Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu dem „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die ‚EU-Cybersicherheitsagentur' (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (‚Rechtsakt zur Cybersicherheit')"

(COM(2017) 477 final/2 2017/0225 (COD))

(2018/C 227/13)

Berichterstatter: **Alberto MAZZOLA**

Mitberichterstatter: **Antonio LONGO**

Befassung	Europäisches Parlament, 23.10.2017
	Rat der Europäischen Union, 25.10.2017
Rechtsgrundlage	Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft
Annahme in der Fachgruppe	5.2.2018
Verabschiedung auf der Plenartagung	14.2.2018
Plenartagung Nr.	532
Ergebnis der Abstimmung	206/1/2
(Ja-Stimmen/Nein-Stimmen/Enthaltungen)	

1. Schlussfolgerungen und Empfehlungen

1.1. Der EWSA ist der Auffassung, dass das von der Kommission vorgeschlagene neue, ständige Mandat der ENISA zur besseren Abwehrfähigkeit der europäischen Systeme beiträgt. Die der ENISA in Verbindung damit zugeteilten vorläufigen Haushaltsmittel und Ressourcen werden jedoch nicht zur Erfüllung ihres Auftrags ausreichen.

1.2. Der EWSA empfiehlt allen Mitgliedstaaten, ein klares und gleichwertiges Pendant zur ENISA zu schaffen, was die meisten von ihnen noch nicht getan haben.

1.3. Der EWSA vertritt darüber hinaus die Ansicht, dass die ENISA beim Ausbau ihrer Kapazitäten den Maßnahmen für die Unterstützung elektronischer Behördendienste Vorrang einräumen sollte ([1]). Die globale und europäische digitale Identität von Personen, Organisationen und Objekten ist ein vordringliches Anliegen; die Verhütung und die Bekämpfung von Identitätsdiebstahl und Online-Betrug sollten ganz oben auf der Tagesordnung stehen.

1.4. Der EWSA empfiehlt, dass die ENISA regelmäßige Berichte über die Cyber-Abwehrbereitschaft der Mitgliedstaaten vorlegen und sich dabei schwerpunktmäßig mit den Sektoren befassen sollte, die im Anhang II der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) genannt werden. Bei einer jährlichen europäischen Cyberübung sollten die Abwehrbereitschaft der Mitgliedstaaten und die Wirksamkeit des europäischen Krisenreaktionsmechanismus getestet und entsprechende Empfehlungen abgeleitet werden.

1.5. Der EWSA unterstützt den Vorschlag, ein Kompetenznetz für Cybersicherheit aufzubauen. Das Cybersicherheits-Kompetenznetz soll durch ein Europäisches Forschungs- und Kompetenzzentrum für Cybersicherheit untermauert werden. Dieses Netzwerk könnte zur europäischen digitalen Souveränität beitragen, indem eine wettbewerbsfähige europäische industrielle Basis für spitzentechnologische Fähigkeiten geschaffen wird, und zwar auf der Grundlage der Arbeiten der vertraglichen öffentlich-privaten Partnerschaft (cPPP), die zu einem dreigliedrigen gemeinsamen Unternehmen weiterentwickelt werden sollte.

1.6. Der Faktor Mensch ist eine der wichtigsten Ursachen für Cyberunfälle. Der EWSA meint, dass solide Internetkompetenz und Cyber-Hygiene durch Aufklärungsarbeit bei Bürgern und Unternehmen gefördert werden müssen. Der EWSA befürwortet EU-zertifizierte Lehrpläne für Sekundarschulen sowie für die Ausbildung von Fachkräften.

([1]) Digitaler Binnenmarkt: Halbzeitüberprüfung.

1.7. Der EWSA ist der Auffassung, dass es in einem europäischen digitalen Binnenmarkt auch eine einheitliche Auslegung der Cybersicherheitsvorschriften und eine gegenseitige Anerkennung zwischen den Mitgliedstaaten geben muss; in einem Zertifizierungsrahmen und in sektorspezifischen Zertifizierungssystemen könnten gemeinsame Mindestanforderungen festgelegt werden. Allerdings müssen sektorspezifische Ansätze in Anpassung an die Funktionsweise der verschiedenen Sektoren vorgesehen werden. Der EWSA ist deshalb der Auffassung, dass die sektorspezifischen EU-Agenturen (EASA, ERA, EMA usw.) in diesen Prozess einbezogen werden müssen. In einigen Fällen sollten sie, im Einvernehmen mit der ENISA zur Sicherstellung von Kohärenz, mit der Erarbeitung von Cybersicherheitssystemen beauftragt werden. Europäische Mindeststandards für die Sicherheit im IT-Bereich sollten in Zusammenarbeit mit CEN, Cenelec und ETSI festgelegt werden.

1.8. Die von der ENISA unterstützte Europäische Gruppe für die Cybersicherheitszertifizierung soll sich aus den nationalen Aufsichtsbehörden für die Zertifizierung, privatwirtschaftlichen Akteuren einschl. Akteuren aus verschiedenen Anwendungsbereichen sowie Akteuren aus der Wissenschaft und der Zivilgesellschaft zusammensetzen.

1.9. Der EWSA vertritt die Auffassung, dass die Agentur im Auftrag der Kommission durch Prüfungen und Kontrollen die Leistung und Entscheidungsfindung der nationalen Aufsichtsbehörden überwachen sollte und dass in der Verordnung Pflichten und Strafen bei Nichteinhaltung von Normen festgelegt werden sollten.

1.10. Der EWSA ist der Auffassung, dass zur Zertifizierung unbedingt auch ein zweckdienliches System der Kennzeichnung gehört, das auch auf Importprodukte anzuwenden ist, um das Vertrauen der Verbraucher zu stärken.

