RAT DER EUROPÄISCHEN UNION

Brüssel, den 8. Februar 2013 (11.02)
(OR. en)

6225/13

POLGEN 17
JAI 87
TELECOM 20
PROCIV 20
CSC 10
CIS 4
RELEX 115
JAIEX 14
RECH 36
COMPET 83
IND 35
COTER 17
ENFOPOL 34
DROIPEN 13
CYBER 1

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	7. Februar 2013
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	JOIN(2013) 1 final
Betr.:	Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum

Die Delegationen erhalten in der Anlage das Kommissionsdokument JOIN(2013) 1 final.

Anl.: JOIN(2013) 1 final

EUROPÄISCHE
KOMMISSION

HOHE VERTRETERIN DER
EUROPÄISCHEN UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 7.2.2013
JOIN(2013) 1 final

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Cybersicherheitsstrategie der Europäischen Union –

ein offener, sicherer und geschützter Cyberraum

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Cybersicherheitsstrategie der Europäischen Union –

ein offener, sicherer und geschützter Cyberraum

1. EINLEITUNG

1.1. Hintergrund

Der Einfluss des Internets und generell des Cyberraums auf alle Teile der Gesellschaft war in den letzten zwanzig Jahren enorm. Unser Alltag, die Gewährleistung unserer Grundrechte, das gesellschaftliche Leben und die Wirtschaft sind davon abhängig, dass die Informations- und Kommunikationstechnologien nahtlos funktionieren. Der offene und freie Cyberraum hat überall in der Welt zur politischen und sozialen Integration beigetragen, Schranken zwischen Ländern, Gemeinschaften und Bürgern beseitigt und so die Interaktion und den Austausch von Informationen und Ideen weltweit ermöglicht. Er war ein Forum für die Ausübung der Meinungsfreiheit und anderer Grundrechte und hat die Menschen in ihrem Streben nach einer demokratischen und gerechteren Gesellschaft entscheidend unterstützt – am sichtbarsten war dies während des „arabischen Frühlings".

Damit der Cyberraum auch in Zukunft durch Offenheit und Freiheit geprägt bleibt, sollten „online" dieselben Normen, Grundsätze und Werte gelten, für die die EU auch „offline" eintritt. Grundrechte, Demokratie und Rechtsstaatlichkeit müssen auch im Cyberraum geschützt werden. Unsere Freiheit und unser Wohlstand beruhen in immer stärkeren Maße auf einem robusten und innovativen Internet, das auch weiterhin florieren wird, wenn durch Innovationen des Privatsektors und die Zivilgesellschaft eine entsprechende Wachstumsdynamik geschaffen wird. Voraussetzung für die Freiheit im Online-Umfeld sind jedoch auch die technische Sicherheit und die Gefahrenabwehr. Der Cyberraum sollte vor Sicherheitsvorfällen, böswilligen Aktivitäten und Missbrauch geschützt werden. Die Regierungen haben bei der Gewährleistung eines freien und sicheren Cyberraums eine wichtige Rolle zu spielen. Sie müssen seine Zugänglichkeit und Offenheit sicherstellen, die Grundrechte online respektieren und schützen und die Zuverlässigkeit und Interoperabilität des Internets aufrechterhalten. Große Teile des Cyberraums befinden sich jedoch im Besitz von Privatunternehmen und werden von diesen betrieben, daher müssen diesbezügliche Initiativen, wenn sie erfolgreich sein sollen, die führende Rolle des Privatsektors anerkennen.

Die Informations- und Kommunikationstechnologien bilden inzwischen die Basis unseres Wirtschaftswachstums und stellen eine kritische Ressource dar, auf die sich sämtliche Wirtschaftssektoren stützen. Sie sind die Grundlage für die komplexen Systeme, von denen zentrale Sektoren unserer Volkswirtschaften wie Finanzen, Gesundheit, Energie und Verkehr abhängig sind. Viele Geschäftsmodelle gehen im Übrigen von der ununterbrochenen Verfügbarkeit des Internets und einem reibungslosen Funktionieren der Informationssysteme aus.

Durch die Vollendung des digitalen Binnenmarktes könnte Europa sein BIP um fast 500 Mrd. EUR jährlich steigern[1], d. h. um durchschnittlich 1000 EUR für jeden Bürger. Damit die damit verbundenen Technologien wie elektronische Zahlungen, Cloud-Computing oder die Maschine-Maschine-Kommunikation[2] sich durchsetzen können, muss bei den Bürgern das entsprechende Vertrauen vorhanden sein. Leider hat eine Eurobarometer-Umfrage 2012[3] ergeben, dass fast ein Drittel der Europäer dem Internet bei der Erledigung von Bankoperationen oder Käufen nicht trauen. Eine überwältigende Mehrheit gab ferner an, aus Sicherheitsgründen online keine persönlichen Daten preiszugeben. In der EU war bereits mehr als jeder zehnte Internetnutzer Opfer von Online-Betrug.

In den vergangenen Jahren wurden zum einen die enormen Vorteile der Digitalisierung, zum anderen aber auch die Anfälligkeit des digitalen Umfelds deutlich. Vorsätzlich ausgelöste oder unbeabsichtigte Sicherheitsvorfälle im Cyberraum[4] nehmen mit alarmierender Geschwindigkeit zu; sie könnten die Bereitstellung grundlegender, für die Bürger selbstverständlicher Dienste (Wasserversorgung, Gesundheitsfürsorge, Strom, Mobilfunk) stören. Die Bedrohungen können auf unterschiedliche Ursachen zurückzuführen sein: Sie können kriminell oder politisch motiviert sein, oder es kann sich um terroristische oder staatlich unterstützte Anschläge, Naturkatastrophen oder unbeabsichtigte Fehler handeln.

Die EU-Wirtschaft hat bereits heute unter der Cyberkriminalität[5] gegen Privatunternehmen und Privatpersonen zu leiden. Cyberstraftäter setzen immer raffiniertere Methoden ein, um sich in Informationssysteme einzuschleusen, wichtige Daten zu entwenden oder Unternehmen zu erpressen. Die Zunahme der Wirtschaftsspionage und staatlich unterstützter Aktivitäten im Cyberraum führt zu einer neuen Art der Bedrohung für staatliche Stellen und für Unternehmen in der EU.

In Ländern außerhalb der EU kann es auch vorkommen, dass Regierungen den Cyberraum zur Überwachung und Kontrolle ihrer Bürger missbrauchen. Die EU kann solchem Missbrauch entgegenwirken, indem sie die Freiheit des Internets unterstützt und die Wahrung der Grundrechte im Internet gewährleistet.

Aus all diesen Gründen haben Regierungen weltweit begonnen, Cybersicherheitsstrategien zu entwickeln und den Cyberraum als international immer wichtigeres Thema zu behandeln. Es ist an der Zeit, dass die EU ihre Maßnahmen in diesem Bereich verstärkt. Dieser Vorschlag

---

1 http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

2 z. B. wenn Pflanzen mit Sensoren ausgestattet sind, die dem Berieselungssystem mitteilen, wann sie bewässert werden müssen.

3 „Special Eurobarometer“ 390 zur Cybersicherheit (2012).

4 Der Begriff „Cybersicherheit“ bezeichnet im Allgemeinen die Sicherheitsfunktionen und Maßnahmen, die sowohl im zivilen als auch im militärischen Bereich zum Schutz des Cyberraums vor Bedrohungen eingesetzt werden können, die im Zusammenhang mit seinen voneinander abhängigen Netzen und Informationsstrukturen stehen oder diese beeinträchtigen können. Bei der Cybersicherheit geht es darum, die Verfügbarkeit und Integrität von Netzen und Infrastrukturen sowie die Vertraulichkeit der darin enthaltenen Informationen zu erhalten.

5 Unter dem Begriff „Cyberkriminalität“ werden unterschiedlichste kriminelle Tätigkeiten zusammengefasst, bei denen Computer und Informationssysteme entweder Hauptinstrument oder Hauptziel sind. Die Cyberkriminalität umfasst herkömmliche Straftaten (z. B. Betrug, Fälschung, Identitätsdiebstahl), inhaltsbezogene Straftaten (z. B. Verbreitung von kinderpornografischem Material über das Internet, Anstachelung zum Rassismus) und Straftaten, die nur über Computer und Informationssysteme möglich sind (z. B. Angriffe auf Informationssysteme, Überlastungsangriffe, Schadprogramme).

für eine Cybersicherheitsstrategie der Europäischen Union wird von der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik („Hohe Vertreterin“) gemeinsam vorgelegt. Er enthält die einschlägigen Zukunftsvorstellungen der EU, klärt Aufgaben und Zuständigkeiten und beschreibt die erforderlichen Maßnahmen. Grundlage ist hierbei der umfassende und wirksame Schutz der Rechte der Bürger und deren umfassende und wirksame Förderung, um so das Online-Umfeld in der EU zum weltweit sichersten zu machen.

1.2. Grundlagen der Cybersicherheit

Das grenzübergreifende und vielschichtige Internet wurde zu einer der wirkungsvollsten Triebkräfte für den globalen Fortschritt, die ohne staatliche Aufsicht oder Regulierung auskommen. Der Privatsektor sollte zwar weiterhin beim Ausbau und der routinemäßigen Verwaltung des Internets eine führende Rolle spielen, es wird jedoch immer deutlicher, dass Vorgaben in Bezug auf Transparenz, Verantwortlichkeiten und Sicherheit notwendig sind. In dieser Strategie werden die Grundsätze erläutert, auf die sich die Cybersicherheitspolitik in der EU und auf internationaler Ebene stützt.

Die Grundwerte der EU gelten in der digitalen Welt ebenso wie in der realen Welt.

Im Cyberraum gelten dieselben Gesetze und Normen wie in anderen Lebensbereichen.

