogenannten "letzten Meile" (die Übermittlung der Ergebnisse aus den Hauptstädten der Mitgliedstaaten an Brüssel) besonders kritisch, da es kein gemeinsames Sicherheitskonzept dafür gibt und auch keines dafür getestet wurde[178].

Das von der Kommission kürzlich vorgelegte Wahlpaket umfasste Maßnahmen zur Verbesserung der Cybersicherheit für Wahlen, wie die Benennung nationaler Kontaktstellen zur Koordinierung und zum Informationsaustausch im Vorfeld der Wahlen. Der Austausch von bewährten Verfahren und gewonnenen Erkenntnissen ist besonders wichtig[179].

Wahlsysteme gelten nicht als kritische Infrastruktur[180] und fallen auch nicht unter die NIS-Richtlinie. Trotzdem hat die Kooperationsgruppe einen praktischen Leitfaden für die Sicherheit der bei Wahlen eingesetzten Technologien erstellt, um die Behörden zu unterstützen. Für Anfang 2019 ist eine Sitzung der nationalen Kontaktstellen geplant[181]. Zudem sind die Mitgliedstaaten aufgefordert, die Bedrohungslage durch Cyberangriffe auf ihre Wahlverfahren Risikobewertungen zu unterziehen.

Desinformation

Desinformation gewinnt bei hybriden Angriffen mit Cyberattacken und dem Hacken von Netzen zunehmend an Bedeutung. Sie kann eingesetzt werden, um die Gesellschaft zu spalten, Misstrauen zu säen und das Vertrauen in demokratische Prozesse oder andere Themen zu untergraben (Beispiele hierfür sind die Anti-Impf-

Bewegung oder die Leugnung des Klimawandels). Desinformation hat in Bezug auf Dimension, Tempo und Reichweite zugenommen und stellt eine echte Bedrohung für die EU dar.

Die EU hat eine Reihe von Maßnahmen ergriffen, um die Desinformation zu bekämpfen. Im Jahr 2015 wurde beim EAD die East StratCom Taskforce eingerichtet, um Russlands Desinformationskampagnen entgegenzuwirken[182]. Experten haben sich anerkennend zur Tätigkeit der Taskforce hinsichtlich der Förderung der Politik der EU, der Unterstützung unabhängiger Medien in den Nachbarländern sowie der Vorwegnahme, dem Aufspüren und der Bekämpfung von Desinformation geäußert[183]. Gemessen an der Größenordnung und Komplexität von Desinformationskampagnen sind die Ressourcen der Taskforce jedoch begrenzt[184]. Eine systematischere Interaktion mit den vorhandenen EU-Strukturen und eine bessere Zusammenarbeit im Bereich der strategischen Kommunikation sind notwendig[185]. Der Europäische Rat hat im Dezember 2018 einen neuen Aktionsplan gebilligt[186].

Kürzlich hat die Kommission vor dem Hintergrund ihrer Mitteilung über die Bekämpfung von Desinformation im Internet von April 2018[187] einen Verhaltenskodex zur Selbstregulierung (auf freiwilliger Basis)[188] ausgearbeitet, der auf vorhandenen politischen Instrumenten beruht und zu dem sich Online-Plattformen und die Werbewirtschaft bekannten[189]. Zu den Maßnahmen gehören die Stärkung der Vertrauenswürdigkeit von Inhalten und die Unterstützung der Bemühungen zur Verbesserung der Medien- und Nachrichtenkompetenz. Ein unabhängiges europäisches Netz von Faktenprüfern wurde ebenfalls eingerichtet.

Die Kommission hat für den Fall, dass der Verhaltenskodex nicht eingehalten wird, die Möglichkeit weiterer Regulierungsmaßnahmen angekündigt. Die Bestimmung der Wirksamkeit der Maßnahmen wird ganz entscheidend sein, insbesondere die Frage, wie Steigerungen bei Vertrauen, Transparenz und Rechenschaftspflicht gemessen werden können.

Eine weitere Herausforderung besteht darin, Wege zu finden, wie sich Desinformation besser erkennen, analysieren und enthüllen lässt[190]. Eine aktive strategische Überwachung und Analyse offener Datenquellen ist ebenfalls erforderlich[191]. Bei dem Versuch, sich ein besseres Bild der Bedrohungslage zu verschaffen, sollten auch neue Trends wie Deepfakes (mithilfe künstlicher Intelligenz und Deep Machine Learning gefälschte Videos) berücksichtigt werden, sowie die zu ihrer Erkennung erforderlichen Tools.

Stärkung der Autonomie

116 Die EU ist bei Cybersicherheitsprodukten und -diensten Nettoimporteur, was das Risiko der technologischen Abhängigkeit von Unternehmen aus Drittländern und die Anfälligkeit ihnen gegenüber erhöht[192]. Besonders gefährdet ist dadurch die Sicherheit der kritischen Infrastrukturen der EU, die sich ebenfalls auf komplexe globale Lieferketten stützen. Dieses Risiko wird noch verschärft, wenn Unternehmen aus Drittländern europäische Cybersicherheitsunternehmen kaufen. Für die Überprüfung ausländischer Direktinvestitionen sind die Mitgliedstaaten zuständig, und derzeit gibt es keinen EU-weiten Überprüfungsmechanismus[193].

117 Größere strategische Autonomie wird in der Globalen Strategie der EU und der Mitteilung "Abwehrfähigkeit, Abschreckung und Abwehr"[194] als Ziel genannt. Die Bewältigung der unzähligen in diesem Themenpapier genannten Herausforderungen wird zur Stärkung der gewünschten Autonomie beitragen. Mit Einzelmaßnahmen ist dies nicht zu bewerkstelligen.

Denkanstöße – Wirksame Reaktion

- Was hat sich durch die NIS-Richtlinie bei der Meldung von Cybervorfällen in kritischen Sektoren und darüber hinaus verbessert?
- Wie gut funktioniert die Koordinierung der Krisenreaktion der EU-Organe auf interner Ebene bei einem großen Cybervorfall?
- Wie kann die Cyberdiplomatie im auswärtigen Handeln der EU eine wichtigere Rolle spielen?
- Sind die derzeitigen Strukturen und Maßnahmen angemessen im Verhältnis zu Größenordnung und Komplexität des Problems?

Abschließende Bemerkungen

118 In den letzten Jahren haben die EU und die Mitgliedstaaten die Cybersicherheit stärker in den Vordergrund gerückt, um die allgemeine Cyber-Resilienz zu verbessern. In der Union ein höheres Maß an Cybersicherheit zu erzielen bleibt jedoch eine Mammutaufgabe. In diesem Themenpapier zeigen wir einige der größten Herausforderungen auf, die sich für die EU bei ihrem Ziel, das weltweit sicherste digitale Umfeld zu schaffen, stellen.

119 Unsere Analyse zeigt, dass ein Übergang zu einer Leistungskultur mit integrierten Evaluierungsverfahren erforderlich ist, um eine angemessene **Evaluierung und Rechenschaftspflicht** sicherzustellen. Einige **rechtliche Lücken bestehen noch und die geltenden Rechtsvorschriften werden von den Mitgliedstaaten nicht kohärent umgesetzt**. Dadurch können die Rechtsvorschriften möglicherweise nicht voll und ganz greifen. Eine weitere vom Hof ausgemachte Herausforderung betrifft die **Angleichung des Investitionsniveaus an die strategischen Ziele**, die eine Aufstockung der Investitionen und ihrer Auswirkungen erfordert. Dies gestaltet sich schwieriger, wenn die EU und ihre Mitgliedstaaten keinen **klaren Überblick über die EU-Ausgaben** für Cybersicherheit haben. Zudem gibt es **Engpässe bei der Ausstattung der für Cyberfragen zuständigen EU-Agenturen mit angemessenen Mitteln**, einschließlich von Problemen bei der dauerhaften Anwerbung von Talenten.