1.11. Europa sollte mehr Mittel für Investitionen mobilisieren und verschiedene EU-Fonds, nationale Mittel und privatwirtschaftliche Investitionen bündeln und auf strategische Ziele im Rahmen einer engen öffentlich-privaten Zusammenarbeit ausrichten, auch durch die Schaffung eines EU-Cybersicherheitsfonds für Innovation und FuE im aktuellen und künftigen Forschungsrahmenprogramm. Zudem sollte Europa einen Fonds für die Umsetzung von Cybersicherheitsmaßnahmen einrichten, mit dem ein neues Finanzierungsfenster in der aktuellen und künftigen Fazilität „Connecting Europe“ sowie im nächsten EFSI 3.0 geöffnet wird.

1.12. Nach Ansicht des EWSA ist ein Mindestsicherheitsstandard für „normale“ IoP-Geräte (IoP = Internet of People) notwendig. Hier wäre die Zertifizierung das Vorgehen der Wahl, um die Sicherheit zu verbessern. Die Sicherheit des Internets der Dinge (IoT) sollte Priorität haben.

2. **Derzeitiger Rahmen für die Cybersicherheit**

2.1. Cybersicherheit ist eine grundlegende Voraussetzung für Wohlstand und nationale Sicherheit wie auch für das Funktionieren unserer Demokratien, Freiheiten und Werte selbst. Cybersicherheit entsteht laut dem Globalen Index für Cybersicherheit der Vereinten Nationen, wenn Gesetze, Organisationen, Kompetenzen, Kooperation und die technische Umsetzung harmonisch und so wirkungsvoll wie möglich miteinander verzahnt werden. Weiterhin wird darauf verwiesen, dass Sicherheitsbelange bei den Überlegungen der Entscheidungsträger eine immer größere Rolle spielen.

2.2. Systemische Sicherheit wird im Zuge der Internetrevolution immer notwendiger. Durch diese Revolution haben sich nicht nur die Beziehungen zwischen Unternehmen und Verbrauchern (business-to-consumer, B2C) in einschlägigen Branchen wie etwa Medien, Einzelhandel und Finanzdienstleistungen grundlegend gewandelt, sondern diese Revolution löst überdies auch gewaltige Veränderungen in Bereichen wie Fertigung, Energie, Landwirtschaft, Verkehr und anderen industriellen Branchen aus, die zusammengenommen beinahe zwei Drittel des globalen BIP ausmachen; auch die Infrastrukturen der Versorgungsunternehmen und der Behördenverkehr der Bürger werden davon erfasst.

2.3. Bei der Strategie für den digitalen Binnenmarkt geht es um die Verbesserung des Zugangs zu Waren, Dienstleistungen und Inhalten, die Schaffung geeigneter rechtlicher Rahmenbedingungen für digitale Netze und Dienstleistungen sowie um die Erschließung des Potenzials einer datengestützten Wirtschaft. Schätzungen zufolge kann die Strategie 415 Mrd. EUR jährlich zur Wirtschaftsleistung der EU beitragen. In Europa werden im Privatsektor bis zum Jahr 2022 voraussichtlich 350 000 Fachkräfte mit entsprechenden Kompetenzen im Bereich Cybersicherheit fehlen ([2]).

([2]) JOIN(2017) 450 final.

2.4. In einer Studie aus dem Jahr 2014 wurde der durch die Cyberkriminalität in der Europäischen Union verursachte wirtschaftliche Schaden auf 0,41 % des BIP der EU beziffert (rund 55 Mrd. EUR im Jahr 2013) ([3]).

2.5. Laut dem Spezial-Eurobarometer 464a zum Cybersicherheitsbewusstsein der Europäer sorgen sich 73 % der Internetnutzer um die Sicherheit online übertragener personenbezogener Daten bei der Nutzung von Websites, während 65 % befürchten, dass diese Daten von Behörden nicht sicher aufbewahrt werden. Die meisten Befragten haben die Sorge, Opfer der diversen Formen von Cyberkriminalität zu werden, vor allem von Malware (69 %), Identitätsdiebstahl (69 %) und Bankkarten- sowie Online-Banking-Betrug (66 %) ([4]).

2.6. Bislang konnte kein Rechtsrahmen mit dem Tempo der digitalen Innovation Schritt halten; durch verschiedene Rechtsakte wird Stück für Stück ein angemessener Rahmen aufgebaut: die Neufassung des Kodex für die elektronische Kommunikation, die Datenschutz-Grundverordnung (GDPR), die Richtlinie über Netz- und Informationssicherheit (NIS-Richtlinie), die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (e-IDAS-Verordnung), den EU-US-Datenschutzschild, den Vorschlag für eine Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln usw.

2.7. Neben der „EU-Cybersicherheitsagentur" ENISA befasst sich noch eine Reihe von Organisationen mit der Cybersicherheit: Europol, das IT-Notfallteam Cert-EU (Computer Emergency Response Team of the European Union), das EU-Zentrum für Informationsgewinnung und -analyse (EU INTCEN), die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), die Informationsaustausch- und -analysezentren (ISAC), die Europäische Cybersicherheitsorganisation (ECSO), die Europäische Verteidigungsagentur (EDA), das Kompetenzzentrum der NATO für kooperativen Schutz vor Computerangriffen, und die VN-Gruppen von Regierungssachverständigen (UN-GGE) im Bereich Information und Telekommunikation im Kontext der internationalen Sicherheit.

2.8. Der Grundsatz der eingebauten Sicherheit ist Voraussetzung für hochwertige Waren und Dienstleistungen, denn intelligente Geräte sind nicht besonders intelligent, wenn sie unsicher sind. Gleiches gilt für intelligente Autos, intelligente Städte und intelligente Krankenhäuser: sie alle sind auf eingebaute Sicherheit von Geräten, Systemen, Architekturen und Dienstleistungen angewiesen.