Schutz der Grundrechte, der Meinungsfreiheit, der personenbezogenen Daten und der Privatsphäre

Die Sicherheit im Cyberraum kann nur zufriedenstellend und wirksam gewährleistet werden, wenn sie auf den in der Charta der Grundrechte der Europäischen Union garantierten Grundrechten und Grundfreiheiten und auf den Grundwerten der EU basiert. Die Rechte des Einzelnen können ihrerseits nur geschützt werden, wenn Netze und Systeme sicher sind. Bei jeder Weitergabe von Informationen im Interesse der Cybersicherheit müssen – soweit es um personenbezogene Daten geht – die EU-Datenschutzvorschriften eingehalten und die Rechte des Einzelnen in diesem Zusammenhang umfassend berücksichtigt werden.

Allgemeine Zugänglichkeit

Ein eingeschränkter Internetzugang oder gar kein Zugang sowie Computer-Analphabetismus sind angesichts der Allgegenwart der digitalen Welt in allen Bereichen des gesellschaftlichen Lebens von Nachteil für den Bürger. Jeder sollte Zugang zum Internet und zu einem uneingeschränkten Informationsangebot haben. Die Integrität und die Sicherheit des Internets müssen im Interesse eines sicheren Zugangs für alle garantiert sein.

Partizipative, demokratische und effiziente Verwaltung

Die digitale Welt wird nicht von einer einzigen Instanz kontrolliert. An der routinemäßigen Verwaltung der Internetressourcen, -protokolle und -standards sowie an der Weiterentwicklung des Internets sind vielmehr zahlreiche Interessenträger beteiligt, von denen viele nicht staatliche Einrichtungen mit kommerziellen Interessen sind. Die EU hebt

erneut die Bedeutung aller Beteiligten des derzeitigen Internetverwaltungsmodells hervor und unterstützt die derzeitige Vorgehensweise, bei der viele Interessenträger einbezogen werden[6].

Gemeinsame Verantwortung im Interesse der Sicherheit

Die zunehmende Abhängigkeit von den Informations- und Kommunikationstechnologien in allen Bereichen des Lebens hat zu Anfälligkeiten geführt, die genau umrissen, eingehend analysiert und behoben bzw. reduziert werden müssen. Alle relevanten Akteure, ob es sich nun um Behörden, den Privatsektor oder einzelne Bürger handelt, müssen diese gemeinsame Verantwortung anerkennen, Maßnahmen zu ihrem eigenen Schutz ergreifen und gegebenenfalls auf koordinierte Weise reagieren, um die Cybersicherheit zu stärken.

2. STRATEGISCHE PRIORITÄTEN UND MAßNAHMEN

Die EU sollte zum Nutzen aller ein möglichst freies und sicheres Online-Umfeld bewahren. Es wird anerkannt, dass die Gefahrenabwehr im Cyberraum vor allem Aufgabe der Mitgliedstaaten ist; dennoch werden in dieser Strategie spezifische Maßnahmen vorgeschlagen, die die Gesamtsicherheit in der EU erhöhen können. Dabei handelt es sich sowohl um kurzfristige als auch um langfristige Maßnahmen, die sich auf unterschiedliche strategische Instrumente[7] und Akteure (EU-Organe, Mitgliedstaaten, Industrie) stützen.

Die im Rahmen der vorliegenden Strategie dargelegten Zielvorstellungen der EU können in fünf strategischen Prioritäten zusammengefasst werden, mit denen die oben beschriebenen Herausforderungen angegangen werden:

- Widerstandsfähigkeit gegenüber Cyberangriffen
- drastische Eindämmung der Cyberkriminalität
- Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik (CSDP)
- Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit
- Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

2.1. Widerstandsfähigkeit gegenüber Cyberangriffen

Zur Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen in der EU müssen Behörden und Privatsektor Kapazitäten aufbauen und wirksam zusammenarbeiten. Auf der Grundlage der positiven Ergebnisse der bisherigen Maßnahmen[8] können weitere EU-Maßnahmen dazu beitragen, insbesondere die grenzübergreifenden Risiken und Bedrohungen im Cyberraum einzudämmen und in Notfällen auf koordinierte Weise zu reagieren. Hierdurch

---

6 Siehe auch KOM(2009) 277: „Mitteilung der Kommission an das Europäische Parlament und den Rat - Verwaltung des Internet: die nächsten Schritte".

7 Bei Maßnahmen mit Informationsaustausch, bei denen auch personenbezogene Daten betroffen sind, sind die EU-Datenschutzvorschriften einzuhalten.

8 Siehe Verweise in dieser Mitteilung sowie in der Folgenabschätzung (Arbeitsunterlage der Kommissionsdienststellen) zu dem Vorschlag der Kommission für eine Richtlinie über die Netz- und Informationssicherheit, insbesondere in den Abschnitten 4.1.4 und 5.2, Anhang 2, Anhang 6 und Anhang 8.

wird die das reibungslose Funktionieren des Binnenmarktes sehr unterstützt und die innere Sicherheit der EU gestärkt.

Europa wird ohne beträchtliche Anstrengungen im öffentlichen und im privaten Bereich zum Ausbau der Kapazitäten, zur Aufstockung der Ressourcen und zur Verbesserung der Prozesse im Hinblick auf die Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen im Cyberraum weiterhin Angriffsflächen bieten. Daher hat die Kommission eine Strategie für die Netz- und Informationssicherheit (NIS) entwickelt[9]. Die **Europäische Agentur für Netz- und Informationssicherheit (ENISA)** wurde 2004 eingerichtet[10]; derzeit erörtern Rat und Parlament eine neue Verordnung zur Stärkung der ENISA und zur Aktualisierung ihres Auftrags[11]. Außerdem ist in der Rahmenrichtlinie für die elektronische Kommunikation[12] vorgeschrieben, dass Anbieter elektronischer Kommunikationsnetze oder -dienste angemessene Maßnahmen zur Beherrschung der Risiken für die Sicherheit ihrer Netze ergreifen und signifikante Sicherheitsverletzungen melden. Gemäß den EU-Datenschutzvorschriften[13] müssen ferner die für die Datenverarbeitung Verantwortlichen dafür sorgen, dass Datenschutzvorschriften eingehalten und Schutzmaßnahmen, einschließlich Sicherheitsmaßnahmen, ergriffen werden; im Bereich öffentlich zugänglicher elektronischer Kommunikationsdienste müssen sie außerdem den zuständigen nationalen Behörden Vorfälle melden, bei denen der Schutz personenbezogener Daten verletzt wurde.

Trotz einiger Fortschritte aufgrund freiwilliger Verpflichtungen bestehen in der EU noch Mängel, insbesondere in Bezug auf die nationalen Kapazitäten, die Koordinierung bei grenzübergreifenden Sicherheitsvorfällen und die Einbeziehung und Abwehrbereitschaft des Privatsektors. Gleichzeitig mit dieser Strategie wird ein Vorschlag für einen **Rechtsakt** vorgelegt, der folgende Ziele verfolgt:

- die Festlegung gemeinsamer Mindestanforderungen für die NIS auf nationaler Ebene, aufgrund deren die Mitgliedstaaten verpflichtet wären, für die NIS zuständige nationale Behörden zu benennen, ein gut funktionierendes CERT (IT-Notfallteam/Computer Emergency Response Team) einzurichten sowie eine nationale NIS-Strategie und einen nationalen NIS-Kooperationsplan aufzustellen. Der Kapazitätsaufbau und die Koordinierung betrifft auch die EU-Organe: 2012 wurde ein ständiges IT-Notfallteam („CERT-EU“) eingerichtet, das für die Sicherheit der IT-Systeme der Organe, Einrichtungen und sonstigen Stellen der EU zuständig ist;
- die Einrichtung koordinierter Mechanismen für Prävention, Erkennung, Folgenminderung und Reaktion, um Informationsaustausch und Amtshilfe zwischen den für die NIS zuständigen nationalen Behörden zu ermöglichen. Die nationalen NIS-Behörden werden aufgefordert, eine angemessene EU-weite Zusammenarbeit zu gewährleisten, insbesondere auf der Grundlage eines NIS-Kooperationsplans, der für den Umgang mit grenzübergreifenden Cybervorfällen konzipiert ist. Diese Zusammenarbeit wird sich auch

---

9 2001 verabschiedete die Kommission eine Mitteilung „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“ (KOM(2001) 298) und 2006 eine Strategie für eine sichere Informationsgesellschaft (KOM(2006) 251). Seit 2009 hat die Kommission ferner einen Aktionsplan und eine Mitteilung über den Schutz kritischer Informationsinfrastrukturen (CIIP) angenommen (KOM(2009) 149, bestätigt durch die Entschließung des Rates 2009/C 321/01, sowie die Mitteilung KOM(2011) 163, bestätigt durch die Schlussfolgerungen des Rates 10299/11.

10 Verordnung (EG) Nr. 460/2004.

11 KOM(2010) 521. Die in dieser Strategie vorgeschlagenen Maßnahmen beinhalten keine Änderung des bestehenden oder künftigen Auftrags der ENISA.

12 Artikel 13 Buchstaben a und b der Richtlinie 2002/21/EG.

13 Artikel 17 der Richtlinie 95/46/EG, Artikel 4 der Richtlinie 2002/58/EG.

auf die Fortschritte im Rahmen des Europäischen Forums der Mitgliedstaaten (EFMS)[14] stützen, in dem produktive Diskussionen und ein nützlicher Austausch zur staatlichen NIS-Politik stattgefunden haben und das in die Kooperationsmechanismen integriert werden kann, sobald diese existieren;

- Verbesserung der Abwehrbereitschaft und der Beteiligung des Privatsektors. Da der überwiegende Teil der Netz- und Informationssysteme im Besitz von Privatunternehmen ist und von diesen betrieben wird, ist eine stärkere Einbeziehung des Privatsektors bei der Förderung der Cybersicherheit von höchster Bedeutung. Der Privatsektor sollte selbst technische Kapazitäten zur Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen entwickeln und sektorübergreifend bewährte Praktiken austauschen. Die von der Industrie für die Reaktion auf Sicherheitsvorfälle, die Ermittlung der Ursachen und die Durchführung cyberforensischer Untersuchungen entwickelten Instrumente sollten vom öffentlichen Sektor genutzt werden können.