120 Verfügbare Studien kommen zu dem Schluss, dass die **Cybersicherheits-Governance verstärkt werden kann**, um die Fähigkeit der internationalen Gemeinschaft, auf Cyberangriffe und -vorfälle zu reagieren, zu verbessern. Doch auch dann lassen sich nicht alle Angriffe verhindern. Eine **rasche Erkennung und Reaktion** sowie der **Schutz kritischer Infrastrukturen und gesellschaftlicher Funktionen** sind daher zusammen mit einem **besseren Informationsaustausch und einer besseren Abstimmung** zwischen dem öffentlichen und dem privaten Sektor zentrale Herausforderungen, die es zu bewältigen gilt. Und schließlich bedeutet das zunehmende weltweite Kompetenzdefizit im Bereich der Cybersicherheit, dass **Kompetenzsteigerung und größeres Problembewusstsein** in allen Sektoren und auf allen Ebenen der Gesellschaft ebenfalls eine wesentliche Herausforderung ist.

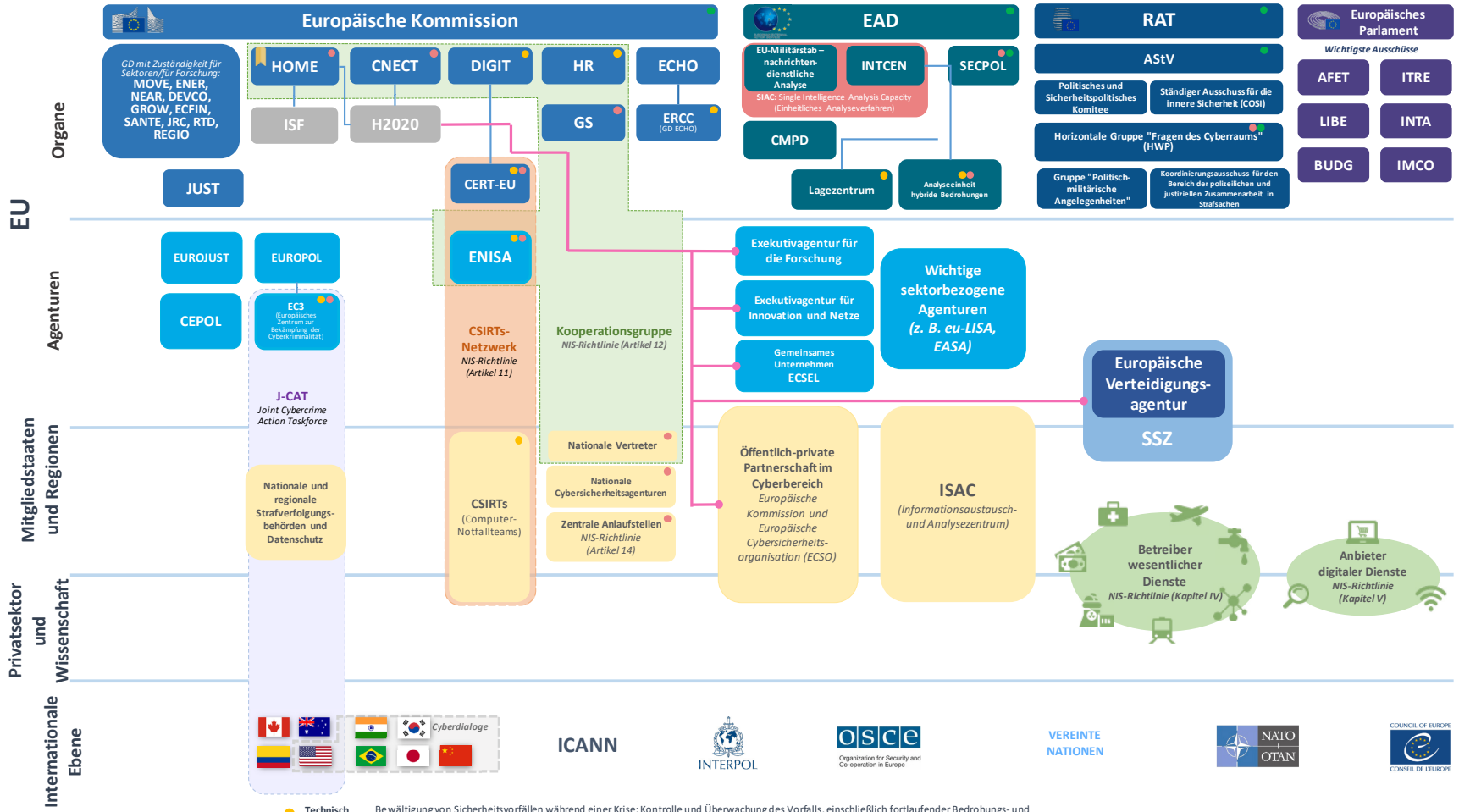
121 Die derzeitige Bedrohungslage durch Cyberangriffe, mit denen die EU und das breitere internationale Umfeld konfrontiert sind, erfordert unentwegtes Engagement und ein unverbrüchliches Bekenntnis zu den Werten der EU.

Dieses Themenpapier wurde von Kammer III in ihrer Sitzung vom 14. Februar 2019 angenommen.

Für den Rechnungshof

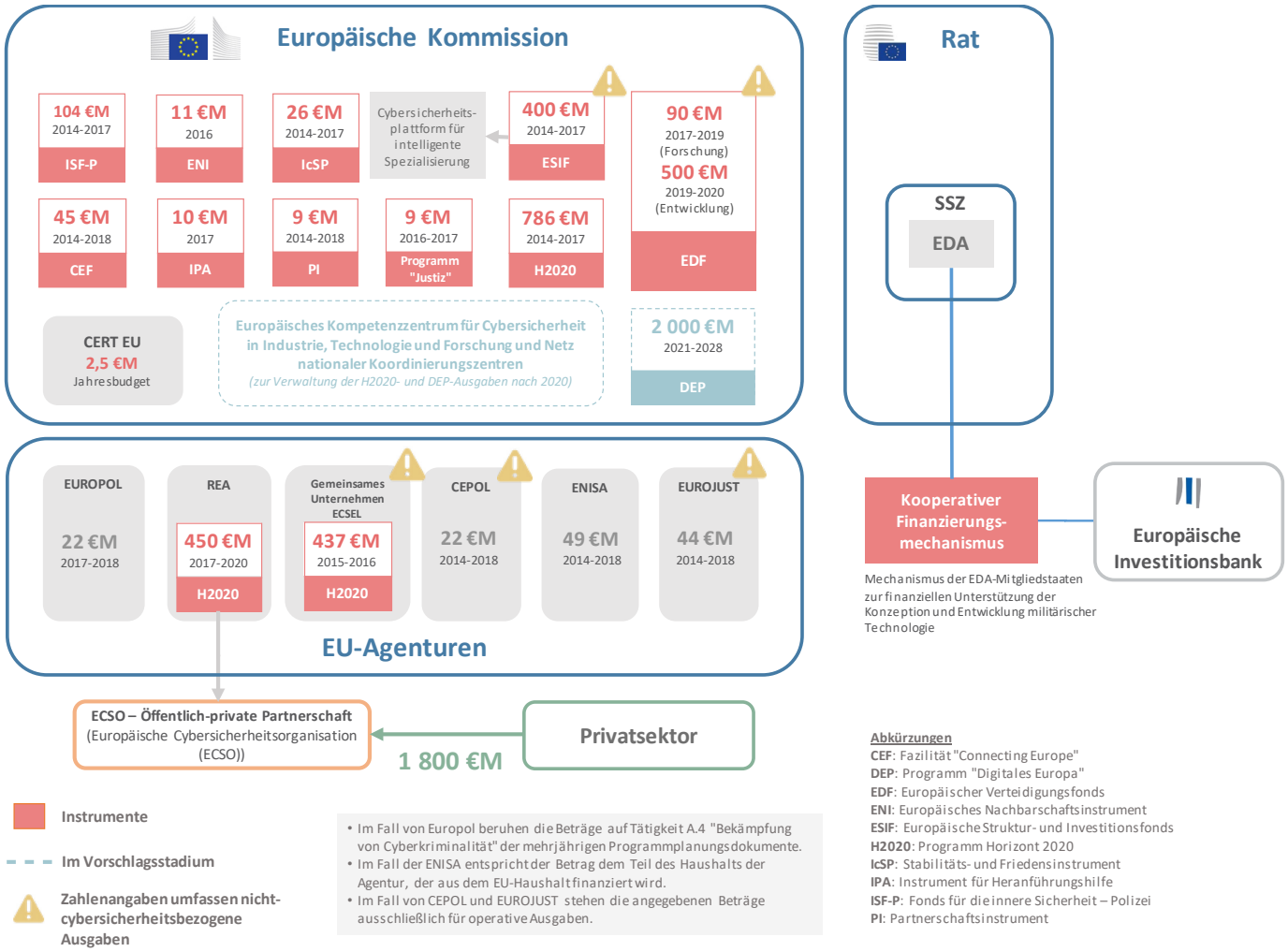
Klaus-Heiner Lehne
Präsident

Anhang I — Ein komplexes, vielschichtiges Umfeld mit vielen Akteuren



Quelle: Europäischer Rechnungshof.

