Rat der
Europäischen Union

**Brüssel, den 7. Juli 2016**
**(OR. en)**

**11013/16**

**CYBER 83**
**COMPET 411**
**IND 158**
**RECH 246**
**TELECOM 129**

**ÜBERMITTLUNGSVERMERK**

| | |
|---|---|
| Absender: | Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission |
| Eingangsdatum: | 5. Juli 2016 |
| Empfänger: | Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union |
| Nr. Komm.dok.: | COM(2016) 410 final |
| Betr.: | MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche |

Die Delegationen erhalten in der Anlage das Dokument COM(2016) 410 final.

Anl.: COM(2016) 410 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 5.7.2016
COM(2016) 410 final

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

## Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche

## 1. EINFÜHRUNG UND KONTEXT

Sicherheitsvorfälle im Cyberraum verursachen jeden Tag erheblichen wirtschaftlichen Schaden für europäische Unternehmen und die gesamte Wirtschaft. Dadurch wird das Vertrauen der Bürgerinnen und Bürger und der Unternehmen in die digitale Gesellschaft untergraben. Der Diebstahl von Geschäftsgeheimnissen, Geschäftsinformationen und personenbezogenen Daten sowie die Störung von – teilweise grundlegenden – Diensten und Infrastrukturen ziehen wirtschaftliche Verluste in einer Größenordnung von mehreren hundert Milliarden Euro pro Jahr[1] nach sich. Außerdem können sie sich auf die Wahrung der Grundrechte der Bürgerinnen und Bürger und auf die Gesellschaft insgesamt auswirken.

Die Cybersicherheitsstrategie für die Europäischen Union von 2013[2] (im Folgenden „EU-Cybersicherheitsstrategie“) und ihr Hauptergebnis, die Richtlinie über Netz- und Informationssicherheit (im Folgenden „NIS-Richtlinie“)[3], die in Kürze verabschiedet werden soll, sowie die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme bilden bislang den Kern der politischen Antwort der Europäischen Union auf diese sicherheitsbezogenen Herausforderungen im Cyberraum. Darüber hinaus kann die EU auf spezialisierte Einrichtungen wie die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und das IT-Notfallteam (*Computer Emergency Response Team*, CERT-EU) zurückgreifen. In jüngster Zeit wurden verschiedene sektorbezogene Initiativen (u. a. im Bereich Energie und Verkehr) ins Leben gerufen, um die Cybersicherheit in verschiedenen systemrelevanten Wirtschaftssektoren zu erhöhen.

Trotz dieser positiven Entwicklungen ist die EU nach wie vor durch Cybervorfälle gefährdet. Diese könnten nicht nur den digitalen Binnenmarkt, sondern das gesamte wirtschaftliche und soziale Leben ins Wanken bringen. Die Auswirkungen solcher Vorfälle können aber auch über die Wirtschaft hinausgehen. So können im Falle hybrider Bedrohungen[4] Cyberangriffe in Koordinierung mit anderen Störaktionen eingesetzt werden, um ein Land zu destabilisieren oder politische Einrichtungen anzugreifen.

Vor diesem Hintergrund könnte ein großer Cybervorfall, der mehrere Mitgliedstaaten gleichzeitig beträfe, die EU vor erhebliche Herausforderungen stellen. Unter Einbeziehung der Mitteilung über die Abwehr hybrider Bedrohungen und der Mitteilung über die Umsetzung der Europäischen Sicherheitsagenda[5] untersucht die Kommission gegenwärtig, wie mit der sich fortwährend wandelnden Realität im Bereich der Cybersicherheit umzugehen ist, und prüft zusätzliche Maßnahmen, die möglicherweise erforderlich sind, um die Cybersicherheit in der EU zu erhöhen und ihre Abwehr- und Reaktionsfähigkeit bei Sicherheitsvorfällen im Cyberraum zu verbessern.

Des Weiteren befasst sich die Kommission mit den Kapazitäten der Cybersicherheitsbranche in der EU. Selbst wenn im Bereich der digitalen Technologien nicht die gesamte Wertschöpfungskette in Europa beherrscht werden kann, müssen zumindest bestimmte

[1] *Net Losses: Estimating the Global Cost of Cybercrime – Economic impact of cybercrime II* (Nettoverluste: Schätzung der globalen Kosten der Cyberkriminalität – Wirtschaftliche Folgen der Cyberkriminalität II); Center for Strategic and International Studies; Juni 2014.
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

grundlegende Kapazitäten in Europa bewahrt und weiterentwickelt werden. Ein Angebot an Produkten und Diensten, die größtmögliche Cybersicherheit bieten, ist eine Chance für die Cybersicherheitsbranche in Europa und könnte sich zu einem bedeutenden Wettbewerbsvorteil entwickeln. Der globale Cybersicherheitsmarkt gehört erwartungsgemäß zu den am schnellsten wachsenden Marktsegmenten des IKT-Sektors[6]. Der Aufstieg der EU zu einem führenden Akteur in diesem Bereich muss von einer starken Datenschutz- und Datensicherheitskultur (auch für personenbezogene Daten) sowie von wirksamen Reaktionsmechanismen für Sicherheitsvorfälle begleitet werden. Dies gilt als ein gewichtiges Argument für Investitionen in der EU und wird dabei helfen, die ehrgeizigen Ziele des digitalen Binnenmarkts in Bezug auf Wachstum und Beschäftigung zu erreichen.

Es bedarf eines starken Engagements, all dies zu verwirklichen, insbesondere durch:

*i) Intensivierung der Zusammenarbeit zur Verbesserung der Abwehrbereitschaft und zur Bewältigung von Cybervorfällen*

Bestehende und vereinbarte Kooperationsverfahren müssen ausgebaut werden, um die Abwehrfähigkeit und die Abwehrbereitschaft der EU zu stärken, auch mit Blick auf eine mögliche gesamteuropäische Cybersicherheitskrise. Diese Kooperationsmechanismen sollten sich auf alle Phasen von Sicherheitsvorfällen, von der Prävention bis hin zur Strafverfolgung, erstrecken. Für eine wirksame Zusammenarbeit zwischen den Mitgliedstaaten und die praktische Umsetzung von Sicherheitsanforderungen bei infrastrukturrelevanten Betreibern sind auch zuverlässige technische Lösungen aus der Cybersicherheitsbranche erforderlich.

Um die Resilienz systemrelevanter Cyberanlagen überall in der EU gewährleisten zu können, werden zugleich kontinuierliche Anstrengungen nötig sein, um sektorübergreifend Synergien zu erschließen und die Anforderungen an die Cybersicherheit in allen relevanten Politikbereichen der EU durchgehend zu berücksichtigen. Die Kommission wird prüfen, ob es notwendig ist, die EU-Cybersicherheitsstrategie von 2013 bald zu überarbeiten.