Für die Akteure der Privatwirtschaft gibt es immer noch keine wirksamen Anreize, zuverlässige Daten über Auftreten oder Auswirkungen von NIS-Vorfällen zu liefern, eine Risikomanagementkultur zu schaffen oder in Sicherheitsmaßnahmen zu investieren. Mit dem vorgeschlagenen Rechtsakt soll daher sichergestellt werden, dass die Akteure in einigen wichtigen Bereichen (Energie, Verkehr, Banken, Börsen, Betreiber von Infrastruktur für zentrale Internetdienste, öffentliche Verwaltungen) ihre Risiken im Bereich der Cybersicherheit einschätzen, durch ein angemessenes Risikomanagement dafür sorgen, dass Netze und Informationssysteme zuverlässig und robust sind, und die ermittelten Informationen den nationalen NIS-Behörden mitteilen. Die Einführung einer Cybersicherheitskultur könnte die Geschäftsmöglichkeiten des Privatsektors erweitern und die Wettbewerbsfähigkeit erhöhen; die Cybersicherheit könnte so zu einem Verkaufsargument werden.

Die Akteure würden den nationalen NIS-Behörden alle Vorfälle melden, die sich beträchtlich auf die Kontinuität der wichtigsten Dienste und Warenlieferungen auswirken, die von Netz- und Informationssystemen abhängig sind.

Die für die NIS zuständigen Behörden sollten zusammenarbeiten und Informationen mit anderen Regulierungsstellen, insbesondere mit den für Datenschutz zuständigen Behörden, austauschen. Die NIS-Behörden sollten ihrerseits die Strafverfolgungsbehörden über die Sicherheitsvorfälle informieren, bei denen ein schwerwiegender krimineller Hintergrund vermutet wird. Die nationalen NIS-Behörden sollten ferner auf einer eigenen Website regelmäßig nicht geheime Informationen über aktuelle Warnungen in Bezug auf Sicherheitsvorfälle und Risiken sowie über die koordinierte Reaktion darauf veröffentlichen. Rechtliche Verpflichtungen sollten den Aufbau einer informellen freiwilligen Zusammenarbeit nicht ersetzen oder gar verhindern, die der Erhöhung der Sicherheit und dem Austausch von Informationen und empfehlenswerten Verfahren dient. Dies gilt auch für die Zusammenarbeit zwischen öffentlichem und privatem Sektor. Vor allem die Europäische öffentlich-private Partnerschaft für Robustheit (European Public-Private Partnership for

[14] Das Europäische Forum der Mitgliedstaaten wurde mit der Mitteilung KOM(2009) 149 für den Austausch zwischen den Behörden der Mitgliedstaaten über bewährte politische Praktiken in Bezug auf die Sicherheit und Robustheit kritischer Informationsinfrastrukturen eingerichtet.

Resilience/EP3R)[15] ist eine solide und sinnvolle Plattform auf EU-Ebene und sollte weiter ausgebaut werden.

Mit der Fazilität „Connecting Europe“ (CEF)[16] sollen wichtige Infrastrukturen finanziell unterstützt werden, die die NIS-Kapazitäten der Mitgliedstaaten miteinander verbinden und so die EU-weite Zusammenarbeit erleichtern.

Schließlich sind EU-weite Übungen für Cybervorfälle unbedingt erforderlich, um die Zusammenarbeit zwischen den Mitgliedstaaten und zwischen Mitgliedstaaten und Privatsektor zu simulieren. Die erste derartige Übung unter Beteiligung der Mitgliedstaaten wurde 2010 durchgeführt („Cyber Europe 2010“), die zweite, an der auch der Privatsektor teilnahm, im Oktober 2012 („Cyber Europe 2012“). Im November 2011 fand eine Planübung EU/USA statt („Cyber Atlantic 2011“). Weitere Übungen sind für die nächsten Jahre geplant, auch auf internationaler Ebene.

Die Kommission wird

- ihre Arbeiten zur Ermittlung von NIS-Anfälligkeiten europäischer kritischer Infrastrukturen und zur Förderung der Entwicklung robuster Systeme fortsetzen, die von der Gemeinsamen Forschungsstelle in enger Abstimmung mit den Behörden der Mitgliedstaaten sowie mit Eigentümern und Betreibern kritischer Infrastrukturen durchgeführt werden;
- Anfang 2013 ein von der EU kofinanziertes Pilotprojekt[17] zur **Bekämpfung von Botnets und Schadprogrammen** einleiten, das den Rahmen für die Koordinierung und Zusammenarbeit zwischen den EU-Mitgliedstaaten, Privatunternehmen (z. B. Anbietern von Internetdiensten) und internationalen Partnern liefern soll.

Die Kommission beauftragt die ENISA,

- die Mitgliedstaaten bei der Entwicklung leistungsfähiger **nationaler Kapazitäten zur Erhöhung der Widerstandsfähigkeit gegenüber Cyberangriffen** zu entwickeln, insbesondere durch den Aufbau von Kompetenzen im Bereich der Sicherheit und Robustheit industrieller Steuerungssysteme und der Verkehrs- und Energieinfrastrukturen;
- 2013 die Realisierbarkeit von ICS-CSIRT (Computer Security Incident Response Teams for Industrial Control Systems/Notfallteams für die IT-Sicherheit industrieller Steuerungssysteme) in der EU zu prüfen;

[15] Die Europäische öffentlich-private Partnerschaft für Robustheit wurde mit der Mitteilung KOM(2009) 149 ins Leben gerufen. Im Rahmen dieser Plattform wurden Arbeiten eingeleitet und die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor gefördert. Gegenstand sind die Ermittlung wesentlicher Komponenten, Ressourcen und Funktionen sowie grundlegender Anforderungen im Hinblick auf die Robustheit, ferner Kooperationsbedarf und -mechanismen bei Störungen großen Ausmaßes, die sich auf die elektronische Kommunikation auswirken.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF-Haushaltslinie 09 03 02 – Telekommunikationsnetze (Förderung des Zusammenschlusses und der Interoperabilität nationaler öffentlicher Dienstleistungen online sowie des Zugangs zu solchen Netzen).

[17] CIP-ICT PSP-2012-6, 325188. Das Gesamtbudget beläuft sich auf 15 Mio. EUR, der EU-Betrag auf 7,7 Mio. EUR.

- auch in Zukunft die Mitgliedstaaten und die EU-Organe bei der Durchführung regelmäßiger **EU-weiter Übungen für Cybervorfälle** zu unterstützen, die auch die Grundlage für die Beteiligung der EU an entsprechenden internationalen Übungen sein werden.

Die Kommission ersucht das Europäische Parlament und den Rat,

- den Vorschlag für eine Richtlinie über Maßnahmen zur **Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union** zügig zu verabschieden, in der es um die Kapazitäten und die Abwehrbereitschaft auf nationaler Ebene, die Zusammenarbeit auf EU-Ebene, die Einführung von Risikomanagementmethoden und den Informationsaustausch über die NIS geht;

Die Kommission bittet die Industrie,

- eine führende Rolle bei **Investitionen** in eine hohe Cybersicherheit zu übernehmen und in der Branche sowie mit den Behörden empfehlenswerte Vorgehensweisen zu entwickeln und einen Informationsaustausch einzuführen; Ziel ist der umfassende und wirksame Schutz von Vermögenswerten und Personen, insbesondere durch öffentlich-private Partnerschaften wie EP3R und Trust in Digital Life (TDL)[18].

Sensibilisierung

Für die Gewährleistung der Cybersicherheit sind alle gemeinsam verantwortlich. Die Endnutzer spielen bei der Gewährleistung der Sicherheit von Netzen und Informationssystemen eine entscheidende Rolle; ihnen müssen die Risiken, denen sie sich online aussetzen, bewusst gemacht werden, und sie müssen in die Lage versetzt werden, einfache Schutzmaßnahmen selbst zu ergreifen.

Diesbezüglich gab es in den letzten Jahren mehrere Initiativen, die fortgeführt werden sollten. An den Sensibilisierungsmaßnahmen war insbesondere die ENISA beteiligt, die Berichte veröffentlicht, Expertenworkshops organisiert und öffentlich-private Partnerschaften aufgebaut hat. Auch Europol, Eurojust und die nationalen Datenschutzbehörden sind in diesem Bereich aktiv. Im Oktober 2012 organisierte die ENISA gemeinsam mit einigen Mitgliedstaaten zum ersten Mal den „European Cybersecurity Month“ (Monat der Cybersicherheit). Die Sensibilisierung ist einer der Arbeitsbereiche der Arbeitsgruppe EU-USA zur Cybersicherheit und Cyberkriminalität[19]; sie ist ferner ein wichtiger Aspekt des Programms für ein sicheres Internet[20] (Schwerpunkt: Sicherheit der Kinder bei der Internetnutzung).

---

18 http://www.trustindigitallife.eu/

19 Diese Arbeitsgruppe wurde anlässlich des Gipfels EU-USA im November 2010 (MEMO/10/597) eingesetzt und mit der Entwicklung kooperativer Konzepte für zahlreiche Themen des Bereichs Cybersicherheit und Cyberkriminalität beauftragt.