Anhang II — EU-Ausgaben für Cybersicherheit seit 2014



Quelle: Europäischer Rechnungshof auf der Grundlage von Unterlagen der Europäischen Kommission und von EU-Agenturen.

Anhang III — Berichte der Rechnungskontrollbehörden der EU-Mitgliedstaaten

Art	Titel (mit Hyperlink)	Jahr	Mitgliedstaat
Compliance-Prüfungen	*Note d'évaluation du contrôle interne* (Bewertungsvermerk der internen Kontrolle)	2014	FR
	Bescheinigungsbericht über die Rechnung des allgemeinen Sozialversicherungssystems (Verteidigungsministerium, Außenministerium)	2016	FR
	Certification des comptes de l'Etat (Bescheinigung der Rechnungen des Staates)	2016	FR
	Ensuring the security and preservation of Estonian national databases of critical importance (Gewährleistung der Sicherheit und Funktionsfähigkeit der estnischen nationalen Datenbanken, die von entscheidender Bedeutung sind)	Fin. 2018/noch nicht veröffentlicht	EE
	Effectiveness of internal controls in the protection of personal data in national databases (Wirksamkeit interner Kontrollen beim Schutz personenbezogener Daten in nationalen Datenbanken)	2008	EE
Wirtschaftlichkeitsprüfungen	*Report on mitigation of cyber attacks* (Bericht über die Eindämmung von Cyberangriffen)	2013	DK
	RiR 2014:23 *Information security in the civil public administration* (Informationssicherheit in der zivilen öffentlichen Verwaltung)	2014	SE
	Report on the government's processing of confidential data on persons and companies (Bericht über die Verarbeitung vertraulicher personen- oder unternehmensbezogener Daten durch die Regierung)	2014	DK
	The National Cyber Security Programme (Das nationale Cybersicherheitsprogramm)	2014	UK
	Bericht an den Haushaltsausschuss des Deutschen Bundestages nach § 88 Abs. 2 BHO - IT-Konsolidierung Bund	2015	DE
	Report on the access to IT systems that support the provision of essential services to the Danish society (Bericht über den Zugang zu IT-Systemen, die die Erbringung wesentlicher Dienste für die dänische Gesellschaft unterstützen)	2015	DK
	Plaine de France – Öffentliche Planungsbehörde	2015	FR
	Cybersecurity Environment in Lithuania (Cybersicherheitsumfeld in Litauen) Auf Litauisch Zusammenfassung in englischer Übersetzung	2015	LT
	Public bodies" performance of cyber-security tasks in Poland (Wahrnehmung von Cybersicherheitsaufgaben durch öffentliche Stellen in Polen; auf Polnisch)	2015	PL

Art	Titel (mit Hyperlink)	Jahr	Mitgliedstaat
	RiR 2015:21 *Cybercrime – police and prosecutors can be more efficient* (Cyberkriminalität – Polizei und Staatsanwaltschaft könnten effizienter sein)	2015	SE
	Digital Skills Gap in Government (Survey) (Fehlende digitale Kompetenzen bei staatlichen Stellen (Umfrage))	2015	UK
	Rapport de la Cour des comptes transmis à la Chambre des représentants (Bericht an das belgische Parlament): *Perception des droits de succession par le SPF Finances* (Staatsfinanzen: Erhebung der Erbschaftssteuer)	2016	BE
	Report on management of IT security in systems outsourced to external suppliers (Bericht über die Handhabung der IT-Sicherheit bei extern verwalteten Systemen)	2016	DK
	Audit report *of the loan activity of the Official Credit Institute 2016* (Prüfungsbericht über die Darlehenstätigkeit des Instituto de Crédito Oficial 2016)	2016	ES
	Steering of the Government Security Network (Steuerung des von der Regierung verwendeten Sicherheitsnetzwerks)	2016	FI
	Ensuring the security of IT systems used for public tasks (Gewährleistung der Sicherheit von IT-Systemen, die zur Erfüllung öffentlicher Aufgaben eingesetzt werden)	2016	PL
	Prevention and combat of cyber-bullying among children and young people (Verhütung und Bekämpfung von Cybermobbing bei Kindern und Jugendlichen)	2016	PL
	Information security work at nine agencies (Gestaltung der Informationssicherheit in neun Agenturen) – Eine weitere Prüfung der Informationssicherheit beim Staat. RIR 2016:8	2016	SE
	Protecting Information across government (Datenschutz auf allen Regierungsebenen)	2016	UK
	Report on the protection of IT systems and health data in three Danish regions (Bericht über den Schutz von IT-Systemen und Gesundheitsdaten in drei dänischen Regionen)	2017	DK
	Note on the results of the international parallel audit "Effectiveness of internal controls in the protection of personal data in national databases" (Vermerk zu den Ergebnissen der internationalen parallelen Prüfung zum Thema "Wirksamkeit interner Kontrollen beim Schutz personenbezogener Daten in nationalen Datenbanken")	2017	EE
	Cyber protection arrangements (Regelungen zum Schutz vor Cyberangriffen)	2017	FI

Art	Titel (mit Hyperlink)	Jahr	Mitgliedstaat
	Steering of the operational reliability of electronic services (Steuerung der operativen Zuverlässigkeit elektronischer Dienste)	2017	FI
	Les chambres d'agriculture (Synthese) (Die Landwirtschaftskammern)	2017	FR
	La Chambre de Commerce et d'Industrie de Vaucluse (Industrie- und Handelskammer Vaucluse; Prüfungsdurchführung: Regionale Prüfungskammer Provence-Alpes-Côte d'Azur)	2017	FR
	Ensuring the security and preservation of Estonian national databases of critical importance (Gewährleistung der Sicherheit und Funktionsfähigkeit der estnischen nationalen Datenbanken, die von entscheidender Bedeutung sind)	Fin. 2018/noch nicht veröffentlicht	EE
	State Electronic Communications Infrastructure Development (Entwicklung der elektronischen Kommunikationsinfrastrukturen auf staatlicher Ebene) Auf Litauisch Zusammenfassung in englischer Übersetzung	2017	LT
	Information Technology Audit: Cyber Security across Government Entities (Prüfung der Informationstechnologie: Cybersicherheit in allen Regierungsstellen)	2017	MT
	The national registries system: security, performance and usability (Das nationale Registrierungssystem: Sicherheit, Leistung und Benutzerfreundlichkeit)	2017	PL
	The WannaCry incident (Der *Wannacry*-Vorfall)	2017	UK
	Online Fraud (Online-Betrug)	2017	UK
	Report on protection against ransomware attacks (Bericht über den Schutz vor Ransomware-Angriffen)	2018	DK
	Centre hospitalier d'Arpajon (Krankenhaus Arpajon; Prüfungsdurchführung: regionale Prüfungskammer Île-de-France)	2018	FR
	Management of Critical State Information Resources (Verwaltung wichtiger staatlicher Informationsquellen)	2018	LT
	Electronic Crimes (Computerkriminalität)	2019	LT
	Information security in Poland (Informationssicherheit in Polen)	2019	PL
Sonstige	Datenbank öffentlicher Stellen	-	BE
	Umfrage zur Strategie in Sachen Sicherheit und Risikoanalyse (im Gange)	-	BE

Akronyme und Abkürzungen

CERT -EU: *Computer Emergency Response Team* (IT-Notfallteam)

cPPP: *contractual Public-Private Partnership* (vertragliche öffentlich-private Partnerschaft)

CSIRT: *Computer Security Incident Response Team* (Computer-Notfallteam)

DDoS: *Distributed Denial of Service*

DEP: Programm "Digitales Europa"