*ii) Bewältigung der Herausforderungen für den europäischen Binnenmarkt im Bereich der Cybersicherheit*

In der Strategie für einen digitalen Binnenmarkt[7] wird eingeräumt, dass bei den durch raschen Wandel geprägten Technologien und Lösungen für die Online-Netzsicherheit nach wie vor Defizite bestehen. Zugleich zeigen Marktuntersuchungen, dass der EU-Binnenmarkt beim Angebot an Produkten und Diensten für die Cybersicherheit geografisch immer noch fragmentiert ist[8]. Diese Mitteilung stellt verschiedene marktorientierte Strategien zur Behebung dieser Defizite und Probleme im Binnenmarkt vor.

*iii) Ausbau der Kapazitäten des Sektors auf dem Gebiet der Cybersicherheit*

In der EU-Cybersicherheitsstrategie und in der Strategie für einen digitalen Binnenmarkt hat sich die Kommission dazu verpflichtet, ein verstärktes Angebot an Produkten und Diensten des Cybersicherheitssektors der EU zu fördern. Deshalb fasst sie nun auch einen Beschluss, der den Weg für eine Vereinbarung über eine vertragliche öffentlich-private Partnerschaft (cPPP) für Cybersicherheit ebnet, mit der eine auf Spitzenniveau agierende europäische Forschungs- und Innovationsagenda zur Steigerung Wettbewerbsfähigkeit vorangebracht werden soll.

[6] Siehe SWD(2016) 216.
[7] COM(2015) 192.
[8] Siehe SWD(2016) 216.

## 2. AUSBAU DER ZUSAMMENARBEIT, DES KNOW-HOWS UND DER KAPAZITÄTEN

Die EU-Cybersicherheitsstrategie und insbesondere die kommende NIS-Richtlinie[9] werden den Auftakt zu einer intensiveren Zusammenarbeit zwischen den Mitgliedstaaten auf EU-Ebene geben. Die zügige und wirksame Umsetzung der Richtlinie wird angesichts der zunehmenden Digitalisierung des wirtschaftlichen und gesellschaftlichen Lebens (auch unter Berücksichtigung des Cloud-Computings, des Internets der Dinge und der Maschine-Maschine-Kommunikation), der zunehmenden grenzüberschreitenden Zusammenschaltung der Netze und der sich rasch wandelnden Cyberbedrohungen von zentraler Bedeutung sein[10]. In diesem Zusammenhang muss die EU sich auf die Möglichkeit einer großen Cyberkrise einstellen[11], z. B. auf gleichzeitige massive Angriffe auf systemrelevante Informationssysteme in mehreren Mitgliedstaaten[12].

Die Zusammenarbeit auf EU-Ebene ist daher außerordentlich wichtig, um sowohl auf kleinere, potenziell aber immer häufigere Sicherheitsvorfälle als auch auf einen eventuellen Cybergroßangriff in mehreren Mitgliedstaaten reagieren zu können. Die EU muss Aspekte der Sicherung des Cyberraums in die bestehenden Mechanismen des Krisenmanagements integrieren. Außerdem muss sie wirksame Mechanismen für die Zusammenarbeit und den Informationsaustausch zwischen den einzelnen Sektoren und Mitgliedstaaten schaffen, damit Sicherheitsvorfälle bewältigt und eingedämmt werden können. Darüber hinaus sollten diese Mechanismen in abgestimmter Weise zusammenwirken und so zur Bekämpfung des Terrorismus, der organisierten Kriminalität und der Cyberkriminalität beitragen. Dadurch könnte die EU sich auch mit ihren internationalen Partnern bei globalen Bedrohungen und Sicherheitsvorfällen besser abstimmen.

### 2.1 NIS-Kooperationsmechanismen bestmöglich nutzen und auf ENISA 2.0 hinarbeiten

Ein zentraler Teil der nationalen Kapazitäten, die nach der NIS-Richtlinie zur Verfügung stehen müssen, sind die IT-Noteinsatzteams (*Computer Security Incident Response Teams* – CSIRT), die schnell auf Cyberbedrohungen und Cybervorfälle reagieren können müssen. Sie sollen das CSIRT-Netz zur Förderung einer wirksamen operativen Zusammenarbeit im Falle konkreter Cybersicherheitsvorfälle sowie des Informationsaustauschs über Risiken bilden. Ferner wird durch die Richtlinie eine Kooperationsgruppe eingerichtet, die die strategische Zusammenarbeit zwischen den Mitgliedstaaten unterstützen und erleichtern und das gegenseitige Vertrauen stärken soll.

Angesichts der Art und Vielzahl der Cyberbedrohungen ermuntert die Kommission die Mitgliedstaaten, die NIS-Kooperationsmechanismen bestmöglich zu nutzen, aber auch die grenzüberschreitende Zusammenarbeit im Bereich der Abwehrbereitschaft gegenüber großen Cybervorfällen zu intensivieren. Ein koordinierter Ansatz für die Zusammenarbeit in Krisensituationen, bei dem die verschiedenen Elemente des Cyberökosystems

[9] Die NIS-Richtlinie wird vorsehen, dass die Mitgliedstaaten bestimmte Betreiber grundlegender Dienste benennen, etwa in den Bereichen Energie, Verkehr, Finanzen und Gesundheit, damit diese sich für Bedrohungen der Cybersicherheit rüsten und damit sichergestellt wird, dass auch bestimmte Anbieter digitaler Dienste geeignete Maßnahmen ergreifen, um sich entsprechend abzusichern.
[10] Siehe SWD(2016) 216.
[11] Siehe z. B. ENISA-Bericht: *Common practices of EU-level crisis management and applicability to cyber crises* (Gemeinsame Verfahren für das Krisenmanagement auf EU-Ebene und deren Anwendbarkeit auf Cyberkrisen) (April 2016).
[12] Siehe SWD(2016) 216.

zusammenwirken, würde einer solchen zusätzlichen Zusammenarbeit im Hinblick auf einen ernsten Cybervorfall zugutekommen. Ein solcher Ansatz lässt sich in einem „Konzeptentwurf“ festhalten, der auch Synergien und Kohärenz mit bestehenden Krisenbewältigungsmechanismen[13] gewährleisten sollte. Dieses Konzept sollte anschließend regelmäßig im Rahmen von (Cyber-)Krisenmanagementübungen auf den Prüfstand gestellt werden. EU-Einrichtungen wie ENISA und CERT-EU sowie das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) würden darin ebenso eine Rolle spielen wie im Rahmen des CSIRT-Netzes entwickelte Werkzeuge. In der ersten Hälfte des Jahres 2017 wird die Kommission der Kooperationsgruppe, dem CSIRT-Netz und anderen einschlägigen Akteuren einen solchen Konzeptentwurf für die Zusammenarbeit zur Erörterung vorlegen.

