Europäischer Wirtschafts- und Sozialausschuss

INT/930
Cybersicherheitsstrategie

STELLUNGNAHME

Europäischer Wirtschafts- und Sozialausschuss

Gemeinsame Mitteilung an das Europäische Parlament und den Rat

Die Cybersicherheitsstrategie der EU für die digitale Dekade

[JOIN(2020) 18 final]

Berichterstatter: **Philip VON BROCKDORFF**

Befassung	Europäische Kommission, 21/04/2021
Rechtsgrundlage	Artikel 304 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Binnenmarkt, Produktion, Verbrauch
Annahme in der Fachgruppe	31/03/2021
Verabschiedung im Plenum	27/04/2021
Plenartagung Nr.	560
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	238/0/3

1. Schlussfolgerungen und Empfehlungen

1.1 Der Europäische Wirtschafts- und Sozialausschuss (EWSA) erachtet die vorgeschlagene Strategie als wichtigen Schritt zum Schutz der Regierungen, Bürger und Unternehmen in der gesamten EU vor globalen Cyberbedrohungen und zur Sicherung des Wirtschaftswachstums.

1.2 Nach Ansicht des EWSA sollten müssen öffentliche Unternehmen Zugang zu zusätzlichen Finanzierungsquellen für Investitionen in Cybersicherheitsinfrastrukturen haben, um wirksam auf Krisen wie z. B. eine Pandemie reagieren zu können.

1.3 Der EWSA begrüßt den Vorschlag zum Ausbau eines europaweiten Netzes von Sicherheitseinsatzzentren und befürwortet die Zusammenarbeit der Agentur der Europäischen Union für Cybersicherheit (ENISA) mit allen Interessenträgern, um die mit dem 5G-Ausbau verbundenen Risiken einzudämmen.

1.4 Der EWSA begrüßt ferner den Vorschlag, die Rolle von Europol als Kompetenzzentrum für Cyberkriminalität weiter auszubauen. Er erachtet auch die Zusammenarbeit mit der Multi-Stakeholder-Gemeinschaft und auf internationaler Ebene als wichtig.

1.5 Der EWSA warnt vor der Kompetenzlücke im Bereich Cybersicherheit und empfiehlt die Entwicklung eines EU-Instruments für Karriereentwicklung im Cybersicherheitsbereich, mit dessen Hilfe Interessenten einschlägige berufliche Möglichkeiten entdecken, planen und ausbauen können.

1.6 Der EWSA macht auf das Problem der Desinformation aufmerksam. Die Verbreitung von Desinformation könnte schwerwiegende Folgen haben, weshalb die Verhinderung von Desinformation Teil jeder Cybersicherheitsstrategie sein sollte.

1.7 Der EWSA empfiehlt, dass alle ausländischen Investitionen in strategischen Sektoren in der EU im Einklang mit der Sicherheitspolitik der EU stehen sollten.

1.8 Der EWSA warnt vor den mit Quantencomputern verbundenen Risiken und hält die Migration zu Quantencomputer-resistenten Verfahren bzw. zu einer Post-Quanten-Kryptografie für notwendig.

1.9 Der EWSA empfiehlt, die Cybersicherheitsstrategie der Kommission regelmäßig, mindestens aber alle zwei Jahre zu aktualisieren, um wirksam auf neue Technologien und Risiken reagieren zu können.

1.10 Schließlich hebt der EWSA die Bedeutung des sozialen Dialogs bei der Aufstellung von Cybersicherheitskonzepten hervor, die einen wirksamen Schutz der Endbenutzer bei Telearbeit und allgemeinen Online-Tätigkeiten zum Ziel haben.

2. **Mitteilung der Europäischen Kommission**

2.1 Diese Mitteilung ist ein Bekenntnis der EU zur Gewährleistung eines Online-Umfelds für ihre Bürgerinnen und Bürger, das größtmögliche Freiheit und Sicherheit bietet.