20 Im Rahmen des Programms „Sicheres Internet“ wird ein Netz von NRO finanziert, die im Bereich des Schutzes von Kindern im Online-Umfeld tätig sind, ferner ein Netz von Strafverfolgungsbehörden, die Informationen und empfehlenswerte Praktiken im Zusammenhang mit der kriminellen Nutzung des Internets zur Verbreitung von Material über den sexuellen Missbrauch von Kindern austauschen, und ein Netz von Forschern, die Informationen über Nutzung, Risiken und Folgen der Online-Technologien für das Leben von Kindern sammeln.

Die Kommission beauftragt die ENISA,

- 2013 einen Fahrplan für einen „Netz- und Informationssicherheits-Führerschein“ vorzuschlagen (Programm für eine freiwillige Zertifizierung, zur Förderung von Befähigungen und Kompetenzen der im IT-Bereich Tätigen, z. B. der Verwalter von Websites).

Die Kommission wird

- 2014 mit Unterstützung der ENISA einen Cybersicherheits**wettbewerb** veranstalten, bei dem Hochschulstudenten NIS-Lösungen vorschlagen sollen.

Die Kommission fordert die Mitgliedstaaten auf[21],

- ab 2013 jedes Jahr mit Unterstützung der ENISA und unter Einbeziehung des Privatsektors einen „**Monat der Cybersicherheit**“ zu organisieren, um die Endnutzer für das Thema zu sensibilisieren. Ab 2014 findet in der EU und den USA gleichzeitig ein Monat der Cybersicherheit statt.
- **Verstärkung der Maßnahmen der Mitgliedstaaten im Bereich NIS-Ausbildung und Schulung** durch die Einführung von NIS-Ausbildungsprogrammen in den Schulen bis 2014, von Ausbildungsmaßnahmen zur NIS, zur Entwicklung sicherer Software und zum Schutz personenbezogener Daten für Informatik-Studenten, sowie einer NIS-Grundausbildung für die Mitarbeiter öffentlicher Verwaltungen.

Die Kommission bittet die Industrie,

- **auf allen Ebenen für die Cybersicherheit zu sensibilisieren**, sowohl auf Unternehmensebene als auch im Kontakt mit Kunden. Die Unternehmen sollten insbesondere Möglichkeiten prüfen, wie Geschäftsführer und Leitungsorgane in Bezug auf die Gewährleistung der Cybersicherheit stärker in die Verantwortung genommen werden könnten.

2.2. Drastische Eindämmung der Cyberkriminalität

Je stärker die Digitalisierung unserer Welt voranschreitet, umso mehr Möglichkeiten bieten sich für Cyberkriminelle. Die Cyberkriminalität ist eine der Kriminalitätsformen, deren Bedeutung derzeit am raschesten zunimmt; täglich werden mehr als eine Million Menschen Opfer einer Online-Straftat. Cyberkriminelle werden immer raffinierter und ihre Netze immer komplexer. Wir benötigen geeignete Instrumente und Kapazitäten, um ihnen entgegenzutreten. Die Cyberkriminalität ist sehr profitabel und mit geringen Risiken verbunden, denn die Straftäter nutzen häufig die Anonymität der Internetdomänen. Cyberkriminalität kennt keine Grenzen. Da das Internet die ganze Welt umspannt, muss bei der Strafverfolgung gemeinsam, koordiniert und grenzübergreifend vorgegangen werden, um dieser wachsenden Bedrohung Herr zu werden.

[21] Unter Beteiligung der zuständigen nationalen Behörden (u. a. der NIS- und Datenschutzbehörden).

Durchgreifende und wirksame Rechtsvorschriften

Die EU und ihre Mitgliedstaaten brauchen zur Bekämpfung der Cyberkriminalität durchgreifende und wirksame Rechtsvorschriften. Das Übereinkommen des Europarats über Computerkriminalität (auch: Budapester Übereinkommen) ist ein verbindliches internationales Übereinkommen, das einen wirksamen Rahmen für die Verabschiedung nationaler Rechtsvorschriften bildet.

Die EU hat bereits Vorschriften zur Cyberkriminalität erlassen, u. a die Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie[22]. Sie steht ferner vor der Verabschiedung einer Richtlinie über Angriffe gegen Informationssysteme (insbesondere durch Botnetze).

Die Kommission wird

- die rasche Umsetzung und Anwendung der Richtlinien zur Cyberkriminalität sicherstellen,
- die Mitgliedstaaten, die das **Budapester Übereinkommen des Europarats über Computerkriminalität** noch nicht ratifiziert haben, auffordern, dies zu tun und die Bestimmungen des Übereinkommens so rasch wie möglich umzusetzen.

Verbesserung der operativen Kapazitäten zur Bekämpfung der Cyberkriminalität

Das technologische Arsenal der Cyberkriminellen hat sich rasch weiterentwickelt, und die Strafverfolgungsbehörden können diese Art von Straftaten nicht mit veralteten Werkzeugen bekämpfen. Derzeit verfügen nicht alle Mitgliedstaaten über die erforderlichen operativen Kapazitäten für eine wirksame Bekämpfung der Cyberkriminalität. Alle Mitgliedstaaten müssen über effektive nationale Stellen verfügen, die diese Straftaten bekämpfen.

Die Kommission wird

- über ihre Finanzierungsprogramme[23] die Mitgliedstaaten bei der **Ermittlung von Mängeln und dem Ausbau ihrer Kapazitäten** zur Untersuchung und Bekämpfung der Cyberkriminalität unterstützen, Die Kommission wird außerdem Gremien unterstützen, die Forschungseinrichtungen/Hochschulen, Strafverfolgungsbehörden und Privatsektor zusammenführen, ähnlich den in einigen Mitgliedstaaten bereits existierenden Exzellenzzentren für die Bekämpfung der Cyberkriminalität, die von der Kommission finanziell unterstützt werden;
- ihre Bemühungen um die Ermittlung empfehlenswerter Vorgehensweisen und der besten verfügbaren Technologien zur Bekämpfung der Cyberkriminalität mit den Maßnahmen der Mitgliedstaaten abstimmen, u. a. mit Unterstützung der JRC

[22] Richtlinie 2011/93/EU zur Ersetzung des Rahmenbeschlusses 2004/68/JI.

[23] 2013 im Rahmen des Programms ISEC (Kriminalprävention und Kriminalitätsbekämpfung), nach 2013 im Rahmen des Fonds für innere Sicherheit (neues Instrument des MFF).

(z. B. bei der Entwicklung und Verwendung cyberforensischer Werkzeuge und bei der Analyse von Bedrohungen);

- eng mit dem kürzlich eingerichteten **Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3), Europol und Eurojust** zusammenarbeiten, um die entsprechenden strategischen Konzepte mit den besten Vorgehensweisen im operativen Bereich in Einklang zu bringen.

Bessere Koordinierung auf EU-Ebene

Die EU kann die Arbeiten der Mitgliedstaaten dadurch ergänzen, dass sie die Koordinierung und Zusammenarbeit erleichtert und Strafverfolgungs- und Justizbehörden sowie Beteiligte des öffentlichen und des privaten Sektors innerhalb und außerhalb der EU zusammenbringt.

Die Kommission wird

- das kürzlich eingerichtete **Europäische Zentrum zur Bekämpfung der Cyberkriminalität** (EC3) unterstützen, das als zentrale Anlaufstelle für den europaweit geführten Kampf gegen die Cyberkriminalität dienen soll. Das EC3 wird Analysen und Informationen liefern, Untersuchungen unterstützen, hochwertige forensische Arbeiten ausführen, die Zusammenarbeit erleichtern, Kanäle für den Informationsaustausch zwischen den zuständigen Behörden der Mitgliedstaaten, dem Privatsektor und anderen Akteuren bereitstellen und mit der Zeit als Sprachrohr der Strafverfolgungsbehörden insgesamt fungieren[24].

- im Einklang mit dem Unionsrecht (einschließlich der Datenschutzvorschriften) Bemühungen um die Zuweisung einer größeren Verantwortung an Registrierstellen für Domänennamen und die Korrektheit der Informationen über die Eigentümer von Websites unterstützen, wobei sie sich insbesondere auf die Empfehlungen („Law Enforcement Recommendations“) an die Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) stützt;

- sich auf kürzlich verabschiedete Rechtsvorschriften stützen, um die Bemühungen der EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern im Internet weiter zu verstärken. Die Kommission hat eine Europäische Strategie für ein besseres Internet für Kinder[25] verabschiedet und gemeinsam mit EU-Mitgliedstaaten und Ländern außerhalb der EU ein **Globales Bündnis gegen sexuellen Missbrauch von Kindern im Internet** (Global Alliance against Child Sexual Abuse Online)[26] ins Leben gerufen. Das Bündnis ist ein Forum für weitere von der Kommission und dem EC3 unterstützte Aktionen der Mitgliedstaaten.

[24] Die Europäische Kommission verabschiedete am 28. März 2012 die Mitteilung „Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität“.

[25] KOM(2012) 196 endg.

[26] Schlussfolgerungen des Rates zu einem Globalen Bündnis gegen sexuellen Missbrauch von Kindern im Internet (gemeinsame Erklärung EU-USA) vom 7. und 8. Juni 2012 und Erklärung zur Einrichtung der „Global Alliance against Child Sexual Abuse Online“ (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

Die Kommission fordert Europol (EC3) auf,

- seine operative und analytische Unterstützung der Mitgliedstaaten bei den Untersuchungen im Bereich der Cyberkriminalität zunächst auf die Zerschlagung und Störung cyberkrimineller Netze vor allem in den Bereichen des sexuellen Missbrauchs von Kindern, des Zahlungsbetrugs, der Botnets und des unrechtmäßigen Eindringens zu konzentrieren,
- regelmäßig strategische und operative Berichte über Trends und neue Bedrohungen vorzulegen, so dass Prioritäten aufgestellt und die Untersuchungen der für die Bekämpfung der Cyberkriminalität zuständigen Teams in den Mitgliedstaaten gezielt durchgeführt werden können.