2.9. Am 19./20. Oktober 2017 forderte der Europäische Rat im Zusammenhang mit dem vorgeschlagenen Reformpaket für die EU „ein gemeinsames Konzept für die Cybersicherheit: Die digitale Welt setzt Vertrauen voraus, und dieses Vertrauen kann nur aufgebaut werden, wenn wir bei allen digitalpolitischen Maßnahmen für eine stärker proaktive konzeptionsintegrierte Sicherheit ('security by design') sorgen, eine adäquate Sicherheitszertifizierung für Produkte und Dienste verfügbar machen und unsere Fähigkeit verbessern, Cyberangriffen vorzubeugen, sie zu verhindern, sie aufzudecken und ihnen entgegenzutreten" ([5]).

2.10. In seiner Entschließung vom 17. Mai 2017 verwies das Europäische Parlament darauf, „dass in der gesamten Wertschöpfungskette für Finanzdienstleistungen durchgängige Sicherheit erforderlich ist; weist darauf hin, dass von Cyberattacken, die gegen unsere Finanzmarktinfrastrukturen, das Internet der Dinge, unsere Währungen und unsere Daten gerichtet sind, große und vielfältige Gefahren ausgehen; […] fordert die Europäischen Aufsichtsbehörden auf, […] die bestehenden operativen Standards regelmäßig zu überprüfen, die für die mit IKT verbundenen Risiken gelten, denen Finanzinstitute ausgesetzt sind; fordert zudem, dass die Europäischen Aufsichtsbehörden Leitlinien zur Überwachung dieser Risiken erstellen […]; hebt hervor, dass das technologische Know-how in den Europäischen Aufsichtsbehörden von großer Bedeutung für die Erfüllung ihrer Aufgaben ist; […]" ([6]).

2.11. Der EWSA hatte bereits mehrfach Gelegenheit, sich mit dieser Thematik auseinanderzusetzen ([7]), u. a. auf der anlässlich des Gipfeltreffens in Tallinn veranstalteten Konferenz zur künftigen Entwicklung der elektronischen Behördendienste ([8]), und er hat die temporäre Studiengruppe Digitale Agenda eingerichtet.

([3]) Arbeitsunterlage der Kommissionsdienststellen — Folgenabschätzung — Begleitdokument zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates, Teil 1/6, S. 21, Brüssel, 13.9.2017 (nur EN).

([4]) Special Eurobarometer 464a — Wave EB87.4 — Europeans' attitudes towards cyber security, September 2017.

([5]) Schlussfolgerungen des Europäischen Rates vom 19. Oktober 2017.

([6]) Entschließung des Europäischen Parlaments vom 17. Mai 2017, A8-0176/2017.

([7]) Digitaler Binnenmarkt: Halbzeitüberprüfung. ABl. C 75 vom 10.3.2017, S. 124, ABl. C 246 vom 28.7.2017, S. 8, ABl. C 345 vom 13.10.2017, S. 52, ABl. C 288 vom 31.8.2017, S. 62, ABl. C 271 vom 19.9.2013, S 133.

([8]) EWSA-Pressemitteilung Nr. 31/2017 — Civil Society debates E-government and cybersecurity with incoming Estonian Presidency: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incomingestonian-Presidency.

3. **Die Vorschläge der Kommission**

3.1. Das Paket zur Cybersicherheit umfasst eine gemeinsame Mitteilung zur Überprüfung der bisherigen EU-Strategie für Cybersicherheit (2013) sowie einen Rechtsakt zur Cybersicherheit, in dessen Mittelpunkt das neue Mandat der ENISA steht und ein Zertifizierungsrahmen vorgeschlagen wird.

3.2. Diese Strategie umfasst drei große Maßnahmenbereiche: Abwehrfähigkeit, Abschreckung und internationale Zusammenarbeit. Bei den Abschreckungsmaßnahmen geht es in erster Linie um Cyberkriminalität und u. a. um die Anwendung des Übereinkommens von Budapest; bei der internationalen Zusammenarbeit stehen Cyberabwehr, Cyberdiplomatie und die Zusammenarbeit mit der NATO im Vordergrund.

3.3. Zu den neuen Initiativen, die in dem Vorschlag vorgesehen sind, gehören:

— der Aufbau einer schlagkräftigeren EU-Agentur für Cyber-Sicherheit;

— die Einführung eines EU-weiten Zertifizierungssystems für Cybersicherheit;

— die rasche Umsetzung der NIS-Richtlinie.

3.4. Im Bereich Abwehrfähigkeit werden Maßnahmen rund um die Cybersicherheit vorgeschlagen, insbesondere in Bezug auf Marktprobleme, NIS-Richtlinie, die rasche Reaktion im Notfall, Aufbau von EU-Kompetenz sowie Bildungs- und Schulungsmaßnahmen in den Bereichen Cyberfähigkeiten, Cyber-Hygiene und Cyberbewusstsein).

3.5. Parallel dazu wird im Rechtsakt zur Cybersicherheit die Schaffung eines EU-Zertifizierungsrahmens für die Cybersicherheit von IKT-Produkten und -Diensten vorgeschlagen.

3.6. Ferner wird im Rechtsakt zur Cybersicherheit auch eine größere Rolle für die ENISA als EU-Agentur für die Cybersicherheit mit einem ständigen Mandat anvisiert. Zusätzlich zu ihren aktuellen Aufgaben soll die ENISA neue, unterstützende und koordinierende Aufgaben wahrnehmen, und zwar im Zusammenhang mit der Förderung der Umsetzung der NIS-Richtlinie, der Cybersicherheitsstrategie der EU, dem EU-Konzeptentwurf, dem Aufbau von Kapazitäten, Wissen und Information, Sensibilisierung, marktbezogenen Aufgaben wie der Unterstützung von Normung und Zertifizierung, Forschung und Innovation, europaweiten Cybersicherheits-Übungen zur Cybersicherheit und der Wahrnehmung der Sekretariatsgeschäfte des CSIRT-Netzes (Netz der Computer-Notfallteams).

