Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu der „Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: EU-Cyberabwehrpolitik“

(Initiativstellungnahme)

(2023/C 293/04)

Berichterstatter: **Anastasis YIAPANIS**

Ko-Berichterstatter: **Alberto MAZZOLA**

Beschluss des Plenums	20.9.2022
Rechtsgrundlage	Artikel 52 Absatz 2 der Geschäftsordnung
	Initiativstellungnahme
Zuständiges Arbeitsorgan	Beratende Kommission für den industriellen Wandel (CCMI)
Annahme in der CCMI	27.3.2023
Verabschiedung im Plenum	14.6.2023
Plenartagung Nr.	579
Ergebnis der Abstimmung	
(Ja-Stimmen/Nein-Stimmen/Enthaltungen)	208/1/2

1. **Schlussfolgerungen und Empfehlungen**

1.1. Der Europäische Wirtschafts- und Sozialausschuss (EWSA) unterstützt den Vorschlag für eine EU-Cyberabwehrpolitik, hätte jedoch erwartet, dass der organisierten Zivilgesellschaft eine gewichtigere Rolle bei der Ausarbeitung dieser Vorschläge eingeräumt wird. Der Ausschuss hält es für schwierig, zum jetzigen Zeitpunkt zu beurteilen, ob die in der gemeinsamen Mitteilung skizzierten künftigen Initiativen umgesetzt und dabei die angestrebten Ergebnisse erzielt werden. Er fordert die EU-Organe und die Mitgliedstaaten nachdrücklich auf, die angekündigten Initiativen vorrangig zu behandeln und rasch voranzubringen.

1.2. Der EWSA betont, dass zusätzliche Maßnahmen erforderlich sind, um die Fähigkeit der EU zur Erkennung von Cyberbedrohungen zu verbessern, und fordert, dass die Mittel für Forschung und Entwicklung in die Entwicklung modernster EU-Kapazitäten investiert werden. Die Verzahnung zwischen dem privaten und dem öffentlichen Sektor ist von wesentlicher Bedeutung und darf nicht einseitig sein. Der EWSA hält eine Koordinierung auf EU-Ebene für erforderlich, um die Fragmentierung anzugehen und die Zusammenarbeit und gemeinsame Investitionen zwischen den Mitgliedstaaten sicherzustellen.

1.3. Der EWSA unterstützt die Einrichtung des EU-Koordinierungszentrums für die Cyberabwehr. Er empfiehlt den Mitgliedstaaten, sich zu einer rund um die Uhr einsatzbereiten Sofortreaktion zu verpflichten und die Cyberbereitschaft sowie die Leistungsfähigkeit der EU-Instrumente für die Reaktion auf Cyberkrisen zu prüfen. Dabei sollte der Schwerpunkt sowohl auf den militärischen Fähigkeiten als auch auf den in der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [1] (NIS-2-Richtlinie) genannten kritischen Sektoren liegen. Der Ausschuss unterstützt die Ausweitung des Mandats des Europäischen Kompetenzzentrums für Cybersicherheit zur Förderung der Tätigkeit des EU-Koordinierungszentrums für die Cyberabwehr.

1.4. Zur Stärkung der strategischen Autonomie und Souveränität der Union im Bereich der Cybersicherheit sollte nach Ansicht des EWSA eine dynamische Plattform für Echtzeittests und Informationsaustausch vom Privatsektor entwickelt bzw. übernommen werden, um die derzeitigen Lücken bei den bestehenden Fähigkeiten zu ermitteln. Sie könnte auch für den Austausch bewährter Verfahren, die Meldung von Cybervorfällen und die Erstellung einer EU-Liste aller Cyberkriminellen genutzt werden.

---

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

1.5. Der EWSA hält eine bessere Vorbereitung auf Cyberangriffe gegen kritische Infrastrukturen — wie die russischen Cyberattacken in der Ukraine — für notwendig. Die Verzahnung der zivilen und militärischen Ökosysteme ist entscheidend für ein effizientes Krisenmanagement, für die Interoperabilität sowie zur Vermeidung von Doppelarbeit und -investitionen. Zu diesem Zweck sollten auch simulierte Cyberangriffe eingesetzt werden.