DSGVO: Datenschutz-Grundverordnung

EAD: Europäischer Auswärtiger Dienst

EC3: *Europol's European Cybercrime Centre* (Europäisches Zentrum zur Bekämpfung der Cyberkriminalität von Europol)

ECSEL *Electronic Components and Systems for European Leadership* (Elektronikkomponenten und -systeme für eine Führungsrolle Europas)

ECSM: *European Cyber Security Month* (Europäischer Monat der Cybersicherheit)

ECSO: *European Cyber Security Organisation* (Europäische Cybersicherheitsorganisation)

EDA: Europäische Verteidigungsagentur

ENISA: Europäische Agentur für Netz- und Informationssicherheit

ESI-Fonds: Europäische Struktur- und Investitionsfonds

EU: Europäische Union

EuRH: Europäischer Rechnungshof

FDI: *Foreign Direct Investment* (Ausländische Direktinvestitionen)

GD CNECT: Generaldirektion Kommunikationsnetze, Inhalte und Technologien

GD DIGIT: Generaldirektion Informatik

GD HOME: Generaldirektion Migration und Inneres

GD JUST: Generaldirektion Justiz und Verbraucher

GSVP: Gemeinsame Sicherheits- und Verteidigungspolitik

HWPCI: *Horizontal Working Party on Cyber Issues* (Horizontale Gruppe "Fragen des Cyberraums")

ISF-P: *Internal Security Fund – Police* (Fonds für die innere Sicherheit – Polizei)

ISSB: *Information System Security Steering Board* (Lenkungsausschuss für Informationssicherheit)

JRC: *Joint Research Centre* (Gemeinsame Forschungsstelle)

KMU: Kleine und mittlere Unternehmen

LISO: *Local Information Security Officer* (Beauftragter für die lokale IT-Sicherheit)

NCIRC: *NATO's Computer Incident Response Capability*

NIS-Richtlinie: Richtlinie über Netz- und Informationssicherheit

NKB: Nationale Rechnungskontrollbehörde

SSZ: Ständige Strukturierte Zusammenarbeit

GLOSSAR

Adware: Schadsoftware, die Werbebanner oder Pop-ups anzeigt, die Codes enthalten, mit denen das Online-Verhalten des Opfers aufgezeichnet werden kann.

Altsystem: Computersystem, Anwendung oder Programmiersprache, die veraltet oder überholt, aber noch in Gebrauch sind, für die der Anbieter jedoch möglicherweise keine Upgrades oder keine Unterstützung (auch keine Sicherheitsunterstützung) mehr anbietet.

Botnet: Netz von mit Schadsoftware infizierten Computern, die – ohne Wissen der Nutzer – aus der Ferne gesteuert werden, um Spam-Mails zu versenden, Informationen abzugreifen oder koordinierte Cyberangriffe auszuführen.

Cloud Computing: Bedarfsbezogene Bereitstellung von IT-Ressourcen – wie Speicherplatz, Rechnerleistung oder Kapazitäten für die gemeinsame Datennutzung – über das Internet durch Speicherung auf standortfernen Servern.

Crime-as-a-service (Caas)-Modell (Verbrechen als Dienstleistung): Kriminelles Geschäftsmodell hinter der digitalen Schattenwirtschaft, das eine Vielzahl von kommerziellen Diensten und Tools bereitstellt, mit denen auch nicht versierten Cyberkriminellen der Einstieg in die Cyberkriminalität gelingt.

Cyberabwehr: Teilbereich der Cybersicherheit mit dem Ziel, den Cyberraum mit militärischen und anderen geeigneten Mitteln zu verteidigen, um militärstrategische Ziele zu erreichen.

Cyberangriff: Versuch, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder eines Computersystems zu untergraben oder zu zerstören.

Cyberkriminalität: Unterschiedliche kriminelle Aktivitäten, bei denen Computer und IT-Systeme entweder Hauptinstrument oder Hauptziel sind. Diese Aktivitäten umfassen herkömmliche Straftaten (z. B. Betrug, Fälschung und Identitätsdiebstahl), inhaltsbezogene Straftaten (z. B. Verbreitung von kinderpornografischem Material im Internet, Anstachelung zum Rassismus) und Straftaten, die nur über Computer und Informationssysteme möglich sind (z. B. Angriffe auf Informationssysteme, Überlastungsangriffe und Schadprogramme).

Cyberökosystem: Ein komplexes System aus interagierenden Geräten, Daten, Netzen, Menschen, Prozessen und Organisationen sowie das Prozess- und Technologieumfeld, das diese Interaktion beeinflusst und unterstützt.

Cyberraum: Das virtuelle globale Umfeld, in dem Menschen mithilfe von Computernetzen und technischen Geräten über Software mit Diensten online kommunizieren.

Cyber-Resilienz: Die Fähigkeit, Cyberangriffe und Vorfälle zu verhindern, sich darauf vorzubereiten, ihnen standzuhalten und sich davon zu erholen.

Cybersicherheit: Alle Vorkehrungen und Maßnahmen zum Schutz von IT-Systemen und ihren Daten vor unbefugten Zugriffen, vor Angriffen und vor Schaden, um ihre Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten.

Cybervorfall: Ereignis, das die Resilienz und Sicherheit eines IT-Systems und der mit diesem System verarbeiteten, gespeicherten oder übermittelten Daten direkt oder indirekt schädigt oder bedroht.

Desinformation: Nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können.

Digitale Inhalte: Alle in einem digitalen Format gespeicherten Daten (zum Beispiel Text-, Ton-, Bild- oder Videomaterial).

Distributed Denial of Service (DDoS): Cyberangriff, der die rechtmäßigen Nutzer am Zugang zu Online-Diensten oder -Ressourcen hindert, indem diese mit Anfragen überlastet werden.

Durch den Cyberraum ermöglichte Straftaten: Herkömmliche Straftat, die durch Nutzung von IT-Systemen in größerem Ausmaß begangen wird.

Exploit-Kit: Von Cyberkriminellen verwendete Form von Werkzeug zur Ausspähung von Schwachstellen in Netz- und Informationssystemen, über die Schadprogramme installiert oder andere böswillige Handlungen begangen werden können.

Hacktivist: Einzelpersonen oder Personengruppen, die sich unbefugten Zugang zu Informationssystemen und -netzen verschaffen, um soziale oder politische Ziele voranzubringen.

Hybride Bedrohung: Bekundung feindlicher Absichten durch Gegner, die eine Mischung aus konventioneller und nicht konventioneller Kriegsführung (d. h. militärische, politische, wirtschaftliche und technologische Mittel) einsetzen, um ihre Ziele gewaltsam durchzusetzen.

Informationssicherheit: Reihe von Prozessen und Instrumenten zum Schutz von physischen und digitalen Daten vor Zugriff, Verwendung, Preisgabe, Störung, Änderung, Erfassung oder Zerstörung durch Unbefugte.

Integrität: Schutz vor unzulässiger Änderung oder Zerstörung von Informationen und Gewährleistung ihrer Authentizität.

Internet der Dinge: Netz alltäglicher Gegenstände, die mit Elektronik, Software und Sensoren ausgestattet sind, und so über das Internet kommunizieren und Daten austauschen können.

Kritische Infrastruktur: Physische Ressourcen, Dienste und Anlagen, deren Störung oder Zerstörung gravierende Auswirkungen auf das Funktionieren von Wirtschaft und Gesellschaft hätte.

Kryptowährung: Digitaler Vermögenswert, der – unabhängig von Zentralbanken – mithilfe von Verschlüsselungstechniken ausgegeben und getauscht wird. Kryptowährungen werden von den Mitgliedern der virtuellen Gemeinschaft als Zahlungsmittel anerkannt.

Malware: Schadsoftware. Computerprogramm, das Computer, Server oder Netze beschädigen soll.

Mit dem Cyberraum zusammenhängende Straftaten: Straftaten, die nur mithilfe von IT-Geräten begangen werden können.

Netzsicherheit: Teilbereich der Cybersicherheit, der den Schutz von Daten betrifft, die über Geräte im gleichen Netz verschickt werden, damit diese Daten nicht abgegriffen oder geändert werden können.