2.2 Zunächst wird die Vision der EU für diesen Bereich dargelegt. Es werden Zuständigkeiten geklärt und Verantwortlichkeiten zugewiesen und spezifische Maßnahmen auf EU-Ebene vorgeschlagen, um für einen starken und wirksamen Schutz zu sorgen, gleichzeitig die Rechte der Bürgerinnen und Bürger zu wahren und so ein sicheres und geschütztes Online-Umfeld sicherzustellen.

2.3 Mit den vorgeschlagenen Maßnahmen werden folgende Ziele verfolgt:

- Gewährleistung der Cyber-Resilienz durch den Ausbau von Kapazitäten, Verbesserung der Abwehrbereitschaft, Zusammenarbeit, Informationsaustausch und Bewusstseinsförderung im Bereich der Netz- und Informationssicherheit im öffentlichen und privaten Sektor sowie auf nationaler und EU-Ebene;
- EU-weit standardisierte Cyberabwehr-Verfahrensabläufe sowie Aufbau einer Datenbank mit einschlägigen Informationen, aus denen Erkenntnisse über Bedrohungen gefährdeter Bereiche oder Branchen abgeleitet werden können;
- erhebliche Eindämmung der Cyberkriminalität durch Erweiterung des Fach- und Sachwissens der für die Ermittlung und Strafverfolgung zuständigen Stellen, durch eine bessere EU-weite Koordinierung zwischen den Strafverfolgungsbehörden und durch Förderung der Zusammenarbeit mit anderen Akteuren;
- EU-weite Einführung von Ausbildungsprogrammen für Experten für Cybersicherheit und Anerkennung der Qualifikationen von Fachleuten mit den erforderlichen Fähigkeiten, um unionsweit ein einheitliches Kompetenzniveau zu erreichen;
- Entwicklung eines EU-Konzepts für die Cyberabwehr und Ausbau der Kapazitäten im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik;
- Förderung der industriellen und technologischen Ressourcen, die erforderlich sind, um vom digitalen Binnenmarkt profitieren zu können. Dies wird zur Entstehung einer europäischen Industrie und eines europäischen Markts für sichere IKT, zu Wachstum und Wettbewerbsfähigkeit der EU-Wirtschaft und zur Erhöhung der öffentlichen und privaten Ausgaben für Forschung und Entwicklung im Bereich Cybersicherheit (FuE) beitragen;
- Stärkung der internationalen Cyberraumpolitik der EU, um die Grundwerte der EU zu fördern, Normen für verantwortungsvolles Verhalten festzulegen, für die Anwendung des geltenden Völkerrechts im Cyberspace einzutreten und Drittländer beim Aufbau von Cybersicherheitskapazitäten zu unterstützen;
- Entwicklung und Einführung eines EU-Sicherheitssiegels für Produkte, Dienstleistungen und Technologien, die die Cybersicherheitsnormen und -anforderungen erfüllen.

2.4 Die vorgeschlagene Strategie umfasst die Gewährleistung der Sicherheit wesentlicher Dienste wie Krankenhäuser, Energienetze und Schienenverkehr sowie der wachsenden Zahl vernetzter Geräte in unseren Wohnungen, Büros und Fabriken durch den Aufbau kollektiver Fähigkeiten,

Cyberangriffe abzuwehren, sowie durch eine Zusammenarbeit mit Partnern in der ganzen Welt im Hinblick auf weltweite Sicherheit und Stabilität im Cyberraum.

2.5 Da Cyberbedrohungen fast immer grenzübergreifend sind und ein Cyberangriff in einem Land mehrere Mitgliedstaaten oder auch die gesamte EU betreffen kann, schlägt die Kommission auch die Einrichtung einer gemeinsamen Cyberstelle mit Zugriff auf die kollektiven Ressourcen und Fachkenntnisse der EU und der Mitgliedstaaten als schlagkräftigste Antwort auf Cyberbedrohungen vor.