1.6. Nach Auffassung des EWSA sollten Investitionen in die Cyberabwehr vorrangig auf den Schutz der EU-Bürgerinnen und -Bürger sowie kritischer Infrastrukturen ausgerichtet sein. Hierzu gehört auch der Einsatz vertrauenswürdiger Hardware- und Softwareanbieter. Er drängt nachdrücklich auf zeitnahe Aktualisierungen der Prioritäten und Investitionen, die von der EU und den Mitgliedstaaten unter Beteiligung einschlägiger privater Interessenträger vereinbart werden müssen.

1.7. Die EU muss die erforderlichen Kapazitäten bewahren und ausbauen, um ihre digitale Wirtschaft, Gesellschaft, Demokratie und kritischen Technologien zu sichern und wichtige Cybersicherheitsdienste bereitzustellen. Zur Gewährleistung der strategischen Autonomie der EU ist es von entscheidender Bedeutung, die Abhängigkeiten von Drittländern zu verringern. Der EWSA hält es für wesentlich, dass die EU mittelfristig die Autonomie in Bezug auf Schlüsseltechnologien anstrebt. Er spricht sich nachdrücklich dafür aus, dass Forschungs- und Produktionsanlagen von in der EU ansässigen Unternehmen im Rahmen einer auf ein autonomes Cyber-Ökosystem ausgerichteten, angemessenen Industriepolitik der EU eingerichtet werden.

1.8. KMU sollten gezielte Unterstützung und Zugang zu Finanzierungsprogrammen erhalten, die ihre Resilienz gegenüber Cyberangriffen steigern, ebenso wie Hilfe und Schulungs- und Bildungsmöglichkeiten in Bezug auf Cyberrisiken und dem möglichen Schutz davor. Die EU sollte ein Anreizinstrument schaffen, anhand dessen KMU sich schrittweise mit dieser Thematik vertraut machen und ihre Innovationsfähigkeit steigern können.

1.9. Der EWSA unterstützt den Plan zur Einrichtung einer Akademie für Cyberkompetenzen und fordert die Europäische Kommission auf, groß angelegte Aus- und Weiterbildungsprogramme zu koordinieren und finanzieren, an denen alle Mitgliedstaaten beteiligt sind, um Fachkräfte für alle im Bereich der Cyberabwehr tätigen Agenturen und Organisationen sowie für private zivile Netzwerke auszubilden.

1.10. Nach Auffassung des Ausschusses ist die Sensibilisierung der Bürgerinnen und Bürger für die Cybersicherheit entscheidend, um die Gefährdung durch Cyberangriffe zu verringern. Er fordert Lehrpläne für Cybersicherheit und Programme für lebenslanges Lernen, deren Schwerpunkt auf der Verbesserung der Cyberkompetenzen und -kenntnisse liegt. Der EWSA befürwortet es, die Cybersicherheit bei allen künftigen EU-Politikbereichen durchgängig zu berücksichtigen und die breite Öffentlichkeit über Cyberbedrohungen zu informieren.

1.11. Nach Ansicht des EWSA muss der Schwerpunkt einer engen militärischen Zusammenarbeit mit NATO-Verbündeten auf umfassender Koordinierung und Gegenseitigkeit, gemeinsamen FEI-Projekten, dem Austausch bewährter Verfahren, umfangreichen Schulungsprogramme und Simulationen von Cyberangriffen liegen. Ihr Hauptziel muss in der Stärkung der gemeinsamen Reaktionsfähigkeit bestehen.

1.12. Der Ausschuss fordert den Hohen Vertreter auf, die derzeitigen bilateralen Cyberdialoge zu prüfen und zusätzliche Gespräche mit anderen Ländern und einschlägigen internationalen Organisationen aufzunehmen, um einen globalen Rahmen für die Einhaltung des Völkerrechts im Cyberraum zu schaffen. Hierbei kommt es besonders auf Gegenseitigkeit an. Schließlich hält der Ausschuss die EU dank ihres stabilen Fundaments grundlegender demokratischer Freiheiten für prädestiniert, eine führende Rolle in internationalen Debatten über die Zukunft der Cybersicherheit, insbesondere in den Beratungen der Vereinten Nationen, zu übernehmen.