Die Kommission fordert die Europäische Polizeiakademie (CEPOL) auf, in Zusammenarbeit mit Europol

- die Konzipierung und Planung von Schulungen zu koordinieren, damit die Polizei über die erforderlichen Fachkenntnisse und Kompetenzen für eine wirksame Verfolgung von Cyberstraftaten verfügt.

Die Kommission fordert Eurojust auf,

- die wichtigsten Hindernisse bei der justiziellen Zusammenarbeit im Bereich der Cyberkriminalität und bei der Abstimmung der Mitgliedstaaten untereinander und mit Drittländern zu ermitteln sowie die Untersuchung und Verfolgung von Cyberstraftaten sowohl operativ und strategisch als auch durch einschlägige Schulungsmaßnahmen zu unterstützen.

Die Kommission fordert Eurojust und Europol (EC3) auf,

- eng zusammenzuarbeiten, u. a. mittels des Austauschs von Informationen, um so entsprechend ihrem jeweiligen Auftrag und ihrer jeweiligen Zuständigkeit effektiver gegen die Cyberkriminalität vorgehen zu können.

2.3. Entwicklung einer Cyberverteidigungspolitik und Aufbau von Kapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik (CSDP)

Bei den Cybersicherheitsmaßnahmen in der EU wird auch der Aspekt der Cyberverteidigung berücksichtigt. Um die Robustheit der Kommunikations- und Informationssysteme zu erhöhen, die dem Schutz der Verteidigungs- und Sicherheitsinteressen der Mitgliedstaaten dienen, sollte der Schwerpunkt bei der Entwicklung der Cyberverteidigungskapazitäten auf der Erkennung komplexer Cyberbedrohungen, der Reaktion darauf und der Wiederherstellung danach liegen.

Da die Bedrohungen vielfältige Aspekte aufweisen, sind Synergien zwischen dem Vorgehen auf ziviler und auf militärischer Ebene beim Schutz kritischer Cyberanlagen und -daten (cyber assets) verstärkt zu nutzen. Diese Bemühungen sollten durch Forschungs- und

Entwicklungsmaßnahmen sowie durch eine engere Zusammenarbeit zwischen Behörden, Privatsektor und Hochschulen in der EU gestützt werden. Um Doppelarbeit zu vermeiden wird die EU Möglichkeiten prüfen, wie sich die Maßnahmen der EU und der NATO zur Stärkung der Robustheit kritischer staatlicher, verteidigungsrelevanter und sonstiger Informationsinfrastrukturen, von denen beide Organisationen abhängen, gegenseitig ergänzen könnten.

Die Hohe Vertreterin legt den Schwerpunkt auf folgende wichtige Maßnahmen und bittet die Mitgliedstaaten und die Europäische Verteidigungsagentur um ihre Mitarbeit:

- Prüfung der operativen Anforderungen an die Cyberverteidigung der EU und Förderung der Entwicklung von Cyberverteidigungskapazitäten und -technologien auf EU-Ebene, wobei alle Aspekte des Kapazitätsaufbaus zu behandeln sind (u. a. grundlegende Ziele, Leitung, Organisation, Personal, Schulung, Technologie, Infrastruktur, Logistik und Interoperabilität);

- Entwicklung eines EU-Rahmens für die Cyberverteidigungspolitik, um die Netze bei GSVP-Missionen und -Operationen zu schützen, unter Einbeziehung eines dynamischen Risikomanagements, einer besseren Bedrohungsanalyse der Bedrohungen und des Informationsaustauschs; Verbesserung der Möglichkeiten der militärischen Seite (im europäischen und multinationalen Kontext), Cyberverteidigungsschulungen und -übungen zu besuchen bzw. durchzuführen (u. a. durch Einbeziehung von Cyberverteidigungsaspekten bei bestehenden Übungen);

- Förderung des Dialogs und der Koordinierung zwischen zivilen und militärischen Beteiligten in der EU, wobei der Schwerpunkt vor allem auf dem Austausch empfehlenswerter Vorgehensweisen, dem Informationsaustausch, der frühzeitigen Warnung, der Reaktion auf Sicherheitsvorfälle, der Risikobewertung, der Sensibilisierung bzw. der Herstellung der Cybersicherheit insgesamt liegen sollte;

- Pflege des Dialogs mit den Partnern auf internationaler Ebene, u. a. mit der NATO, anderen internationalen Organisationen und multinationalen Exzellenzzentren, um effektive Verteidigungskapazitäten zu gewährleisten, Bereiche einer möglichen Zusammenarbeit zu ermitteln und Doppelarbeit zu vermeiden.

2.4. Entwicklung industrieller und technischer Ressourcen für die Cybersicherheit

Europa verfügt zwar über ausgezeichnete Kapazitäten im Bereich Forschung und Entwicklung, viele der weltweit führenden Unternehmen für innovative IKT-Produkte und -Dienste sind jedoch außerhalb der EU angesiedelt. Es besteht das Risiko, dass Europa zu sehr nicht nur von andernorts produzierter IKT, sondern auch von außerhalb Europas entwickelten Sicherheitslösungen abhängig wird. Es ist unbedingt sicherzustellen, dass in der EU oder in Drittländern produzierte Hardware- und Softwarekomponenten, die für kritische Dienste und Infrastrukturen und verstärkt in mobilen Geräten eingesetzt werden, vertrauenswürdig und sicher sind und den Schutz personenbezogener Daten gewährleisten.

Förderung eines Binnenmarkts für Cybersicherheitsprodukte

Eine hohe Sicherheit kann nur dann gewährleistet werden, wenn für alle Beteiligen der Wertschöpfungskette (Ausrüstungshersteller, Softwareentwickler, Dienstleister der

Informationsgesellschaft usw.) die Sicherheit eine Priorität ist. Offensichtlich[27] betrachten jedoch zahlreiche Akteure die Sicherheit immer noch beinahe als „zusätzliches Ärgernis“; die Nachfrage nach Sicherheitslösungen ist gering. Für die gesamte Wertschöpfungskette der in Europa verwendeten IKT-Produkte müssen geeignete Leistungsanforderungen in Bezug auf die Cybersicherheit gelten. Privatunternehmen benötigen Anreize für die Gewährleistung einer hohen Cybersicherheit. Durch Leistungsangaben in diesem Bereich könnten z. B. Unternehmen mit einer guten einschlägigen Leistung und Bilanz dies als Verkaufsargument und Wettbewerbsvorteil nutzen. Die in dem Vorschlag für die NIS-Richtlinie enthaltenen Verpflichtungen würden einen bedeutenden Beitrag dazu leisten, dass sich die Wettbewerbsfähigkeit der betroffenen Branchen erhöht.

Europaweit sollte auch die Marktnachfrage nach besonders sicheren Produkten angeregt werden. Zum Ersten sollen durch diese Strategie die Zusammenarbeit und Transparenz bezüglich der Sicherheit von IKT-Produkten verbessert werden. Es wird eine Plattform angestrebt, die die einschlägigen europäischen Interessenträger des öffentlichen und des privaten Sektors zusammenführt, damit sie empfehlenswerte Cybersicherheitsverfahren in der gesamten Wertschöpfungskette ermitteln und für die Entwicklung und Einführung sicherer IKT-Lösungen günstige Marktbedingungen schaffen. Sehr wichtig ist, dass Anreize für ein angemessenes Risikomanagement und die Einführung von Sicherheitsnormen und -lösungen geschaffen werden, außerdem könnten gegebenenfalls freiwillige, EU-weite Zertifizierungsregelungen eingeführt werden, die auf in der EU und auf internationaler Ebene existierenden Systemen aufbauen. Die Kommission wird die Einführung mitgliedstaatsübergreifend einheitlicher Konzepte fördern, damit durch etwaige Unterschiede keine Standortnachteile für die Unternehmen entstehen.

Zum Zweiten wird die Kommission die Aufstellung von Sicherheitsnormen unterstützen und einen Beitrag zu EU-weiten freiwilligen Zertifizierungsregelungen im Bereich des Cloud-Computing leisten, wobei der Datenschutz angemessen zu berücksichtigen ist. Die Arbeiten sollten sich auf die Sicherheit der Lieferkette konzentrieren, insbesondere in den kritischen Wirtschaftszweigen (industrielle Steuerungssysteme, Energie- und Verkehrsinfrastruktur). Sie sollten sich auf die laufenden Normungsarbeiten der europäischen Normenorganisationen (CEN, CENELEC und ETSI)[28] und der Koordinierungsgruppe für die Cybersicherheit (CSCG) sowie auf die Fachkenntnis der ENISA, der Kommission und anderer relevanter Akteure stützen.

Die Kommission wird

- 2013 eine öffentlich-private **Plattform für NIS-Lösungen** ins Leben rufen, die Anreize für die Einführung sicherer IKT-Lösungen und die Gewährleistung einer hohen Cybersicherheit entwickeln soll, die bei in Europa verwendeten IKT-Produkten Anwendung finden sollen;
- 2014 auf der Grundlage der Arbeiten dieser Plattform Empfehlungen vorschlagen, mit denen die Cybersicherheit in der gesamten IKT-Wertschöpfungskette sichergestellt werden soll,

[27] Siehe Folgenabschätzung (Arbeitsunterlage der Kommissionsdienststellen) zu dem Vorschlag der Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit, Punkt 4.1.5.2.

[28] Insbesondere im Rahmen der Norm für intelligente Netze M/490 (erste Normen für intelligente Netze, Referenzarchitektur).

- prüfen, auf welche Weise große IKT-Hardware- und Software-Hersteller die zuständigen nationalen Behörden über festgestellte Schwachstellen mit möglicherweise beträchtlichen Auswirkungen auf die Sicherheit informieren könnten.