Patching: Einspielung einer Reihe von Änderungen an einer Software bzw. Update, Reparatur oder Verbesserung einer Software, einschließlich der Beseitigung von Sicherheitslücken.

Personenbezogene Daten: Informationen über eine bestimmbare natürliche Person.

Phishing: Senden von E-Mails aus einer scheinbar vertrauenswürdigen Quelle, um die Empfänger dazu zu verleiten, auf schädliche Links zu klicken oder personenbezogene Daten preiszugeben.

Ransomware: Schadsoftware, die den Opfern den Zugriff auf ein Computersystem verwehrt oder Dateien – in der Regel durch Verschlüsselung – unlesbar macht. Die Angreifer erpressen in der Regel anschließend das Opfer, indem sie sich weigern, den Zugang vor Zahlung eines Lösegeldes wieder freizugeben.

Schwachstellenmanagement: Integraler Bestandteil der Computer- und Netzsicherheit, der dazu dient, die Nutzung von System- und Softwareschwachstellen proaktiv einzudämmen oder zu verhindern, indem sie ermittelt, klassifiziert und beseitigt werden.

Skimming: Diebstahl von Kredit- oder Bankkartendaten bei Eingabe im Internet.

Social Engineering: Im Bereich der Informationssicherheit die psychologische Manipulation von Menschen, um sie zur Durchführung einer Aktion oder Preisgabe vertraulicher Informationen zu verleiten.

Textvektorisierung: Die Umwandlung von Wörtern, Sätzen oder ganzen Dokumenten in numerische Vektoren, damit sie von Algorithmen für das maschinelle Lernen genutzt werden können.

Verfügbarkeit: Gewährleistung, dass der Zugriff auf und die Nutzung von Informationen zeitnah und zuverlässig möglich ist.

Verschlüsselung: Umwandlung von Klartext in codierten Text, um ihn zu schützen. Um den Text lesen zu können, muss der Nutzer einen geheimen Schlüssel oder ein Passwort haben.

Vertrauensdienste: Dienste zur Erhöhung der Rechtswirksamkeit eines elektronischen Vorgangs, wie elektronische Signaturen, Siegel, Zeitstempel, Zustellung elektronischer Einschreiben und Website-Authentifizierung.

Vertraulichkeit: Schutz von Informationen, Daten oder Vermögenswerten vor unbefugtem Zugriff oder vor Preisgabe.

Wahlinfrastruktur: Dazu gehören für Wahlkampagnen eingesetzte IT-Systeme und Datenbanken, vertrauliche Informationen über Kandidaten sowie Systeme zur Wählerregistrierung und -verwaltung.

Wiper-Malware: Ziel dieser Art von Schadsoftware ist es, die Festplatte des infizierten Computers zu löschen.

Zugangsdaten: Informationen über die Login- und Logout-Aktivitäten eines Nutzers beim Zugang zu einem Dienst, wie Uhrzeit, Datum und IP-Adresse.

[1] Gemäß dem Entwurf des Rechtsakts zur Cybersicherheit umfasst sie "alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, deren Nutzer und betroffene Personen vor Cyberbedrohungen zu schützen". Der Rechtsakt wird vom Europäischen Parlament und vom Rat voraussichtlich Anfang 2019 angenommen.

[2] Europol, *Internet Organised Crime Threat Assessment 2017*.

[3] Europäische Cybersicherheitsorganisation (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, Juni 2016.

[4] Europäisches Parlament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, Studie im Auftrag des LIBE-Ausschusses des Europäischen Parlaments, September 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18. Januar 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018*.

[7] Europol, *ebd.*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper No 2/18, Februar 2018.

[9] Europäische Kommission, Rede des Präsidenten zur Lage der Union 2017.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, Pressemitteilung, 25. April 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017*.

[12] Factsheet der Europäischen Kommission zur Cybersicherheit, September 2017.

[13] Zu den potenziellen Kosten gehören entgangene Einnahmen, Kosten für die Wiederherstellung beschädigter Systeme, potenzielle Haftung für gestohlene Vermögenswerte oder Informationen, Anreize für die Kundenbindung, höhere Versicherungsprämien, höhere Kosten für Schutzmaßnahmen (neue Systeme, Angestellte, Schulungen), potenzielle Begleichung von Compliance-Kosten oder Gerichtskosten.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] Die Ransomware *Wannacry* nutzte Schwachstellen in einem Microsoft Windows Protokoll, die es möglich machten, Computer aus der Ferne zu übernehmen. Nachdem Microsoft die Sicherheitslücke erkannt hatte, stellte es einen Patch bereit. Hundertausende Computer waren jedoch noch nicht aktualisiert worden, und viele davon wurden später infiziert. Quelle: A. Greenberg, *Hold North Korea Accountable For Wannacry – and the NSA, too*, WIRED, 19. Dezember 2017.

[16] Europäische Kommission, *Europeans' attitudes towards cybersecurity*, Spezial-Eurobarometer-Umfrage 464a, September 2017. Eine Folgeumfrage wird voraussichtlich Anfang 2019 veröffentlicht.

[17] Das Übereinkommen von Budapest ist ein verbindliches internationales Grundsatzdokument für Länder, die Rechtsvorschriften zur Ahndung von Cyberkriminalität ausarbeiten. Es bietet einen Rahmen für die internationale Zusammenarbeit zwischen Vertragsstaaten. Die EU ist derzeit durch die Kommission, den Rat der Europäischen Union, Europol, ENISA und Eurojust vertreten.

[18] Europäische Kommission, *Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum*, JOIN(2013) 1 final vom 7. Februar 2013.

[19] Europäische Kommission, *Die Europäische Sicherheitsagenda*, COM(2015) 185 final vom 28. April 2015.

[20] Europäische Kommission, *Strategie für einen digitalen Binnenmarkt für Europa*, COM(2015) 192 final vom 6. Mai 2015.

[21] EAD, *Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union*, Juni 2016.

[22] Centre for European Policy Studies, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, November 2018.

[23] Die Schadsoftware hinter dem *WannaCry*-Angriff, der laut den Vereinigten Staaten, dem Vereinigten Königreich und Australien von Nordkorea ausgegangen sein soll, wurde ursprünglich von der US-amerikanischen *National Security Agency* entwickelt und geheim gehalten, um Schwachstellen in Windows zu nutzen. Quelle: A. Greenberg, ebd., WIRED, 19. Dezember 2017. Nach den Angriffen verurteilte Microsoft die Geheimhaltung von Software-Schwachstellen durch Regierungen und forderte erneut eine Digitale Genfer Konvention.

[24] Zusätzlich zu Land, See, Luft und Weltraum.

[25] EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018), 14413/18 vom 19. November 2018.

[26] Europäische Kommission/Europäischer Auswärtiger Dienst, *Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union*, JOIN(2016) 18 final vom 6. April 2016.

[27] Gemeinsame Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des Generalsekretärs der Nordatlantikvertrags-Organisation (NATO) vom 8. Juli 2016 und 10. Juli 2018.

[28] Europäische Kommission/Europäischer Auswärtiger Dienst, *Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen*, JOIN(2017) 450 final vom 13. September 2017.

[29] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

[30] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[31] Diese Teams sind Teil der in der Richtlinie vorgesehenen Kooperationsstrukturen, nämlich des CSIRTs-Netzwerks (eines aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU bestehenden Netzwerks, dessen Sekretariatsgeschäfte von der ENISA geführt werden) und der Kooperationsgruppe (zur Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustauschs zwischen den Mitgliedstaaten, deren Sekretariatsgeschäfte von der Kommission geführt werden).

[32] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[33] Europäische Kommission, *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit")*, COM(2017) 477 final vom 13. September 2017.

[34] Europäische Kommission, *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen*, COM(2018) 225 final vom 17. April 2018.

[35] Europäische Kommission, *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren*, COM(2018) 226 final vom 17. April 2018.

[36] Europäische Kommission, *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren*, COM(2018) 630 final vom 12. September 2018.

[37] H. Carrapico und A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, Vol. 55, No. 6, 2017.

[38] Europäische Kommission, ebd., SWD (2017) 295 final vom 13. September 2017.

[39] Wissenschaftlicher Dienst des Europäischen Parlaments, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, Dezember 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27. November 2014.

[41] Eine Ausnahme bildet Artikel 14 ("Kontrolle und Statistiken") der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates.