1.13. Die EU sollte jede Art von sozialem Scoring-System gegen die Bürgerinnen und Bürger entschieden ablehnen. Der EWSA stellt klar, dass eine echte Demokratie ohne einen effektiven Schutz personenbezogener Daten nicht existieren kann. Er ist der Ansicht, dass eine verantwortungsvolle und effiziente Datenverwaltung unerlässlich ist, um Hyperkonnektivität zu einem Wettbewerbsvorteil zu machen.

2. **Einleitung und allgemeine Bemerkungen**

2.1. Die digitale Durchdringung der Gesellschaft geht mit einer Vielzahl an Bedrohungen der Cybersicherheit einher, die durch Technologiesprünge möglich werden. In den letzten Jahren sind Cyberangriffe zahlreicher und raffinierter geworden, und sie gefährden die Sicherheit sowohl öffentlicher als auch privater Einrichtungen. Angriffsformen wie etwa Ransomware, Schadsoftware, E-Mail-Angriffe, Datenschutzverletzungen, Desinformation, verteilte DDoS-Attacken (distributed denial-of-service = verteilter Dienstverweigerungsangriff) sind allesamt eine konstante und kontinuierliche Bedrohung der Sicherheit der gesamten EU.

2.2. Der EWSA begrüßt die Gemeinsame Mitteilung über die *EU-Cyberabwehrpolitik* ([2]) und hält nunmehr dringende und koordinierte Maßnahmen auf EU-Ebene für erforderlich, die sowohl die zivilen als auch die militärischen Cyberraum-Ökosysteme umfassen und einen angemessenen Investitionsrahmen für Cyberabwehrfähigkeiten gewährleisten. Der Ausschuss bedauert indes, dass die Mitteilung lediglich eine Absichtserklärung und eine Liste künftiger EU-Initiativen ist, die umgesetzt werden sollten. Er kann daher nicht beurteilen, ob diese künftigen Verpflichtungen tatsächlich umgesetzt werden, da die weiteren Verhandlungen zwischen den Mitgesetzgebern das Endergebnis des EU-Aktionsplans für Cybersicherheit beeinflussen werden.

2.3. Der russische Angriff auf das Satellitennetz KA-SAT, der zu einer Störung der Kommunikation zwischen den ukrainischen Streitkräften führte, sowie der jüngste Skandal um Éric Léandri, der von einigen Verteidigungsunternehmen mit Cyberspionage beauftragt wurde, zeigen, dass die Cybersicherheit nunmehr eine der größten Sicherheitsbedrohungen der EU darstellt. Zwar ist die Datenschutz-Grundverordnung (DSGVO) ein solider Rechtsakt der EU und seit mehreren Jahren in Kraft, doch zeigt sich deutlich, dass die zunehmende Menge der in Online-Archiven gespeicherten Daten anfällig für Attacken ist. Das Risiko, dass Dritte die Grenze der Legalität überschreiten, steigt von Tag zu Tag.

2.4. Angesichts des transnationalen Charakters von Cyberangriffen ist eine Koordinierung durch die EU erforderlich, um die derzeitige Fragmentierung zu verringern und die Bereitschaft der Mitgliedstaaten zur Zusammenarbeit und zu gemeinsamen Investitionen zu gewährleisten. Dies ist besonders wichtig, wenn ein Mitgliedstaat ins Visier genommen werden sollte. Dann sollten alle anderen Mitgliedstaaten imstande sein, einzugreifen und ihn unverzüglich zu unterstützen.