Die Kommission beauftragt die ENISA,

- in Zusammenarbeit mit den zuständigen nationalen Behörden, den einschlägigen Interessenträgern, internationalen und europäischen Normenorganisationen und der Gemeinsamen Forschungsstelle der Europäischen Kommission **technische Leitlinien und Empfehlungen für die Festlegung von NIS-Normen und empfehlenswerten Verfahren** im öffentlichen und privaten Sektor zu entwickeln.

Die Kommission fordert die Akteure des öffentlichen und des privaten Sektors auf,

- die Entwicklung und Verabschiedung von **Sicherheitsnormen**, technischen Normen und Grundsätzen für eingebaute Schutz- und Sicherheitsfunktionen unter Federführung der Industrie (IKT-Produkthersteller und -Dienstleister, einschließlich Cloud-Anbieter) anzuregen, neue Generationen von Software und Hardware mit **leistungsstärkeren, integrierten und nutzerfreundlichen Sicherheit**sfunktionen auszustatten,
- Normen für die Cybersicherheitsleistung der Unternehmen unter Federführung der Branche zu entwickeln und die Informationen für die Öffentlichkeit durch eine **Sicherheitskennzeichnung** zu verbessern, damit die Verbraucher sich besser auf dem Markt zurechtfinden.

Förderung von FuE-Investitionen und Innovation

Mit Forschung und Entwicklung können wir eine überzeugende Industriepolitik betreiben, die Vertrauenswürdigkeit der europäischen IKT-Branche stärken, den Binnenmarkt fördern und die Abhängigkeit Europas von Technologien aus dem Ausland reduzieren. Forschungs- und Entwicklungsmaßnahmen dürften zur Schließung der technologischen Lücken im Bereich der IKT-Sicherheit beitragen, der Vorbereitung auf die nächste Generation von Herausforderungen im Sicherheitsbereich sowie der Einbeziehung der sich ständig wandelnden Nutzerbedürfnisse dienen und von Dual-use-Technologien profitieren. Mit solchen Maßnahmen sollte auch in Zukunft die Kryptografie weiterentwickelt werden. Ergänzend müssen zur Erleichterung der Umsetzung der FuE-Ergebnisse in kommerzielle Lösungen die erforderlichen Anreize gegeben und geeignete Rahmenbedingungen geschaffen werden.

Die EU sollte das Rahmenprogramm Horizont 2020[29] für Forschung und Innovation, das 2014 anlaufen wird, bestmöglich nutzen. Der Kommissionsvorschlag enthält spezifische Ziele

[29] Horizont 2020 ist das Finanzierungsinstrument, mit dem die Innovationsunion umgesetzt werden soll, eine Leitinitiative der Strategie Europa 2020 zur Sicherstellung der internationalen Wettbewerbsfähigkeit der EU. Das neue Rahmenprogramm für Forschung und Innovation der EU (2014-2020) ist Teil der Bemühungen um Wachstum und Arbeitsplätze in Europa.

für die Vertrauenswürdigkeit der IKT und die Bekämpfung der Cyberkriminalität, die sich mit dieser Strategie im Einklang befinden. Horizont 2020 wird Arbeiten zur Sicherheitsforschung im Zusammenhang mit neuen IKT unterstützen, Lösungen für durchgehend sichere IKT-Systeme, -Dienste und -Anwendungen bereitstellen, Anreize für die Übernahme und Anwendung bereits bestehender Lösungen geben und sich mit der Interoperabilität von Netzen und Informationssystemen befassen. Besonderes Augenmerk gilt auf EU-Ebene der Optimierung und besseren Koordinierung unterschiedlicher Finanzierungsprogramme (Horizont 2020, Fonds für innere Sicherheit, EDA einschließlich der EFC (European Framework Cooperation)).

Die Kommission wird

- „Horizont 2020" nutzen, um einige Bereiche des Datenschutzes und der Sicherheit im IKT-Bereich zu behandeln (von FuE bis zu Innovation und Einführung). Im Rahmen von „Horizont 2020" sollen auch Instrumente zur Bekämpfung krimineller und terroristischer Aktivitäten im Cyberraum entwickelt werden.
- Mechanismen einrichten, die eine bessere Koordinierung der Forschungspläne der EU-Organe und Einrichtungen und der Mitgliedstaaten ermöglichen und Anreize für die Mitgliedstaaten entwickeln, stärker in FuE zu investieren.

Die Kommission fordert die Mitgliedstaaten auf,

- bis Ende 2013 empfehlenswerte Vorgehensweisen zur Nutzung der **Kaufkraft der öffentlichen Verwaltungen** zu entwickeln (z. B. über die öffentliche Auftragsvergabe), um die Konzipierung und Einführung von Sicherheitsfunktionen bei IKT-Produkten und -Dienstleistungen zu stimulieren;
- die frühzeitige Einbeziehung von Industrie und Hochschulen in die Entwicklung und Koordinierung von Sicherheitslösungen zu fördern. Dies sollte durch eine maximale Nutzung der industriellen Basis Europas und der einschlägigen, durch FuE erreichten technologischen Innovationen geschehen, wobei die Forschungspläne ziviler und militärischer Einrichtungen zu koordinieren sind.

Die Kommission fordert Europol und die ENISA auf,

- neue Trends und Bedürfnisse im Zusammenhang mit den sich weiterentwickelnden Mustern in den Bereichen Cyberkriminalität und Cybersicherheit zu ermitteln, so dass geeignete cyberforensische Werkzeuge und Technologien entwickelt werden können.

Die Kommission fordert die Akteure des öffentlichen und des privaten Sektors auf,

- in Zusammenarbeit mit den Versicherungen **harmonisierte metrische Verfahren für die Berechnung von Risikoprämien** zu entwickeln, so dass Unternehmen, die in Sicherheit investiert haben, geringere Versicherungsbeiträge zahlen müssen.

2.5. Entwicklung einer einheitlichen Cyberraum-Strategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU

Die Bewahrung eines offenen, freien und sicheren Cyberraums ist eine globale Herausforderung, der sich die EU gemeinsam mit den relevanten internationalen Partnern und Organisationen, dem Privatsektor und der Zivilgesellschaft stellen sollte.

Mit ihrer internationalen Cyberraum-Politik wird sich die EU für ein offenes und freies Internet einsetzen, Bemühungen um die Aufstellung von Verhaltensnormen unterstützen und das bestehende internationale Recht im Cyberraum anwenden. Die EU wird sich auch um die Überbrückung der „digitalen Kluft" bemühen und sich aktiv an den internationalen Maßnahmen zum Aufbau von Cybersicherheitskapazitäten beteiligen. Das internationale Engagement der EU in Fragen des Cyberraums wird sich auf die Grundwerte der EU (Menschenwürde, Freiheit, Demokratie, Chancengleichheit, Rechtsstaatlichkeit und Grundrechte) stützen.

Einbeziehung von Themen des Cyberraums in die Außenbeziehungen und die Gemeinsame Außen- und Sicherheitspolitik der EU

Die Kommission, die Hohe Vertreterin und die Mitgliedstaaten sollten eine einheitliche EU-Cyberraum-Politik auf internationaler Ebene vertreten, mit der eine intensivere Zusammenarbeit mit und engere Beziehungen zu wichtigen internationalen Partnern und Organisationen sowie zur Zivilgesellschaft und zum Privatsektor angestrebt werden. Die Konsultationen der EU mit internationalen Partnern zu Fragen des Cyberraums sollten so geplant, koordiniert und durchgeführt werden, dass sie einen zusätzlichen Nutzen gegenüber den bilateralen Kontakten der EU-Mitgliedstaaten mit Drittländern bringen. Die EU wird Gespräche mit Drittländern erneut in den Vordergrund rücken und dabei vor allem auf ähnlich gesinnte Partner zugehen, die dieselben Werte wie die EU zugrunde legen. Sie wird sich um ein hohes Datenschutzniveau bemühen, auch bei der Übertragung personenbezogener Daten in Drittländer. Im Hinblick auf die Bewältigung der globalen Herausforderungen im Cyberraum wird sich die EU um eine engere Zusammenarbeit mit in diesem Bereich aktiven Organisationen bemühen, z. B. mit dem Europarat, der OECD, den Vereinten Nationen, der OSZE, der NATO, der AU, ASEAN und der OAS. Auf bilateraler Ebene ist die Zusammenarbeit mit den USA von besonderer Bedeutung; diese wird ausgebaut, insbesondere im Rahmen der Arbeitsgruppe EU-USA für Cybersicherheit und Cyberkriminalität.

Eines der wichtigsten Elemente der internationalen Cyberpolitik der EU ist die Bewahrung des Cyberraums als freien Raum, in dem die Grundrechte geachtet werden. Die Erweiterung des Zugangs zum Internet sollte demokratische Reformen weltweit unterstützen und fördern. Mit der immer größeren globalen Vernetzung sollte keine Zensur oder umfassende Überwachung verbunden sein. Die EU sollte die soziale Verantwortung der Unternehmen fördern[30] und internationale Initiativen zur Verbesserung der weltweiten Koordinierung in diesem Bereich einleiten.

[30] Eine neue EU-Strategie (2011-14) für die soziale Verantwortung der Unternehmen (CSR) (KOM(2011) 681 endg.).

Die Verantwortung für einen sichereren Cyberraum tragen alle Akteure der globalen Informationsgesellschaft, vom einzelnen Bürger bis zu den Regierungen. Die EU unterstützt die Bemühungen um die Aufstellung von Verhaltensnormen für den Cyberraum, die alle Beteiligten einhalten sollten. Sie erwartet von den Bürgern, dass sie ihren Bürgerpflichten, ihrer sozialen Verantwortung und den Gesetzen auch online nachkommen; ebenso sollten auch Staaten geltende Normen und Gesetze einhalten. Im Bereich der internationalen Sicherheit unterstützt die EU die Entwicklung vertrauensbildender Maßnahmen zur Cybersicherheit, um die Transparenz zu erhöhen und das Risiko zu verringern, dass das staatliche Vorgehen falsch eingeschätzt wird.