4. **Allgemeine Bemerkungen — Übersicht**

4.1. ***Kontext: Abwehrfähigkeit***

4.1.1. *Binnenmarkt für Cybersicherheit*

Sorgfaltspflicht: Der vorgeschlagene Grundsatz der „Sorgfaltspflicht", der in der Gemeinsamen Mitteilung im Zusammenhang mit dem Einsatz sicherer Lebenszyklusentwicklungsprozesse genannt wird, ist interessant und sollte gemeinsam mit der Industrie in der EU weiterentwickelt werden, um letztlich zu einem übergreifenden Ansatz für Rechtskonformität in der EU zu führen. Bei künftigen Entwicklungen sollte der Grundsatz „standardmäßige Sicherheit" gelten.

Haftung: Die Zertifizierung wird dazu beitragen, im Fall von Streitigkeiten Haftungsfragen einfacher zu lösen.

4.1.2. NIS-Richtlinie: Energie, Verkehr, Bank- und Finanzwesen, Gesundheit, Wasserversorgung, digitale Infrastruktur, elektronische Behördendienste.

Für den EWSA ist die umfassende und wirksame Umsetzung der NIS-Richtlinie eine Voraussetzung für die Abwehrfähigkeit nationaler kritischer Bereiche.

Der EWSA ist der Ansicht, dass der Austausch von Informationen zwischen öffentlichen und privatwirtschaftlichen Akteuren mithilfe sektorbezogener Informationsaustausch- und -analysezentren (ISAC) verstärkt werden sollte. Es sollte ein geeigneter Mechanismus für den sicheren Austausch vertraulicher Daten innerhalb der ISAC sowie zwischen CSIRT und den ISAC gefunden werden, der auf einer Auswertung/Analyse des derzeit verwendeten Mechanismus beruht.

4.1.3. *Rasche Reaktion im Notfall*

Der „Konzeptentwurf" wäre ein Ansatz, mit dem auf Ebene der Union und der Mitgliedstaaten ein wirksames Verfahren für eine operative Reaktion auf massive Cybersicherheitsvorfälle zur Verfügung gestellt werden könnte. Der EWSA hält die Einbeziehung des Privatsektors für notwendig, und auch die Betreiber wesentlicher Dienste im Rahmen des operativen Reaktionsmechanismus sollten berücksichtigt werden, da sie wertvolle Informationen über Bedrohungen liefern und/oder Unterstützung bei der Erkennung von Bedrohungen und größeren Krisen sowie bei der Reaktion darauf leisten können.

In der Gemeinsamen Mitteilung wird vorgeschlagen, die Mechanismen der EU zur Krisenbewältigung auch auf Cybervorfälle auszuweiten. Der EWSA teilt zwar die Ansicht, dass im Falle eines Cyberangriffs eine gemeinsame Reaktion sowie Solidarität erforderlich sind, doch stellt sich hier die Frage, wie dies angesichts der Tatsache, dass Cyberbedrohungen gewöhnlich nicht vor Landesgrenzen Halt machen, bewerkstelligt werden kann. Instrumente, die im nationalen Notfall zum Einsatz kommen, können im Fall einer lokalen Bedrohung nur bedingt genutzt werden.

4.1.4. *Entwicklung der Kompetenz der EU*

Um die globale Wettbewerbsfähigkeit der EU zu sichern und ein solides technologisches Fundament aufzubauen, muss ein kohärenter, langfristiger, alle Stufen der Cybersicherheitswertschöpfungskette umfassender Rahmen geschaffen werden. In diesem Kontext ist die Förderung der Zusammenarbeit zwischen den regionalen Ökosystemen Europas für den Aufbau einer europäischen Wertschöpfungskette im Bereich der Cybersicherheit wesentlich. Der EWSA begrüßt den Vorschlag, ein Kompetenznetz für Cybersicherheit aufzubauen.

Dieses Netz könnte durch den Aufbau einer wettbewerbsfähigen europäischen industriellen Basis und die Verringerung der Abhängigkeit von Know-how aus Drittländern für spitzentechnologische Fähigkeiten die digitale Souveränität Europas fördern, technische Schulungen, Workshops und selbst Fortbildungen für elementare Cyber-Hygiene für Fachleute und Laien anbieten und auf der Grundlage der von der vertraglichen öffentlich-privaten Partnerschaft geleisteten Arbeit die Entwicklung eines Netzes nationaler öffentlich-privater Organisationen fördern, um den Aufbau eines Marktes in Europa zu unterstützen. „Eine Ausweitung der vertraglichen öffentlich-privaten Partnerschaft sollte dazu führen, dass diese optimiert, an die jeweiligen Bedingungen angepasst und ausgeweitet wird" (Arbeitsprogramm des Dreiervorsitzes Estland-Bulgarien-Österreich zum Thema Cybersicherheit), und zwar durch Errichtung eines dreigliedrigen gemeinsamen Unternehmens, an dem Kommission, Mitgliedstaaten und Firmen beteiligt sind.

Das Netz sollte auf einem wohlüberlegten Governancesystem fußen, um auf europäischer Ebene seine Wirksamkeit entfalten und die vorgeschlagenen Ziele erreichen zu können.

Dem Netz würde auf europäischer Ebene ein Europäisches Forschungs- und Kompetenzzentrum für Cybersicherheit zur Seite stehen, das die nationalen Kompetenzzentren in der gesamten EU miteinander verknüpft. Es wäre nicht nur für die Koordinierung und das Management der Forschung zuständig, wie es bei anderen Gemeinsamen Unternehmen der Fall ist, sondern würde darüber hinaus den Aufbau eines europäischen Ökosystems für Cybersicherheit ermöglichen, durch das die Einführung und Etablierung von EU-Innovationen gefördert würde.

4.2. ***Kontext: Abschreckung***

4.2.1. Die Bekämpfung der Cyberkriminalität gehört zu den wichtigsten Prioritäten auf nationaler und europäischer Ebene und erfordert starkes politisches Engagement. Abschreckungsmaßnahmen sollten auf der Grundlage einer starken Partnerschaft zwischen dem öffentlichen und privaten Sektor durchgeführt werden, um so auf nationaler und europäischer Ebene einen effizienten Informationsaustausch und Aufbau von Fachwissen zu ermöglichen. Die Möglichkeit einer Ausweitung der Tätigkeit von Europol im Bereich der Cyberforensik und -überwachung könnte ins Auge gefasst werden.