3. **Gemeinsames Handeln für eine stärkere Cyberabwehr**

3.1. Der Ausschuss nimmt die angekündigten ehrgeizigen Initiativen zur Kenntnis: Einrichtung eines EU-Koordinierungszentrums für die Cyberabwehr, Entwicklung des Projekts CyDEf-X, Schaffung von Soforteinsatzteams für Cybervorfälle, Entwicklung einer EU-Initiative zur Cybersolidarität und Prüfung der Entwicklung von Systemen für die Zertifizierung der Cybersicherheit von IKT-Produkten, -Diensten und -Verfahren. Der EWSA empfiehlt, dass sich alle Mitgliedstaaten zum Aufbau einer rund um die Uhr einsatzbereiten Sofortbereitschaft verpflichten. Das EU-Koordinierungszentrum sollte an der Bewertung und Ausarbeitung regelmäßiger Berichte über die Cyberbereitschaft der Mitgliedstaaten und die Wirksamkeit des europäischen Mechanismus für die Reaktion auf Cyberkrisen beteiligt sein. Der Schwerpunkt sollte sowohl auf den militärischen Fähigkeiten als auch auf den in der NIS-2-Richtlinie genannten kritischen Bereichen liegen. Jeder Mitgliedstaat sollte über speziell geschulte Fachleute verfügen, die bei Cybervorfällen eingreifen können und ihre Einsatzfähigkeit in anderen Mitgliedstaaten regelmäßig testen.

3.2. Die Mitteilung umfasst eine lange Liste schrittweiser Verbesserungen. Allerdings hätte der EWSA gern auch einen expliziten Fahrplan für die Umsetzung dieser Initiativen mit klaren Entscheidungsstrukturen und genauen Fristen für Einreichung und Annahme gesehen. Darüber hinaus hätte der Ausschuss erwartet, dass der organisierten Zivilgesellschaft eine gewichtigere Rolle bei der Ausarbeitung dieser Vorschläge eingeräumt wird.

3.3. Nach Ansicht des EWSA sollten die Mitgliedstaaten ihre internen Kapazitäten zur Abwehr von Cyberbedrohungen stärken und zugleich Kooperationsprojekte durchführen sowie Informationen und bewährte Verfahren mit ihren Amtskollegen in anderen Mitgliedstaaten austauschen. Sämtliche Mitgliedstaaten müssen rasch in die Cyberabwehrfähigkeiten, den beschleunigten Technologieeinsatz ([3]) und die gemeinsame Abwehrbereitschaft investieren, um Cyberangriffe zur erkennen, zu überwinden und abzuwehren. Zur Unterstützung der Autonomie der EU im Bereich der Cybersicherheit sollte nach Ansicht des Ausschusses eine dynamische Plattform für Tests und Informationsaustausch in Echtzeit entwickelt oder vom Privatsektor übernommen werden, um die derzeitigen Lücken aufzudecken.

3.4. Der EWSA teilt die Auffassung, dass militärische Cyberraum-Operationen zum gegenwärtigen Zeitpunkt ausschließlich in der Zuständigkeit der Mitgliedstaaten verbleiben sollten; der Ausschuss unterstützt die angekündigte Zusammenarbeit zwischen den militärischen IT-Notfallteams der EU (milCERT), den Computer-Notfallteams (Computer Security Incident Response Teams, CSIRT) und dem IT-Notfallteam der EU-OESS (CERT-EU).

3.5. Mit der kürzlich angenommenen NIS2-Richtlinie und der Richtlinie über die Resilienz kritischer Einrichtungen (CER) ([4]) wurden bereits spezifische nationale und sektorale Aufgaben für den EU-Rahmen zur Cyberabwehr eingeführt. Es bedarf weiterer Maßnahmen zur Verbesserung der kollektiven Aufdeckungsfähigkeit der EU, und der EWSA dringt auf FuE-Investitionen zur Entwicklung modernster EU-Kapazitäten.

([2]) Mitteilung der Kommission — EU-Cyberabwehrpolitik.
([3]) Wie die NATO-Initiative DIANA (Innovation Accelerator for the North Atlantic).
([4]) CER-Richtlinie.