Die EU fordert keine neuen internationalen Rechtsinstrumente für Cyberthemen.

Die rechtlichen Verpflichtungen, die im Internationalen Pakt über bürgerliche und politische Rechte, der Europäischen Menschenrechtskonvention und der EU-Grundrechtecharta festgelegt sind, sollten auch online gelten. Die EU wird sich vor allem damit beschäftigen, wie diese Instrumente auch im Cyberraum durchgesetzt werden können.

Zur Bekämpfung der Cyberkriminalität ist das Budapester Übereinkommen ein Instrument, das allen Drittländern offensteht. Es kann als Grundlage für die Abfassung der nationalen Rechtsvorschriften im Bereich der Cyberkriminalität und für die internationale Zusammenarbeit dienen.

Bei Ausdehnung bewaffneter Konflikte auf den Cyberraum gelten das humanitäre Völkerrecht und gegebenenfalls die Rechtsinstrumente zum Schutz der Menschenrechte.

Kapazitätsausbau im Bereich Cybersicherheit und robuste Informationsinfrastrukturen in Drittländern

Eine verstärkte internationale Zusammenarbeit dient dem reibungslosen Funktionieren der Infrastrukturen, die Kommunikationsdienste bereitstellen und ermöglichen. Dazu gehören u. a. der Austausch von Informationen und empfehlenswerten Vorgehensweisen, die frühzeitige Warnung sowie gemeinsame Übungen für die Bewältigung von Sicherheitsvorfällen. Die EU wird hierzu beitragen, indem sie sich für eine Intensivierung der laufenden internationalen Bemühungen zur Stärkung der Kooperationsnetze zum Schutz kritischer Informationsinfrastrukturen (CIIP), an denen Regierungen und Privatsektor beteiligt sind, einsetzt.

Nicht in allen Teilen der Welt können derzeit die Vorteile des Internets genutzt werden, da noch nicht überall ein offener, sicherer, interoperabler und zuverlässiger Zugang vorhanden ist. Die Europäische Union wird daher auch in Zukunft andere Länder bei ihren Bemühungen um den Ausbau der Zugänglichkeit des Internets für ihre Bürger und seiner Nutzung, die Gewährleistung der Integrität und Sicherheit des Internets und die wirksame Bekämpfung der Cyberkriminalität unterstützen.

In Zusammenarbeit mit den Mitgliedstaaten werden die Kommission und die Hohe Vertreterin

- auf eine einheitliche EU-Cyberraum-Politik auf internationaler Ebene

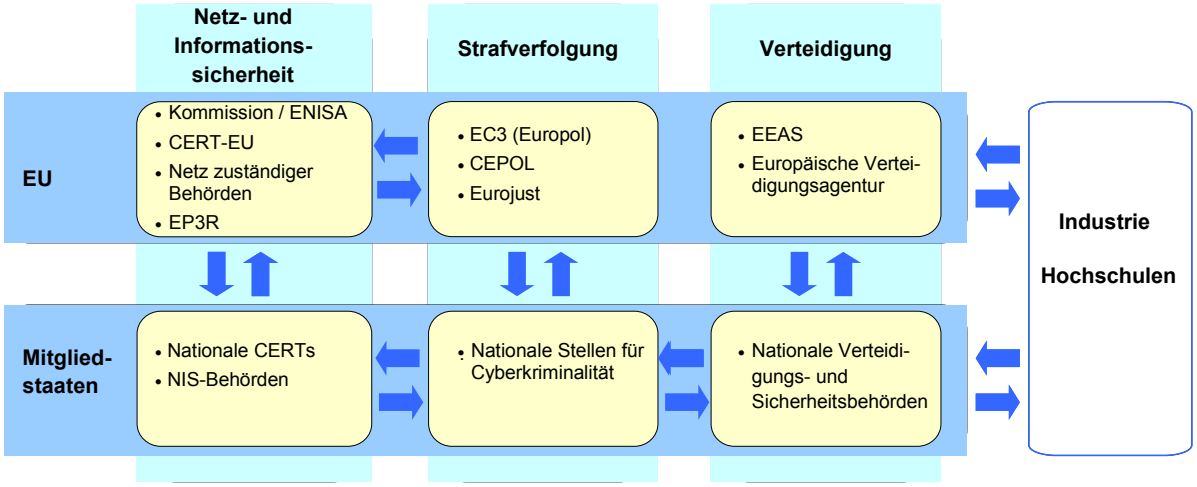
hinarbeiten, um die Zusammenarbeit mit wichtigen internationalen Partnern und Organisationen zu intensivieren, Cyberthemen in die Gemeinsame Außen- und Sicherheitspolitik zu integrieren und die Koordinierung globaler Fragen des Cyberraums zu verbessern;

- die Entwicklung von Verhaltensnormen und vertrauensbildenden Maßnahmen im Bereich der Cybersicherheit unterstützen, den Austausch darüber erleichtern, wie bestehende internationale Rechtsvorschriften im Cyberraum angewendet werden können, und die Anwendung des Budapester Übereinkommens zur Bekämpfung der Cyberkriminalität fördern;
- die Anwendung und den Schutz der Grundrechte fördern, einschließlich des Zugangs zu Informationen und der Meinungsfreiheit, mit folgenden Schwerpunkten: a) Entwicklung neuer zu veröffentlichender Leitlinien für die Meinungsfreiheit online und offline; b) Überwachung der Ausfuhr von Produkten und Diensten, die für die Online-Zensur oder die umfassende Online-Überwachung verwendet werden könnten; c) Entwicklung von Maßnahmen und Werkzeugen zur Erweiterung des Internet-Zugangs sowie der Offenheit und Robustheit des Internets, um der Zensur oder umfassenden Überwachung durch Kommunikationstechnik entgegenzuwirken; d) Befähigung der Beteiligten, die Kommunikationstechnik zur Förderung der Grundrechte einzusetzen;
- mit internationalen Partnern und Organisationen, dem Privatsektor und der Zivilgesellschaft zusammenarbeiten, um den Aufbau von Kapazitäten in Drittländern der ganzen Welt im Interesse eines leichteren Zugangs zu Informationen und einem offenen Internet zu unterstützen, Cyberbedrohungen (auch unbeabsichtigter Art), Cyberkriminalität und Cyberterrorismus zu verhindern bzw. darauf zu reagieren und eine Koordinierung der Geber aufzubauen, damit Kapazitätsaufbaumaßnahmen gelenkt werden können;
- unterschiedliche EU-Finanzierungsinstrumente für den Kapazitätsaufbau im Bereich der Cybersicherheit einsetzen, auch zur Unterstützung der Schulung des Personals der Strafverfolgungs- und Justizbehörden und von technischem Personal zur Bekämpfung von Cyberbedrohungen, außerdem zur Unterstützung der Einführung entsprechender nationaler Strategien, Maßnahmen und Einrichtungen in Drittländern;
- die Koordinierung der Politik und den Informationsaustausch im Rahmen der internationalen Netze zum Schutz kritischer Informationsinfrastrukturen (wie Meridian) und die Zusammenarbeit zwischen den für NIS zuständigen Behörden und anderen Beteiligten verstärken.

3. AUFGABEN UND ZUSTÄNDIGKEITEN

Sicherheitsvorfälle im Cyberraum kennen in der vernetzten digitalen Wirtschaft und Gesellschaft keine Grenzen. Alle Akteure (u. a. die NIS-Behörden, CERTs, Strafverfolgungsbehörden, Industrie) müssen sowohl auf nationaler als auch auf EU-Ebene Verantwortung übernehmen und im Hinblick auf eine höhere Cybersicherheit zusammenarbeiten. Da dies unterschiedliche rechtliche Systeme und Zuständigkeitsbereiche berühren kann, liegt eine der wichtigsten Herausforderungen für die EU darin, die Aufgaben und Zuständigkeiten der zahlreichen Akteure zu klären.

Angesichts der Komplexität des Gegenstands und des breiten Spektrums der Beteiligten ist eine zentralisierte Aufsicht auf EU-Ebene nicht angezeigt. Die nationalen Regierungen sind hier am besten in der Lage, Prävention und Reaktion auf Cybervorfälle und -angriffe zu organisieren und im Rahmen ihrer bestehenden Strategien und Rechtssysteme mit dem Privatsektor und der Öffentlichkeit Kontakte zu pflegen und Netze zu bilden. Gleichzeitig dürfte jedoch aufgrund des potenziell oder konkret grenzübergreifenden Charakters der Risiken die Beteiligung der EU häufig Voraussetzung für ein wirksames Vorgehen auf nationaler Ebene sein. Damit das Thema der Cybersicherheit umfassend behandelt wird, sollten sich die Maßnahmen auf die drei zentralen Bereiche NIS, Strafverfolgung und Verteidigung erstrecken, für die unterschiedliche Rechtsrahmen gelten:



3.1. Koordinierung zwischen NIS-Behörden/CERTs, Strafverfolgungs- und Verteidigungsbehörden

Nationale Ebene

Die Mitgliedstaaten sollten entweder bereits über Strukturen für Fragen der Widerstandsfähigkeit gegenüber Cyberangriffen, der Cyberkriminalität und der Cyberverteidigung verfügen oder solche Strukturen infolge dieser Strategie einrichten. Sie sollten außerdem die notwendigen Kapazitäten besitzen, um Cybervorfälle bewältigen zu können. Angesichts der Anzahl der Stellen, die in den verschiedenen Bereichen der Cybersicherheit für die operative Seite zuständig sind, und angesichts der Bedeutung der Einbeziehung des Privatsektors sollte auf nationaler Ebene eine optimale Koordinierung über Ministerien hinweg erfolgen. Die Mitgliedstaaten sollten in ihren nationalen Cybersicherheitsstrategien die Aufgaben und Zuständigkeiten ihrer verschiedenen nationalen Stellen festlegen.