2.6 Die für die Strategie erforderlichen 2 Mrd. EUR werden über das Programm „Digitales Europa" und über Horizont Europa bereitgestellt. Hinzu kommen Investitionen der Mitgliedstaaten und der Industrie.

3. Allgemeine Bemerkungen

3.1 Cybersicherheit gilt heutzutage allgemein als wesentliche Voraussetzung für das reibungslose Funktionieren der Institutionen und Agenturen der EU wie auch der Mitgliedstaaten und ihrer Volkswirtschaften. Cybersicherheit ist maßgebend für die Energieinfrastruktur und den Ausbau intelligenter Netze[1] in der EU wie auch die Digitalisierung und Ökologisierung ihrer Volkswirtschaften. Ebenso wichtig ist, dass Cybersicherheit den Schutz und die Wahrung der Grundrechte und -freiheiten der Bürgerinnen und Bürger gewährleistet. Die Wahrung der Rechte und Freiheiten ist umso relevanter, als Cyberangriffe den Bürgerinnen und Bürgern sowie den Haushalten (und auch Unternehmen, Organisationen und Behörden) schaden könnten. So bedrohte der kürzliche Hackerangriff auf ein Krankenhaus in Tournai, Belgien, nicht nur Wirtschaftsgüter, sondern gefährdete Menschenleben, da geplante Operationen verschoben werden mussten[2].

3.2 Laut DIGITALEUROPE[3] stellen Cyberbedrohungen ein großes Hemmnis für die Schaffung von mehr Wohlstand in Europa dar. Die bis Ende 2020 durch Cyberkriminalität verursachten Verluste der Weltwirtschaft werden auf 2,5 Billionen EUR veranschlagt. 74 % aller Unternehmen weltweit dürften 2021 Ziel eines Hackerangriffs werden. Und trotzdem haben nur 32 % der europäischen Unternehmen ein Cybersicherheitskonzept. Cyberbedrohungen erfordern eindeutig und unweigerlich eine koordinierte Reaktion der EU und eine Cybersicherheitsstrategie, mit der sowohl die aktuellen Herausforderungen bewältigt als auch Organisationen und Bürger vor der nächsten Generation von Cyberbedrohungen geschützt werden können. Ganz besonders gilt dies für Behörden, die Unmengen personenbezogener und sensibler Daten verwalten und deshalb geschützt werden müssen. Cyberabwehrfähigkeit und digitale Resilienz sind ferner Voraussetzung für europäische Datensouveränität und die Gewährleistung der Vertraulichkeit von Daten innerhalb der Union. Dadurch wird die Schaffung von mehr Wohlstand in der EU ermöglicht.

---

1 Ein Cyberangriff auf ein intelligentes Netz könnte die Energieversorgung von Verbrauchern und Unternehmen beeinträchtigen.

2 https://www.databreaches.net/chwapi-hospital-hit-by-ransomware-operations-canceled-and-another-city-hit/.

3 https://www.digitaleurope.org/.

3.3 Zu den enormen wirtschaftlichen Verlusten, die Cyberangriffe verursachen können, gehören u. a.:

- Verlust geistigen Eigentums und vertraulicher Geschäftsinformationen;
- Online-Betrug und Finanzkriminalität, häufig infolge des Diebstahls personenbezogener Daten;
- finanzielle Manipulation vermöge gestohlener sensibler Geschäftsinformationen über potenzielle Unternehmenszusammenschlüsse oder Vorabkenntnis von Leistungsberichten börsennotierter Unternehmen;
- Opportunitätskosten, u. a. aufgrund von Produktions- oder Dienstunterbrechungen und Verlust von Vertrauen in Online-Aktivitäten;
- Kosten für die Absicherung der Netzwerke, darunter für den Erwerb einer Cyberversicherung[4] und die Behebung des durch einen Cyberangriff verursachten Schadens;
- Reputations- und Markenschäden und Haftungsrisiken für das angegriffene Unternehmen wie auch vorübergehende negative Auswirkungen auf den Aktienkurs des betroffenen Unternehmens.