4.3. ***Kontext: Internationale Zusammenarbeit***

4.3.1. Der Aufbau und die Aufrechterhaltung einer vertrauensvollen Zusammenarbeit mit Drittstaaten durch Cyberdiplomatie und Unternehmenspartnerschaften ist von großer Bedeutung, um die Fähigkeit Europas zu stärken, großangelegte Cyberangriffe zu verhindern und ihnen vorzubeugen und entgegenzutreten. Europa sollte seine Zusammenarbeit mit den USA, China, Israel, Indien und Japan ausbauen. Durch eine Modernisierung der EU-Ausfuhrkontrollen sollten nicht nur Menschenrechtsverletzungen und der Missbrauch von Technologien gegen die eigene Sicherheit der EU verhindert werden; sie sollte auch gewährleisten, dass die Industrie der EU in Bezug auf Angebote von Drittländern nicht benachteiligt wird. Für Beitrittsländer sollte eine Ad-hoc-Strategie ins Auge gefasst werden, um sie auf den grenzübergreifenden Austausch sensibler Daten vorzubereiten. U. a. könnten sie als Beobachter an einigen Tätigkeiten von ENISA-Mitgliedstaaten teilnehmen. Anhand der Bereitschaft zur Bekämpfung der Cyberkriminalität könnte eine Rangliste und eventuell sogar eine schwarze Liste erstellt werden.

4.3.2. Der EWSA begrüßt die Einführung einer Cyberabwehr in der geplanten zweiten Phase eines möglichen künftigen EU-Kompetenzzentrums für Cybersicherheit. Aus diesem Grund könnte Europa sich in der Zwischenzeit um den Aufbau von Kompetenzen mit doppeltem Verwendungszweck kümmern und unter anderem dafür sorgen, dass der europäische Verteidigungsfonds Fahrt aufnimmt und die bis 2018 geplante Einrichtung einer Plattform zur Aus- und Weiterbildung im Bereich der Cyberabwehr vorangetrieben wird. In Anbetracht des auf beiden Seiten vorhandenen Wissens um Fähigkeiten und Bedrohungen hält der EWSA den Ausbau der Zusammenarbeit zwischen EU und NATO für erforderlich, wobei auch die europäische Industrie die Entwicklungen in der Zusammenarbeit zwischen der EU und der NATO für eine verstärkte Interoperabilität der Cybersicherheitsnormen sowie andere Formen der Zusammenarbeit im Rahmen der EU-Cyberabwehrstrategie aufmerksam verfolgen sollte.

4.4. ***EU-Zertifizierungsrahmen***

4.4.1. Der EWSA ist der Auffassung, dass Europa die Fragmentierung im Bereich der Cybersicherheit durch eine einheitliche Auslegung der Regeln wie auch die gegenseitige Anerkennung zwischen den Mitgliedstaaten nach gemeinsamen Rahmenvorgaben überwinden muss, um den Schutz des digitalen Binnenmarktes zu erleichtern. In einem Zertifizierungsrahmen könnten gemeinsame Anforderungen (gegebenenfalls mit spezifischen Vorschriften auf höherer Ebene) festgelegt werden, sodass Synergien zwischen vertikal integrierten Sektoren entstehen und die derzeitige Fragmentierung verringert wird.

4.4.2. Der EWSA begrüßt die Schaffung eines Cybersicherheitszertifizierungsrahmens sowie von Zertifizierungssystemen für die verschiedenen Sektoren auf der Grundlage geeigneter Voraussetzungen und in Zusammenarbeit mit den wichtigsten Interessenträgern. Die Zeit bis zur Marktreife jedoch und die Zertifizierungskosten sowie die Qualität und Sicherheit sind grundlegende Elemente, die berücksichtigt werden müssen. Zertifizierungssysteme dienen der Verbesserung der Sicherheit im Einklang mit dem aktuellen Bedarf und Bedrohungswissen, wobei diese Systeme flexibel und erweiterbar ausgelegt werden sollten, um Aktualisierungen zu ermöglichen. Allerdings müssen sektorspezifische Ansätze in Anpassung an die Funktionsweise der verschiedenen Sektoren vorgesehen werden. Der EWSA ist deshalb der Auffassung, dass die sektorspezifischen EU-Agenturen (EASA, EBA, ERA, EMA usw.) in diesen Prozess einbezogen werden sollten und in einigen Fällen im Einvernehmen mit der ENISA — zur Vermeidung von Doppelarbeit und zur Sicherstellung von Kohärenz — beauftragt werden sollten, Systeme für die Cybersicherheit zu erarbeiten.

4.4.3. Für den EWSA ist es wichtig, den Zertifizierungsrahmen auf gemeinsam festgelegte und, soweit möglich, international anerkannte europäische Normen für Cybersicherheit und IKT zu gründen. In Anbetracht des Zeitrahmens und der nationalen Vorrechte sollten europäische Mindeststandards für die Sicherheit im IT-Bereich in Zusammenarbeit mit CEN/Cenelec/ETSI festgelegt werden. Fachliche Normen sollten als positiv angesehen werden, sie sollten allerdings nicht rechtlich bindend sein oder den Wettbewerb behindern.

4.4.4. Es liegt klar auf der Hand, dass die verschiedenen Vertrauenswürdigkeitsstufen auf der Grundlage der möglichen Auswirkungen von Bedrohungen mit Verbindlichkeiten verknüpft werden müssen. Durch die Aufnahme eines Dialogs mit Versicherungsgesellschaften könnten wirksame Anforderungen an die Cybersicherheit für die einzelnen Branchen, in denen sie Anwendung finden sollen, festgelegt werden. Nach Ansicht des EWSA sollten Unternehmen, die die Vertrauenswürdigkeitsstufe „hoch" anstreben, mit unterstützenden Maßnahmen und Anreizen gefördert werden, insbesondere wenn es um lebenswichtige Geräte und Systeme geht.