4. **Sicherung des Verteidigungsökosystems der EU**

4.1. Nach Auffassung des EWSA haben die inhärenten Komplexitäten und die rasante technische Entwicklung das Verteidigungsökosystem verändert. Mittlerweile ist die Cybersicherheit zu einer Angelegenheit geworden, die für den militärischen und den zivilen Sektor sowie für die Bürgerinnen und Bürger der EU gleichermaßen relevant ist. Die Zusammenarbeit zwischen zivilen und militärischen Ökosystemen ist heute wichtiger denn je und dürfte Vorteile im Hinblick auf ein wirksameres Krisenmanagement sowie kontinuierliche Fortschritte und Interoperabilität mit sich bringen. Auch die Wiederholung oder Vervielfachung derselben Anstrengungen und Investitionen ließe sich so vermeiden. Die Mitgliedstaaten sollten nationale Stresstests für kritische Infrastrukturen durchführen, um die Resilienz gegenüber künftigen Cyberangriffen zu bewerten und zu erhöhen.

4.2. Nach Auffassung des EWSA müssen Investitionen in die Cyberabwehr vorrangig auf den Schutz der EU-Bürgerinnen und -Bürger sowie kritischer Infrastrukturen ausgerichtet sein. Angesichts des rasanten digitalen Wandels und der raschen Weiterentwicklung der Bedrohungslage fordert der EWSA nachdrücklich, dass die EU und die Mitgliedstaaten zeitnahe Aktualisierungen der Prioritäten und Investitionen vereinbaren und dabei einschlägige private Interessenträger umfassend konsultieren. Geräte des Internets der Dinge (IoT) bieten oftmals mehr Angriffsfläche als herkömmliche Geräte, und der EWSA fordert, dass über Plattformen für Identitäts- und Zugriffsmanagement ein Mindestmaß an Sicherheit gewährleistet wird. Da Zertifizierung eine wichtige Methode für ein höheres Sicherheitsniveau ist, fordert der Ausschuss zudem, dass im neuen EU-Zertifizierungskonzept ein stärkerer Fokus auf die Sicherheit des Internets der Dinge gelegt wird.

4.3. Die EU muss ihre Resilienz gegenüber Cyberangriffen stärken und eine wirksame Cyber-Abschreckung schaffen. Kritische zivile Infrastrukturen müssen vor jeglichen Cyberangriffen, auch durch Verteidigungssysteme der EU, geschützt werden. Nach Ansicht des Ausschusses liegt es im strategischen Interesse der EU, dass sie die Wahrung und Weiterentwicklung wesentlicher Fähigkeiten gewährleistet, die zur Sicherung ihrer digitalen Wirtschaft, Gesellschaft und Demokratie von entscheidend sind. Die vollständige digitale Souveränität ist die einzige Möglichkeit, kritische Technologien zu schützen und zentrale Cybersicherheitsdienste effektiv bereitzustellen. Die Verringerung der Abhängigkeiten von Drittländern ist auch für die strategische Autonomie der EU von entscheidender Bedeutung. Nach Auffassung des EWSA sollten sektorspezifische EU-Agenturen (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA usw.) daran beteiligt werden und Orientierungshilfen für die Entwicklung von Cybersicherheitsprogrammen beisteuern.

4.4. Die COVID-19-Pandemie hat den digitalen Wandel beschleunigt. Herkömmliche Arbeitsplätze wurden in Hybrid- und/oder Homeoffice-Arbeitsplätze umgewandelt, wodurch neue Arbeitsbeziehungen und Erwartungen sowie eine neue Klasse digitaler Nomaden entstanden sind, die immer zahlreicher werden. Der EWSA nimmt die raschen Veränderungen auf dem Arbeitsmarkt zur Kenntnis, die Unternehmen zur Einführung einer „Zero-Trust-Architektur" durch Lösungen mit IAM (Identity and Access Management) und PAM (Privileged Access Management) veranlasst haben. Nach Ansicht des Ausschusses bringt ein derartiges Management von Unternehmensressourcen neue Lösungen im Bereich Cyberbedrohungen hervor. Er ist der Auffassung, dass der Privatsektor bei der Stärkung des Sicherheitsniveaus seiner innovativen digitalen Lösungen unterstützt werden muss.