3.4 Laut dem jüngsten Bericht des Center for Strategic and International Studies (CSIS) über die wirtschaftlichen Auswirkungen der Cyberkriminalität weist Europa mit 0,84 % des BIP der EU die höchsten damit verbundenen Verluste auf (im Vergleich dazu Nordamerika mit 0,78 %).

3.5 In Anbetracht dieser Sachlage kommt der Vorschlag für eine Strategie, dem eine ausführliche Konsultation der Interessenträger vorausging, zu einem denkbar günstigen Zeitpunkt, zumal Experten davon ausgehen, dass die Zahl der vernetzten Geräte weltweit bis 2025 auf 25 Milliarden ansteigen wird. Ein Viertel dieser Geräte wird sich in Europa befinden.

3.6 Gleichzeitig mit der Ankündigung der Strategie wurde bekannt, dass Computer in US-Regierungsbehörden infolge eines Hackerangriffs auf ein US-amerikanisches Unternehmen, das Software für Netzmanagement und IT-System-Verwaltung für Unternehmen entwickelt, infiltriert worden waren. Von dem Angriff in Form eines manipulierten Softwareupdates, das von tausenden Kunden des betroffenen US-amerikanischen Unternehmens heruntergeladen wurde, waren auch hunderte US-Konzerne betroffen. Dieser Vorfall unterstreicht die Cyberanfälligkeit von Behörden und Regierungen wie auch Unternehmen in allen Bereichen und der Gesellschaft insgesamt.

3.7 Es ist deshalb wenig überraschend, dass Schlüsselbereiche wie Datendienstleister und Cloud-Anbieter, Telekommunikation, IT-Systeme von Regierungen und das verarbeitende Gewerbe in die Strategie einbezogen werden. Weitere ernste Gefährdungen der Cybersicherheit könnten sich im Zusammenhang mit Kontaktverfolgungs-Apps ergeben, wie sie bspw. im Zusammenhang mit COVID-19 eingesetzt werden. Es liegt auf der Hand, dass sichere

[4] Allerdings stoßen Cyberversicherungen an Grenzen. Im Zuge der COVID-19-Krise ist deutlich geworden, dass die Cyberversicherbarkeit durch Risikohäufung erschwert wird. Neueren Untersuchungen von AON zufolge machen Versicherungskosten nur einen geringen Teil (5 %) der Kosten für Cyber-Abwehrbereitschaft aus. Cybersicherheitsprüfungen und Ausbildungsmaßnahmen schlagen demnach mehr zu Buche.

Kontaktverfolgungs-Apps dazu beitragen, das öffentliche Vertrauen in den Schutz persönlicher Daten im Rahmen von notwendigen Pandemiebekämpfungsmaßnahmen zu stärken.

3.8 Die COVID-19-Pandemie hat zu einer beschleunigten Veränderung der Arbeitsmuster geführt. 2020 sind 40 % der Arbeitnehmer in der EU zur Telearbeit übergegangen[5]. Indes hatten rund 40 % der Nutzerinnen und Nutzer in der EU 2020 Sicherheitsprobleme, und mehr als 12 % der Unternehmen waren von Cyberangriffen betroffen.

4. Besondere Bemerkungen

4.1 Der EWSA erachtet die vorgeschlagene Strategie als Schritt in die richtige Richtung, um Regierungen, Bürger und Unternehmen in der gesamten EU vor globalen Cyberbedrohungen zu schützen, Maßstäbe im Cyberraum zu setzen und gleichzeitig sicherzustellen, dass die Vorteile des Internets und der Technologienutzung allen zugutekommen.