4.4.5. In Anbetracht der seit der Annahme der Richtlinie 85/374/EWG verstrichenen Zeit ([9]) und der aktuellen technologischen Entwicklungen appelliert der EWSA an die Europäische Kommission, zu prüfen, ob nicht einige der in diesem Verordnungsvorschlag dargelegten Szenarien in den Geltungsbereich der Richtlinie aufgenommen werden sollten, um sicherere Produkte mit einem hohen Schutzniveau zu gewährleisten.

4.4.6. Die geplante und von der ENISA unterstützte Europäische Gruppe für die Cybersicherheitszertifizierung sollte sich nach Meinung des EWSA aus den nationalen Aufsichtsbehörden für die Zertifizierung, privatwirtschaftlichen Akteuren und Akteuren aus verschiedenen Anwendungsbereichen zusammensetzen, um die Entwicklung umfassender Zertifizierungssysteme sicherzustellen. Darüber hinaus sollte durch die Ernennung von Sachverständigen eine Zusammenarbeit zwischen dieser Gruppe und Branchenverbänden aus der EU bzw. dem EWR (z. B. vertragliche öffentlich-private Partnerschaften, Banken, Verkehr, Energie, Gewerkschaften usw.) ins Auge gefasst werden. Diese Gruppe sollte in der Lage sein, die Erfolge Europas im Bereich der Zertifizierung (hauptsächlich auf der Grundlage des SOG-IS-Abkommens über die gegenseitige Anerkennung sowie nationaler und geschützter Programme) zu prüfen, und sich dafür einsetzen, die europäischen Wettbewerbsvorteile zu wahren.

([9]) ABl. L 210 vom 7.8.1985, S. 29.

4.4.7. Der EWSA schlägt vor, diese Gruppe von Interessenträgern damit zu beauftragen, gemeinsam mit der Europäischen Kommission Zertifizierungssysteme zu erarbeiten. Die branchenspezifischen Anforderungen sollten ebenfalls durch einvernehmliche Vereinbarungen zwischen den Interessenträgern des öffentlichen und privaten Sektors (Nutzer und Anbieter) festgelegt werden.

4.4.8. Darüber hinaus sollte die Gruppe regelmäßig und unter Berücksichtigung der Erfordernisse der jeweiligen Branche die Zertifizierungssysteme überprüfen und nötigenfalls anpassen.

4.4.9. Der EWSA befürwortet die schrittweise Abschaffung der nationalen Zertifizierungssysteme nach Einführung eines europäischen Systems, wie es in Artikel 49 der Verordnung vorgeschlagen wird. Ein Binnenmarkt kann nicht mit unterschiedlichen und miteinander konkurrierenden nationalen Vorschriften funktionieren. Daher schlägt der EWSA vor, eine Bestandsaufnahme aller nationalen Systeme durchzuführen.

4.4.10. Der EWSA schlägt vor, dass die Europäische Kommission eine Kampagne zur Förderung der Cybersicherheitszertifizierung und -zertifikate in der EU und zur Unterstützung ihrer Anerkennung in allen internationalen Handelsabkommen durchführt.

4.5. ***ENISA***

4.5.1. Der EWSA ist der Auffassung, dass das von der Kommission vorgeschlagene neue ständige Mandat der ENISA maßgeblich dazu beitragen wird, die Abwehrfähigkeit der europäischen Systeme zu verbessern. Die damit einhergehenden vorläufigen Haushaltsmittel und Ressourcen, die der reformierten ENISA zugeteilt werden, reichen jedoch möglicherweise nicht aus, damit die Agentur ihren Auftrag erfüllen kann.

4.5.2. Der EWSA empfiehlt allen Mitgliedstaaten, ein klares und vergleichbares Pendant zur ENISA zu schaffen, was die meisten von ihnen noch nicht getan haben. Ein strukturiertes Programm für die Abordnung nationaler Sachverständiger zur ENISA sollte gefördert werden, um den Austausch bewährter Verfahren zu unterstützen und das Vertrauen zu stärken. Der EWSA empfiehlt ferner, dass die Europäische Kommission dafür sorgen sollte, dass die in den Mitgliedstaaten bewährten Verfahren und wirksamen Maßnahmen erfasst und ausgetauscht werden.

4.5.3. Der EWSA vertritt darüber hinaus die Ansicht, dass die ENISA beim Ausbau ihrer Kapazitäten den Maßnahmen für die Unterstützung elektronischer Behördendienste Vorrang einräumen sollte ([10]). Die globale und EU-weite digitale Identität für Personen, Organisationen, Unternehmen und Objekte ist von zentraler Bedeutung, und die Verhütung und Bekämpfung von Identitätsdiebstahl und Online-Betrug sowie die Bekämpfung des Diebstahls von gewerblichem geistigen Eigentum sollten ganz oben auf der Tagesordnung stehen.

4.5.4. Die ENISA sollte ferner regelmäßige Berichte über die Cyber-Abwehrbereitschaft der Mitgliedstaaten vorlegen und sich dabei schwerpunktmäßig mit den Sektoren befassen, die im Anhang II der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) genannt werden. Im Rahmen einer jährlichen europäischen Cyberübung sollten die Abwehrbereitschaft der Mitgliedstaaten und die Wirksamkeit des europäischen Krisenreaktionsmechanismus getestet und entsprechende Empfehlungen abgeleitet werden.

4.5.5. Der EWSA ist besorgt darüber, dass die Mittel für eine operative Zusammenarbeit, u. a. im Rahmen des CSIRT-Netzes, nicht ausreichen werden.