Der Informationsaustausch zwischen staatlichen Stellen und dem Privatsektor sollte gefördert werden, damit beide einen Gesamtüberblick über die unterschiedlichen Bedrohungen behalten und über neue Trends und Techniken informiert sind, die sowohl für die Durchführung von Cyberangriffen als auch für eine rasche Reaktion darauf verwendet werden. Nationale NIS-Kooperationspläne, die bei Cybervorfällen angewandt werden, sollten den Mitgliedstaaten die eindeutige Zuweisung von Aufgaben und Zuständigkeiten und die Optimierung von Gegenmaßnahmen ermöglichen.

EU-Ebene

Wie auf nationaler Ebene gibt es auch auf EU-Ebene eine Reihe von Akteuren, die im Bereich der Cybersicherheit tätig sind. Insbesondere die ENISA, Europol/EC3 und die EDA sind in Bezug auf NIS, Strafverfolgung und Verteidigung aktiv. Die Mitgliedstaaten sind in den Verwaltungsräten dieser Agenturen vertreten, die ein Forum für die EU-weite Koordinierung bieten.

Koordinierung und Zusammenarbeit zwischen ENISA, Europol/EC3 und EDA werden in mehreren Bereichen unterstützt, in denen sie gemeinsam tätig sind (insbesondere bei Trendanalyse, Risikobewertung, Schulung und Austausch empfehlenswerter Vorgehensweisen). Die Agenturen sollten zusammenarbeiten, jedoch ihre besonderen Zuständigkeiten behalten, und gemeinsam mit dem CERT-EU, der Kommission und den Mitgliedstaaten den Aufbau einer vertrauenswürdigen Gemeinschaft technischer und politischer Experten in diesem Bereich unterstützen.

Die informellen Kanäle für Koordinierung und Zusammenarbeit werden durch stärker strukturierte ergänzt. Der EU-Militärstab und das EDA-Projektteam zur Cyberverteidigung können zur Koordinierung der Verteidigungsmaßnahmen genutzt werden. Im Programmausschuss von Europol/EC3 werden u. a. EUROJUST, CEPOL, die Mitgliedstaaten[31], ENISA und die Kommission vertreten sein; er wird die Möglichkeit bieten, die jeweiligen spezifischen Fachkenntnisse weiterzugeben und sicherzustellen, dass die Maßnahmen des EC3 partnerschaftlich durchgeführt und den besonderen Kompetenzen und Aufträgen aller Akteure Rechnung getragen wird. Durch den neuen Auftrag der ENISA dürften die Verbindungen zu Europol und zu den Akteuren aus der Industrie verstärkt werden können. Am wichtigsten ist, dass durch den NIS-Legislativvorschlag der Kommission mit dem Netz der für die NIS zuständigen nationalen Behörden ein Rahmen für die Zusammenarbeit bereitgestellt und der Informationsaustausch zwischen NIS-Behörden und Strafverfolgungsbehörden geregelt würde.

Internationale Ebene

Die Kommission und die Hohe Vertreterin gewährleisten gemeinsam mit den Mitgliedstaaten eine koordinierte Cybersicherheitspolitik auf internationaler Ebene. Dabei werden die Kommission und die Hohe Vertreterin für die Grundwerte der EU eintreten und eine friedliche, offene und transparente Nutzung der Cybertechnologien unterstützen. Die Kommission, die Hohe Vertreterin und die Mitgliedstaaten nehmen den politischen Dialog mit internationalen Partnern und internationalen Organisationen wie dem Europarat, der OECD, der OSZE, der NATO und den Vereinten Nationen auf.

3.2. EU-Unterstützung bei einem großen Cybervorfall oder -angriff

Große Cybervorfälle oder -angriffe dürften sich auf staatliche Stellen, Unternehmen und Bürger in der EU auswirken. Infolge dieser Strategie und insbesondere der vorgeschlagenen NIS-Richtlinie dürften sich Prävention, Erkennung und Reaktion auf Cybervorfälle verbessern. Auch die gegenseitige Information der Mitgliedstaaten und der Kommission über

[31] über die Vertreter in der EU-Task Force „Cyberkriminalität“, die sich aus den Leitern der für Cyberkriminalität zuständigen Stellen der Mitgliedstaaten zusammensetzt.

große Vorfälle oder Angriffe dürfte umfassender sein. Die Reaktionsmechanismen werden jedoch von Art, Umfang und grenzübergreifenden Auswirkungen des Sicherheitsvorfalls abhängig sein.

Hat der Vorfall einschneidende Folgen für die Betriebskontinuität, wird in der NIS-Richtlinie die Aktivierung nationaler oder EU-weiter NIS-Kooperationspläne vorgeschlagen, je nachdem, ob der Vorfall sich grenzübergreifend auswirkt oder nicht. In diesem Fall würde für Informationsaustausch und Unterstützung auf das Netz der NIS-Behörden zurückgegriffen. So dürfte es möglich sein, die betroffenen Netze und Dienste aufrechtzuerhalten bzw. wiederherzustellen.

Wenn es Hinweise darauf gibt, dass der Sicherheitsvorfall kriminellen Ursprungs ist, sollten Europol/EC3 davon unterrichtet werden, so dass sie – gemeinsam mit den Strafverfolgungsbehörden der betroffenen Länder – eine Untersuchung einleiten, Beweismaterial sichern, die Täter ermitteln und letztendlich deren strafrechtliche Verfolgung veranlassen können.

Handelt es sich bei einem Vorfall um Cyberspionage oder einen staatlich veranlassten Angriff oder um einen Vorfall mit Folgen für die nationale Sicherheit, werden die für die nationale Sicherheit und Verteidigung zuständigen Behörden ihre jeweiligen Kollegen davon unterrichten, so dass diese von dem Angriff wissen und Abwehrmaßnahmen ergreifen können. In solchen Fällen kommen Frühwarnmechanismen zum Einsatz und gegebenenfalls Krisenmanagement- oder sonstige Verfahren. Ein besonders schwerer Cybervorfall oder -angriff könnte dazu führen, dass ein Mitgliedstaat die „Solidaritätsklausel“ (Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union) geltend macht.

Ist bei dem Vorfall vermutlich unbefugt auf personenbezogene Daten zugegriffen worden, sind die nationalen Datenschutzbehörden oder die nationalen Regulierungsbehörden nach der Richtlinie 2002/58/EG zu benachrichtigen.

Schließlich wird man bei der Bewältigung von Cybervorfällen und -angriffen auf Kontaktnetze und die Unterstützung internationaler Partner zurückgreifen können. Dies kann die Bereiche technische Schadensbegrenzung, strafrechtliche Untersuchung und Aktivierung von Reaktionsmechanismen für das Krisenmanagement betreffen.

4. FAZIT UND FOLGEMASSNAHMEN

Die hier von der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vorgelegte Cybersicherheitsstrategie der Europäischen Union gibt die Zielvorstellungen der EU und die dafür erforderlichen Maßnahmen wieder; mit ihr wird ein hoher Schutz der Rechte der Bürger und deren Förderung angestrebt, damit das Online-Umfeld in der EU zum weltweit sichersten wird[32].

[32] Die Strategie soll im Rahmen der für die relevanten Politikbereiche (CEF, Horizont 2020, Fonds für innere Sicherheit, CFSP und externe Zusammenarbeit, insbesondere Stabilitätsinstrument) vorgesehen Beträge finanziert werden, wie sie im Vorschlag der Kommission für den mehrjährigen Finanzrahmen 2014-2020 vorgesehen sind (vorbehaltlich der Genehmigung durch die Haushaltsbehörde und der endgültigen Beträge, die für den MFF 2014-2020 verabschiedet werden). Damit insgesamt die Anzahl

Die Verwirklichung dieser Zielvorstellungen ist nur durch eine echte Partnerschaft zwischen zahlreichen Akteuren möglich, die Verantwortung übernehmen und die zu erwartenden Herausforderungen bewältigen.

Die Kommission und die Hohe Vertreterin fordern daher den Rat und das Europäische Parlament auf, diese Strategie zu unterstützen und zur Umsetzung der beschriebenen Maßnahmen beizutragen. Auch vom Privatsektor und der Zivilgesellschaft sind umfassende Unterstützung und Engagement vonnöten; beide sind zentrale Akteure im Hinblick auf eine höhere Sicherheit und den Schutz der Rechte der Bürger.

Der Zeitpunkt des Handelns ist gekommen. Die Kommission und die Hohe Vertreterin sind entschlossen, mit allen Beteiligten zusammenzuarbeiten, um das für Europa notwendige Niveau an Sicherheit zu erreichen. Um sicherzustellen, dass die Strategie unverzüglich umgesetzt und im Lichte möglicher neuer Entwicklungen überprüft wird, werden die relevanten Akteure zu einer Konferenz mit hochrangigen Vertretern gebeten und die Fortschritte nach einem Jahr überprüft.

---

der für dezentrale Agenturen zur Verfügung stehenden Stellen nicht überschritten wird und die Teilobergrenzen für diese Agenturen in den einzelnen Rubriken des nächsten MFF eingehalten werden, werden die Agenturen, die im Rahmen dieser Mitteilung mit neuen Aufgaben betraut werden (CEPOL, EDA ENISA, EUROJUST und EUROPOL/EC3), aufgefordert, diese in dem Maße zu übernehmen, wie sie über die tatsächliche Möglichkeit zur Aufnahme neuer Ressourcen verfügen und alle Möglichkeiten für eine Umschichtung geprüft wurden.