4.2 Der EWSA sieht in der Cybersicherheit eine wesentliche Voraussetzung für die Sicherstellung der Wirtschaftstätigkeit und die Förderung des Wirtschaftswachstums sowie für die Gewährleistung des Vertrauens der Nutzer in Online-Aktivitäten. Auch er hält es für erforderlich, durch beherzte Maßnahmen dafür zu sorgen, dass die Menschen in Europa auf sichere Weise von Innovation, Konnektivität und Automatisierung profitieren können.

4.3 Der EWSA räumt ein, dass die Wirtschaftssektoren der EU zunehmend von der Informations- und Kommunikationstechnik sowie auch voneinander abhängig sind. Auch die Nutzung von im Internet der Dinge vernetzten Geräten durch Verbraucher und Unternehmen sowie in industriellen Umgebungen, bspw. der Fertigungsindustrie, hat sich enorm ausgeweitet, und FinTech und RegTech gehören inzwischen zur Normalität. Der 5G-Ausbau schreitet rascher voran, und in jüngster Zeit hat die COVID-19-Krise die Digitalisierung zahlreicher Unternehmen und Behörden, die praktisch über Nacht auf Telearbeit umstellen mussten, und damit die Nutzung Cloud-gestützter Dienste vorangetrieben. Derartige Entwicklungen erfordern eine wirksame, zeitnahe und inklusive Reaktionsfähigkeit im Bereich Cybersicherheit.

4.4 Diese Veränderungen haben das Risiko für Behörden und die Industrie erhöht. Der EWSA begrüßt deshalb die neue Strategie mitsamt den Vorschlägen zur Verbesserung der Cyber-Resilienz innerhalb und außerhalb der EU. Obwohl öffentliche Unternehmen EU-Mittel im Rahmen der verschiedenen Programme zur Förderung von Investitionen in diesem Bereich in Anspruch nehmen können (z. B. Horizont 2020/Horizont Europa), sind nach Ansicht des EWSA für öffentliche und gemischtwirtschaftliche Unternehmen möglicherweise weitere Finanzierungsmöglichkeiten für Investitionen in eine angemessene Cybersicherheitsinfrastruktur erforderlich, um die Versorgungssicherheit für die Bürgerinnen und Bürger insbesondere in Krisenzeiten (z. B. während einer Pandemie) sicherzustellen.

5 Eurofound (2020), Leben, Arbeiten und COVID-19, Reihe COVID-19, Amt für Veröffentlichungen der Europäischen Union, Luxemburg.

4.5 Der Vorschlag der Europäischen Kommission zum Ausbau eines europaweiten Netzes von Sicherheitseinsatzzentren, das mit verstärkter Unterstützung durch künstliche Intelligenz (KI) und maschinelles Lernen zur verbesserten Entdeckung von Bedrohungen und Vorfällen sowie zu einer rascheren Analyse und Reaktion beitragen soll, ist relevant und zeitgerecht. Der EWSA ist sich darüber im Klaren, dass es aufgrund der hohen Zahl täglicher Warnmeldungen, die bei den Sicherheitsteams eingehen, und des allgemeinen Fachkräftemangels immer schwieriger wird, Cyberangriffe manuell zu verhindern. Deshalb ist eine Automatisierung der Sicherheitseinsatzzentren unweigerlich notwendig.

4.6 Der EWSA begrüßt die Ziele und Maßnahmen im Bereich der 5G-Sicherheit als unverzichtbare Voraussetzung für die Eindämmung neuer Risiken, die sich aus der größeren Angriffsfläche der 5G-Netzinfrastrukturen ergeben. Insbesondere befürwortet er die an die Agentur der Europäischen Union für Cybersicherheit (ENISA) und die Mitgliedstaaten gerichtete Aufforderung, mit allen Interessenträgern zusammenzuarbeiten, um die neuen 5G-Sicherheitstechnologien und -Fähigkeiten sowie Bedrohungen besser zu verstehen. Der Strategie liegt offenkundig auch die Erkenntnis zugrunde, dass die bei 5G eingesetzten neuen Technologien wie Netzwerkvirtualisierung, Network Slicing und Edge Computing besondere Risiken aufweisen, die zusätzliche Sicherheitsmaßnahmen erfordern.