4.5.6. Mit Blick auf die marktbezogenen Aspekte vertritt der EWSA die Ansicht, dass eine intensivere Zusammenarbeit mit den Mitgliedstaaten und die Schaffung eines formalen Netzes der Agenturen für Cybersicherheit dazu beitragen würden, die Zusammenarbeit zwischen den Interessenträgern zu verbessern. ([11]) Die Zeit bis zur Marktreife ist sehr kurz, und es ist ausgesprochen wichtig für die Unternehmen in der EU, auf diesem Gebiet konkurrieren zu können, weshalb die ENISA in der Lage sein muss, dementsprechend zu reagieren. Der EWSA ist der Ansicht, die ENISA könnte, wie andere Agenturen der EU auch, künftig ein Gebühren- und Abgabensystem verwenden. Der EWSA ist besorgt darüber, dass die Zuständigkeitskonkurrenz zwischen der EU und den nationalen Agenturen, wie auf anderen Gebieten bereits geschehen, zu einer Verzögerung der ordnungsgemäßen Schaffung des EU-Regelungsrahmens führen und dem EU-Binnenmarkt schaden könnte.

4.5.7. Er weist darauf hin, dass Aufgaben im Zusammenhang mit Forschung und Innovation sowie internationaler Zusammenarbeit derzeit kaum ins Gewicht fallen.

([10]) Digitaler Binnenmarkt: Halbzeitüberprüfung.
([11]) ABl. C 75 vom 10.3.2017, S. 124.

4.5.8. Die Cybersicherheit sollte in den gemeinsamen Sitzungen der im Bereich Justiz und Inneres tätigen Agenturen regelmäßig erörtert werden. Auch sollten die ENISA und Europol regelmäßig zusammenarbeiten.

4.5.9. Da die Cyberwelt sehr innovativ ist, sollten die Normen sorgfältig abgewägt werden, damit der Innovation, die dynamische Rahmenbedingungen braucht, keine Hindernisse in den Weg gelegt werden. Soweit möglich sollte Aufwärts- und Abwärtskompatibilität gewährleistet werden, um die Bürger, aber auch die Investitionen der Unternehmen, zu schützen.

4.5.10. Angesichts der Bedeutung der nationalen Aufsichtsbehörden für Zertifizierung schlägt der EWSA vor, dass durch diese Verordnung bereits ein formales Netz geschaffen wird, dem alle Behörden angehören sollten, die mit der Lösung grenzübergreifender Fragen beauftragt sind und dabei von der ENISA unterstützt werden. Das Netz könnte zu einem späteren Zeitpunkt zu einer einzigen Agentur zusammengefasst werden.

4.5.11. Vertrauen ist zwar von grundlegender Bedeutung, doch kann die ENISA weder Beschlüsse fassen noch Prüfberichte vorlegen. Der EWSA vertritt die Auffassung, dass die Agentur im Auftrag der Kommission durch Prüfungen und Kontrollen die Leistung und Entscheidungsfindung der nationalen Aufsichtsbehörden überwachen sollte.

4.5.12. Industrie und Verbraucher sollten als Beobachter an den Sitzungen des ENISA-Verwaltungsrats teilnehmen können.

4.6. ***Industrie, KMU, Finanzierung/Investitionen und innovative Geschäftsmodelle***

4.6.1. *Industrie und Investitionen*

Um die globale Wettbewerbsfähigkeit der europäischen Unternehmen auf dem Gebiet der IKT zu erhöhen, müssen Maßnahmen getroffen werden, die auf mehr Wachstum und Beschäftigung in der IKT-Branche einschließlich der KMU ausgerichtet sind.

Europa sollte mehr Investitionen mobilisieren und dazu verschiedene EU-Fonds, nationale Mittel und privatwirtschaftliche Investitionen bündeln und auf strategische Ziele im Rahmen einer engen öffentlich-privaten Zusammenarbeit ausrichten. Die Investitionen in Schlüsselbereichen sollten aufgestockt und durch die Schaffung eines EU-Fonds für Cybersicherheit für Innovation und FuE im aktuellen und künftigen Forschungsrahmenprogramm flankiert werden. Zudem sollte Europa einen Fonds für die Umsetzung von Cybersicherheitsmaßnahmen einrichten, mit dem ein neues Finanzierungsfenster in der aktuellen und künftigen Fazilität „Connecting Europe“ sowie im nächsten EFSI 3.0 geöffnet wird.

Die EU-Mitgliedstaaten sollten durch Anreize dazu angehalten werden, nach Möglichkeit europäische Lösungen zu kaufen und europäische Lieferanten zu wählen, sofern es sie gibt, insbesondere wenn es um sensible Anwendungen geht. Die EU sollte das Wachstum von europäischen Spitzenunternehmen aus der IT- und Hightech-Branche unterstützen, die auf dem globalen Markt wettbewerbsfähig sind.

4.6.2. *KMU*

Aufgrund der Fragmentierung des Marktes muss für mehr Klarheit bezüglich der Kundennachfrage gesorgt werden, um den Markt besser in den Griff zu bekommen. Ohne eine strukturierte Nachfrage können KMU und Unternehmensneugründungen nicht in raschem Tempo wachsen. In diesem Kontext wäre die Errichtung einer europäischen KMU-Plattform für Cybersicherheit begrüßenswert.

Die Cybersicherheitstechnik ist einem schnellen Wandel unterworfen, und KMU können dank ihrer Beweglichkeit die innovativen Lösungen bieten, die erforderlich sind, um wettbewerbsfähig zu bleiben. Im Gegensatz zu Drittländern ist die EU immer noch auf der Suche nach einem passenden Geschäftsmodell für KMU.

Es könnten speziell auf Unternehmensneugründungen und KMU ausgerichtete Maßnahmen konzipiert werden, um einen Beitrag zur Deckung der Kosten für die Zertifizierung zu leisten und ihren großen Schwierigkeiten abzuhelfen, die für ihre technische und wirtschaftliche Entwicklung nötigen Mittel aufzubringen.