[42] Europäischer Wirtschafts- und Sozialausschuss, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, März 2018. CEPS-ECRI Task Force, Cybersecurity in Finance: Getting the policy mix right!, Juni 2018.

[43] 24 von 28 nationalen Rechnungskontrollbehörden antworteten auf die Umfrage des Hofes.

[44] Das heißt so grundsatzorientiert und technologieneutral wie möglich.

[45] Mechanismus für wissenschaftliche Beratung der Europäischen Kommission, Scientific Opinion 2/2017 vom 24. März 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, September 2018. European Centre for Political Economy, ebd., Occasional Paper No 2/18, Februar 2018.

[47] Europäische Kommission, *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte*, COM(2015) 634 final vom 9. Dezember 2015.

[48] Europäische Kommission, *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte des Online-Warenhandels und anderer Formen des Fernabsatzes von Waren*, COM(2015) 635 final vom 9. Dezember 2015.

[49] Niederländischer Rat für Cybersicherheit, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, Juni 2018.

[51] Europäische Kommission, *Bestmögliche Netz- und Informationssicherheit – hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*, COM(2017) 476 final/2 vom 4. Oktober 2017.

[52] Europol, ebd., 2017.

[53] Rat der Europäischen Union, *Abschlussbericht über die siebte Runde der gegenseitigen Begutachtung "Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität"*, 12711/1/17 REV 1 vom 9. Oktober 2017.

[54] Europäische Kommission, *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment*, SWD(2017) 298 final vom 13. September 2017. Im Dezember 2018 wurde eine politische Einigung über die neuen Rechtsvorschriften erzielt, mit deren Verabschiedung Anfang 2019 gerechnet wird.

[55] Europol, ebd., 2017.

[56] C-362/14: Maximillian Schrems gegen Data Protection Commissioner (Irland), 6. Oktober 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13. März 2017.

[58] Europäische Kommission, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 final vom 13. September 2017.

[59] Wissenschaftlicher Dienst des Europäischen Parlaments, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, PE589.832.

[60] Entschließung des Europäischen Parlaments, *Menschenrechte und Technologie: die Auswirkungen von Systemen zur Ausspähung und Überwachung auf die Menschenrechte in Drittstaaten*, (2014/2232(INI)) vom 8. September 2015. Güter und Dienste mit doppeltem Verwendungszweck, wozu Software und Technologie gehören, können zivil und militärisch genutzt werden.

[61] Die öffentlich zugänglichen Informationen werden in der von ICANN (Zentralstelle für die Vergabe von Internet-Namen und -Adressen) verwalteten Datenbank WHOIS gespeichert. ICANN betreut das Domänennamensystem. Die missbräuchliche Verwendung von Domänennamen erleichtert die Cyberkriminalität.

[62] Artikel 3 der NIS-Richtlinie, ebd.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10. September 2015.

[64] The White House, *Cybersecurity spending fiscal year 2019*.

[65] Europäische Kommission, *Commission Staff Working Document: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'*, SWD(2018) 305 final vom 6. Juni 2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, Dezember 2016.

[67] Europäische Kommission, ebd., COM(2018) 630 final vom 12. September 2018.

[68] Referat Wissenschaftliche Vorausschau des Wissenschaftlichen Dienstes des Europäischen Parlaments, *Achieving a sovereign and trustworthy ICT industry in the EU*, Dezember 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31. Juli 2017.

[70] Referat Wissenschaftliche Vorausschau des Wissenschaftlichen Dienstes des Europäischen Parlaments, ebd., Dezember 2017.

[71] Ebd.

[72] Europäische Kommission, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (Teil 1/4) vom 12. September 2018.

[73] Europäische Kommission, ebd., COM(2018) 630 final vom 12. September 2018.

[74] Sonderbericht Nr. 13/2018 des Hofes: "Bekämpfung von Radikalisierung als Wegbereiterin von Terrorismus".

[75] Die in diesem Abschnitt genannten Zahlen sind öffentlich zugänglichen Unterlagen der Kommission entnommen. Ausgenommen hiervon ist der in Ziffer ***51*** aufgeführte Betrag von 42 Millionen Euro, den die Kommission dem Hof direkt genannt hat.

[76] Horizont 2020 ist das mit 80 Milliarden Euro ausgestattete EU-Programm für Forschung und Innovation, das die Innovationsunion unterstützt und darauf abzielt, die internationale Wettbewerbsfähigkeit der EU sicherzustellen.

[77] Horizont 2020 – Gesellschaftliche Herausforderung 7 "Sichere Gesellschaften – Schutz der Freiheit und Sicherheit Europas und seiner Bürger".

[78] Der Hof analysierte im CORDIS-Datensatz geführte Horizont-2020-Projekte. Er vektorisierte jede Projektbeschreibung mithilfe der Cybersicherheits-Systematik der Gemeinsamen Forschungsstelle (siehe ***Kasten 5*** im nächsten Kapitel), um Projekte mit wahrscheinlichem Bezug zur Cybersicherheit zu ermitteln. Darauf folgte eine manuelle Kontrolle und Analyse der Ergebnisse.

[79] Europäische Cybersicherheitsorganisation, *ECS cPPP Progress Monitoring Report 2016-2017*, 29. Oktober 2018.

[80] Artikel 9 Absatz 2 der NIS-Richtlinie, ebd.

[81] GLACY+ (Global Action on Cybercrime+) ist ein Gemeinschaftsprojekt mit dem Europarat. Es unterstützt 12 Länder in Afrika, im asiatisch-pazifischen Raum, in Lateinamerika sowie im karibischen Raum, die wiederum als Zentren für die Weitergabe ihrer Erfahrungen in den jeweiligen Regionen fungieren könnten.

[82] Das European Political Strategy Centre (EPSC), der Thinktank der Kommission, hat auf das Risiko hingewiesen, dass ein "digitaler blinder Fleck" entstehen könnte, wenn sich die Kluft zwischen der EU und ihren Nachbarn auf dem Westbalkan weiter verbreitert. Länder wie China und Russland investieren erhebliche Summen in die Region, wodurch die EU Gefahr läuft, in diesen Ländern als Akteur im Cyberbereich verdrängt zu werden. Quelle: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17. Mai 2018.

[83] Europäische Investitionsbank, *Operativer Rahmen und Operativer Gesamtplan 2018 der EIB-Gruppe* vom 12. Dezember 2017. Weitere Informationen waren zum Zeitpunkt der Ausarbeitung des vorliegenden Themenpapiers nicht verfügbar.

[84] Europäische Kommission, *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Aufstellung des Programms "Digitales Europa" für den Zeitraum 2021-2027*, COM(2018) 434 final vom 6. Juni 2018.

[85] Europäische Kommission, *Verordnung (EU) 2018/1092 des Europäischen Parlaments und des Rates vom 18. Juli 2018 zur Einrichtung des Europäischen Programms zur industriellen Entwicklung im Verteidigungsbereich zwecks Förderung der Wettbewerbsfähigkeit und der Innovation in der Verteidigungsindustrie der Union*, ABl. L 200 vom 7.8.2018, S. 30. Außerdem wurde 2017 eine vorbereitende Maßnahme im Bereich Verteidigungsforschung auf den Weg gebracht, die für den Zeitraum 2017-2019 mit insgesamt 90 Millionen Euro (aus Mitteln des Programms Horizont 2020) ausgestattet ist. Ob dies auch Ausgaben für den Cyberbereich umfasst, ist nicht klar.

[86] Der Hof plant für 2019 die Veröffentlichung eines gesonderten Themenpapiers zur EU-Verteidigung.

[87] Für das EC3 von Europol, die ENISA, den EAD, die Europäische Verteidigungsagentur und das CERT-EU sind insgesamt 159 Mitarbeiter tätig. Nicht in dieser Zahl enthalten sind die für Cyberfragen zuständigen Mitarbeiter der Europäischen Kommission oder der Mitgliedstaaten. Quelle: Centre for European Policy Studies, ebd., November 2018.

[88] *ENISA evaluation*, 2017.