Kenntnisse und Fachwissen im Bereich der Cybersicherheit sind derzeit auf EU-Ebene zwar verfügbar, allerdings lediglich in zerstreuter und unstrukturierter Form. Um die NIS-Kooperationsmechanismen zu unterstützen, sollten die Informationen auf einer „Informationsplattform“ zusammengetragen werden, damit sie für alle Mitgliedstaaten auf Anfrage leicht zugänglich sind. Diese „Plattform“ wäre eine zentrale Ressource, die den EU-Organen und EU-Mitgliedstaaten im Bedarfsfall den Austausch von Informationen ermöglichen würde. Ein leichterer Zugang zu besser strukturierten Informationen über Cyberrisiken und potenzielle Problemlösungen dürfte den Mitgliedstaaten dabei helfen, ihre Kapazitäten auszubauen und ihre Verfahren aufeinander abzustimmen, sodass die Abwehrfähigkeit insgesamt gestärkt wird. Die Kommission wird die Einrichtung der Plattform und deren Zukunftsfähigkeit mit der Unterstützung von ENISA, CERT-EU und dem Know-how der Gemeinsamen Forschungsstelle voranbringen.

Darüber hinaus sollte auf EU-Ebene eine ständige hochrangige Beratungsgruppe[14] zum Thema Cybersicherheit eingerichtet werden, in der Sachverständige und Entscheidungsträger aus Wirtschaft, Wissenschaft, Zivilgesellschaft und anderen einschlägigen Organisationen vertreten sind. Über die Gruppe soll die Kommission in offener und transparenter Weise auf externe Sachkenntnis und Beiträge für ihre Politik im Rahmen der Cybersicherheitsstrategie und ihre möglichen rechtlichen und sonstigen politischen Maßnahmen zurückgreifen können. Sie würde als Ergänzung und Verbindungspunkt zu anderen Strukturen im Bereich der Cybersicherheit dienen[15].

Darüber hinaus muss die Kommission bis zum 20. Juni 2018 eine Bewertung der ENISA vornehmen, deren neues Mandat gegebenenfalls bis zum 19. Juni 2020 angenommen werden müsste[16]. Angesichts der derzeitigen Cybersicherheitslage beabsichtigt die Kommission, die Bewertung zeitlich vorzuziehen und in Abhängigkeit von ihren Ergebnissen so bald wie möglich einen Vorschlag vorzulegen.

Bei der Prüfung, ob das Mandat der ENISA geändert werden muss, wird die Kommission den oben beschriebenen Herausforderungen im Bereich der Cybersicherheit und insgesamt den

---

[13] Insbesondere die „Integrierte EU-Regelung für die politische Reaktion auf Krisen“, einschließlich des Beschlusses über die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union (24. Juli 2014) und der Entscheidungsprozesse im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik.

[14] Die Expertengruppen der Kommission unterliegen den horizontalen Bestimmungen des Beschlusses C(2016) 3301 der Kommission.

[15] Zum Beispiel die NIS-Plattform, die cPPP für Cybersicherheit sowie sektorspezifische Plattformen, wie z. B. die EECSP (*Energy Expert Cyber Security Platform*). Sie sollte auch eine Verbindung zu den in der Mitteilung über die Digitalisierung der europäischen Industrie, COM(2016) 180 final, angekündigten hochrangigen Rundtischgesprächen herstellen.

[16] Verordnung (EG) Nr. 526/2013 zur Aufhebung der Verordnung (EU) Nr. 460/2004.

Bemühungen zur Intensivierung der Zusammenarbeit und des Wissensaustauschs Rechnung tragen. Dieser Prozess wird die Gelegenheit bieten zu prüfen, ob die Leistungsfähigkeit und die Kapazitäten der Agentur mit Blick auf eine nachhaltige Unterstützung der Mitgliedstaaten beim Ausbau ihrer Abwehrfähigkeit im Bereich der Cybersicherheit verbessert werden müssen. Bei den Überlegungen über das Mandat der ENISA müssten auch die neuen Zuständigkeiten der Agentur gemäß der NIS-Richtlinie, die neuen politischen Ziele bezüglich der Förderung des Cybersicherheitssektors (die Strategie für einen digitalen Binnenmarkt und insbesondere die cPPP), die sich wandelnden Erfordernisse im Bereich der Sicherung systemrelevanter Sektoren sowie neue Herausforderungen im Zusammenhang mit grenzüberschreitenden Sicherheitsvorfällen, einschließlich der koordinierten Reaktion auf Cyberkrisen, berücksichtigt werden.

Die Kommission wird

- in der ersten Jahreshälfte 2017 einen Konzeptentwurf zur Zusammenarbeit vorlegen, der sich mit der Bewältigung schwerwiegender Cybervorfälle auf EU-Ebene beschäftigt;
- die Einrichtung einer Informationsplattform für den Informationsaustausch zwischen EU-Einrichtungen und Mitgliedstaaten voranbringen;
- eine hochrangige Beratungsgruppe zum Thema Cybersicherheit einsetzen;
- die Bewertung der ENISA bis Ende 2017 abschließen. Darin wird sie auf die Notwendigkeit einer Änderung oder Erweiterung des Mandats der ENISA eingehen, um gegebenenfalls so bald wie möglich einen entsprechenden Vorschlag vorzulegen.

## 2.2 Verstärkte Aus- und Weiterbildung und Übungen zur Cybersicherheit

Angemessene Kompetenzen und Ausbildung sowohl in Bezug auf die Prävention von Cybersicherheitsvorfällen als auch die Bewältigung und Eindämmung ihrer Folgen gehören zu den wichtigsten Aspekten beim Aufbau der Abwehrfähigkeit im Cyberraum.

Durch das Erstellen von Handbüchern, durch Veranstaltungen, Schulungen und Übungen zur Cybersicherheit übernehmen die ENISA und die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG) in Zusammenarbeit mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol und der Europäischen Polizeiakademie (CEPOL) gemeinsam eine wichtige Rolle bei der Unterstützung des Kapazitätenaufbaus (u. a. in der Cyberforensik).

Da der Cyberraum ein Bereich ist, der sich rasch wandelt und in dem das Know-how über Güter mit doppeltem Verwendungszweck eine wichtige Rolle spielt, müssen die zivil-militärische Zusammenarbeit ebenso wie Synergien bei der Ausbildung und bei Übungen zur Verbesserung der Abwehr- und Reaktionsfähigkeit der EU ausgebaut werden.

Dafür werden die Dienststellen der Kommission zusätzlich zur Annahme der NIS-Richtlinie und des EU-Politikrahmens für die Cyberabwehr[17] in Zusammenarbeit mit den Mitgliedstaaten, dem Europäischen Auswärtigen Dienst (EAD), der ENISA und anderen einschlägigen Einrichtungen der EU[18] eine Plattform für Schulungen, Übungen und Ausbildung im Bereich Cybersicherheit schaffen, die Synergien zwischen ziviler und verteidigungsbezogener Ausbildung erschließen hilft.

