Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren“

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Berichterstatter: **Antonio LONGO**

Mitberichterstatter: **Alberto MAZZOLA**

Befassung	Europäischer Rat, 5.10.2018 Europäisches Parlament, 1.10.2018
Rechtsgrundlage	Artikel 173 Absatz 3, Artikel 188 und Artikel 304 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft
Annahme in der Fachgruppe	9.1.2019
Verabschiedung auf der Plenartagung	23.1.2019
Plenartagung Nr.	540
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	143/5/2

1. Schlussfolgerungen und Empfehlungen

1.1. Der Europäische Wirtschafts- und Sozialausschuss (EWSA) begrüßt die Initiative der Europäischen Kommission und erachtet sie als zweckmäßig für die Entwicklung einer Industriestrategie für Cybersicherheit und als strategisch wichtig für die Erreichung einer soliden und weitreichenden digitalen Autonomie. Diese Faktoren sind angesichts des derzeit stattfindenden Cyberkriegs, der das politische, wirtschaftliche und soziale Gefüge gefährdet, für die Stärkung der europäischen Schutzinstrumente unerlässlich.

1.2. Der EWSA unterstreicht, dass keine Cybersicherheitsstrategie ohne allgemeines Problembewusstsein und sichere Verhaltensweisen aller Nutzer auskommt.

1.3. Der EWSA unterstützt die allgemeinen Ziele des Vorschlags und ist sich der Tatsache bewusst, dass bestimmte operative Aspekte Gegenstand einer anschließenden Untersuchung sein werden. Da es sich aber um eine Verordnung handelt, vertritt er die Auffassung, dass die sensiblen Aspekte in Bezug auf die Verwaltung, Finanzierung und Verwirklichung der gesteckten Ziele im Voraus festgelegt werden sollten. Es ist wichtig, dass das künftige Netz und das Zentrum möglichst weitgehend auf den Cyberfähigkeiten und Fachkenntnissen der Mitgliedstaaten aufbauen und dass die Zuständigkeiten nicht in dem einzurichtenden Zentrum gebündelt werden. Ferner muss verhindert werden, dass sich die Tätigkeitsbereiche des künftigen Netzes und des Zentrums mit bestehenden Kooperationsmechanismen und Einrichtungen überschneiden.

1.4. Der EWSA befürwortet die Ausweitung der Zusammenarbeit auf die Industrie auf der Grundlage fester Zusagen in den Bereichen Wissenschaft und Investitionen sowie ihre künftige Beteiligung am Verwaltungsrat. Im Falle einer trilateralen Zusammenarbeit zwischen Europäischer Kommission, Mitgliedstaaten und Industrie muss die Präsenz von Unternehmen aus Drittstaaten auf diejenigen beschränkt werden, die schon seit langem auf europäischem Boden niedergelassen und umfassend an der technologischen und industriellen Basis beteiligt sind, sofern sie angemessenen Überprüfungs- und Kontrollverfahren unterliegen und den Grundsatz der Gegenseitigkeit und die Geheimhaltungspflichten einhalten.

1.5. Die Cybersicherheit muss eine gemeinsame Anstrengung aller Mitgliedstaaten sein, die deshalb auf noch festzulegende Art und Weise am Verwaltungsrat beteiligt sein müssen. Was den finanziellen Beitrag der Mitgliedstaaten angeht, so könnte auf die für jedes Land bereitgestellten EU-Mittel zurückgegriffen werden.

1.6. In dem Vorschlag sollte besser erklärt werden, wie das Kompetenzzentrum bei der Koordinierung der Finanzmittel der Programme „Digitales Europa“und „Horizont Europa“tätig werden kann und vor allem entsprechend welcher Leitlinien etwaige Aufträge erstellt und vergeben werden. Dies ist entscheidend, um Doppelarbeit oder Überschneidungen zu vermeiden. Zur Erhöhung der Finanzausstattung wird außerdem empfohlen, die Synergien mit anderen EU-Finanzierungsinstrumenten (z. B. Regionalfonds, Strukturfonds, Fazilität „Connecting Europe“, EEF, InvestEU ...) zu verstärken.

1.7. Der EWSA hält es für wesentlich, die Modalitäten für die Zusammenarbeit und die Beziehungen zwischen dem europäischen Zentrum und den nationalen Zentren festzulegen. Es ist auch wichtig, dass die nationalen Zentren von der EU — zumindest hinsichtlich der Verwaltungskosten — finanziert werden, um die Harmonisierung in Verwaltungs- und Zuständigkeitsfragen zu erleichtern und so die bestehende Kluft zwischen den EU-Mitgliedstaaten zu verringern.

1.8. Der Ausschuss unterstreicht die Bedeutung des Humankapitals und hofft, dass das Kompetenzzentrum in Zusammenarbeit mit den Hochschulen, Forschungs- und Weiterbildungszentren hochwertige Bildungs- und Ausbildungsmaßnahmen fördern kann, mittels spezifischen Bildungsangeboten in den weiterführenden Schulen und Hochschulen. Genauso entscheidend ist eine gezielte Unterstützung für Start-ups und KMU.

1.9. Der EWSA hält es für wesentlich, die jeweiligen Zuständigkeits- und Aufgabenbereiche des Zentrums und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) genauer abzustecken und die Kooperationsbedingungen und die gegenseitige Unterstützung klar zu definieren, um Kompetenzüberschneidungen und Doppelarbeit zu vermeiden. Ähnliche Probleme ergeben sich bezüglich anderer Organisationen, die sich mit Cybersicherheit beschäftigen, wie etwa EDA, Europol und CERT-EU. Zwischen den unterschiedlichen Organisationen sollten weitere Mechanismen für einen strukturierten Dialog eingerichtet werden.

2. **Aktueller Rechtsrahmen für Cybersicherheit**

2.1. Cybersicherheit ist eines der vorrangigen Themen der EU-Agenda, weil es sich dabei um einen unerlässlichen Faktor für den Schutz der Institutionen, der Unternehmen und der Bürgerinnen und Bürger sowie um ein notwendiges Instrument für die Wahrung der Demokratien handelt. Zu den besorgniserregenden Phänomenen zählt die exponentielle Zunahme von Schadsoftware, die im Netz durch automatische Systeme verbreitet werden (ein Anstieg von 130000 im Jahr 2007 auf 8 Mio. im Jahr 2017). Darüber hinaus ist die EU ein Nettoimporteur von Produkten und Lösungen der Cybersicherheit, was ein Problem in Bezug auf die wirtschaftliche Wettbewerbsfähigkeit und die zivile und militärische Sicherheit darstellt.

2.2. Die EU verfügt zwar über wichtige Zuständigkeiten und Erfahrungen auf dem Gebiet der Cybersicherheit; die Industrie dieser Branche, die Hochschulen und die Forschungszentren scheinen jedoch nach wie vor fragmentiert und uneinheitlich zu sein, und sie verfügen über keine gemeinsame Entwicklungsstrategie. Dies ist darauf zurückzuführen, dass die von der Cybersicherheit am meisten betroffenen Sektoren (z. B. Energie, Raumfahrt, Verteidigung und Verkehr) nur eine unzureichende Unterstützung erfahren. Auch werden die Synergien zwischen der Cybersicherheit im zivilen Bereich und im Verteidigungssektor nicht genutzt.

2.3. Um den wachsenden Herausforderungen zu begegnen, hat die EU 2013 eine Cybersicherheitsstrategie zur Förderung eines zuverlässigen, sicheren und offenen Cyberökosystems festgelegt ([1]). Im Jahr 2016 ergriff die EU dann die ersten spezifischen Maßnahmen für die Sicherheit von Netz- und Informationssystemen ([2]). Dies führte schließlich zur Gründung der öffentlich-privaten Partnerschaft für Cybersicherheit („cPPP“).

2.4. In der Mitteilung *Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen* ([3]) wurde die Notwendigkeit anerkannt, dass die EU wesentliche technische Kapazitäten im Bereich der Cybersicherheit behält und weiterentwickelt, die zur Sicherung ihres digitalen Binnenmarkts unverzichtbar sind, damit insbesondere kritische Netze und Informationssysteme geschützt und zentrale Cybersicherheitsdienste bereitgestellt werden können.

([1]) JOIN(2013) 1 final.
([2]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).
([3]) JOIN(2017) 450 final.

2.5. Die EU muss demnach in der Lage sein, ihre digitalen Ressourcen und Verfahren selbst zu sichern und im Wettbewerb auf dem globalen Cybersicherheitsmarkt zu bestehen, um eine solide und weitreichende digitale Autonomie zu erreichen ([4]).

3. Vorschläge der Kommission

3.1. Das Kompetenzzentrum hat zum Ziel, die Arbeit und Koordinierung des Netzes der nationalen Zentren zu erleichtern und die Kompetenzgemeinschaft für Cybersicherheit zu fördern, die Technologieagenda im Bereich der Cybersicherheit voranzutreiben und den Zugang zu den erworbenen Fachkenntnissen zu erleichtern.

3.2. Insbesondere sollte das Kompetenzzentrum die Durchführung der betreffenden Teile der Programme „Digitales Europa"und „Horizont Europa", die Vergabe von Finanzhilfen und die Abwicklung der Auftragsvergabe übernehmen. Angesichts der beträchtlichen Investitionen in die Cybersicherheit, die in anderen Teilen der Welt getätigt werden, und der Notwendigkeit, die einschlägigen Ressourcen in Europa zu koordinieren und zu bündeln, wird vorgeschlagen, das Kompetenzzentrum in Form einer europäischen Partnerschaft mit einer zweifachen Rechtsgrundlage einzurichten, wodurch gemeinsame Investitionen durch die EU, die Mitgliedstaaten und/oder die Industrie vereinfacht werden.

3.3. In dem Vorschlag ist vorgesehen, dass die Mitgliedstaaten einen angemessenen Betrag zu den Maßnahmen des Kompetenzzentrums und des Netzes beisteuern müssen. Die von der EU vorgesehene Finanzausstattung beläuft sich auf ca. 2 Mrd. EUR im Rahmen des Programms „Digitales Europa". Der aus dem Programm „Horizont Europa"stammende Betrag ist noch festzulegen. Der Gesamtbeitrag der Mitgliedstaaten sollte mindestens so groß sein wie der Beitrag der EU.

3.4. Das wichtigste Entscheidungsgremium ist der Verwaltungsrat, in dem zwar alle Mitgliedstaaten vertreten sind, aber nur jene Mitgliedstaaten, die sich auch finanziell beteiligen, ein Stimmrecht haben. Die Beschlussfassung erfolgt nach dem Grundsatz der doppelten Mehrheit, dem zufolge 75 % der finanziellen Beiträge und 75 % der Stimmen erforderlich sind. Die Kommission verfügt über 50 % der Stimmen. Das Kompetenzzentrum wird von einem wissenschaftlich-technischen Beirat unterstützt, um für einen regelmäßigen Dialog mit Unternehmen, Verbrauchern und anderen relevanten Interessenträgern zu sorgen.

3.5. In enger Zusammenarbeit mit dem Netz nationaler Koordinierungszentren und der Kompetenzgemeinschaft für Cybersicherheit wäre das Kompetenzzentrum die wichtigste Durchführungsstelle für die Verwendung der EU-Finanzmittel, die im Rahmen der vorgeschlagenen Programme „Digitales Europa"und „Horizont Europa"für die Cybersicherheit bereitgestellt werden.

3.6. Die nationalen Koordinierungszentren werden von den Mitgliedstaaten ausgewählt. Die Zentren sollten entweder über technisches Fachwissen im Bereich der Cybersicherheit verfügen oder direkten Zugang dazu haben, insbesondere auf Gebieten wie Kryptografie, IKT-Sicherheitsdienste, Intrusionserkennung, Systemsicherheit, Netzsicherheit, Software- und Anwendungssicherheit oder menschliche und gesellschaftliche Aspekte der Sicherheit und der Privatsphäre. Sie sollten auch in der Lage sein, sich wirksam mit der Industrie und dem öffentlichen Sektor auszutauschen und abzustimmen, einschließlich der gemäß der Richtlinie (EU) 2016/1148 benannten Behörden.

4. Allgemeine Bemerkungen

4.1. Der EWSA begrüßt die Initiative der Europäischen Kommission und hält sie für strategisch wichtig für die Entwicklung der Cybersicherheit im Einklang mit den auf dem Gipfel in Tallinn im September 2017 gefassten Beschlüssen. Bei dieser Gelegenheit forderten die Staats- und Regierungschefs die EU auf, *„Europa bis zum Jahr 2025 weltweit zum Vorreiter in Sachen Cybersicherheit [zu] machen, um das Vertrauen, die Zuversicht und den Schutz unserer Bürger, Verbraucher und Unternehmen online zu sichern und ein freies und durch Gesetze gesichertes Internet zu ermöglichen"*.

4.2. Der EWSA weist erneut darauf hin, dass derzeit ein echter Cyberkrieg stattfindet, der das politische, wirtschaftliche und soziale Gefüge gefährdet, indem IT-Systeme von Institutionen, kritische Infrastrukturen (Energie, Verkehr, Banken und Finanzinstitute usw.) und Unternehmen angegriffen und mithilfe gezielter Falschmeldungen Wahlen und demokratische Prozesse im Allgemeinen beeinflusst werden ([5]). Notwendig sind deshalb ein starkes Problembewusstsein und eine deutliche und rechtzeitige Reaktion. Aus diesen Gründen ist es erforderlich, eine klare und angemessen unterstützte Industriestrategie für Cybersicherheit als unabdingbare Voraussetzung für die Erreichung der digitalen Autonomie festzulegen. Der EWSA ist der Ansicht, dass im Arbeitsprogramm den Sektoren Priorität eingeräumt werden sollte, die in der Richtlinie (EU) 2016/1148 genannt werden, welche aufgrund ihrer gesellschaftlichen Bedeutung auf öffentliche oder private Anbieter wesentlicher Dienstleistungen Anwendung findet ([6]).

([4]) ABl. C 227 vom 28.6.2018, S. 86.

([5]) Informationsbericht zum Thema „Nutzung der Medien zur Einflussnahme auf gesellschaftliche und politische Prozesse in der EU und ihren östlichen Nachbarländern", Vareikytė, 2014.

([6]) ABl. C 227 vom 28.6.2018, S. 86.

4.3. Der EWSA unterstreicht, dass keine Cybersicherheitsstrategie ohne allgemeines Problembewusstsein und sichere Verhaltensweisen aller Nutzer auskommt. Aus diesem Grund muss jede Technologieinitiative mit entsprechenden Informations- und Sensibilisierungskampagnen einhergehen, um eine „Kultur der digitalen Sicherheit“zu schaffen ([7]).

4.4. Der EWSA unterstützt die allgemeinen Ziele des Vorschlags und ist sich der Tatsache bewusst, dass bestimmte operative Aspekte Gegenstand einer anschließenden Untersuchung sein werden. Da es sich aber um eine Verordnung handelt, vertritt er die Auffassung, dass die sensiblen Aspekte in Bezug auf die Verwaltung, Finanzierung und Verwirklichung der gesteckten Ziele im Voraus festgelegt werden sollten. Es ist wichtig, dass das künftige Netz und das Zentrum möglichst weitgehend auf den Cyberfähigkeiten und Fachkenntnissen der Mitgliedstaaten aufbauen und dass die Zuständigkeiten nicht in dem einzurichtenden Zentrum gebündelt werden. Ferner muss verhindert werden, dass sich die Tätigkeitsbereiche des künftigen Netzes und des Zentrums mit bestehenden Kooperationsmechanismen und Einrichtungen überschneiden.

4.5. Der EWSA erinnert daran, dass er in seiner Stellungnahme über den Rechtsakt zur Cybersicherheit (TEN/646) ([8]) eine trilaterale Zusammenarbeit im Rahmen einer öffentlich-privaten Partnerschaft zwischen der Europäischen Kommission, den Mitgliedstaaten und der Industrie unter Einschluss der KMU vorgeschlagen hat. Die derzeitige Struktur, deren Rechtsform noch eingehender behandelt werden muss, sieht im Wesentlichen eine öffentlich-private Partnerschaft zwischen Kommission und Mitgliedstaaten vor.

4.6. Der EWSA befürwortet die Ausweitung der Zusammenarbeit auf die Industrie auf der Grundlage fester Zusagen in den Bereichen Wissenschaft und Investitionen sowie ihre künftige Beteiligung am Verwaltungsrat. Es könnte sein, dass die Einsetzung eines wissenschaftlich-technischen Beirates keinen regelmäßigen Dialog mit Unternehmen, Verbrauchern und anderen relevanten Interessenträgern gewährleistet. In dem neuen von der Kommission beschriebenen Kontext erscheint es nicht klar, welche Rolle die auf Initiative der Kommission im Juni 2016 errichtete Europäische Cybersicherheitsorganisation (ECSO) spielen soll, die als Partner der Kommission fungiert und deren Kapital an Vernetzung und Wissen nicht verschwendet werden sollte.

4.6.1. Im Falle einer trilateralen Zusammenarbeit sollte den aus Drittstaaten stammenden Unternehmen Aufmerksamkeit geschenkt werden. Der EWSA unterstreicht insbesondere, dass diese Zusammenarbeit auf einem starken Mechanismus basieren sollte, um die Präsenz von Unternehmen aus Drittstaaten zu verhindern, die die Sicherheit und Autonomie der EU beeinträchtigen könnten. Die relevanten Bestimmungen des EDIDP ([9]) sollten auch in diesem Zusammenhang Anwendung finden.

4.6.2. Gleichzeitig erkennt der EWSA an, dass sich bestimmte Unternehmen, die zwar aus Drittstaaten stammen, aber schon seit langem in Europa niedergelassen und an der europäischen Technologie- und Industriebasis umfassend beteiligt sind, bei EU-Projekten als sehr nützlich erweisen könnten und dazu Zugang haben sollten, sofern die Mitgliedstaaten angemessene Überprüfungs- und Kontrollverfahren für diese Unternehmen festlegen und der Grundsatz der Gegenseitigkeit und die Geheimhaltungspflichten eingehalten werden.

4.7. Die Cybersicherheit muss eine gemeinsame Anstrengung aller Mitgliedstaaten sein, die deshalb auf noch festzulegende Art und Weise am Verwaltungsrat beteiligt sein müssen. Ferner ist es wichtig, dass alle Mitgliedstaaten einen angemessenen finanziellen Beitrag zur Initiative der Kommission leisten. Was den finanziellen Beitrag der Mitgliedstaaten angeht, so könnte auf die für jedes Land bereitgestellten EU-Mittel zurückgegriffen werden.

4.8. Der EWSA ist damit einverstanden, dass jeder Mitgliedstaat frei über die Ernennung eines eigenen Vertreters im Verwaltungsrat des Europäischen Kompetenzzentrums entscheiden kann. Der EWSA empfiehlt, die Anforderungsprofile der nationalen Vertreter klar zu definieren und darin strategische und technische Kompetenzen mit Management-, Verwaltungs- und Finanzkenntnissen zu verbinden.

4.9. In diesem Zusammenhang sollte in dem Vorschlag deutlich gemacht werden, wie das Kompetenzzentrum bei der Koordinierung der Finanzmittel der Programme „Digitales Europa“und „Horizont Europa“ — bis heute Gegenstand von Verhandlungen — tätig werden kann und vor allem entsprechend welcher Leitlinien etwaige Aufträge erstellt und vergeben werden. Dies ist entscheidend, um Doppelarbeit oder Überschneidungen zu vermeiden. Zur Erhöhung der Finanzausstattung wird außerdem empfohlen, die Synergien mit anderen EU Finanzierungsinstrumenten (z. B. Regionalfonds, Strukturfonds, Fazilität „Connecting Europe“, EEF, InvestEU ...) zu verstärken. Der EWSA hofft, dass das Netz der nationalen Zentren an der Verwaltung und Koordinierung der Mittel beteiligt wird.

([7]) ABl. C 227 vom 28.6.2018, S. 86.
([8]) ABl. C 227 vom 28.6.2018, S. 86.
([9]) COM(2017) 294.

4.10. Der EWSA stellt fest, dass der wissenschaftlich-technische Beirat aus 16 Mitgliedern bestehen soll und nicht deutlich gemacht wird, wie diese aus den Bereichen Unternehmen, Hochschulen, Forschung und Verbraucher rekrutiert werden sollen. Der EWSA hält es für sinnvoll und zweckmäßig, dass sich die Mitglieder dieses Beirats durch profunde Kenntnisse der Materie auszeichnen und die verschiedenen beteiligten Bereiche ausgewogen vertreten.

4.11. Der EWSA hält es für wesentlich, die Modalitäten für die Zusammenarbeit und die Beziehungen zwischen dem europäischen Zentrum und den nationalen Zentren festzulegen. Es ist auch wichtig, dass die nationalen Zentren von der EU — zumindest hinsichtlich der Verwaltungskosten — finanziert werden, um die Harmonisierung in Verwaltungs- und Zuständigkeitsfragen zu erleichtern und so die bestehende Kluft zwischen den EU-Mitgliedstaaten zu verringern.

4.12. Im Einklang mit seinen früheren Stellungnahmen ([10]) bekräftigt der EWSA, wie wichtig eine ausgezeichnete Bildung und Ausbildung der im Bereich Cybersicherheit tätigen Personen ist, die u. a. im Zuge spezifischer Schul-, Hochschul- und Postgraduiertenkurse erfolgen kann. Es ist auch wichtig, die KMU und Start-ups der Branche ([11]), die für die Entwicklung der Spitzenforschung grundlegend sind, angemessen finanziell zu unterstützen.

4.13. Der EWSA hält es für wesentlich, die jeweiligen Zuständigkeits- und Aufgabenbereiche des Zentrums und der ENISA genauer abzustecken und die Kooperationsbedingungen und die gegenseitige Unterstützung klar zu definieren, um Kompetenzüberschneidungen und Doppelarbeit zu vermeiden ([12]). Im Verordnungsvorschlag ist vorgesehen, dass ein Vertreter der ENISA als ständiger Beobachter im Verwaltungsrat mitwirkt, was aber keine Garantie für einen strukturierten Dialog zwischen den beiden Einrichtungen ist. Ähnliche Probleme ergeben sich bezüglich anderer Organisationen, die sich mit Cybersicherheit beschäftigen, z. B. EDA, Europol oder CERT-EU. In diesem Zusammenhang ist die im Mai 2018 von ENISA, EDA, Europol und CERT-EU unterzeichnete gemeinsame Absichtserklärung von Interesse.

Brüssel, den 23. Januar 2019

Der Präsident
des Europäischen Wirtschafts- und Sozialausschusses
Luca JAHIER

([10]) ABl. C 451 vom 16.12.2014, S. 25.
([11]) ABl. C 227 vom 28.6.2018, S. 86.
([12]) ABl. C 227 vom 28.6.2018, S. 86.