4.5. Der EWSA ist eigentlich enttäuscht über die Aussage der Kommission, dass in „Zusammenarbeit mit den Mitgliedstaaten ein Umsetzungsplan erstellt werden [könnte]", denn aus seiner Sicht ist solch ein Umsetzungsplan ein Muss. Seiner Ansicht nach sollte er gemeinsam mit den Mitgliedstaaten ausgearbeitet und so bald wie möglich umgesetzt werden. Der Ausschuss hält die Herangehensweise der Kommission für zu zaghaft. Er fordert die EU-Institutionen und die Mitgliedstaaten nachdrücklich auf, den Weg für rasche Fortschritte bei den angekündigten Initiativen zu ebnen.

5. **Investitionen in Cyberabwehrfähigkeiten**

5.1. Die technische Entwicklung schreitet rasch voran, weshalb Kriege mittlerweile nicht mehr nur zu Lande, zu Wasser, in der Luft und im Weltraum geführt werden, sondern seit neuestem auch im Cyberraum. Dadurch sind breite Betätigungsmöglichkeiten für böswillige Cyberakteure entstanden — von unabhängigen Hackern bis hin zu professionellen Kriminellen und sogar staatlichen Akteuren.

5.2. Investitionen in Forschung und Entwicklung sind von entscheidender Bedeutung, und der EWSA begrüßt die bestehenden zweckgebundenen Mittel in dem Programm „Digitales Europa", im Europäischen Verteidigungsfonds, in Horizont Europa und in nationalen Aufbauprogrammen. Allerdings würde der Ausschuss mehr transnationale Vorhaben mit Schwerpunkt auf der Zusammenarbeit und Interoperabilität zwischen den Cyberabwehrsystemen aller Mitgliedstaaten sowie mehr Synergien zwischen den Finanzierungsinstrumenten, insbesondere für innovative KMU, begrüßen.

5.3. Wie bereits 2020 in der EU-Cybersicherheitsstrategie angekündigt, stellt der Ausschuss fest, dass die Frist für die Einrichtung der Gemeinsamen Cyber-Einheit dieses Jahr ausläuft. Der Ausschuss erwartet aktuelle Informationen darüber, wie weit das Vorhaben gediehen ist, und wie es um die Bereitschaft der EU bestellt ist, auf große Cybervorfälle zu reagieren. Der EWSA erwartet, dass dadurch die Lage-Erfassung sowie die Reaktions- und Erholungsfähigkeit der EU insgesamt verbessert wird.

5.4. Der EWSA unterstützt die Ausweitung des Mandats des Europäischen Kompetenzzentrums für Cybersicherheit zur Förderung der Tätigkeit des EU-Koordinierungszentrums für die Cyberabwehr. Darüber hinaus könnte dieses Netzwerk die digitale Souveränität Europas fördern, indem eine wettbewerbsfähige europäische industrielle Basis für spitzentechnologische Fähigkeiten — teilweise auf Grundlage der Arbeiten vertraglicher öffentlich-privater Partnerschaften (ÖPP) — entwickelt wird. ÖPP haben sich als das wirksamste Konzept zur Verbesserung der Cybersicherheit des gesamten digitalen Ökosystems erwiesen. Sie dürfen allerdings keine Einbahnstraße sein, und öffentliche Einrichtungen müssen auch ihre Erkenntnisse an die Privatwirtschaft weitergeben.

5.5. Die EU muss aus Sicht des EWSA unverzüglich in Spitzentechnologien wie die Post-Quanten-Kryptographie investieren, um künftigen Hackingversuchen durch Quantencomputer abzuwehren. Nach Ansicht des Ausschusses muss Europa mittelfristig autonom werden, und er plädiert nachdrücklich für den Ausbau von Forschungs- und Produktionsanlagen durch Unternehmen mit Sitz in der EU. Der EWSA hält es für wichtig, die EU-Mittel für digitale FuI aufzustocken und Investitionen von Betreibern und Anbietern in neue technische Sicherheitsfunktionen — auch im Zusammenhang mit neuen Trends wie der erweiterten Realität und dem Metaversum — zu unterstützen. Vor allem muss dringend eine europäische dezentrale Cloud-Infrastruktur aufgebaut werden, die europäischen Regeln für Datenspeicherung und -verarbeitung unterliegt ([5]).