4.7. ***Der Faktor Mensch: Verbrauchererziehung und -schutz***

4.7.1. Der EWSA stellt fest, dass der Faktor Mensch als treibende Kraft des digitalen Wandels, sei es als Nutznießer oder als Urheber großer Cybervorfälle, im Vorschlag der Kommission keine angemessene Berücksichtigung findet.

4.7.2. Der Aufbau solider Cyberfähigkeiten, die Verbesserung der Cyber-Hygiene und die Sensibilisierung von Bürgern und Unternehmen sind von großer Bedeutung. Zu diesem Zweck sollten gezielte Investitionen, ausreichend Zeit, um Ausbilder zu schulen, und wirksame Sensibilisierungskampagnen ins Auge gefasst werden. Zur Umsetzung dieser drei Aktionsbereiche ist es erforderlich, nationale und regionale Behörden (die für die Einrichtung und Finanzierung wirksamer Bildungsprogramme zuständig sind) sowie Unternehmen und KMU in einem gemeinsamen Ansatz einzubeziehen.

4.7.3. Es sollte auch die Möglichkeit in Betracht gezogen werden, unter aktiver Beteiligung der ENISA und ihrer nationalen Entsprechungen EU-zertifizierte Lehrpläne für Sekundarschulen und die Ausbildung von Fachkräften zusammenzustellen. Darüber hinaus muss die Gleichstellung der Geschlechter bei der Konzipierung der Bildungsprogramme berücksichtigt werden, um den Beschäftigungsgrad in der Cybersicherheit zu erhöhen.

4.7.4. Der EWSA ist der Auffassung, dass die Zertifizierung ein geeignetes System zur Kennzeichnung von Hardware und Software nach dem Vorbild vieler anderer Produktkategorien (z. B. energieverbrauchende Produkte) umfassen sollte. Diese Maßnahme hätte den dreifachen Vorteil, die Kosten für die Unternehmen zu verringern, die Marktfragmentierung aufgrund der unterschiedlichen Zertifizierungssysteme, die bereits auf nationaler Ebene geschaffen wurden, zu verringern und die Verbraucher verständlicher über die Qualität und Merkmale der gekauften Waren zu informieren. In diesem Zusammenhang ist es wichtig, dass aus Drittländern importierte Produkte den gleichen Zertifizierungs- und Kennzeichnungsverfahren unterliegen. Schließlich ist der EWSA der Auffassung, dass die Schaffung eines Gütesiegels helfen könnte, die Verbraucher und Nutzer unmittelbar über die Zuverlässigkeit erworbener Produkte bzw. die Vertrauenswürdigkeit der Websites aufzuklären, über die sie Käufe getätigt oder an die sie vertrauliche Daten übermittelt haben.

4.7.5. Die ENISA sollte die wichtige Informations- und Sensibilisierungsarbeit auf mehreren Ebenen übernehmen, um das Bewusstsein für den „sicheren" Umgang mit der Digitaltechnik zu schärfen und das Vertrauen der Nutzer in das Internet zu stärken. Zu diesem Zweck sind die Unternehmens- und Verbraucherverbände und andere im Bereich der digitalen Dienste tätige Organisationen einzubeziehen.

4.7.6. Ergänzend zum Rechtsakt zur Cybersicherheit ist es nach Auffassung des EWSA von entscheidender Bedeutung (und wurde bereits in der Stellungnahme INT/828 zum Ausdruck gebracht), dass möglichst bald eine breit angelegte europäische Agenda für die allgemeine und berufliche digitale Bildung auf den Weg gebracht wird, um allen Bürgern die erforderlichen Instrumente an die Hand zu geben und den Übergang so gut wie möglich zu meistern. Der EWSA ist sich zwar der spezifischen Zuständigkeiten der Mitgliedstaaten in diesem Bereich bewusst, spricht sich aber dennoch dafür aus, dass im Rahmen eines solchen Programms, das an den Schulen ansetzen soll, die Kenntnisse der Lehrkräfte erweitert, die Lern- und Lehrpläne an die digitalen Technologien (einschl. E-Learning) angepasst und hochwertige Bildungs- und Ausbildungsgänge für alle Schüler und Studierenden angeboten werden. Seine natürliche Fortsetzung wird dieses Programm im lebenslangen Lernen finden, das dazu dient, die Kompetenzen aller Arbeitnehmer neu auszurichten bzw. aufzufrischen ([12]).

5. **Besondere Bemerkungen**

5.1. ***Zukunftstechnologien und -lösungen: Das Internet der Dinge***

Die Zahl der vernetzten Geräte steigt ständig weiter an und wird die Zahl der auf der Erde lebenden Menschen voraussichtlich um ein Vielfaches übersteigen. Grund dafür sind die Digitalisierung von Komponenten, Systemen und Lösungen sowie verbesserte Internetanbindungen. Dieser Trend eröffnet der Cyberkriminalität neue Möglichkeiten, vor allem, weil die Geräte im Internet der Dinge (IoT) häufig nicht so gut geschützt sind wie herkömmliche Geräte.

Branchenübergreifende europäische Sicherheitsstandards für die Nutzung von IoT-Geräten können den Entwicklungs-, Zeit- und Geldaufwand für alle industriellen Teilnehmer der Wertschöpfungskette der vernetzten Produkte verringern.

Ein Mindestsicherheitsniveau durch Identitäts- und Zugangsmanagement (IAM), Patches und Geräteverwaltung dürfte auch für „normale" IoP-Geräte (IoP = Internet of People) erforderlich sein. Da Zertifizierung das Vorgehen der Wahl ist, um das Sicherheitsniveau zu verbessern, sollte im neuen Ansatz der EU für die Zertifizierung der Schwerpunkt verstärkt auf die Sicherheit des Internets der Dinge gelegt werden.

Brüssel, den 14. Februar 2018.

Der Präsident
des Europäischen Wirtschafts- und Sozialausschusses
Georges DASSIS

([12]) Digitaler Binnenmarkt: Halbzeitüberprüfung.