4.7 Der EWSA begrüßt ferner den Vorschlag, die Rolle von Europol als Kompetenzzentrum für Cyberkriminalität weiter auszubauen, um die nationalen Strafverfolgungsbehörden zu unterstützen, sowie die geplante Stärkung der Finanzausstattung und des Mandats des CERT-EU. Beide Stellen leisten eine wesentliche Unterstützung für Cybersicherheitsmaßnahmen in der gesamten EU, die zweifellos zur Verbesserung der Cybersicherheit der EU-Institutionen und -Agenturen u. a. m. beitragen werden.

4.8 Der EWSA heißt gut, dass ein Schwerpunkt der Strategie auf die Zusammenarbeit der EU mit anderen Ländern gelegt wird, bspw. über Cyberdiplomatie in den internationalen Beziehungen, verstärkte bilaterale Dialoge mit Drittländern und den Aufbau von Cyberkapazitäten in Drittländern. Bedrohungen der Cybersicherheit sind globaler Natur und treten nicht nur regional begrenzt auf, weshalb wirksame Gegenmaßnahmen ebenfalls global ausgelegt sein müssen.

4.9 Der EWSA nimmt den hohen Stellenwert zur Kenntnis, der dem Dialog und der Zusammenarbeit innerhalb der Multi-Stakeholder-Gemeinschaft, insbesondere durch einen regelmäßigen Austausch mit dem privaten und dem öffentlichen Sektor, den Sozialpartnern und der Wissenschaft, eingeräumt wird. Er begrüßt diesen Ansatz und erachtet ihn als wesentlich, um die in der Strategie unterbreiteten Vorschläge weiterzuentwickeln und wichtigen Trends, etwa der Sicherheitsproblematik in Verbindung mit Telearbeit, Rechnung zu tragen. Alle relevanten Interessenträger sollten fortwährend eingebunden werden, denn Cyberkriminelle setzen immer ausgefeiltere Techniken ein.

4.10 Der EWSA befürwortet, dass der generellen Entwicklung der erforderlichen Cyberabwehrfähigkeiten große Bedeutung beigemessen wird. Für die meisten europäischen Unternehmen und insbesondere die KMU wird indes die Abwehr von Cybersicherheitsbedrohungen nach wie vor ungemein durch zunehmende Kompetenzlücken erschwert. Nach Meinung des EWSA kann diese Kompetenzlücke nur durch ein EU-Instrument

für Karriereentwicklung im Cybersicherheitsbereich geschlossen werden, das es Interessenten ermöglicht, durch den Zugang zu den Kenntnissen, Kompetenzen und Fähigkeiten, die für den Einstieg in oder Umstieg auf einen Cybersicherheitsberuf oder für eine entsprechende Karriereplanung erforderlich sind, berufliche Möglichkeiten im Bereich Cybersicherheit zu entdecken, zu planen und auszubauen. Dieses Instrument sollte auch spezifische Programme zu Barrierefreiheit und Vielfalt im Cybersicherheitsraum umfassen. Die Unterstützung eines solchen EU-Instruments für Karriereentwicklung im Cybersicherheitsbereich durch die Berufsbildungseinrichtungen ist unverzichtbar. Die EU sollte sich zunehmend um gemeinsame Forschungsinitiativen (innerhalb der EU und mit Drittländern) bemühen, um kompetente und qualifizierte Cybersicherheitsfachkräfte auszubilden. Dabei sind Inklusionsgrundsätze zu berücksichtigen, denn die technologische Entwicklung ermöglicht die Gestaltung inklusiverer Arbeitsplätze und die Schaffung einer inklusiveren Gesellschaft. Schließlich sollte praktisch erwogen werden, Studiengänge im Bereich Cybersicherheit durch die Vergabe von Stipendien für entsprechende Bachelor-, Master- und Graduiertenabschlüsse zu fördern; als Gegenleistung wäre nach Studienabschluss eine Tätigkeit bei einer EU-Institution oder -Agentur oder einer Behörde in der EU zu absolvieren.

4.11 Der EWSA stellt fest, dass der Zusammenhang zwischen Cybersicherheit und Desinformation in der Cybersicherheitsstrategie nicht angesprochen wird, und verweist auf die von der Fachabteilung Bürgerrechte und konstitutionelle Angelegenheiten des Europäischen Parlaments in Auftrag gegebene Studie zu diesem Thema[6]. Im Zeitalter der Digitalisierung könnte die Verbreitung von Desinformation im Cyberraum schwerwiegende Folgen haben. Durch grenzübergreifende Angriffe auf Informationszentren, staatliche oder europäische Institutionen können Falschinformationen verbreitet und dadurch das Vertrauen in Behörden und Institutionen untergraben werden. Deshalb ist es wichtig, in jeder Cybersicherheitsstrategie einen Schwerpunkt auf die Verhinderung von Desinformation zu legen.

4.12 Der EWSA gibt ferner zu bedenken, dass ausländische Investitionen in strategischen Sektoren, der Erwerb kritischer Anlagen, Technologien und Infrastrukturen in der Union sowie die Versorgung mit kritischen Ausrüstungen ebenfalls eine Gefahr für die Sicherheit der EU darstellen können. Er empfiehlt in diesem Zusammenhang und im Einklang mit den vergaberechtlichen Bestimmungen, bei der Auftragsvergabe Sicherheitserwägungen stärker einzubeziehen.

4.13 Des Weiteren weist der EWSA darauf hin, dass Quantencomputer, die in spätestens zehn Jahren öffentlich verfügbar sein werden, eine Bedrohung für die Sicherheit der gängigen Verschlüsselungssoftware und -systeme darstellen. Die deshalb notwendige Migration zu Quantencomputer-resistenten Verfahren bzw. zu einer Post-Quanten-Kryptografie ist Gegenstand verschiedener globaler Standardisierungsinitiativen, u. a. des „NIST Post-Quantum Cryptography Standardization Process“ der US-amerikanischen Behörde für Standardisierungsprozesse, der „Quantum Safe Cryptography (QSC) Working Group“ des Europäischen Instituts für Telekommunikationsnormen (ETSI) und des Post-Quanten-Kryptografie-Wettbewerbs der chinesischen Vereinigung für Kryptologie-Forschung (Chinese Association for Cryptologic Research).

6 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

4.14 Der EWSA empfiehlt eine Überarbeitung der nationalen Cybersicherheitsstrategien, um die Übereinstimmung mit der Strategie der Kommission zu gewährleisten und sicherzustellen, dass sich Entscheidungen der Mitgliedstaaten mit den in der Strategie der Kommission enthaltenen Vorschlägen decken. Die EU-Strategie und die nationalen Strategien sollten aufeinander abgestimmt werden, um jetzt und künftig eine wirksame Abwehr von Cyberbedrohungen zu ermöglichen.

4.15 Da sich künftige Risiken kaum absehen lassen, empfiehlt der EWSA eingedenk seiner Bemerkungen in Ziffer 4.13, die Cybersicherheitsstrategie der Kommission regelmäßig, mindestens aber alle zwei Jahre zu aktualisieren, um wirksam auf neue Technologien und Risiken reagieren zu können. Wie bereits erwähnt, werden auch die Einbindung der Interessenträger und die Spitzenforschung für die Aktualisierung der Cybersicherheitsstrategien von entscheidender Bedeutung sein.

Brüssel, den 27. April 2021

Christa SCHWENG
Präsidentin des Europäischen Wirtschafts- und Sozialausschusses