[89] Europol beantragte im Mehrjahresplan 2018-2020 eine jährliche Personalaufstockung um 70 Bedienstete auf Zeit, für 2018 wurden aber nur 26 Stellen bewilligt. Im Entwurf des Mehrjahresplans 2019-2021 nahm Europol in der Annahme, dass einem umfangreicheren Antrag nicht entsprochen würde, nur eine geringe Aufstockung vor. Quelle: Konsultation zum Entwurf der mehrjährigen Programmplanung 2019-2021, die dem Gemeinsamen parlamentarischen Kontrollausschuss vorgelegt wurde, A 000834, 1. Februar 2018.

[90] *ENISA evaluation*, 2017. Im Zeitraum 2014-2016 wendete die ENSIA rund 80 % ihrer operativen Mittel für die Vergabe von Studien auf.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, Dezember 2017.

[92] ISACA (früher "Information Systems Audit and Control Association"), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2. Ausgabe, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, S. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, Juli 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21. Februar 2018.

[96] Ein Forum für Zusammenarbeit zwischen der Europäischen Bankenaufsichtsbehörde, der Europäischen Wertpapier- und Marktaufsichtsbehörde und der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung.

[97] Europäische Wertpapier- und Marktaufsichtsbehörde, *Joint Committee report on risks and vulnerabilities in the EU financial system*, April 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, Dezember 2015.

[99] Mit Blick auf die EU-Mitgliedstaaten merkte der Mechanismus für wissenschaftliche Beratung der Kommission an, dass hinsichtlich der Grundsätze und -werte eine grundlegende unwidersprochene Übereinstimmung herrsche und ein gemeinsames strategisches Interesse bestehe, die den Kern einer wirksamen Cybersicherheits-Governance der EU bilden könnten. Quelle: Scientific Opinion 2/2017, 24. März 2017.

[100] Vereinigte Staaten, China, Japan, Südkorea, Indien und Brasilien.

[101] Europäisches Sicherheits- und Verteidigungskolleg (T. Renard und A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23. November 2018.

[102] Rat der Europäischen Union, *Aktionsplan zur Umsetzung der Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen*, 15748/17 vom 12. Dezember 2017.

[103] Europäische Kommission, *Digitalstrategie der Europäischen Kommission: Eine digital gewandelte, nutzerorientierte und datengesteuerte Kommission*, C(2018) 7118 final vom 21. November 2018.

[104] Antwort von Kommissionsmitglied Gabriel auf eine schriftliche parlamentarische Anfrage (E-004294-17) vom 28. Juni 2017.

[105] Rat der Europäischen Union, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, 15870/17 vom 19. Dezember 2017.

[106] In den Beschlüssen (EU, Euratom) 2015/443, 2015/444 und 2017/46 wird die Sicherheit der Kommunikations- und Informationssysteme der Kommission geregelt. Mit Beschluss C(2018) 7706 der Kommission vom 21. November 2018 wird ein Informationstechnik- und Cybersicherheitsbeirat eingerichtet, in dem der frühere IT-Beirat und der Lenkungsausschuss für Informationssicherheit zusammengeführt werden.

[107] Europäischer Wirtschafts- und Sozialausschuss, ebd., März 2018.

[108] Europäisches Parlament, ebd., September 2015.

[109] Die Analyseeinheit für hybride Bedrohungen wurde 2016 geschaffen und ist Teil des EU-Zentrums für Informationsgewinnung und -analyse beim EAD. Sie erhält von verschiedenen Interessenträgern aus vertraulichen und frei zugänglichen Quellen Informationen über hybride Bedrohungen.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, November 2013.

[111] Europäische Kommission, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final (Teil 1/6) vom 13. September 2017.

[112] Europäische Kommission, ebd., SWD(2018) 403 final vom 12. September 2018.

[113] Das *Résaux IP Européens Network Coordination Centre* ist die regionale Internet-Registrierungsstelle für Europa und als solche zuständig für die Vergabe und Registrierung von IP-Adressen.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, November 2012 .

[115] The Centre for Cyber Safety and Education, in Zusammenarbeit mit Booz Allen Hamilton, Alta Associates and Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Europäischer Wirtschafts- und Sozialausschuss, ebd., März 2018.

[117] House of Lords, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017-19*, 16. Juli 2018.

[118] Europol/Eurojust, *Common challenges in combatting cybercrime*, 7021/17, 13. März 2017.

[119] Europol/Eurojust, ebd., 7021/17, 13. März 2017.

[120] Europäische Kommission, ebd., SWD(2018) 403 final vom 12. September 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, 20. November 2018.

[122] Etwa die Zusammenarbeit zwischen dem EAD, den Mitgliedstaaten, Agenturen und Einrichtungen wie CEPOL, ECTEG oder ESVK.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, Dezember 2017.

[124] Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität.

[125] Europäische Kommission, Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Dreizehnter Fortschrittsbericht, COM(2018) 46 final vom 24. Januar 2018.

[126] Auf der Grundlage der Bemerkungen in Sonderbericht Nr. 14/2018, ebd.

[127] Entschließung des Europäischen Parlaments vom 13. Juni 2018 zur Cyberabwehr (2018/2004(INI)). Rat der Europäischen Union, ebd., 15870/17 vom 19. Dezember 2017.

[128] Schweiz, Nordmazedonien, Ukraine, Bosnien und Herzegowina, Kosovo (diese Bezeichnung berührt nicht die Standpunkte zum Status und steht im Einklang mit der Resolution 1244/1999 des UN-Sicherheitsrates und dem Gutachten des Internationalen Gerichtshofs zur Unabhängigkeitserklärung des Kosovo), Türkei und Vereinigte Staaten.

[129] Europol, *Internet Organised Crime Threat Assessment 2018*.

[130] Europäische Kommission, ebd., SWD (2017) 295 final vom 13. September 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman und S. Furman, *Security Fatigue*, "IT Professional", Vol. 18, No. 5, 2016, S. 26-32. Siehe auch NIST.

[132] Europäische Kommission/Europäischer Auswärtiger Dienst, *Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen*, JOIN(2018) 16 final vom 13. Juni 2018.

[133] Beispielsweise die Abschaltung von AlphaBay und Hansa in einer gemeinsamen Operation, die vom FBI und der niederländischen Polizei geleitet und von Europol unterstützt wurde. Bei AlphaBay und Hansa handelte es sich um zwei der größten Märkte für den Handel mit illegalen Waren wie Drogen, Feuerwaffen und Tools der Cyberkriminalität wie Malware. Quelle: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, Pressemitteilung, 29. Mai 2018.

[134] Rat der Europäischen Union, ebd., 12711/1/17 REV 1 vom 9. Oktober 2017.

[135] Europäische Kommission, ebd., SWD(2018) 403 final vom 12. September 2018.

[136] Europäische Kommission, ebd., SWD (2017) 295 final vom 13. September 2017.

[137] Europäische Kommission/Europäischer Auswärtiger Dienst, ebd., JOIN(2018) 16 final vom 13. Juni 2018.

[138] Europäische Kommission, SWD (2017) 500 final vom 13. September 2017.

[139] *Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU*, 23. Mai 2018.

[140] Europäisch Kommission, Ausschreibung: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap* vom 27. Oktober 2017.

[141] Jean-Claude Juncker, Mission letter for the Commissioner for the Security Union vom 2. August 2016. Verteidigung fällt nicht in den Zuständigkeitsbereich der Taskforce.

[142] Rat der Europäischen Union, *EU cybersecurity roadmap*, 8901/17 vom 11. Mai 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues*, 5th ed., November 2017.

[144] Technische Berichte der JRC, European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy*. Impact assessment on the proposed research competence centre and network of national coordination centres, SWD(2018) 403 final vom 12. September 2018.

[145] Europäische Kommission, ebd., SWD (2017) 295 final vom 13. September 2017.

[146] Europäische Kommission, ebd., SWD(2018) 403 final vom 12. September 2018.

[147] Dem Europäischen Informations- und Analysezentrum für Finanzinstitute beispielsweise gehören Vertreter aus dem Finanzsektor, nationalen IT-Notfallteams, Strafverfolgungsbehörden, der ENISA, Europol, der Europäischen Zentralbank, dem Europäischen Zahlungsverkehrsausschuss und der Europäischen Kommission an.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14. Februar 2018.

[149] Rat der Europäischen Union, ebd., 12711/1/17 REV 1 vom 9. Oktober 2017.