5.6. Finanzierungsprogramme zur Verbesserung der Abwehrbereitschaft gegen Cyberangriffe sowie zu Hilfs-, Ausbildungs- und Schulungsprogrammen sollten KMU-gerecht gestaltet werden, damit die KMU Cyberrisiken verstehen und sich schützen können. Die EU sollte ein Anreizinstrument schaffen, anhand dessen KMU sich schrittweise mit dieser Thematik vertraut machen können.

5.7. Die Kommission beziffert das bestehende Kompetenzdefizit im Bereich der Cybersicherheit auf eine halbe Million Beschäftigte, weshalb der EWSA den Vorschlag zur Einrichtung einer Akademie für Cyberkompetenzen begrüßt. Die Anstrengungen der Mitgliedstaaten reichen offensichtlich nicht aus, um das Qualifikationsdefizit zu verringern. Der Ausschuss schlägt daher vor, dass die Kommission die Dynamik des Europäischen Jahres der Kompetenzen nutzt und zusammen mit der Einrichtung der Akademie auch großangelegte Ausbildungs- und Berufsbildungsprogramme auf EU-Ebene koordiniert und finanziert, die alle Mitgliedstaaten umfassen und deren Schwerpunkt auf der Bereitstellung qualifizierter Arbeitskräfte für alle mit der Cyberabwehr befassten Agenturen und Stellen sowie für private zivile Netzwerke liegt. Im Mittelpunkt sollte dabei die Schulung der Beschäftigten, namentlich in den Bereichen Mathematik, Informatik, Naturwissenschaften und Technik (MINT), stehen.

5.8. Darüber hinaus hält es der EWSA für entscheidend, das Bewusstsein der Bürgerinnen und Bürger für die Cybersicherheit zu schärfen, um die Gefährdung durch Cyberangriffe zu verringern, insbesondere hinsichtlich grundlegender Cyberverbrechen, die auf die breite Bevölkerung abzielen. Der EWSA fordert Lehrpläne für Cybersicherheit und diesbezügliche lebenslange Schulungsprogramme mit dem Schwerpunkt, die Cyberkompetenzen und -kenntnisse zu verbessern und die Bürgerinnen und Bürger, insbesondere die jüngere Generation, besser mit Cybersicherheit vertraut zu machen und sie dafür zu interessieren. Der EWSA plädiert dafür, Überlegungen zur Cybersicherheit in allen künftigen EU-Politikbereichen durchgängig zu berücksichtigen und die breite Öffentlichkeit über Cyberbedrohungen und zu informieren, unter anderem durch kostenlose Schulungsprogramme für die breite Bevölkerung, kostenlose Informationsapps für Mobiltelefone und Informationen während der Hauptsendezeit im Fernsehen. Parallel zu diesen Maßnahmen muss ein umfassender Einstellungswandel auf allen Ebenen der Gesellschaft gefördert werden, damit Cybersicherheit als wichtig wahrgenommen wird.

5.9. Der EWSA hält es für unabdingbar, das Risikoprofil von Lieferanten zu bewerten und entsprechende Beschränkungen für als besonders bedenklich eingestufte Akteure und Anwendungen anzuwenden. Dazu gehören auch notwendige Verbote für zentrale Ressourcen und Anwendungen, die in der koordinierten Risikobewertung der EU als kritisch und sensibel definiert werden, sowie die Zertifizierung vertrauenswürdiger Hardware- und Softwareanbieter.

6. **Partner bei der Bewältigung gemeinsamer Herausforderungen**

6.1. Die Abwehrbereitschaft gegen künftige Cyberangriffe ist in den einzelnen Mitgliedstaaten sehr unterschiedlich ausgeprägt. Nach Ansicht des EWSA sollte als unverzüglicher erster Schritt eine Plattform für die Verbreitung bewährter Verfahren innerhalb der EU eingerichtet werden, auf der die in Cyberfragen am weitesten fortgeschrittenen Mitgliedstaaten ihr Wissen mit den anderen Ländern austauschen und die dortige unverzügliche Einführung erleichtern können. Dies würde das gegenseitige Vertrauen zwischen nationalen Stellen verbessern. Zweitens ist nach Auffassung des Ausschusses eine engere Zusammenarbeit zwischen staatlichen und nichtstaatlichen Akteuren in der gesamten EU erforderlich, um die Cybersicherheit von Produkten und Dienstleistungen im Binnenmarkt zu verbessern. Der EWSA schlägt ferner die Schaffung einer gemeinsamen EU-Plattform für die Meldung von Cybervorfällen vor, darunter auch eine schwarze EU-Liste aller Cyberkriminellen.

([5]) Etwa die deutsch-französische Initiative Gaia-X.

6.2. Der EWSA ist der Ansicht, dass eine enge militärische Zusammenarbeit mit unseren NATO-Verbündeten nicht nur den Aufbau von Kapazitäten und die Früherkennung, sondern auch gemeinsame Projekte für Forschung, Entwicklung und Innovation, den Austausch von bewährten Verfahren und Informationen zwischen Fachleuten, umfangreiche Schulungsprogramme und Simulationen von Cyberangriffen umfassen muss. Das Hauptziel sollte darin bestehen, die gemeinsame diplomatische Reaktionsfähigkeit zu erweitern und Synergien für die Abwehr künftiger hybrider Bedrohungen gemäß den gemeinsamen Erklärungen von Warschau (2016) und Brüssel (2018) zu schaffen. In der Zusammenarbeit zwischen der EU und der NATO gibt es immer noch Wege, die noch nicht beschritten wurden. Hier könnten schnelle Fortschritte die Sicherheit für unsere Bürgerinnen und Bürger und unsere Gesellschaften entscheidend verbessern.

6.3. Der Ausschuss ist der Auffassung, dass die Beratungen mit globalen und internationalen Partnern den Weg in Richtung auf einen globalen und offenen Cyberraum ebnen sollten. In einem solchen Cyberraum sollten die Menschenrechte, die Grundfreiheiten und die Rechtsstaatlichkeit geschützt werden, und er sollte mit Blick auf die Entwicklung verbindlicher internationaler Standards in Bereichen mit schneller digitaler Entwicklung gestaltet werden. Der EWSA empfiehlt dem Hohen Vertreter, die bestehenden bilateralen Cyberdialoge zu überprüfen und weitere Verhandlungen mit anderen Ländern und einschlägigen internationalen Organisationen aufzunehmen, um einen globalen Rahmen für die Anwendung des Völkerrechts im Cyberraum auf der Grundlage strikter Gegenseitigkeit zu fördern.

6.4. Schließlich hält der Ausschuss die EU dank ihres stabilen Fundaments grundlegender demokratischer Freiheiten für prädestiniert, eine führende Rolle in internationalen Debatten über die Zukunft der Cybersicherheit, insbesondere in den Beratungen der Vereinten Nationen, zu übernehmen. Die EU muss sich auch totalitären Regimen entgegenstellen, welche die Daten ihrer Bevölkerung überwachen und deren Rechte und Freiheiten verletzen. Sie sollte sich außerdem entschieden gegen jegliches System zur Bewertung des Sozialverhaltens (social scoring) zum Nachteil der Bürgerinnen und Bürger positionieren. Der EWSA stellt klar, dass es ohne den wirkungsvollen Schutz personenbezogener Daten keine echte Demokratie geben kann. Er ist der Ansicht, dass eine verantwortungsvolle und effiziente Datenverwaltung von entscheidender Bedeutung ist, um die Hyperkonnektivität zu einem Vorteil zu machen.

Brüssel, den 14. Juni 2023

Der Präsident
des Europäischen Wirtschafts- und Sozialausschusses
Oliver RÖPKE