[17] Annahme durch den Rat (Auswärtige Angelegenheiten) der Europäischen Union vom 18. November 2014 (Dok. 15585/14).
[18] Zum Beispiel das Europäische Sicherheits- und Verteidigungskolleg, EC3, CEPOL und die Europäische Verteidigungsagentur (EDA).

Die Kommission wird

- eng mit den Mitgliedstaaten, dem EAD, der ENISA und anderen einschlägigen Einrichtungen der EU zusammenarbeiten, um eine Ausbildungsplattform zur Cybersicherheit einzurichten.

## 2.3 Sektorübergreifende Abhängigkeiten und Resilienz wichtiger öffentlicher Netzinfrastrukturen

Ein wichtiger Faktor bei der Einschätzung der Gefahr und der potenziellen Folgen eines großen Cybervorfalls ist das Maß an grenz- und sektorübergreifenden wechselseitigen Abhängigkeiten. Ein ernster Cybervorfall in einem Wirtschaftssektor oder einem Mitgliedstaat kann direkt oder indirekt andere Sektoren oder andere Mitgliedstaaten treffen oder sich auf diese ausbreiten.

Die grenz- und sektorübergreifende Zusammenarbeit ermöglicht den Austausch von Informationen und Know-how und trägt damit zu einer erhöhten Abwehrbereitschaft und Resilienz bei. Mit der Umsetzung des Europäischen Programms für den Schutz systemrelevanter Infrastrukturen[19] unterstützt die Kommission bereits die Bemühungen verschiedener Sektoren, solche wechselseitigen Abhängigkeiten besser zu verstehen.

Für die Bewältigung sektorübergreifender Risiken ist es zudem unbedingt erforderlich, dass die einzelnen Sektoren in der Lage sind, Cybervorfälle zu erkennen, sich dafür zu rüsten und darauf zu reagieren. Die Kommission wird untersuchen, welches Risiko von Cybervorfällen in stark miteinander verflochtenen Sektoren und insbesondere in den unter die NIS-Richtlinie fallenden Sektoren – innerhalb nationaler Grenzen und darüber hinaus – ausgeht, und hierbei auch die Entwicklungen auf internationaler Ebene[20] berücksichtigen. Im Anschluss an diese Untersuchung wird die Kommission erwägen, ob weitere besondere Vorschriften und/oder Leitlinien zur Risikovorsorge in solchen systemrelevanten Sektoren erforderlich sind.

Auf europäischer Ebene können sektorbezogene Informationsaustausch- und -analysezentren[21] (*Information Sharing and Analysis Centres* – ISAC) sowie die entsprechenden CSIRT eine zentrale Rolle bei der Abwehrbereitschaft gegenüber Cybervorfällen und die Reaktion darauf spielen. Um einen effektiven Informationsfluss in Bezug auf die Entwicklung der Bedrohungslage zu gewährleisten und die Reaktionsfähigkeit bei Cybervorfällen zu verbessern, sollten die ISAC dazu angehalten werden, sich an dem im Rahmen der NIS-Richtlinie vorgesehenen CSIRT-Kooperationsnetz zu beteiligen und mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, dem CERT-EU und einschlägigen Strafverfolgungsbehörden zusammenzuarbeiten.

Ein Informationsaustausch zwischen allen Akteuren und mit den Behörden während des gesamten Lebenszyklus von Cybergefahren setzt voraus, dass Beteiligte die Gewissheit haben können, dass sie dadurch kein Haftungsrisiko eingehen. Die Kommission konnte solche Bedenken bei Unternehmen feststellen, die aus diesem Grund davon Abstand nahmen, in ihren Kreisen, über Branchengrenzen hinaus oder gegenüber Behörden wertvolle Informationen über Bedrohungen offenzulegen, insbesondere im Falle eines Austauschs über Landesgrenzen hinweg. Die Kommission wird sich bemühen, derartige Bedenken zu

[19] SWD(2013) 318.
[20] Zum Beispiel der Fahrplan zur Cybersicherheit der Europäischen Agentur für Flugsicherheit und die Arbeiten der Internationalen Zivilluftfahrt-Organisation (ICAO) und der Internationalen Seeschifffahrtsorganisation (IMO).
[21] Siehe z. B. *European Energy ISAC* (http://www.ee-isac.eu).

thematisieren und im Interesse eines besseren Informationsaustauschs über Cyberbedrohungen auszuräumen.

Vertrauenswürdige Meldekanäle, die Vertraulichkeit gewährleisten, sind ebenfalls unerlässlich, damit Unternehmen ermutigt werden, Cyberdiebstähle von Betriebsgeheimnissen zu melden. Auf diese Weise könnte beobachtet und bewertet werden, welcher Schaden für die europäische Wirtschaft (auch durch Absatzeinbußen und Verlust von Arbeitsplätzen) und für Forschungseinrichtungen entsteht. Außerdem wäre dies hilfreich für die Ausarbeitung geeigneter strategischer Antworten. Mit Unterstützung der ENISA, des Amts der Europäischen Union für geistiges Eigentum (EUIPO) und des EC3 bei Europol wird die Kommission – im Dialog mit privaten Akteuren – vertrauenswürdige Kanäle für die freiwillige Meldung eines Cyberdiebstahls von Geschäftsgeheimnissen schaffen. Auf diese Weise können anonymisierte und aggregierte Daten auf EU-Ebene erhoben werden. Diese Daten könnten dann den Mitgliedstaaten zur Verfügung gestellt werden, um diplomatische Bemühungen und Sensibilisierungsmaßnahmen zum Schutz der immateriellen Güter der Europäischen Union vor Cyberspionage zu befördern.

Zur Unterstützung sektorbezogener Cybersicherheitsmaßnahmen wird die Kommission ferner die Einbeziehung der Cybersicherheit in die Ausarbeitung verschiedener sektorspezifischer EU-Strategien, für die dies von Belang ist, fördern.

Nicht zuletzt sollten auch Behörden ihren Beitrag zur Prüfung der Integrität zentraler Internet-Infrastrukturen leisten, damit Probleme erkannt, die Zuständigen der betreffenden Netze informiert und – soweit erforderlich – bei der Behebung bekannter Schwachstellen geholfen werden kann. Die nationalen Regulierungsbehörden können die Kapazitäten der CSIRT nutzen, um regelmäßige Kontrollen öffentlicher Netzinfrastrukturen vorzunehmen. Auf dieser Grundlage könnten sie dann die Betreiber zur Behebung der bei derartigen Kontrollen festgestellten Defizite und Schwachstellen anhalten.

Die Kommission wird daher die erforderlichen rechtlichen und organisatorischen Voraussetzungen prüfen, damit die nationalen Regulierungsbehörden – in Zusammenarbeit mit den nationalen Cybersicherheitsbehörden – die CSIRT mit regelmäßigen Kontrollen öffentlicher Netzinfrastrukturen auf Schwachstellen beauftragen können. Die nationalen CSIRT sollten dazu ermutigt werden, im Rahmen des CSIRT-Netzes an der Entwicklung bewährter Verfahren zur Überwachung von Netzen zusammenzuarbeiten, um so die Prävention großer Cybervorfälle zu erleichtern.

Die Kommission wird

- die Entstehung europäischer sektorbezogener Informationsaustausch- und -analysezentren fördern, deren Zusammenarbeit mit den CSIRT unterstützen und sich um den Abbau von Hindernissen bemühen, die Marktteilnehmer vom Informationsaustausch abhalten;
- das strategische/systemische Risiko analysieren, das von Cybervorfällen in stark miteinander verflochtenen Sektoren innerhalb nationaler Grenzen wie darüber hinaus ausgeht;
- prüfen, ob zusätzliche Vorschriften und/oder Leitlinien zur Cyberrisikovorsorge in systemrelevanten Sektoren erforderlich sind, und diese gegebenenfalls in Betracht ziehen;
- gemeinsam mit ENISA, EUIPO und EC3 vertrauenswürdige Kanäle für freiwillige Meldungen des Cyberdiebstahls von Geschäftsgeheimnissen schaffen;
- die Einbeziehung von Cybersicherheitsmaßnahmen in europäische sektorspezifische Strategien fördern;
- prüfen, welche Voraussetzungen erfüllt sein müssen, damit nationale Behörden die CSIRT

mit regelmäßigen Kontrollen wesentlicher Netzinfrastrukturen beauftragen können.

## 3. BEWÄLTIGUNG DER HERAUSFORDERUNGEN IM EUROPÄISCHEN CYBERSICHERHEITSBINNENMARKT

Europa braucht hochwertige, erschwingliche und interoperable Produkte und Lösungen im Bereich der Cybersicherheit. Allerdings ist das Angebot an IKT-Sicherheitsprodukten und -diensten im Binnenmarkt nach wie vor geografisch stark zersplittert. Dadurch ist es einerseits für europäische Unternehmen schwierig, auf nationaler, europäischer und weltweiter Ebene wettbewerbsfähig zu sein, und andererseits bleibt so die Auswahl an tragfähigen und nutzbaren Technologien für die Cybersicherheit, zu denen Bürger und Unternehmen Zugang haben, beschränkt[22].

Die Cybersicherheitsbranche in Europa hat sich überwiegend aufgrund der Nachfrage der nationalen Regierungen, u. a. für den Verteidigungssektor, entwickelt. Die meisten europäischen Rüstungsunternehmen verfügen inzwischen über eigene Abteilungen für Cybersicherheit[23]. Parallel dazu sind sowohl in Fach- bzw. Nischenmärkten (z. B. Kryptosysteme) als auch auf etablierten Märkten zahllose innovative KMU mit neuen Geschäftsmodellen (z. B. Antivirenprogramme) entstanden.

Die Unternehmen haben jedoch zunehmend Schwierigkeiten, über ihren heimischen, nationalen Markt hinaus zu expandieren. Das fehlende Vertrauen in „grenzüberschreitend" angebotene Lösungen ist eindeutig der Hauptgrund, der durchgehend bei allen Konsultationen der Kommission hierfür genannt wird[24]. Infolgedessen werden viele öffentliche Aufträge nach wie vor innerhalb eines bestimmten Mitgliedstaats vergeben und viele Unternehmen haben Schwierigkeiten, Größenvorteile zu erzielen, die sie sowohl im Binnenmarkt als auch weltweit wettbewerbsfähiger machen würden.

Der Mangel an interoperablen Lösungen (technische Normen), Verfahren (Verfahrensnormen) und EU-weiten Zertifizierungsmechanismen gehört zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. In diesem Zusammenhang wurde die Cybersicherheit als ein IKT-Normungsschwerpunkt für den digitalen Binnenmarkt ausgewählt[25].

Die eingeschränkten Wachstumsperspektiven im Binnenmarkt für Unternehmen der Cybersicherheitsbranche führen zu zahlreichen Fusionen und Übernahmen durch Investoren aus Drittländern[26]. Zwar zeigt diese Entwicklung die Innovationsfähigkeit der europäischen Unternehmer, sie birgt aber auch die Gefahr, dass europäisches Know-how und Expertenwissen verloren gehen und hochqualifizierte Fachkräfte abwandern.

Dringend erforderlich sind Maßnahmen zur Förderung eines stärker integrierten Binnenmarkts für Cybersicherheitsprodukte und -dienste, der eine stärkere Verbreitung praktischer und erschwinglicher Lösungen voranbringt.

Einem Mangel an gegenseitigem Vertrauen unter den europäischen Akteuren aus Wirtschaft und Politik kann durch die Förderung der Zusammenarbeit in der Frühphase des

[22] Siehe SWD(2016) 216.
[23] Siehe SWD(2016) 216.
[24] Siehe SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Siehe SWD(2016) 216.

Innovationzyklus entgegengewirkt werden: innerhalb der Cybersicherheitsbranche selbst, zwischen Anbietern und Abnehmern sowie sektorübergreifend unter Einbeziehung jener Wirtschaftszweige, die bereits Kunden für Cybersicherheitslösungen sind oder in Zukunft wahrscheinlich sein werden.

Gleichzeitig gewinnt in Europa die Entwicklung von Produkten, Dienstleistungen und Technologien mit doppeltem Verwendungszweck zunehmend an Bedeutung. Immer mehr Lösungen werden vom zivilen Markt in den Verteidigungsmarkt überführt[27]. Im Rahmen des zu verabschiedenden europäischen Aktionsplans im Verteidigungsbereich will die Kommission Maßnahmen zur Weiterentwicklung zivil-militärischer Synergien auf europäischer Ebene aufzeigen.

### 3.1 Zertifizierung und Kennzeichnung

Die Zertifizierung spielt für mehr Vertrauen in Produkte und Dienste und deren Sicherheit eine große Rolle. Das gilt auch für neue Systeme, die in hohem Maße digitale Technik nutzen und ein hohes Maß an Sicherheit erfordern, wie z. B. vernetzte und selbstfahrende Autos, elektronische Gesundheitsdienste, industrielle Automatisierungssteuerungssysteme (*Industrial Automation Control Systems* – IACS) und intelligente Netze.

Es entstehen nationale Initiativen, die sich die Festlegung hoher Cybersicherheitsanforderungen an IKT-Komponenten in herkömmlichen Infrastrukturen, einschließlich Zertifizierungsanforderungen, zum Ziel gesetzt haben. Solche Initiativen sind zweifellos wichtig, bergen aber die Gefahr einer Fragmentierung des Binnenmarkts und können Interoperabilitätsprobleme verursachen. Nur in wenigen Mitgliedstaaten gibt es wirksame Zertifizierungsprogramme für die Sicherheit von IKT-Produkten[28]. IKT-Anbieter müssen daher unter Umständen mehrere Zertifizierungsverfahren durchlaufen, um ihre Produkte in mehreren Mitgliedstaaten verkaufen zu können. Schlimmstenfalls können IT-Produkte oder -Dienste, die auf die Sicherheitsanforderungen eines Mitgliedstaats zugeschnitten sind, nicht in einem anderen Mitgliedstaat auf den Markt gebracht werden.

Zur Verwirklichung eines funktionierenden Binnenmarkts im Bereich der Cybersicherheit sollte ein möglicher Rahmen für die Zertifizierung der Sicherheit von IKT-Produkten und -Diensten folgenden Zielen dienen: i) Abdeckung eines breiten Spektrums an IKT-Systemen, -Produkten und –Diensten, ii) Anwendung in allen 28 Mitgliedstaaten und iii) Anwendbarkeit auf alle verschiedenen Niveaus der Cybersicherheit unter Berücksichtigung der Entwicklungen auf internationaler Ebene.

Hierzu wird die Kommission eine eigene Arbeitsgruppe für die Zertifizierung der Sicherheit von IKT-Produkten und -Diensten einrichten, die sich aus Sachverständigen aus den Mitgliedstaaten und der Branche zusammensetzen wird. Diese Gruppe wird das Ziel haben, in Zusammenarbeit mit der ENISA und der Gemeinsamen Forschungsstelle bis Ende 2016 einen Fahrplan aufzustellen, nach dem die Möglichkeit der Ausarbeitung eines Vorschlags für einen europäischen IKT-Sicherheitszertifizierungsrahmen bis Ende 2017 geprüft werden soll. In diesem Zusammenhang wird die Kommission auch der Verordnung (EG) Nr. 2008/765 und

[27] Bereits 2013 machte die Ausfuhr von Gütern mit doppeltem Verwendungszweck rund 20 % (des Wertes) der Gesamtausfuhren der EU aus – einschließlich des Handels innerhalb der EU.

[28] Vgl. die Arbeitsunterlage SWD(2016) 216 in Bezug auf die Vereinbarung der Gruppe hoher Beamter für Informationssysteme (Beschluss 92/242/EWG des Rates vom 31.3.1992) und andere bestehende Systeme, z. B. *Commercial Product Assurance* im Vereinigten Königreich und *Certification Sécuritaire de Premier Niveau* in Frankreich.

den in der Datenschutz-Grundverordnung 2016/679[29] enthaltenen Zertifizierungsbestimmungen Rechnung tragen.

Dieser Prozess beinhaltet auch eine umfassende Konsultation und Folgenabschätzung. So wird die Kommission in der Lage sein, verschiedene Optionen für die Schaffung des Zertifizierungsrahmens für IKT-Produkte und -Dienste auszuloten. Die Kommission wird außerdem prüfen, ob eine IKT-Sicherheitszertifizierung innerhalb der Infrastruktursektoren (z. B. in den Bereichen Luftfahrt, Eisenbahn und Automobilindustrie) und in bestimmten Zertifizierungs- und Validierungsmechanismen für einsatzbereite Technologien (z. B. Cybersicherheit industrieller Automatisierungs-Kontrollsysteme[30], Internet der Dinge, Cloud) möglich ist. Außerdem wird sie sich mit den Schwachstellen befassen, die im Rahmen des oben genannten europäischen IKT-Sicherheitszertifizierungssystems ermittelt werden.

Die Zertifizierungsbemühungen werden so weit wie möglich auf international anerkannten Standards aufbauen und gemeinsam mit internationalen Partnern entwickelt werden.

Zudem wird die Kommission prüfen, wie die IKT-Sicherheitszertifizierung am besten in künftige sektorspezifische Rechtsvorschriften mit Sicherheitsbezug integriert werden kann.

Abgesehen von den möglichen Regulierungsoptionen wird die Kommission außerdem die Möglichkeit der Schaffung eines europäischen kommerziell ausgerichteten, freiwilligen und handlichen Kennzeichnungssystems für die Sicherheit von IKT-Produkten untersuchen. Zusätzlich zur Zertifizierung soll dadurch die Verständlichkeit von Cybersicherheitsangaben bei kommerziellen Produkten verbessert werden, um so deren Wettbewerbsfähigkeit im Binnenmarkt wie auch weltweit zu erhöhen. Die laufenden sektorbezogenen und horizontalen Initiativen der Branche – sowohl von der Angebots- als auch von der Nachfrageseite – werden hierbei gebührend berücksichtigt werden.

Die öffentlichen Verwaltungen werden eng eingebunden sein, damit gemeinsame Spezifikationen verwendet werden können und bei öffentlichen Aufträgen eine einheitliche Bezugnahme auf Zertifizierungen möglich ist. Darüber hinaus wird die Kommission die Verwendung der einschlägigen Zertifizierungsanforderungen bei öffentlichen Aufträgen auf nationaler Ebene, insbesondere bei sektorspezifischen Systemen (Energie, Verkehr, Gesundheit, öffentliche Verwaltung usw.) beobachten und darüber Bericht erstatten.

Die Kommission wird

- bis Ende 2016 einen Fahrplan im Hinblick auf einen Ende 2017 möglicherweise vorzulegenden Vorschlag für einen europäischen IT-Sicherheitszertifizierungsrahmen aufstellen und diesen sowie die Machbarkeit und die Auswirkungen eines handlichen europäischen Rahmens für die Cybersicherheitskennzeichnung prüfen;
- ermitteln, ob eine IKT-Sicherheitszertifizierung im Rahmen bestehender sektorspezifischer Zertifizierungs-/Validierungsmechanismen erforderlich ist und sich gegebenenfalls mit den Defiziten befassen;

[29] Die 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) sieht sowohl Verhaltensregeln vor, die zur korrekten Anwendung der Datenschutzvorschriften beitragen sollen, als auch Zertifizierungsverfahren für die Einhaltung aller Datenschutzgrundsätze, insbesondere der Datensicherheit bei der Verarbeitung personenbezogener Daten.

[30] Siehe die thematische Arbeitsgruppe „Cybersicherheit industrieller Steuerungssysteme“ des Europäischen Referenznetzes für den Schutz kritischer Infrastrukturen (ERNCIP): https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

- die Integration der Sicherheitszertifizierung von IKT-Produkten gegebenenfalls in künftige sektorspezifische EU-Legislativvorschläge aufnehmen;
- eine Beteiligung der öffentlichen Verwaltungen anregen, um die Anwendung der Zertifizierung sowie gemeinsamer Spezifikationen bei öffentlichen Aufträgen zu erleichtern;
- die Anwendung einschlägiger Zertifizierungsanforderungen bei öffentlichen und bei kommerziellen Aufträgen beobachten und nach drei Jahren über die Marktlage Bericht erstatten.

### 3.2 Mehr Investitionen in die Cybersicherheit in Europa und gezielte KMU-Förderung

Obwohl es eine intensive Innovationstätigkeit im Cybersicherheitssektor in Europa gibt, fehlt es in der EU nach wie vor an einer ausreichenden Investitionskultur in diesem Bereich. Es gibt zwar viele innovative KMU in diesem Sektor, häufig können sie ihre Geschäftstätigkeit jedoch nicht ausweiten. Einer der Gründe dafür ist, dass den Unternehmen in der Frühphase ihrer Entwicklung leicht zugängliche Finanzmittel fehlen. Auch haben Unternehmen nur begrenzten Zugang zu Risikokapital in Europa und keine ausreichenden Mittel für Marketing, um ihre Sichtbarkeit zu erhöhen bzw. den unterschiedlichen Anforderungen in Bezug auf Normen und die Einhaltung von Rechtsvorschriften gerecht zu werden.

Gleichzeitig ist die Zusammenarbeit zwischen den verschiedenen Akteuren der Cybersicherheit noch unzulänglich, weshalb weitere Anstrengungen mit Blick auf eine wirtschaftliche Konsolidierung und die Entwicklung neuer Wertschöpfungsketten erforderlich sind[31].

Um die Investitionstätigkeit im Bereich der Cybersicherheit in Europa zu steigern und die KMU-Förderung zu verstärken, muss der Zugang zu Finanzmitteln erleichtert werden. Außerdem muss die Entwicklung weltweit wettbewerbsfähiger Cluster und Exzellenzzentren für Cybersicherheit in regionalen Ökosystemen, die das digitale Wachstum begünstigen, unterstützt werden. Diese Unterstützung muss mit der Umsetzung von Strategien zur intelligenten Spezialisierung und anderen EU-Instrumenten verbunden werden, sodass die Cybersicherheitsbranche in Europa sie besser nutzen kann.

Das Konzept der Kommission wird darin bestehen, in Cybersicherheitskreisen ein Höchstmaß an Sensibilisierung für die Finanzierungsmöglichkeiten auf europäischer, nationaler und regionaler Ebene (sowohl in Bezug auf horizontale Instrumente als auch auf spezifische Aufforderungen[32]) zu erreichen, indem bestehende Instrumente und Kanäle, z. B. das *Enterprise Europe Network*, genutzt werden.

Ergänzend zu diesen Bemühungen wird die Kommission gemeinsam mit der Europäischen Investitionsbank (EIB) und dem Europäischen Investitionsfonds (EIF) prüfen, wie der Zugang zu Finanzmitteln erleichtert werden kann. Dies kann in Form von Beteiligungen und beteiligungsähnlichen Investitionen, Darlehen, Bürgschaften für Projekte oder Rückbürgschaften für Finanzmittler erfolgen, z. B. durch die Schaffung einer

[31] Siehe SWD(2016) 216.

[32] Siehe z. B. die sektorübergreifende Aufforderung zur Einreichung von Vorschlägen 2016 im Rahmen der Fazilität „Connecting Europe“ und die COSMO-Aufforderungen 2016 zum Cluster-Internationalisierungsprogramm.

Investitionsplattform für Cybersicherheit im Rahmen des Europäischen Fonds für strategische Investitionen (EFSI)[33].

Die Kommission würde zudem erwägen, gemeinsam mit interessierten Regionen und Mitgliedstaaten eine Cybersicherheitsplattform für intelligente Spezialisierung[34] zu entwickeln. Dies würde helfen, Cybersicherheitsstrategien zu koordinieren und zu planen und eine strategische Zusammenarbeit der interessierten Seiten in regionalen Ökosystemen aufzubauen. Durch dieses Konzept dürfte auch das Potenzial bestehender europäischer Struktur- und Investitionsfonds für den Cybersicherheitssektor besser abgerufen werden können.

Generell wird die Kommission das Konzept der „eingebauten Sicherheit“ (*Security-by-Design*) fördern. Sie wird darauf hinwirken, dass die Anforderungen an die Cybersicherheit durchgehend bei allen bedeutenden Infrastrukturinvestitionen berücksichtigt werden, die eine digitale Komponente beinhalten und mit europäischen Mitteln kofinanziert werden. Dies wird schrittweise über die Einführung einschlägiger Anforderungen für die Auftragsvergabe und bei Programmregeln geschehen.

Die Kommission wird

- die bestehenden Instrumente für die KMU-Förderung nutzen, um die Cybersicherheitskreise für die bestehenden Finanzierungsmechanismen zu sensibilisieren;

- die Nutzung von EU-Werkzeugen und -Instrumenten vorantreiben, um innovative KMU bei der Suche nach Synergien zwischen dem zivilen Segment und dem verteidigungsbezogenen Segment des Cybersicherheitsmarktes zu unterstützen[35];

- mit der EIB und dem EIF prüfen, ob sich der Zugang zu Investitionsmitteln erleichtern lässt, z. B. mittels einer speziellen Investitionsplattform für Cybersicherheit oder andere Werkzeuge;

- eine Cybersicherheitsplattform für intelligente Spezialisierung entwickeln, um Ländern und Regionen, die an Investitionen im Cybersicherheitssektor (RIS3) interessiert sind, zu helfen;

- das Konzept der „eingebauten Sicherheit“ (*Security-by-Design*) bei wichtigen Infrastrukturinvestitionen, die eine digitale Komponente haben und mit EU-Mitteln kofinanziert werden, fördern.

[33] Im Rahmen des Europäischen Fonds für strategische Investitionen können einzelne Projekte entweder direkt oder indirekt über Investitionsplattformen unterstützt werden. Solche Investitionsplattformen können helfen, kleinere Projekte zu finanzieren und Mittel aus verschiedenen Quellen für diversifizierte Investitionen mit geografischem oder thematischem Schwerpunkt zu bündeln.

[34] Siehe Instrumente für intelligente Spezialisierung (RIS3): http://s3platform.jrc.ec.europa.eu/.

[35] So werden das *Enterprise Europe Network* und das europäische Netz der im Verteidigungssektor engagierten Regionen zum Beispiel den Regionen neue Möglichkeiten bieten, die grenzüberschreitende Zusammenarbeit im Bereich der Güter mit doppeltem Verwendungszweck, einschließlich der Cybersicherheit, zu erproben, und den KMU Gelegenheit geben, Investoren zu finden.

## 4. DIE EUROPÄISCHE CYBERSICHERHEITSBRANCHE DURCH INNOVATION FÖRDERN – GRÜNDUNG DER VERTRAGLICHEN ÖFFENTLICH-PRIVATEN PARTNERSCHAFT (CPPP) FÜR CYBERSICHERHEIT

Zur Förderung der Wettbewerbs- und Innovationsfähigkeit der Cybersicherheitsbranche in Europa wird eine vertragliche öffentlich-private Partnerschaft (cPPP) für Cybersicherheit gegründet werden. Die cPPP wird sich Mittel aus der Branche und aus öffentlichen Quellen beschaffen, um Spitzenleistungen in Forschung und Innovation zu erbringen.

Das Ziel der cPPP ist, durch Förderung der Zusammenarbeit im Frühstadium des Forschungs- und Innovationsprozesses gegenseitiges Vertrauen zwischen den Mitgliedstaaten und den Akteuren der Branche zu schaffen. Ferner soll sie helfen, eine Annäherung von Angebot und Nachfrage zu erreichen. Dadurch soll die Branche in die Lage versetzt werden, künftige Anforderungen anhand des Bedarfs der Endnutzer und der Wirtschaftszweige, die wichtige Kunden auf dem Gebiet der Cybersicherheit stellen (z. B. Energie, Gesundheit, Verkehr, Finanzen), zu ermitteln. Ferner wird sie deren Einbeziehung in die Festlegung gemeinsamer Anforderungen für die digitale Sicherheit, den Schutz der Privatsphäre und den Datenschutz in den einzelnen Sektoren fördern.

Die cPPP für Cybersicherheit wird auch zur bestmöglichen Nutzung der verfügbaren Mittel beitragen. Dies wird erstens durch eine bessere Koordinierung mit den Mitgliedstaaten erreicht. Zweitens werden einige wenige technische Prioritäten stärker in den Mittelpunkt gerückt, um der Cybersicherheitsbranche zu helfen, wichtige technische Durchbrüche zu erzielen und die zentralen künftigen Cybersicherheitstechnologien zu beherrschen. In diesem Zusammenhang kann die Entwicklung quelloffener Software und offener Standards zu mehr Vertrauen, Transparenz und zu bahnbrechenden Innovationen beitragen und sollte deshalb bei den Investitionen in diese cPPP ebenfalls berücksichtigt werden.

Den Arbeiten im Rahmen der cPPP für Cybersicherheit werden auch Synergien mit anderen europäischen Projekten zugutekommen, insbesondere wenn diese sich mit Sicherheitsaspekten befassen. Dazu gehören z. B. die Fabriken der Zukunft, energieeffiziente Gebäude, die PPP für 5G und für Big Data[36] sowie andere sektorspezifische PPP[37] und die Initiative zum Internet der Dinge[38]. Des Weiteren soll eine enge Abstimmung mit der europäischen Cloud für offene Wissenschaft und der europäischen Initiative für Hochleistungsrechnen im Bereich der Cyberquantentechnologien (z. B. Innovation im Quantenschlüsselaustausch und Forschung auf dem Gebiet der Quanteninformatik) gefördert werden.

Die cPPP für Cybersicherheit wird im Rahmen von Horizont 2020[39], dem EU-Rahmenprogramm für Forschung und Innovation für den Zeitraum 2014–2020, eingerichtet werden. Sie wird Finanzmittel aus den beiden Programmpfeilern „Führende Rolle bei grundlegenden und industriellen Technologien“ (*Leadership in Enabling and Industrial Technologies* – LEIT-ICT) und „Gesellschaftliche Herausforderung Sichere Gesellschaften“ (*Societal Challenge Secure Societies* – SC7) mobilisieren. Das Gesamtbudget der cPPP beläuft sich auf bis zu 450 Mio. EUR, mit einer Hebelwirkung von 3 auf Seiten der Branche. Das Thema Cybersicherheit sollte auch mit anderen einschlägigen Teilen von Horizont 2020

[36] Die öffentlich-private Partnerschaft für 5G-Infrastruktur und die öffentlich-private Partnerschaft zum Wert von Big Data.
[37] Die öffentlich-privaten Partnerschaften SESAR und Shift2Rail.
[38] Die *Alliance for Internet of Things Innovation* (Allianz für Innovation durch das Internet der Dinge, AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

angegangen und koordiniert werden (z. B. den gesellschaftlichen Herausforderungen Energie, Verkehr und Gesundheit und dem Teil „Exzellenz“ von Horizont 2020). Dies wird zur Erreichung der Ziele der cPPP für Cybersicherheit beitragen. Diese Koordinierung sollte auch bereits vorab in der Phase der Aufstellung sektoraler Strategien stattfinden.

Die cPPP wird in transparenter Weise mit einer offenen und flexiblen Leitungsstruktur umgesetzt, die an das sich rasch entwickelnde Umfeld der Cybersicherheit angepasst ist. Sie wird auch berücksichtigen, dass bei den Mitgliedstaaten Erörterungsbedarf in Bezug darauf besteht, wie sich der technische Wandel auf den sicheren Betrieb nationaler und grenzüberschreitender Infrastrukturen auswirkt. Die Ergebnisse der Partnerschaft müssen außerdem für einen Zeitraum von mehreren Jahren tragfähig sein, damit die Ziele der cPPP erreicht werden können.

Die cPPP wird von der Europäischen Cybersicherheitsorganisation (ECSO) getragen werden, deren Mitglieder die Vielfalt des Cybersicherheitsmarktes in Europa widerspiegeln. Sie wird auch nationale, regionale und lokale öffentliche Verwaltungen, Forschungszentren, Hochschulen und andere beteiligte Kreise einbeziehen.

Die Kommission wird

- mit der Cybersicherheitsbranche eine vertragliche öffentlich-private Partnerschaft für Cybersicherheit gründen, die im dritten Quartal 2016 ihre Arbeit aufnehmen kann;
- im ersten Quartal 2017 die ersten Aufforderungen zur Einreichung von Vorschlägen im Rahmen von Horizont 2020 in Bezug auf die cPPP für Cybersicherheit veröffentlichen;
- für die Koordinierung der cPPP für Cybersicherheit mit den einschlägigen sektoralen Strategien, den Instrumenten von „Horizont 2020“ und sektorspezifischen öffentlich-privaten Partnerschaften sorgen.

## 5. FAZIT

In dieser Mitteilung werden im Einklang mit der EU-Cybersicherheitsstrategie und der Strategie für einen digitalen Binnenmarkt Maßnahmen zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und zur Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche in Europa vorgestellt. Die Kommission ersucht das Europäische Parlament und den Rat, dieses Herangehen zu unterstützen.