[150] https://www.europol.europa.eu/empact.

[151] Eine von Accenture 2018 in 15 Ländern durchgeführte Studie ergab, dass 87 % der gezielten Cyberangriffe abgewehrt wurden: *2018 State of Cyber Resilience*, 10. April 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Oxford University Politics Blog, 14. September 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14. Juli 2017.

[154] Europäischer Wirtschafts- und Sozialausschuss, *ebd.*, März 2018.

[155] Europäische Kommission, *Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Achter Fortschrittsbericht*, COM(2017) 354 final vom 29. Juni 2017.

[156] Siehe die verschiedenen Veröffentlichungen der NIS-Kooperationsgruppe.

[157] PSD2: Zweite Zahlungsdiensterichtlinie; EZB/SSM: Europäische Zentralbank/Einheitlicher Aufsichtsmechanismus; Target 2: Transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem (zweite Generation), Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Quelle: CEPS-ECRI Task Force, ebd., Juni 2018.

[158] Europäische Kommission, *Empfehlung der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen*, C(2017) 6100 final vom 13. September 2017.

[159] Europäische Kommission, ebd., SWD (2017) 295 final vom 13. September 2017. Es gibt mehrere Krisenmanagementmechanismen, u. a. die integrierte Regelung für die politische Reaktion auf Krisen, Argus (den Krisenreaktionsmechanismus der Kommission), den Krisenreaktionsmechanismus des EAD, das Katastrophenschutzverfahren der Union und das EU-Notfallprotokoll für die Strafverfolgungsbehörden.

[160] Dies kann außerdem Artikel 42 Absatz 7 des Vertrags über die Europäische Union (Beistandsklausel) oder Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union (Solidaritätsklausel) auslösen.

[161] Europäische Kommission/Europäischer Auswärtiger Dienst, ebd., JOIN(2018) 16 final vom 13. Juni 2018. Im Dezember 2018 berichteten die Medien, das diplomatische Kommunikationsnetz des EAD (COREU) sei gehackt worden (Quelle: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*, 18. Dezember 2018). Diese Angelegenheit wird derzeit untersucht.

[162] Auch die Zusammenarbeit bei Frühwarnungen und gegenseitiger Unterstützung muss weiter ausgebaut werden: *Schlussfolgerungen des Rates zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen*, 10086/18 vom 26. Juni 2018.

[163] Wissenschaftlicher Dienst des Europäischen Parlaments, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, September 2018.

[164] Europäischer Wirtschafts- und Sozialausschuss, ebd., März 2018.

[165] Rat der Europäischen Union, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18, Dezember 2018.

[166] Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit; Plattform für den Austausch von Informationen über die Reaktion auf Cyberbedrohungen und -vorfälle. Quelle: Rat der Europäischen Union, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19. November 2018.

[167] Rat der Europäischen Union, Schlussfolgerungen des Rates über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten, 9916/17 vom 7. Juni 2017.

[168] Rat der Europäischen Union, *Schlussfolgerungen des Rates zur Cyberdiplomatie*, 6122/15 vom 11. Februar 2015.

[169] Rat der Europäischen Union, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[170] Die Zuordnung der Verantwortlichkeit für einen Vorfall bleibt eine souveräne politische Entscheidung der Mitgliedstaaten, und nicht alle im Rahmen der Toolbox vorgesehenen Maßnahmen erfordern eine solche Zuordnung.

[171] Die Toolbox führte nicht zu einem gemeinsamen Vorgehen; einzelne Mitgliedstaaten schlossen sich dem Standpunkt der USA an.

[172] Rat der Europäischen Union, *Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten*, 7925/18 vom 16. April 2018.

[173] Computersysteme, die von verschiedenen Branchen, u. a. der Versorgungs- und Chemieindustrie, der industriellen Fertigung, der Lebensmittelverarbeitung, von Verkehrssystemen und -knotenpunkten sowie Logistikdiensten zur Prozesssteuerung verwendet werden.

[174] ENISA, ebd., Dezember 2017.

[175] Etwa die öffentliche Verwaltung, die Chemie- und die Atomindustrie, Fertigung, Lebensmittelverarbeitung, Fremdenverkehr, Logistik und Zivilschutz.

[176] Europäische Kommission, ebd., SWD (2017) 295 final vom 13. September 2017.

[177] Rede von Kommissarin Jourová auf der Plenartagung des Europäischen Parlaments zum Thema *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign*, 14. November 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23. Mai 2018.

[179] Europäisches Zentrum für politische Strategie (L. Past), Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses, in: "Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] Gemäß der Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

[181] Europäische Kommission, Empfehlung zu Wahlkooperationsnetzen, zu Online-Transparenz, zum Schutz vor Cybersicherheitsvorfällen und zur Bekämpfung von Desinformationskampagnen im Zusammenhang mit Wahlen zum Europäischen Parlament, C(2018) 5949 final vom 12. September 2018.

[182] Schlussfolgerungen des Europäischen Rates, EUCO 11/15 vom 20. März 2015. Seitdem sind zwei Taskforces hinzugekommen, und zwar die Taskforce "Westlicher Balkan" und die Taskforce "Südliche Nachbarschaft".

[183] In einem Bericht forderte der Atlantikrat die EU auf, alle Mitgliedstaaten zur Entsendung nationaler Experten in die Taskforce zu verpflichten. Siehe: D. Fried und A. Polyakova, *Democratic Defense Against Disinformation*, 5. März 2018.

[184] Die Taskforce war ursprünglich nicht mit eigenen Haushaltsmitteln ausgestattet. Im Jahr 2018 bewilligte das Europäische Parlament 1,1 Millionen Euro für die Vorbereitende Maßnahme "StratCom Plus".

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ebd., 23. Mai 2018.

[186] Europäische Kommission, Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, *Aktionsplan gegen Desinformation*, JOIN(2018) 36 final. Der Plan hat folgende Schwerpunkte: Ausbau der Fähigkeiten der EU-Organe, Desinformation zu erkennen, zu untersuchen und zu enthüllen; mehr koordinierte und gemeinsame Maßnahmen; Mobilisierung des Privatsektors; Sensibilisierung der Gesellschaft und Ausbau ihrer Widerstandsfähigkeit.

[187] Europäische Kommission, *Bekämpfung von Desinformation im Internet: ein europäisches Konzept*, COM(2018) 236 final vom 26. April 2018.

[188] Nicht zu verwechseln mit dem Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, April 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")*, April 2018.

[191] European Political and Strategy Centre (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, in: ebd., 2018.

[192] Europäische Kommission, ebd., SWD(2018) 403 final vom 12. September 2018.

[193] Der Verordnungsvorschlag (COM(2017) 487 final vom 13. September 2017) für die Überprüfung ausländischer Direktinvestitionen durchläuft derzeit das Legislativverfahren. Er bezieht sich konkret auf kritische Technologien, einschließlich künstliche Intelligenz, Cybersicherheit und Anwendungen mit doppeltem Verwendungszweck.

[194] Europäische Kommission/Europäischer Auswärtiger Dienst, ebd., JOIN(2017) 450 final vom 13. September 2017.

Team des Hofes

Dieses Themenpapier *Herausforderungen für eine wirksame Cybersicherheitspolitik der EU* wurde von Kammer III "Externe Politikbereiche, Sicherheit und Justiz" unter Vorsitz von Bettina Jakobsen, Mitglied des Hofes, angenommen. Die Ausarbeitung stand unter der Leitung von Baudilio Tomé Muguruza, Mitglied des Hofes. Herr Muguruza wurde unterstützt von seinem Kabinettchef Daniel Costa de Magalhaes und Kabinettattaché Ignacio Garcia de Parada, dem Leitenden Manager Alejandro Ballester-Gallardo, dem Aufgabenleiter Michiel Sweerts sowie von Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha, Prüferinnen und Prüfer und dem Praktikanten Johannes Bolkart. Hannah Critoph leistete sprachliche Unterstützung.

Von links nach rechts: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EUROPÄISCHER RECHNUNGSHOF

Amt für Veröffentlichungen

EUROPÄISCHER RECHNUNGSHOF
12, rue Alcide De Gasperi
1615 Luxemburg
LUXEMBURG

Tel. (+352) 4398-1

Kontaktformular: eca.europa.eu/de/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors