Rat der
Europäischen Union

Brüssel, den 14. September 2018
(OR. en)

12104/18

Interinstitutionelles Dossier:
2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	12. September 2018
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2018) 630 final
Betr.:	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 *Ein Beitrag der Europäischen Kommission zur Tagung der Staats- und Regierungschefs vom 19.–20. September 2018 in Salzburg*

Die Delegationen erhalten in der Anlage das Dokument COM(2018) 630 final.

Anl.: COM(2018) 630 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

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

Ein Beitrag der Europäischen Kommission zur Tagung der Staats- und Regierungschefs vom 19.–20. September 2018 in Salzburg

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Da das tägliche Leben und die Wirtschaft in zunehmendem Maße von digitalen Technologien bestimmt werden, sind die Bürger den damit verbundenen Gefahren immer stärker ausgesetzt. Die künftige Sicherheit hängt davon ab, dass sich die Union besser vor Cyberbedrohungen schützen kann, da sowohl die zivile Infrastruktur als auch die militärischen Kapazitäten auf sichere digitale Systeme angewiesen sind.

Um den wachsenden Herausforderungen zu begegnen, hat die Union ihre Tätigkeiten in diesem Bereich stetig ausgebaut; dabei stützt sie sich auf die Cybersicherheitsstrategie[1] von 2013 mit deren Zielen und Grundsätzen zur Förderung eines zuverlässigen, sicheren und offenen Cyberökosystems. Im Jahr 2016 erließ die Union mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[2] über die Sicherheit von Netz- und Informationssystemen ihre ersten Rechtsvorschriften im Bereich der Cybersicherheit.

Angesichts der sich rasch ändernden Cybersicherheitslage legten die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik im September 2017 eine Gemeinsame Mitteilung mit dem Titel „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“[3] vor, um die Abwehrfähigkeit, Abschreckung und Abwehr der EU im Bereich der Cyberangriffe weiter zu stärken. In der gemeinsamen Mitteilung, die auch auf früheren Initiativen aufbaut, wurde eine Reihe von Maßnahmen vorgeschlagen, darunter u. a. die Stärkung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), die Schaffung eines freiwilligen unionsweiten Rahmens für die Cybersicherheitszertifizierung, um die Cybersicherheit von Produkten und Diensten in der digitalen Welt zu erhöhen, sowie ein Konzept für eine rasche und koordinierte Reaktion auf Cybersicherheitsvorfälle und -krisen großen Ausmaßes.

In der gemeinsamen Mitteilung wurde anerkannt, dass es auch im strategischen Interesse der Union liegt, dass sie die Kapazitäten wahrt und weiterentwickelt, die zur Sicherung ihres digitalen Binnenmarkts unverzichtbar sind, damit insbesondere kritische Netze und Informationssysteme geschützt und zentrale Cybersicherheitsdienste bereitgestellt werden können. Die Union muss in der Lage sein, ihre digitalen Werte und Anlagen selbst zu sichern und im Wettbewerb auf dem globalen Cybersicherheitsmarkt zu bestehen.

Derzeit ist die Union ein Nettoimporteur von Cybersicherheitsprodukten und -lösungen und hängt dabei weitgehend von nichteuropäischen Anbietern ab[4]. Der Cybersicherheitsmarkt hat weltweit ein Volumen von 600 Mrd. EUR und der Umsatz, die Zahl der Unternehmen und die Zahl der Beschäftigten auf diesem Markt dürften in den nächsten fünf Jahren voraussichtlich

---

1 Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, 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 Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, JOIN(2017) 450 final.

4 Entwurf des Abschlussberichts über die Cybersicherheitsmarkt-Studie, 2018.

um durchschnittlich etwa 17 % anwachsen. Allerdings finden sich unter den 20 aus Marktsicht im Bereich der Cybersicherheit führenden Ländern nur 6 Mitgliedstaaten[5].

Gleichzeitig gibt es in der Union eine Fülle von Fachwissen und Erfahrungen im Bereich der Cybersicherheit – mehr als 660 Organisationen aus der gesamten EU meldeten sich im Rahmen der von der Kommission jüngst durchgeführten Bestandsaufnahme der Cybersicherheitskompetenzzentren[6]. Würde dieses Fachwissen in marktfähige Produkte und Lösungen überführt, könnte die Union die gesamte Wertschöpfungskette im Bereich der Cybersicherheit abdecken. Allerdings sind die Anstrengungen in Forschung und Industrie fragmentiert; es mangelt an Einheitlichkeit und einer gemeinsamen Zugrichtung. Darunter leidet die Wettbewerbsfähigkeit der EU in diesem Bereich sowie ihre Fähigkeit zur Sicherung ihrer digitalen Werte und Anlagen. Die von der Cybersicherheit am meisten betroffenen Sektoren (z. B. Energie, Raumfahrt, Verteidigung) und Teilbereiche erfahren heute nur eine unzureichende Unterstützung[7]. Auch die Synergien zwischen der Cybersicherheit im zivilen Bereich und im Verteidigungssektor werden in Europa nicht in vollem Umfang genutzt.

Die Gründung der öffentlich-privaten Partnerschaft für Cybersicherheit („cPPP“) in der Union im Jahr 2016 war ein erster konkreter Schritt, um die Fachkreise in Forschung, Industrie und öffentlichem Sektor zusammenzubringen und so die Forschung und Innovation im Bereich der Cybersicherheit zu erleichtern, und sollte innerhalb der Grenzen des Finanzrahmens 2014–2020 zu guten, stärker zielgerichteten Ergebnissen in Forschung und Innovation führen. Die cPPP ermöglichte es den Partnern aus der Industrie, eigene Zusagen in Bezug auf ihre Ausgaben in den in der strategischen Forschungs- und Innovationsagenda der Partnerschaft festgelegten Bereichen zu machen.

Die Union kann jedoch viel größere Investitionen tätigen und benötigt einen wirksameren Mechanismus, mit dem dauerhafte Kapazitäten und Kompetenzen aufgebaut, Anstrengungen koordiniert und die Entwicklung innovativer Lösungen für industrielle Herausforderungen in Bezug auf die Cybersicherheit im Bereich neuer Mehrzwecktechnologien (z. B. künstliche Intelligenz, Quanteninformatik, Blockchain-Technologien und sichere digitale Identitäten) sowie kritischer Sektoren (z. B. Verkehr, Energie, Gesundheit, Finanzen, Regierung, Telekommunikation, Fertigung, Verteidigung, Raumfahrt) gefördert werden.

In der Gemeinsamen Mitteilung wurde die Möglichkeit erwogen, die Cybersicherheitskapazitäten der Union durch ein Netz von Cybersicherheitskompetenzzentren unter dem Dach des Europäischen Kompetenzzentrums für Cybersicherheit zu stärken. Dies würde dazu beitragen, die Bemühungen um den Aufbau von Kapazitäten in diesem Bereich auf Unions- und nationaler Ebene ergänzen. In der Gemeinsamen Mitteilung kündigte die Kommission die Durchführung einer Folgenabschätzung im Jahr 2018 an, um zu untersuchen, welche Optionen zum Aufbau der Struktur zur Verfügung stehen. In einem ersten Schritt und als Grundlage für künftige Überlegungen hat die Kommission im Rahmen von Horizont 2020 eine Pilotphase eingeleitet, damit sich die nationalen Zentren zu einem Netz zusammenschließen und so eine neue Dynamik bei der Entwicklung von Kompetenz und Technik im Bereich der Cybersicherheit entfalten können.

Auf dem Digitalgipfel im September 2017 in Tallinn forderten die Staats- und Regierungschefs die Union auf, „Europa bis zum Jahr 2025 weltweit zum Vorreiter in Sachen

5 Entwurf des Abschlussberichts über die Cybersicherheitsmarkt-Studie, 2018.

6 Technische Berichte der JRC: *European Cybersecurity Centres of Expertise*, 2018.

7 Technische Berichte der JRC: *Outcomes of the Mapping Exercise* (Einzelheiten siehe Anhänge 4 und 5).

Cybersicherheit 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".

In den Schlussfolgerungen des Rates[8] vom November 2017 wurde die Kommission aufgefordert, rasch eine Folgenabschätzung vorzunehmen und bis Mitte 2018 die entsprechenden Rechtsinstrumente für die Durchführung der Initiative vorzuschlagen.

Mit dem *Programm „Digitales Europa"*, das die Kommission im Juni 2018 vorgeschlagen hat[9], sollen die Vorteile des digitalen Wandels für die europäischen Bürger und Unternehmen in allen relevanten Bereichen der EU-Politik ausgebaut und maximiert, die Politik verstärkt und die ehrgeizigen Ziele des digitalen Binnenmarkts unterstützt werden. Das Programm sieht einen kohärenten und übergreifenden Ansatz vor, um die bestmögliche Nutzung fortgeschrittener Technologien und die richtige Kombination von technischen Kapazitäten und menschlichen Kompetenzen für den digitalen Wandel – nicht nur im Bereich der Cybersicherheit, sondern auch in Bezug auf intelligente Dateninfrastrukturen, künstliche Intelligenz, fortgeschrittene Kompetenzen und Anwendungen in der Industrie und in Bereichen von öffentlichem Interesse – zu erreichen. Diese Elemente sind voneinander abhängig, verstärken sich gegenseitig und können – bei gleichzeitiger Förderung – die erforderliche Größenordnung erreichen, damit die Datenwirtschaft gedeihen kann[10]. Auch im Programm „*Horizont Europa*"[11], dem nächsten EU-Rahmenprogramm für Forschung und Entwicklung, zählt die Cybersicherheit zu den Prioritäten.

In diesem Zusammenhang wird mit der vorliegenden Verordnung die Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung mit einem Netz nationaler Koordinierungszentren vorgeschlagen. Um das technologische und industrielle Cybersicherheitsökosystem in Europa anzuregen, sollte dieses zweckgebundene Kooperationsmodell wie folgt funktionieren: Das Kompetenzzentrum erleichtert die Arbeit und die Koordinierung des Netzes und fördert die Kompetenzgemeinschaft für Cybersicherheit, treibt die Technologieagenda im Bereich der Cybersicherheit voran und erleichtert den Zugang zu dem so zusammengeführten Fachwissen. Hierzu übernimmt das Kompetenzzentrum insbesondere die Durchführung der betreffenden Teile der Programme „Digitales Europa" und „Horizont Europa", die Vergabe von Finanzhilfen und die Abwicklung der Auftragsvergabe. 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 das Kompetenzzentrum in Form einer europäischen Partnerschaft[12] eingerichtet, wodurch gemeinsame Investitionen durch die Union, die Mitgliedstaaten und/oder die Industrie

---

8 Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, angenommen vom Rat (Allgemeine Angelegenheiten) am 20. November 2017.

9 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Aufstellung des Programms „Digitales Europa" für den Zeitraum 2021–2027, COM(2018) 434.

10 Siehe SWD(2018) 305.

11 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Rahmenprogramm für Forschung und Innovation „Horizont Europa" sowie über die Regeln für die Beteiligung und die Verbreitung der Ergebnisse, COM(2018) 435.

12 Wie festgelegt in COM(2018) 435, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Rahmenprogramm für Forschung und Innovation „Horizont Europa" sowie über die Regeln für die Beteiligung und die Verbreitung der Ergebnisse; und wie angegeben in COM(2018) 434, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Aufstellung des Programms „Digitales Europa" für den Zeitraum 2021–2027.

vereinfacht werden. Deshalb sieht der Vorschlag vor, dass die Mitgliedstaaten einen angemessenen Betrag zu den Maßnahmen des Kompetenzzentrums und des Netzes beisteuern müssen. 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 im Verwaltungsrat erfolgt nach dem Grundsatz der doppelten Mehrheit, nach dem 75 % der finanziellen Beiträge und 75 % der Stimmen erforderlich sind. In Anbetracht ihrer Verantwortung für den Unionshaushalt hat die Kommission 50 % der Stimmen. Für ihre Arbeit im Verwaltungsrat bedient sich die Kommission gegebenenfalls des Fachwissens des Europäischen Auswärtigen Dienstes. Der Verwaltungsrat wird von einem wissenschaftlich-technischen Beirat unterstützt, um für einen regelmäßigen Dialog mit dem Privatsektor, mit Verbraucherverbänden und mit anderen relevanten Interessenträgern zu sorgen.

In enger Zusammenarbeit mit dem Netz nationaler Koordinierungszentren und der Kompetenzgemeinschaft für Cybersicherheit, die mit dieser Verordnung eingerichtet werden (unter Einbeziehung einer großen und heterogenen Gruppe von Akteuren, die an der Entwicklung der Cybersicherheitstechnik beteiligt sind, z. B. Forschungseinrichtungen, anbietende und nachfragende Branchen sowie der öffentliche Sektor), wäre das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung 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.

Ein solcher umfassender Ansatz würde es ermöglichen, die Cybersicherheit entlang der gesamten Wertschöpfungskette – von der Forschung bis zur Einführung und Verbreitung wichtiger Technologien – zu unterstützen. Die finanzielle Beteiligung der Mitgliedstaaten sollte dem Finanzbeitrag der EU zu dieser Initiative angemessen sein und ist ein unerlässliches Element für den Erfolg dieser Initiative.

Angesichts ihres besonderen Fachwissens und der in ihr breit vertretenen einschlägigen Interessengruppen sollte die Vereinigung Europäische Cybersicherheitsorganisation, die in der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit im Rahmen von Horizont 2020 das Gegenstück zur Kommission darstellt, aufgefordert werden, sich an den Arbeiten des Zentrums und des Netzes zu beteiligen.

Zudem sollte das geplante europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung bessere Synergien zwischen der zivilen und der verteidigungspolitischen Dimension der Cybersicherheit anstreben. Es sollte die Mitgliedstaaten und andere relevante Akteure durch Beratung, Bereitstellung von Fachwissen und Erleichterung der Zusammenarbeit bei Projekten und Maßnahmen unterstützen. Auf Ersuchen der Mitgliedstaaten könnte es ferner als Projektmanager, insbesondere in Verbindung mit dem Europäischen Verteidigungsfonds, tätig werden. Die vorliegende Initiative zielt darauf ab, zur Lösung folgender Probleme beizutragen:

- **Unzureichende Zusammenarbeit zwischen den nachfragenden und anbietenden Marktteilnehmern im Bereich der Cybersicherheit.** Die europäischen Unternehmen stehen vor der Herausforderung, für die eigene Sicherheit sorgen zu müssen und gleichzeitig ihren Kunden sichere Produkte und Dienste zu bieten. Oft sind sie jedoch nicht in der Lage, ihre bestehenden Produkte, Dienste und Anlagen angemessen zu schützen oder sichere innovative Produkte und Dienste zu entwickeln. Wichtige Anlagen im Bereich der Cybersicherheit sind häufig zu kostspielig, um von einzelnen Akteuren entwickelt und eingerichtet werden zu können, deren Kerngeschäft nicht im Bereich der Cybersicherheit

liegt. Gleichzeitig sind die Verbindungen zwischen der Angebots- und der Nachfrageseite auf dem Cybersicherheitsmarkt nicht ausreichend entwickelt, was zu einer suboptimalen Versorgung mit europäischen Produkten und Lösungen, die auf die Bedürfnisse der verschiedenen Sektoren zugeschnitten sind, sowie zu unzureichendem Vertrauen unter den Marktteilnehmern führt.

- **Fehlen eines wirksamen Mechanismus für die Zusammenarbeit zwischen den Mitgliedstaaten beim Aufbau von Kapazitäten in der Industrie.** Derzeit gibt es ebenfalls keinen wirksamen Mechanismus für die Zusammenarbeit der Mitgliedstaaten beim Aufbau der zur Unterstützung der Innovation im Bereich der Cybersicherheit in allen Industriesektoren erforderlichen Kapazitäten und bei der Einführung modernster europäischer Cybersicherheitslösungen. Die bestehenden Mechanismen für die Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit gemäß der Richtlinie (EU) 2016/1148 sehen diese Art von Tätigkeiten in ihrem Mandat nicht vor.
- **Unzureichende Zusammenarbeit innerhalb der und zwischen den Forschungs- und Industriekreisen.** Obwohl Europa theoretisch in der Lage ist, die gesamte Wertschöpfungskette im Bereich der Cybersicherheit abzudecken, gibt es relevante Cybersicherheitssektoren (z. B. Energie, Raumfahrt, Verteidigung, Verkehr) und Teilbereiche, die heute von der Forschung schlecht oder nur von einer begrenzten Zahl von Zentren unterstützt werden (z. B. Postquanten- und Quantenkryptografie, Vertrauen und Cybersicherheit bei der künstlichen Intelligenz). Diese Zusammenarbeit gibt es natürlich, jedoch handelt es sich sehr häufig um kurzfristige Beratungsaufträge, die es nicht erlauben, langfristige Forschungspläne zur Bewältigung der Herausforderungen im Bereich der Cybersicherheit zu verfolgen.
- **Unzureichende Zusammenarbeit zwischen ziviler und militärischer Forschung und Innovation im Bereich der Cybersicherheit.** Das Problem der unzureichenden Zusammenarbeit betrifft auch die zivilen und die militärischen Fachkreise. Die bestehenden Synergien werden nicht in vollem Umfang genutzt, da es an wirksamen Mechanismen mangelt, die es diesen Kreisen ermöglichen, effizient zusammenzuarbeiten und Vertrauen aufzubauen, das sogar mehr als in anderen Bereichen eine Voraussetzung für eine erfolgreiche Zusammenarbeit darstellt. Dies geht einher mit begrenzten finanziellen Kapazitäten auf dem Cybersicherheitsmarkt der EU sowie unzureichenden Mitteln für die Innovationsförderung.
- **Kohärenz mit den bestehenden Vorschriften in diesem Politikbereich**

Das Cybersicherheitskompetenznetz und das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung werden als zusätzliche Unterstützung für bestehende Bestimmungen und Akteure im Bereich der Cybersicherheit dienen. Das Mandat des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung wird die Arbeit der ENISA ergänzen, hat jedoch einen anderen Schwerpunkt und erfordert ein anderes Spektrum an Kompetenzen. Während das Mandat der ENISA eine beratende Funktion in Bezug auf Forschung und Innovation im Bereich der Cybersicherheit in der EU vorsieht, konzentriert sich das für das Kompetenzzentrum vorgeschlagene Mandat in erster Linie auf andere Aufgaben, die für die Stärkung der Abwehrfähigkeit der EU in Cybersicherheitsfragen von entscheidender Bedeutung sind. Darüber hinaus sieht das Mandat der ENISA keine Tätigkeiten vor, die zu den Kernaufgaben des Zentrums und des Netzes gehören, nämlich die Entwicklung und Einführung von Technologien im Bereich der Cybersicherheit zu fördern und den Aufbau von Kapazitäten in diesem Bereich auf EU- und nationaler Ebene zu ergänzen.

Das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung wird mit dem Cybersicherheitskompetenznetz ebenfalls gemeinsam darauf hinarbeiten, die Forschung zu erleichtern und Normungs- und Zertifizierungsverfahren zu beschleunigen, insbesondere im Zusammenhang mit Zertifizierungssystemen für Cybersicherheit im Sinne des vorgeschlagenen Rechtsakts zur Cybersicherheit[13][14].

Bei der vorliegenden Initiative handelt es sich eigentlich um eine Ausweitung der öffentlich-privaten Partnerschaft für Cybersicherheit (cPPP), des ersten EU-weiten Versuchs, die Cybersicherheitsbranche, nachfragende Branchen (Käufer von Cybersicherheitsprodukten und -lösungen, darunter öffentliche Verwaltungen und kritische Sektoren wie Verkehr, Gesundheit, Energie, Finanzen) und die Forschung zusammenzubringen, um einem nachhaltigen Dialog eine Plattform zu geben und die Voraussetzungen für freiwillige Koinvestitionen zu schaffen. Die cPPP wurde 2016 gegründet und hat bis 2020 Investitionen in Höhe von bis zu 1,8 Mrd. EUR bewirkt. Der Vergleich mit dem Umfang der Investitionen, die derzeit in anderen Teilen der Welt getätigt werden (die USA z. B. investierten im Jahr 2017 allein 19 Mrd. USD in die Cybersicherheit), macht jedoch deutlich, dass die EU mehr unternehmen muss, um eine kritische Investitionsmasse zu erreichen und die Fragmentierung der in der EU vorhandenen Kapazitäten zu überwinden.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Das Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung wird als einheitliche Durchführungsstelle verschiedener Programme der Union zur Förderung der Cybersicherheit (Programm „Digitales Europa“ und Programm „Horizont Europa“) und zur Verbesserung der Kohärenz und der Synergien zwischen ihnen dienen.

Diese Initiative wird es außerdem ermöglichen, die Anstrengungen der Mitgliedstaaten zu ergänzen, indem sie geeignete Zuarbeiten für bildungspolitische Entscheidungen liefert, um die Kompetenzen im Bereich der Cybersicherheit zu verbessern (z. B. durch die Entwicklung von Cybersicherheitslehrplänen in zivilen und militärischen Bildungssystemen) und so zur Ausbildung qualifizierter Arbeitskräfte im Bereich der Cybersicherheit in der EU beizutragen – ein wichtiger Vorteil für Cybersicherheitsunternehmen sowie andere Branchen, für die die Cybersicherheit von Bedeutung ist. Im Hinblick auf die Bildung und Schulung im Bereich der Cyberabwehr wird die Initiative mit den andauernden Arbeiten der Plattform für Bildung, Schulung und Übungen im Bereich der Cyberabwehr, die im Rahmen des Europäischen Sicherheits- und Verteidigungskollegs eingerichtet wurde, im Einklang stehen.

Diese Initiative wird die Bemühungen der digitalen Innovationszentren im Rahmen des Programms „Digitales Europa“ ergänzen und unterstützen. Digitale Innovationszentren sind gemeinnützige Organisationen, die Unternehmen – insbesondere Start-ups, KMU und Mid-Cap-Unternehmen – dabei helfen, wettbewerbsfähiger zu werden, indem sie ihre Geschäfts- und Produktionsabläufe sowie ihre Produkte und Dienste durch intelligente Innovation, die durch die digitale Technik ermöglicht wird, verbessern. Digitale Innovationszentren bieten

---

13 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/3.

14 Dies lässt die Zertifizierungsverfahren im Rahmen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), in denen die Datenschutzbehörden im Einklang mit der genannten Verordnung eine Rolle spielen, unberührt.

unternehmensorientierte, innovative Dienstleistungen wie Marktforschung, Finanzierungsberatung, Zugang zu einschlägigen Erprobungs- und Versuchseinrichtungen, Ausbildung und Kompetenzentwicklung, um die erfolgreiche Markteinführung neuer Produkte oder Dienste zu unterstützen oder bessere Produktionsabläufe einzuführen. Einige digitale Innovationszentren mit spezieller Fachkompetenz auf dem Gebiet der Cybersicherheit könnten direkt in die mit dieser Initiative eingerichtete Kompetenzgemeinschaft für Cybersicherheit einbezogen werden. In den meisten Fällen würden jedoch digitale Innovationszentren ohne spezielles Cybersicherheitsprofil den Zugang ihrer Nutzer zu Fachkompetenz, Wissen und Kapazitäten im Bereich der Cybersicherheit, die in der Kompetenzgemeinschaft für Cybersicherheit vorhanden sind, erleichtern, indem sie eng mit dem Netz nationaler Koordinierungszentren und dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung zusammenarbeiten. Die digitalen Innovationszentren würden ferner die Einführung innovativer Cybersicherheitsprodukte und -lösungen unterstützen, die den Bedürfnissen der von ihnen beratenen Unternehmen und anderen Endnutzer entsprechen. Nicht zuletzt könnten sektorspezifische digitale Innovationszentren ihr Wissen über die tatsächlichen Bedürfnisse des Sektors mit dem Netz und dem Zentrum teilen, um die Überlegungen über die Forschungs- und Innovationsagenda, die den Anforderungen der Industrie am besten entspricht, zu bereichern.

Es werden Synergien mit den einschlägigen Wissens- und Innovationsgemeinschaften des Europäischen Innovations- und Technologieinstituts und insbesondere mit EIT-Digital angestrebt.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

• Rechtsgrundlage

Das Kompetenzzentrum sollte aufgrund seiner Art und seiner besonderen Ziele auf einer doppelten Rechtsgrundlage eingerichtet werden. Auf der Grundlage des Artikels 187 AEUV zur Schaffung von Strukturen, die für die ordnungsgemäße Durchführung der Programme für Forschung, technologische Entwicklung und Demonstration der Union erforderlich sind, wird es dem Kompetenzzentrum möglich sein, Synergien zu schaffen und Ressourcen zu bündeln und auf der Ebene der Mitgliedstaaten in die notwendigen Kapazitäten zu investieren oder öffentliche europäische Werte und Anlagen aufzubauen (z. B. durch gemeinsame Beschaffung der erforderlichen Erprobungs- und Versuchsinfrastruktur für Cybersicherheit). In Artikel 188 Absatz 1 ist die Annahme solcher Maßnahmen vorgesehen. Ungeachtet dessen würde Artikel 188 Absatz 1 als alleinige Rechtsgrundlage nicht zulassen, dass die Tätigkeiten über den Bereich der Forschung und Entwicklung hinausgehen; dies ist aber erforderlich, um alle in dieser Verordnung festgelegten Ziele des Kompetenzzentrums zu verwirklichen, darunter die Markteinführung von Cybersicherheitsprodukten und -lösungen zu unterstützen, die europäische Cybersicherheitsbranche wettbewerbsfähiger zu machen und ihren Marktanteil zu steigern sowie einen Mehrwert zu den nationalen Anstrengungen zur Schließung der Qualifikationslücke im Bereich der Cybersicherheit zu schaffen. Hierzu muss Artikel 173 Absatz 3 zusätzlich als Rechtsgrundlage herangezogen werden, der es der Union ermöglicht, Maßnahmen zur Förderung der Wettbewerbsfähigkeit der Industrie zu ergreifen.

• Begründung des Vorschlags im Hinblick auf die Grundsätze der Subsidiarität und der Verhältnismäßigkeit

Die Cybersicherheit ist ein Thema von gemeinsamem Interesse der Union, wie in den genannten Schlussfolgerungen des Rates bestätigt wurde. Der Umfang und der

grenzüberschreitende Charakter von Vorfällen wie *WannaCry* oder *NonPetya* sind typische Beispiele hierfür. Art und Umfang der technischen Herausforderungen im Bereich der Cybersicherheit sowie die unzureichende Koordinierung der Anstrengungen innerhalb der Industrie, des öffentlichen Sektors und der Forschung machen es erforderlich, dass die EU die Koordinierungsbemühungen weiter unterstützt, um eine kritische Masse an Ressourcen zu bilden und bessere Kenntnisse und eine bessere Verwaltung der Ressourcen zu gewährleisten. Dies ist erforderlich angesichts des Ressourcenbedarfs im Zusammenhang mit bestimmten Kapazitäten für Forschung, Entwicklung und Einführung im Bereich der Cybersicherheit, angesichts der Notwendigkeit, Zugang zu interdisziplinärem Fachwissen im Bereich der Cybersicherheit zwischen verschiedenen Fachgebieten zu ermöglichen (häufig nur teilweise auf nationaler Ebene gegeben), und angesichts des globalen Charakters der industriellen Wertschöpfungsketten sowie der Aktivitäten globaler Wettbewerber, die märkteübergreifend tätig sind.

Hierzu sind Ressourcen und Fachwissen in einer Größenordnung nötig, die durch die Maßnahmen eines einzelnen Mitgliedstaats kaum erreicht werden können. So könnte beispielsweise ein gesamteuropäisches Quantenkommunikationsnetz eine EU-Investition in Höhe von rund 900 Mio. EUR erfordern, je nach den Investitionen der Mitgliedstaaten (zu vernetzen/ergänzen) und je nachdem, in welchem Umfang bestehende Infrastrukturen dabei weiterverwendet werden könnten. Die Initiative wird wesentlich dazu beitragen, die Finanzierung zu bündeln und diese Art von Investitionen in der Union überhaupt zu ermöglichen.

Die Mitgliedstaaten können die Ziele dieser Initiative allein nicht in vollem Umfang verwirklichen. Wie dargelegt, können sie auf Unionsebene besser erreicht werden, indem Anstrengungen gebündelt und unnötige Doppelarbeit vermieden werden, sodass eine kritische Investitionsmasse erreicht und eine optimale Nutzung der öffentlichen Mittel gewährleistet wird. Gleichzeitig geht diese Verordnung entsprechend dem Grundsatz der Verhältnismäßig nicht über das für die Erreichung dieses Ziels erforderliche Maß hinaus. Ein Tätigwerden der EU ist daher aus Gründen der Subsidiarität und Verhältnismäßigkeit gerechtfertigt.

Dieses Instrument sieht keine neuen rechtlichen Verpflichtungen für Unternehmen vor. Gleichzeitig dürften Unternehmen und insbesondere KMU die Kosten ihrer Anstrengungen bei der Konzeption innovativer Cybersicherheitsprodukte senken können, da die Initiative es ermöglicht, Ressourcen zu bündeln und auf der Ebene der Mitgliedstaaten in die notwendigen Kapazitäten zu investieren oder gemeinsame europäische Werte und Anlagen aufzubauen (z. B. durch gemeinsame Beschaffung der erforderlichen Erprobungs- und Versuchsinfrastruktur für Cybersicherheit). Diese Werte und Anlagen könnten von Unternehmen und KMU in verschiedenen Sektoren genutzt werden, damit ihre Produkte die Kriterien der Cybersicherheit erfüllen, und um die Cybersicherheit in einen Wettbewerbsvorteil zu verwandeln.

- **Wahl des Instruments**

Mit dem vorgeschlagenen Instrument wird eine Einrichtung zur Durchführung von Cybersicherheitsmaßnahmen im Rahmen des Programms „Digitales Europa“ und des Programms „Horizont Europa“ geschaffen. Es beschreibt ihr Mandat, ihre Aufgaben und ihre Leitungsstruktur. Die Schaffung einer solchen Unionseinrichtung erfordert den Erlass einer Verordnung.

3. KONSULTATION DER INTERESSENTRÄGER UND FOLGENABSCHÄTZUNG

Beim Vorschlag für die Einrichtung eines Cybersicherheitskompetenznetzes, in dessen Mittelpunkt das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung stehen soll, handelt es sich um eine neue Initiative. Sie dient der Fortsetzung und Ausweitung der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit, die 2016 geschaffen wurde.

- **Konsultation der Interessenträger**

Die Cybersicherheit ist ein umfassendes, sektorübergreifendes Thema. Die Kommission verwendete verschiedene Konsultationsmethoden, um sicherzustellen, dass das Interesse der Allgemeinheit in der Union in dieser Initiative voll zum Ausdruck kommt und nicht nur die besonderen Interessen einer kleinen Gruppe von Interessenträgern. So wird die Transparenz und Rechenschaftspflicht bei der Arbeit der Kommission gewährleistet. Zwar wurde aufgrund ihrer Zielgruppe (Industrie- und Forschungskreise sowie Mitgliedstaaten) speziell für diese Initiative keine öffentliche Konsultation durchgeführt, aber die Thematik war bereits Gegenstand mehrerer anderer öffentlicher Konsultationen:

- eine allgemeine öffentliche Konsultation zu EU-Fonds im Bereich Investitionen, Forschung und Innovation, KMU und Binnenmarkt im Jahr 2018;
- eine 12-wöchige öffentliche Online-Konsultation, die 2017 eingeleitet wurde, um die breite Öffentlichkeit (rund 90 Teilnehmer) zur Bewertung und Überprüfung der ENISA-Verordnung zu befragen;
- eine 12-wöchige öffentliche Online-Konsultation, die 2016 anlässlich des Starts der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit durchgeführt wurde (rund 240 Teilnehmer).

Darüber hinaus veranstaltete die Kommission gezielte Konsultationen zu dieser Initiative, darunter Workshops, Sitzungen und gezielte Aufforderungen zur Einreichung von Beiträgen (von ENISA und der Europäischen Verteidigungsagentur). Der Konsultationszeitraum erstreckte sich über sechs Monate von November 2017 bis März 2018. Darüber hinaus hat die Kommission eine Bestandsaufnahme der Fachzentren vorgenommen, die es ermöglichte, Beiträge von 665 Fachzentren für Cybersicherheit zu ihrem Know-how, ihren Tätigkeiten, ihren Arbeitsbereichen und der internationalen Zusammenarbeit zu sammeln. Die Erhebung wurde im Januar eingeleitet; die bis zum 8. März 2018 eingereichten Beiträge wurden im Analysebericht berücksichtigt.

Interessenträger aus Industrie und Forschung waren der Ansicht, dass das Kompetenzzentrum und das Netz einen Mehrwert zu den derzeitigen Anstrengungen auf nationaler Ebene erbringen könnten, wenn sie zur Schaffung eines europaweiten Cybersicherheitsökosystems beitragen, das eine bessere Zusammenarbeit zwischen Forschung und Industrie ermöglicht. Sie hielten es ferner für notwendig, dass die EU und die Mitgliedstaaten in der Cybersicherheitspolitik einen proaktiven, längerfristigen und strategischen Ansatz verfolgen, der über die Forschung und Innovation hinausgeht. Die Interessenträger betonten die Notwendigkeit, Zugang zu wichtigen Anlagen wie Erprobungs- und Versuchseinrichtungen zu erhalten und die Qualifikationslücke im Bereich der Cybersicherheit (z. B. durch groß angelegte europäische Projekte, mit denen die größten Talente angezogen werden) weiter zu schließen. All dies wurde auch als erforderlich angesehen, damit die Union weltweit eine Führungsrolle auf dem Gebiet der Cybersicherheit in Anspruch nehmen kann.

Die Mitgliedstaaten haben im Rahmen der seit dem vergangenen September durchgeführten Konsultationen[15] sowie in den entsprechenden Schlussfolgerungen des Rates[16] die Absicht begrüßt, ein Cybersicherheitskompetenznetz aufzubauen, um die Entwicklung und Einführung von Cybersicherheitstechnik zu fördern; dabei haben sie betont, dass alle Mitgliedstaaten mit ihren bestehenden Exzellenz- und Kompetenzzentren einbezogen werden müssen und dass der Komplementarität besondere Aufmerksamkeit zukommen muss. Insbesondere im Hinblick auf das künftige Kompetenzzentrum hoben die Mitgliedstaaten die Bedeutung seiner koordinierenden Rolle bei der Unterstützung des Netzes hervor. Vor allem im Hinblick auf die nationalen Tätigkeiten und Bedürfnisse im Bereich der Cyberabwehr zeigte die Bestandsaufnahme zu den Bedürfnissen der Mitgliedstaaten im Bereich der Cyberabwehr, die im März 2018 vom Europäischen Auswärtigen Dienst durchgeführt wurde, dass die meisten Mitgliedstaaten einen Mehrwert in der Unterstützung der EU für die Schulung und Bildung im Cyberbereich sowie in der Unterstützung der Industrie durch Forschung und Entwicklung sehen[17]. Die Initiative würde in der Tat gemeinsam mit den Mitgliedstaaten oder den von ihnen unterstützten Einrichtungen umgesetzt. Kooperationen zwischen den Fachkreisen in Industrie, Forschung und/oder öffentlichem Sektor sollten bestehende Einrichtungen zusammenbringen und stärken, ohne neue zu schaffen. Die Mitgliedstaaten würden auch an der Festlegung spezifischer Maßnahmen beteiligt, die auf den öffentlichen Sektor als unmittelbaren Nutzer von Cybersicherheitstechnik und -Know-how abzielen.

- **Folgenabschätzung**

Am 11. April 2017 wurde dem Ausschuss für Regulierungskontrolle eine Folgenabschätzung zur Untermauerung dieser Initiative vorgelegt; dieser gab eine befürwortende Stellungnahme mit Vorbehalten ab. Die Folgenabschätzung wurde anschließend im Lichte der Bemerkungen des Ausschusses überprüft. Die Stellungnahme des Ausschusses und der Anhang, in dem erläutert wird, wie auf die Bemerkungen des Ausschusses eingegangen wurde, werden zusammen mit dem vorliegenden Vorschlag veröffentlicht.

In der Folgenabschätzung wurde eine Reihe von politischen Optionen sowohl legislativer als auch nichtlegislativer Art geprüft. Folgende Optionen wurden für eine eingehende Prüfung ausgewählt:

- Basisszenario: kooperative Option – geht von der Fortsetzung des derzeitigen Konzepts für den Aufbau industrieller und technischer Kapazitäten im Bereich der Cybersicherheit in der EU aus, indem Forschung und Innovation sowie damit verbundene Mechanismen für die Zusammenarbeit im Rahmen des 9. RP unterstützt werden;
- Option 1: Cybersicherheitskompetenznetz und Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung mit einem doppelten Mandat, sowohl zur Förderung von Industrietechnologien als auch im Bereich Forschung und Innovation zu ergreifen;

15 Z. B. hochrangiges Rundtischgespräch zwischen den Mitgliedstaaten, Vizepräsident Ansip und Kommissarin Gabriel, 5. Dezember 2017.

16 Rat (Allgemeine Angelegenheiten): Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen (20. November 2017).

17 EAD, März 2018.

- Option 2: Cybersicherheitskompetenznetz und Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung mit Schwerpunkt auf Forschungs- und Innovationstätigkeiten.

Die bereits in einem frühen Stadium verworfenen Optionen waren: 1) überhaupt keine Maßnahme zu ergreifen, 2) nur das Cybersicherheitskompetenznetz einzurichten, 3) nur eine zentrale Struktur zu schaffen und 4) eine bestehende Agentur (Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), Exekutivagentur für die Forschung (REA) oder Exekutivagentur für Forschung, Innovation und Netze (INEA)) zu beauftragen.

Die Analyse führte zu dem Schluss, dass die Option 1 am besten geeignet ist, um die Ziele der Initiative zu erreichen und zugleich die größte wirtschaftliche, gesellschaftliche und ökologische Wirkung zu erzielen sowie die Interessen der Union zu wahren. Für diese Option sprach vor allem Folgendes: die Möglichkeit, eine echte Industriepolitik für Cybersicherheit zu schaffen, indem nicht nur die Forschung und Entwicklung, sondern auch Tätigkeiten zur Markteinführung gefördert werden; die Flexibilität, unterschiedliche Kooperationsmodelle mit dem Netz von Kompetenzzentren zu ermöglichen, um die Nutzung der vorhandenen Kenntnisse und Ressourcen zu optimieren; die Möglichkeit, die Zusammenarbeit und die gemeinsamen Verpflichtungen der öffentlichen und privaten Akteure aus allen einschlägigen Bereichen, einschließlich der Verteidigung, zu strukturieren. Nicht zuletzt ermöglicht Option 1 auch größere Synergien und kann als Durchführungsmechanismus für zwei verschiedene EU-Finanzierungsströme im Bereich der Cybersicherheit innerhalb des nächsten mehrjährigen Finanzrahmens (Programm „Digitales Europa“ und Programm „Horizont Europa“) dienen.

- **Grundrechte**

Diese Initiative wird es den Behörden und Unternehmen der Mitgliedstaaten ermöglichen, sich wirksamer gegen Cyberbedrohungen zu wappnen und diese abzuwehren, indem sicherere Produkte und Lösungen bereitstehen und sich selbst damit ausrüsten. Dies ist insbesondere für den Schutz des Zugangs zu wesentlichen Dienstleistungen (z. B. Verkehr, Gesundheit, Banken und Finanzdienstleistungen) von Bedeutung.

Die Stärkung der Fähigkeit der Europäischen Union, ihre Produkte und Dienste selbst zu sichern, dürfte ferner den Bürgerinnen und Bürgern helfen, ihre demokratischen Rechte auszuüben und nach ihren Werten zu leben (z. B. durch einen besseren Schutz ihrer in der Charta der Grundrechte verankerten informationellen Rechten, insbesondere des Rechts auf Schutz personenbezogener Daten und des Privatlebens), und damit ihr Vertrauen in die digitale Gesellschaft und Wirtschaft stärken.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung wird in Zusammenarbeit mit dem Cybersicherheitskompetenznetz die wichtigste Durchführungsstelle für die Verwendung von EU-Finanzmitteln für die Cybersicherheit im Rahmen des Programms „Digitales Europa“ und des Programms „Horizont Europa“ sein.

Die Auswirkungen auf den Haushalt im Zusammenhang mit der Durchführung des Programms „Digitales Europa“ sind im Finanzbogen im Anhang dieses Vorschlags im Einzelnen aufgeführt. Der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft“ des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit“ des Programms „Horizont Europa“ (insgesamt 2 800 000 000 EUR) nach Artikel 21 Absatz 1 Buchstabe b wird von der Kommission im Laufe des

Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen. Der Vorschlag stützt sich auf das Ergebnis des strategischen Planungsprozesses gemäß Artikel 6 Absatz 6 der Verordnung XXX [Rahmenprogramm „Horizont Europa“].

5. WEITERE ANGABEN

- **Durchführungspläne sowie Überwachungs-, Bewertungs- und Berichterstattungsmodalitäten**

Dieser Vorschlag sieht eine explizite Bewertungs- und Überprüfungsklausel (Artikel 38) vor, wonach die Kommission eine unabhängige Bewertung durchführen wird, vorgesehen. Die Kommission wird dem Europäischen Parlament und dem Rat in der Folgezeit über die Ergebnisse ihrer Bewertung Bericht erstatten, erforderlichenfalls zusammen mit einem Vorschlag zur Überarbeitung des Rechtsakts, um die Auswirkungen der Verordnung und ihren Mehrwert zu ermitteln. Dabei wird die Bewertungsmethodik der Leitlinien der Kommission für eine bessere Rechtsetzung angewandt werden.

Der Exekutivdirektor sollte dem Verwaltungsrat gemäß Artikel 17 dieses Vorschlags alle zwei Jahre eine Ex-post-Bewertung der Tätigkeiten Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes vorlegen. Außerdem sollte der Exekutivdirektor einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen nachträglicher Bewertungen erstellen und der Kommission alle zwei Jahre über die Fortschritte berichten. Der Verwaltungsrat sollte dafür zuständig sein, die angemessene Weiterbehandlung solcher Schlussfolgerungen gemäß Artikel 16 zu verfolgen.

Mutmaßliche Missstände in der Tätigkeit der Einrichtung können vom Europäischen Bürgerbeauftragten nach Artikel 228 des Vertrags über die Arbeitsweise der Europäischen Union untersucht werden.

2018/0328 (COD)

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

Ein Beitrag der Europäischen Kommission zur Tagung der Staats- und Regierungschefs vom 19.–20. September 2018 in Salzburg

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 173 Absatz 3 und Artikel 188 Absatz 1,

auf Vorschlag der Europäischen Kommission,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[18],

nach Stellungnahme des Ausschusses der Regionen[19],

nach dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Da das tägliche Leben und die Wirtschaft in zunehmendem Maße von digitalen Technologien bestimmt werden, sind die Bürger den damit verbundenen Gefahren immer stärker ausgesetzt. Die künftige Sicherheit hängt unter anderem davon ab, dass die Union die technischen und industriellen Fähigkeiten zum Schutz vor Cyberbedrohungen verbessert, da sowohl die zivile Infrastruktur als auch die militärischen Kapazitäten auf sichere digitale Systeme angewiesen sind.

(2) Die Union hat ihre Maßnahmen zur Bewältigung der wachsenden Herausforderungen im Bereich der Cybersicherheit nach der Cybersicherheitsstrategie[20] von 2013, mit der ein zuverlässiges, sicheres und offenes Cyberökosystem gefördert werden soll, kontinuierlich ausgebaut. Im Jahr 2016 erließ die Union mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[21] über die Sicherheit von Netz- und Informationssystemen ihre ersten Rechtsvorschriften im Bereich der Cybersicherheit.

---

18 ABl. C ... vom ..., S. .

19 ABl. C ... vom ..., S. .

20 Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, JOIN(2013) 1 final.

21 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) Im September 2017 legten die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik eine Gemeinsame Mitteilung mit dem Titel „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“[22] vor, um die Abwehrfähigkeit, Abschreckung und Abwehr der EU im Bereich der Cyberangriffe weiter zu stärken.

(4) Auf dem Digitalgipfel im September 2017 in Tallinn forderten die Staats- und Regierungschefs die Union auf, „Europa bis zum Jahr 2025 weltweit zum Vorreiter in Sachen Cybersicherheit 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“.

(5) Schwere Störungen von Netz- und Informationssystemen können einzelne Mitgliedstaaten und die Union als Ganzes beeinträchtigen. Sichere Netz- und Informationssysteme sind daher unerlässlich für das reibungslose Funktionieren des Binnenmarkts. Derzeit ist die Union von nichteuropäischen Cybersicherheitsanbietern abhängig. Es liegt jedoch im strategischen Interesse der Union, dass sie wesentliche technische Kapazitäten im Bereich der Cybersicherheit wahrt und weiterentwickelt, die zur Sicherung ihres digitalen Binnenmarkts unverzichtbar sind, damit insbesondere kritische Netze und Informationssysteme geschützt und zentrale Cybersicherheitsdienste bereitgestellt werden können.

(6) In der Union gibt es eine Fülle von Fachwissen und Erfahrungen in Forschung, Technologie und industrieller Entwicklung im Bereich der Cybersicherheit, jedoch sind die Anstrengungen in Forschung und Industrie fragmentiert; es mangelt an Einheitlichkeit und einer gemeinsamen Zugrichtung, worunter die Wettbewerbsfähigkeit in diesem Bereich leidet. Diese Anstrengungen und dieses Fachwissen müssen gebündelt, vernetzt und in effizienter Weise genutzt werden, um die vorhandenen Forschungs-, Technologie- und Industriekapazitäten auf Ebene der Union und der Mitgliedstaaten zu stärken und zu ergänzen.

(7) In den Schlussfolgerungen des Rates vom November 2017 wurde die Kommission aufgefordert, rasch eine Folgenabschätzung der möglichen Optionen für die Schaffung eines Netzes von Cybersicherheitskompetenzzentren unter dem Dach des Europäischen Kompetenzzentrums für Cybersicherheitsforschung vorzunehmen und bis Mitte 2018 das einschlägige Rechtsinstrument vorzuschlagen.

(8) Das Kompetenzzentrum sollte das wichtigste Instrument der Union sein, um Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich der Cybersicherheit zu bündeln sowie einschlägige Projekte und Initiativen zusammen mit dem Cybersicherheitskompetenznetz durchzuführen. Es sollte finanzielle Unterstützung aus den Programmen „Horizont Europa“ und „Digitales Europa“ für den Bereich der Cybersicherheit bereitstellen und gegebenenfalls auch für den Europäischen Fonds für regionale Entwicklung und andere Programme offen stehen. Dieser Ansatz sollte dazu beitragen, Synergien zu schaffen und die finanzielle Unterstützung im Zusammenhang mit Forschung, Innovation, Technologie und industrieller Entwicklung im Bereich der Cybersicherheit zu koordinieren und Doppelarbeit zu vermeiden.

[22] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, JOIN(2017) 450 final.

(9) Angesichts der Tatsache, dass die Ziele dieser Initiative am besten erreicht werden können, wenn sich alle Mitgliedstaaten oder so viele Mitgliedstaaten wie möglich beteiligen, und um den Mitgliedstaaten einen Anreiz für die Beteiligung zu geben, sollten nur Mitgliedstaaten, die sich finanziell an den Verwaltungs- und Betriebskosten des Kompetenzzentrums beteiligen, stimmberechtigt sein.

(10) Der Finanzbeitrag der beteiligten Mitgliedstaaten sollte dem der Union zu dieser Initiative angemessen sein.

(11) Das Kompetenzzentrum sollte die Arbeit des Cybersicherheitskompetenznetzes (im Folgenden das „Netz"), das aus den nationalen Koordinierungszentren der einzelnen Mitgliedstaaten besteht, erleichtern und einen Beitrag dazu leisten. Die nationalen Koordinierungszentren sollten eine direkte finanzielle Unterstützung durch die Union erhalten, einschließlich Finanzhilfen, die ohne Aufforderung zur Einreichung von Vorschlägen vergeben werden, um Tätigkeiten im Zusammenhang mit dieser Verordnung durchzuführen.

(12) Die nationalen Koordinierungszentren sollten von den Mitgliedstaaten ausgewählt werden. Zusätzlich zu den erforderlichen Verwaltungskapazitäten sollten die Zentren 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 den Fachkreisen der Industrie, des öffentlichen Sektors – einschließlich der gemäß der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[23] benannten Behörden – und der Forschung auszutauschen und zu koordinieren.

(13) Wird den nationalen Koordinierungszentren eine finanzielle Unterstützung gewährt, um Dritte auf nationaler Ebene zu unterstützen, wird diese im Wege von abgestuften Finanzhilfevereinbarungen an die einschlägigen Akteure weitergegeben.

(14) Neu aufkommende Technologien wie künstliche Intelligenz, das Internet der Dinge, Hochleistungsrechnen (High-Performance Computing, HPC) und Quanteninformatik, Blockchain-Technologie und Konzepte wie sichere digitale Identitäten bringen gleichzeitig neue Herausforderungen für die Cybersicherheit, aber auch neue Lösungen mit sich. Die Bewertung und Validierung der Robustheit bestehender oder künftiger IKT-Systeme wird die Erprobung von Sicherheitslösungen gegen mithilfe von Hochleistungs- und Quantenrechnern ausgeführte Angriffe erforderlich machen. Das Kompetenzzentrum, das Netz und die Kompetenzgemeinschaft für Cybersicherheit sollten helfen, die neuesten Cybersicherheitslösungen voranzubringen und zu verbreiten. Gleichzeitig sollten das Kompetenzzentrum und das Netz Entwicklern und Betreibern in kritischen Bereichen wie Verkehr, Energie, Gesundheit, Finanzen, Behörden, Telekommunikation, Fertigung, Verteidigung und Raumfahrt zur Verfügung stehen, um sie bei der Bewältigung ihre Herausforderungen im Bereich der Cybersicherheit zu unterstützen.

(15) Das Kompetenzzentrum sollte mehrere Schlüsselfunktionen haben. Erstens sollte das Kompetenzzentrum die Arbeit des Europäischen Cybersicherheitskompetenznetzes

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

erleichtern und dessen Koordinierung unterstützen sowie die Kompetenzgemeinschaft für Cybersicherheit fördern. Das Zentrum sollte die Technologieagenda im Bereich der Cybersicherheit vorantreiben und den Zugang zu dem vom Netz und der Kompetenzgemeinschaft für Cybersicherheit zusammengeführten Fachwissen erleichtern. Zweitens sollten die einschlägigen Teile der Programme „Digitales Europa“ und „Horizont Europa“ durch Vergabe von Finanzhilfen, in der Regel nach einer wettbewerbsorientierten Aufforderung zur Einreichung von Vorschlägen, umgesetzt werden. Drittens sollte das Kompetenzzentrum gemeinsame Investitionen der Union, der Mitgliedstaaten und/oder der Industrie erleichtern.

(16) Das Kompetenzzentrum sollte die Zusammenarbeit und Koordinierung der Tätigkeiten der Kompetenzgemeinschaft für Cybersicherheit anregen und unterstützen, wodurch eine große, offene und vielfältige Gruppe von Akteuren entstünde, die sich Cybersicherheitstechnik befassen. Diese Gemeinschaft sollte insbesondere Forschungseinrichtungen, anbietende und nachfragende Branchen sowie den öffentlichen Sektor umfassen. Die Kompetenzgemeinschaft für Cybersicherheit sollte einen Beitrag zu den Tätigkeiten und dem Arbeitsplan des Kompetenzzentrums leisten und auch von den Tätigkeiten des Kompetenzzentrums und des Netzes zum Aufbau der Gemeinschaft profitieren; darüber hinaus sollte sie aber im Hinblick auf Aufforderungen zur Einreichung von Vorschlägen oder Ausschreibungen nicht bevorzugt werden.

(17) Um den Erfordernissen sowohl der anbietenden als auch der nachfragenden Branchen gerecht zu werden, sollte sich der Auftrag des Kompetenzzentrums zur Bereitstellung von Fachwissen und technischer Unterstützung im Bereich der Cybersicherheit für die Industrie auf IKT-Produkte und -Dienste sowie auf alle anderen industriellen und technischen Produkte und Lösungen beziehen, in denen Cybersicherheit einzubinden ist.

(18) Das Kompetenzzentrum und das Netz sollten sich um Synergien zwischen dem zivilen und dem Verteidigungssektor im Bereich der Cybersicherheit bemühen; die im Rahmen des Programms „Horizont Europa“ finanzierten Projekte werden jedoch im Einklang mit der Verordnung XXX [Verordnung über „Horizont Europa“] durchgeführt, in der festgelegt ist, dass bei Forschungs- und Innovationstätigkeiten im Rahmen von „Horizont Europa“ der Schwerpunkt auf zivilen Anwendungen liegen soll.

(19) Um eine strukturierte und nachhaltige Zusammenarbeit zu gewährleisten, sollte die Beziehung zwischen dem Kompetenzzentrum und den nationalen Koordinierungszentren auf einer vertraglichen Vereinbarung beruhen.

(20) Um die Haftung des Kompetenzzentrums zu regeln und seine Transparenz zu gewährleisten, sollten geeignete Regelungen getroffen werden.

(21) Angesichts ihres jeweiligen Fachwissens im Bereich der Cybersicherheit sollten sich die Gemeinsame Forschungsstelle der Kommission (JRC) sowie die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) aktiv an der Kompetenzgemeinschaft für Cybersicherheit und dem wissenschaftlich-technischen Beirat beteiligen.

(22) Erhalten sie einen Finanzbeitrag aus dem Unionshaushalt, sollten die nationalen Koordinierungszentren und die Einrichtungen, die Teil der Kompetenzgemeinschaft für Cybersicherheit sind, öffentlich machen, dass die jeweiligen Tätigkeiten im Rahmen der vorliegenden Initiative durchgeführt werden.

(23) Mit dem Unionsbeitrag zum Kompetenzzentrum sollte die Hälfte der Kosten für die Einrichtung sowie für die Verwaltungs- und Koordinierungstätigkeiten des Kompetenzzentrums finanziert werden. Um eine Doppelfinanzierung zu vermeiden, sollten in diese Tätigkeiten nicht gleichzeitig auch Mittel aus anderen Unionsprogrammen fließen.

(24) Der Verwaltungsrat des Kompetenzzentrums, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, sollte die allgemeine Ausrichtung der Tätigkeit des Kompetenzzentrums festlegen und dafür sorgen, dass es seine Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte über die erforderlichen Befugnisse verfügen, um den Haushaltsplan zu erstellen und dessen Ausführung zu überprüfen, eine angemessene Finanzordnung und transparente Verfahren für die Entscheidungsfindung des Kompetenzzentrums festzulegen, den Arbeitsplan und den mehrjährigen Strategieplan, die die Prioritäten bei der Erfüllung der Ziele und der Aufgaben des Kompetenzzentrums widerspiegeln, sowie seine Geschäftsordnung anzunehmen, den Exekutivdirektor zu ernennen und über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen.

(25) Damit das Kompetenzzentrum seine Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in Funktionsbereichen verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.

(26) Damit das Kompetenzzentrum reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt und seine Aufgaben völlig unabhängig wahrnimmt.

(27) Das Kompetenzzentrum sollte über einen wissenschaftlich-technischen Beirat als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen und sonstigen Interessenträgern sicherzustellen. Der wissenschaftlich-technische Beirat sollte sich auf für die Interessenträger relevante Fragen konzentrieren und sie dem Verwaltungsrat des Kompetenzzentrums zur Kenntnis bringen. Die Zusammensetzung des wissenschaftlich-technischen Beirats und die ihm übertragenen Aufgaben, z. B. seine Befragung im Zusammenhang mit dem Arbeitsplan, sollten eine ausreichende Vertretung der Interessenträger in der Arbeit des Kompetenzzentrums gewährleisten.

(28) Das Kompetenzzentrum sollte durch seinen wissenschaftlich-technischen Beirat während der Laufzeit des Programms Horizont 2020 von dem besonderen Fachwissen und der breiten Vertretung der einschlägigen Interessenträger in der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit profitieren.

(29) Das Kompetenzzentrum sollte Vorschriften zur Vermeidung und Handhabung von Interessenkonflikten haben. Das Kompetenzzentrum sollte die einschlägigen Bestimmungen der Union in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des

Rates[24] anwenden. Die Verarbeitung personenbezogener Daten durch das Kompetenzzentrum unterliegt der Verordnung (EU) XXX/2018 des Europäischen Parlaments und des Rates. Das Kompetenzzentrum sollte die für die Unionsorgane geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der EU, sowie die entsprechenden einzelstaatlichen Rechtsvorschriften befolgen.

(30) Die finanziellen Interessen der Union und der Mitgliedstaaten sollten während des gesamten Ausgabenzyklus durch angemessene Maßnahmen geschützt werden; dazu gehören unter anderem Maßnahmen zur Prävention, Aufdeckung und Untersuchung von Unregelmäßigkeiten, die Rückforderung entgangener, zu Unrecht gezahlter oder nicht widmungsgemäß verwendeter Mittel und gegebenenfalls verwaltungsrechtliche und finanzielle Sanktionen gemäß der Verordnung (EU, Euratom) XXX des Europäischen Parlaments und des Rates[25] [die Haushaltsordnung].

(31) Das Kompetenzzentrum sollte seine Geschäftstätigkeit in offener und transparenter Weise ausüben; daher sollte es alle relevanten Informationen fristgerecht übermitteln und seine Tätigkeiten bekannt machen, unter anderem auch durch an die Öffentlichkeit gerichtete Informations- und Verbreitungsmaßnahmen. Die Geschäftsordnungen der Organe des Kompetenzzentrums sollten öffentlich zugänglich gemacht werden.

(32) Der Interne Prüfer der Kommission sollte gegenüber dem Kompetenzzentrum die gleichen Befugnisse ausüben wie gegenüber der Kommission.

(33) Die Kommission, das Kompetenzzentrum, der Rechnungshof und das Europäische Amt für Betrugsbekämpfung sollten Zugang zu allen Informationen und Räumlichkeiten erhalten, die für die Durchführung von Rechnungsprüfungen und Untersuchungen in Bezug auf die vom Kompetenzzentrum unterzeichneten Finanzhilfen, Aufträge und Vereinbarungen erforderlich sind.

(34) Da die Ziele dieser Verordnung – nämlich die Wahrung und Weiterentwicklung der technischen und industriellen Kapazitäten der Union im Bereich der Cybersicherheit, die Steigerung der Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union und die Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil der anderen Wirtschaftszweige der Union – von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, weil die vorhandenen begrenzten Ressourcen weit verstreut und umfangreiche Investitionen erforderlich sind, sondern vielmehr besser auf Unionsebene zu verwirklichen sind, um unnötige Doppelarbeit bei diesen Anstrengungen zu vermeiden, die kritische Investitionsmasse zu erreichen und sicherzustellen, dass die öffentlichen Mittel optimal genutzt werden, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus —

---

[24] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

[25] [Titel und ABl.-Fundstelle einfügen]

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN UND GRUNDSÄTZE DES KOMPETENZZENTRUMS UND DES NETZES

Artikel 1

Gegenstand

(1) Mit dieser Verordnung werden das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung (im Folgenden das „Kompetenzzentrum“) sowie das Netz nationaler Koordinierungszentren eingerichtet und Bestimmungen für die Benennung nationaler Koordinierungszentren sowie für die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit festgelegt.

(2) Das Kompetenzzentrum trägt zur Umsetzung der Cybersicherheitskomponente des mit der Verordnung (EU) XXX eingerichteten Programms „Digitales Europa“, insbesondere zu den Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) XXX [Programm „Digitales Europa“] und des mit der Verordnung (EU) XXX eingerichteten Programms „Horizont Europa“ sowie insbesondere des Anhangs I Pfeiler II Abschnitt 2.2.6 des Beschlusses XXX über das Spezifische Programm zur Durchführung von Horizont Europa – Rahmenprogramm für Forschung und Innovation [Ref.-Nummer des Spezifischen Programms] – bei.

(3) Sitz des Kompetenzzentrums ist [Brüssel, Belgien].

(4) Das Kompetenzzentrum besitzt Rechtspersönlichkeit. Es verfügt in jedem Mitgliedstaat über die weitestgehende Rechts- und Geschäftsfähigkeit, die Rechtspersonen nach dessen Rechtsvorschriften zuerkannt wird. Es kann insbesondere bewegliches und unbewegliches Vermögen erwerben und veräußern und ist vor Gericht parteifähig.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

(1) „Cybersicherheit“ den Schutz von Netz- und Informationssystemen, deren Nutzern und sonstigen Personen vor Cyberbedrohungen;

(2) „Cybersicherheitsprodukte und -lösungen“ IKT-Produkte, -Dienste oder -Prozesse, die dem besonderen Zweck dienen, Netz- und Informationssysteme, deren Nutzer und betroffene Personen vor Cyberbedrohungen zu schützen;

(3) „Behörde“ eine Regierungsstelle oder andere Stelle der öffentlichen Verwaltung, einschließlich öffentlicher beratender Gremien, auf nationaler, regionaler oder lokaler Ebene oder eine natürliche oder juristische Person, die aufgrund innerstaatlichen Rechts Aufgaben oder bestimmte Pflichten der öffentlichen Verwaltung wahrnimmt;

(4) „beteiligter Mitgliedstaat“ einen Mitgliedstaat, der freiwillig einen Finanzbeitrag zu den Verwaltungs- und Betriebskosten des Kompetenzzentrums leistet.

Artikel 3

Auftrag des Zentrums und des Netzes

(1) Das Kompetenzzentrum und das Netz unterstützen die Union bei

a) der Wahrung und Weiterentwicklung der technischen und industriellen Cybersicherheitskapazitäten, die zur Sicherung des digitalen Binnenmarkts der Union nötig sind;

b) der Steigerung der Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union und der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der Union.

(2) Das Kompetenzzentrum nimmt seine Aufgaben gegebenenfalls in Zusammenarbeit mit dem Netz nationaler Koordinierungszentren und einer Kompetenzgemeinschaft für Cybersicherheit wahr.

Artikel 4

Ziele und Aufgaben des Zentrums

Das Kompetenzzentrum hat folgende Ziele und damit verbundene Aufgaben:

(1) Erleichterung und Unterstützung der Koordinierung der Arbeiten des Netzes nationaler Koordinierungszentren (im Folgenden das „Netz“) gemäß Artikel 6 und der Kompetenzgemeinschaft für Cybersicherheit gemäß Artikel 8;

(2) Beitrag zur Umsetzung der Cybersicherheitskomponente des mit der Verordnung (EU) XXX[26] eingerichteten Programms „Digitales Europa“, insbesondere zu den Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) XXX [Programm „Digitales Europa“] und des mit der Verordnung (EU) XXX[27] eingerichteten Programms „Horizont Europa“ sowie insbesondere des Anhangs I Pfeiler II Abschnitt 2.2.6 des Beschlusses XXX über das Spezifische Programm zur Durchführung von Horizont Europa – Rahmenprogramm für Forschung und Innovation [Ref.-Nummer des Spezifischen Programms] und anderer Unionsprogramme, sofern in Rechtsakten der Union vorgesehen;

(3) Verbesserung der Kapazitäten, des Wissens und der Infrastrukturen im Bereich der Cybersicherheit, die der Industrie, dem öffentlichen Sektor und der Forschung zur Verfügung stehen, indem folgende Aufgaben wahrgenommen werden:

a) in Bezug auf die modernsten industriellen und Forschungsinfrastrukturen im Bereich der Cybersicherheit und zugehörige Dienste: Erwerb, Modernisierung, Betrieb und Bereitstellung solcher Infrastrukturen und zugehöriger Dienste für ein breites Spektrum von Nutzern aus der gesamten Union von der Industrie, darunter KMU, und dem öffentlichen Sektor bis zur Forschung und Wissenschaft;

b) in Bezug auf die modernsten industriellen und Forschungsinfrastrukturen im Bereich der Cybersicherheit und zugehörige Dienste: Unterstützung – auch finanziell – anderer Einrichtungen bei Erwerb, Modernisierung, Betrieb und Bereitstellung solcher Infrastrukturen und zugehöriger Dienste für ein breites

[26] [Vollständigen Titel und ABl.-Fundstelle einfügen]
[27] [Vollständigen Titel und ABl.-Fundstelle einfügen]

Spektrum von Nutzern aus der gesamten Union von der Industrie, darunter KMU, und dem öffentlichen Sektor bis zur Forschung und Wissenschaft;

c) Bereitstellung von Fachwissen und technischer Unterstützung im Bereich der Cybersicherheit für Industrie und Behörden, insbesondere durch Unterstützung von Maßnahmen zur Erleichterung des Zugangs zum Fachwissen, das im Netz und der Kompetenzgemeinschaft für Cybersicherheit verfügbar ist;

(4) Beitrag zur umfassenden Einführung modernster Cybersicherheitsprodukte und -lösungen in der gesamten Wirtschaft, indem folgende Aufgaben wahrgenommen werden:

a) Förderung der Cybersicherheitsforschung und -entwicklung und Verbreitung von Cybersicherheitsprodukten und -lösungen der Union durch Behörden und Anwenderbranchen;

b) Unterstützung von Behörden, nachfragenden Branchen und anderen Nutzern bei der Einführung und Integration der neuesten Cybersicherheitslösungen;

c) Unterstützung insbesondere der Behörden bei der Organisation oder Durchführung der öffentlichen Auftragsvergabe für modernste Cybersicherheitsprodukte und -lösungen im Namen von Behörden;

d) Leistung finanzieller und technischer Unterstützung für Start-ups und KMU im Bereich der Cybersicherheit, um potenzielle Märkte zu erschließen und Investitionen anzuziehen;

(5) Verbesserung des Verständnisses der Cybersicherheit und Beitrag zur Verringerung des Qualifikationsdefizits im Zusammenhang mit der Cybersicherheit in der Union, indem folgende Aufgaben wahrgenommen werden:

a) Unterstützung der weiteren Entwicklung von Cybersicherheitskompetenzen, gegebenenfalls in Zusammenarbeit mit den einschlägigen Agenturen und Einrichtungen der EU, einschließlich der ENISA;

(6) Beitrag zur Stärkung der Cybersicherheitsforschung und -entwicklung in der Union durch:

a) finanzielle Unterstützung der Forschungsbemühungen im Bereich der Cybersicherheit auf der Grundlage einer gemeinsamen, kontinuierlich bewerteten und verbesserten mehrjährigen strategischen Industrie-, Technologie- und Forschungsagenda;

b) Förderung großer Forschungs- und Demonstrationsprojekte im Hinblick auf die nächste Generation der technischen Kapazitäten im Bereich der Cybersicherheit in Zusammenarbeit mit der Branche und dem Netz;

c) Unterstützung von Forschung und Innovation für die Normung auf dem Gebiet der Cybersicherheitstechnik;

(7) Verbesserung der Zusammenarbeit zwischen zivilen und militärischen Fachkreisen in Bezug auf Technologien und Anwendungen mit doppeltem Verwendungszweck im Bereich der Cybersicherheit, indem folgende Aufgaben wahrgenommen werden:

a) Unterstützung der Mitgliedstaaten sowie der Industrie- und Forschungsakteure bei der Forschung, Entwicklung und Einführung;

b) Beitrag zur Zusammenarbeit zwischen den Mitgliedstaaten durch Unterstützung der Ausbildung sowie von Schulungsmaßnahmen und Übungen;

c) Zusammenführung der Interessenträger zur Förderung von Synergien zwischen zivilen und militärischen Forschungstätigkeiten und Märkten im Bereich der Cybersicherheit;

(8) Steigerung der Synergien zwischen der zivilen und verteidigungspolitischen Dimension der Cybersicherheit im Zusammenhang mit dem Europäischen Verteidigungsfonds, indem folgende Aufgaben wahrgenommen werden:

a) Beratung, Austausch von Fachwissen und Erleichterung der Zusammenarbeit zwischen den einschlägigen Beteiligten;

b) auf Antrag der Mitgliedstaaten Verwaltung multinationaler Cyberabwehrprojekte und damit Handeln als Projektmanager im Sinne der Verordnung (EU) XXX [Verordnung zur Einrichtung des Europäischen Verteidigungsfonds].

Artikel 5

Investitionen in Infrastrukturen, Kapazitäten, Produkte oder Lösungen und deren Nutzung

(1) Stellt das Kompetenzzentrum Mittel für Infrastrukturen, Kapazitäten, Produkte oder Lösungen gemäß Artikel 4 Absätze 3 und 4 in Form von Finanzhilfen oder Preisgeldern zur Verfügung, so kann im Arbeitsplan des Kompetenzzentrums insbesondere Folgendes festgelegt werden:

a) Vorschriften für den Betrieb einer Infrastruktur oder Kapazität, gegebenenfalls einschließlich der Übertragung des Betriebs auf eine Aufnahmeeinrichtung auf der Grundlage von Kriterien, die das Kompetenzzentrum festlegt;

b) Vorschriften für den Zugang zu einer Infrastruktur oder Kapazität und deren Nutzung.

(2) Das Kompetenzzentrum kann die Gesamtdurchführung einschlägiger gemeinsamer Vergabeverfahren übernehmen, einschließlich der vorkommerziellen Auftragsvergabe im Namen von Mitgliedern des Netzes, von Mitgliedern der Kompetenzgemeinschaft für Cybersicherheit oder von Dritten, die die Nutzer von Cybersicherheitsprodukten und -lösungen vertreten. Zu diesem Zweck kann das Kompetenzzentrum von einem oder mehreren nationalen Koordinierungszentren oder Mitgliedern der Kompetenzgemeinschaft für Cybersicherheit unterstützt werden.

Artikel 6

Benennung der nationalen Koordinierungszentren

(1) Bis zum [Datum] benennt jeder Mitgliedstaat die Einrichtung, die als nationales Koordinierungszentrum für die Zwecke dieser Verordnung dienen soll, und teilt diese der Kommission mit.

(2) Auf der Grundlage einer Bewertung, ob diese Einrichtung die in Absatz 4 festgelegten Kriterien erfüllt, entscheidet die Kommission innerhalb von sechs Monaten nach der Benennung durch den Mitgliedstaat darüber, ob der Einrichtung die Akkreditierung als nationales Koordinierungszentrum gewährt oder die Benennung abgelehnt wird. Die Liste der nationalen Koordinierungszentren wird von der Kommission veröffentlicht.

(3) Die Mitgliedstaaten können jederzeit eine neue Einrichtung als nationales Koordinierungszentrum für die Zwecke dieser Verordnung benennen. Die Absätze 1 und 2 gelten für die Benennung jeder neuen Einrichtung.

(4) Das benannte nationale Koordinierungszentrum muss in der Lage sein, das Kompetenzzentrum und das Netz bei der Erfüllung ihres Auftrags gemäß Artikel 3 dieser Verordnung zu unterstützen. Es muss entweder über technisches Fachwissen im Bereich der Cybersicherheit verfügen oder direkten Zugang dazu haben und in der Lage sein, sich wirksam mit der Industrie, dem öffentlichen Sektor und der Forschungsgemeinschaft auszutauschen und zu koordinieren.

(5) Die Beziehungen zwischen dem Kompetenzzentrum und den nationalen Koordinierungszentren beruhen auf einer vertraglichen Vereinbarung zwischen dem Kompetenzzentrum und den einzelnen nationalen Koordinierungszentren. Die Vereinbarung regelt die Beziehungen und die Aufgabenverteilung zwischen dem Kompetenzzentrum und den einzelnen nationalen Koordinierungszentren.

(6) Dem Netz nationaler Koordinierungszentren gehören alle von den Mitgliedstaaten benannten nationalen Koordinierungszentren an.

Artikel 7

Aufgaben der nationalen Koordinierungszentren

(1) Die nationalen Koordinierungszentren haben folgende Aufgaben:

a) Unterstützung des Kompetenzzentrums bei der Erreichung seiner Ziele und insbesondere bei der Koordinierung der Kompetenzgemeinschaft für Cybersicherheit;

b) Erleichterung der Beteiligung der Branche und anderer Akteure auf der Ebene der Mitgliedstaaten an grenzübergreifenden Projekten;

c) Beitrag zur Bestimmung und Bewältigung sektorspezifischer Herausforderungen im Bereich der Cybersicherheit, gemeinsam mit dem Kompetenzzentrum;

d) Tätigkeit als Kontaktstelle auf nationaler Ebene für die Kompetenzgemeinschaft für Cybersicherheit und das Kompetenzzentrum;

e) Bemühung um die Schaffung von Synergien mit einschlägigen Tätigkeiten auf nationaler und regionaler Ebene;

f) Durchführung spezifischer Maßnahmen, für die das Kompetenzzentrum Finanzhilfen gewährt hat, unter anderem durch finanzielle Unterstützung Dritter gemäß Artikel 204 der Verordnung XXX [neue Haushaltsordnung] unter den in den betreffenden Finanzhilfevereinbarungen festgelegten Bedingungen;

g) Förderung und Verbreitung der einschlägigen Ergebnisse der Arbeiten des Netzes, der Kompetenzgemeinschaft für Cybersicherheit und des Kompetenzzentrums auf nationaler oder regionaler Ebene;

h) Prüfung der Anträge von Einrichtungen, die in demselben Mitgliedstaat wie das Koordinierungszentrum niedergelassen sind, auf Aufnahme in die Kompetenzgemeinschaft für Cybersicherheit.

(2) Für die Zwecke des Buchstaben f kann die finanzielle Unterstützung Dritter in jeder in Artikel 125 der Verordnung XXX [neue Haushaltsordnung] genannten Form, auch in Form von Pauschalbeträgen, gewährt werden.

(3) Die nationalen Koordinierungszentren können im Einklang mit Artikel 195 Buchstabe d der Verordnung XXX [neue Haushaltsordnung] für die Wahrnehmung der in diesem Artikel festgelegten Aufgaben eine Finanzhilfe der Union erhalten.

(4) Für die Zwecke der in Absatz 1 Buchstaben a, b, c, e und g genannten Durchführungsaufgaben arbeiten die nationalen Koordinierungszentren gegebenenfalls über das Netz zusammen.

Artikel 8

Die Kompetenzgemeinschaft für Cybersicherheit

(1) Die Kompetenzgemeinschaft für Cybersicherheit leistet einen Beitrag zu dem in Artikel 3 festgelegten Auftrag des Kompetenzzentrums und fördert und verbreitet Fachwissen auf dem Gebiet der Cybersicherheit in der gesamten Union.

(2) Die Kompetenzgemeinschaft für Cybersicherheit besteht aus industriellen, akademischen und gemeinnützigen Forschungseinrichtungen und Verbänden sowie öffentlichen und anderen Einrichtungen, die sich mit betrieblichen und technischen Fragen befassen. Sie bringt die wichtigsten Interessenträger im Hinblick auf die technischen und industriellen Kapazitäten im Bereich der Cybersicherheit in der Union zusammen. Sie bezieht die nationalen Koordinierungszentren sowie die Organe und Einrichtungen der Union, die über einschlägiges Fachwissen verfügen, in ihre Arbeiten ein.

(3) Nur Einrichtungen, die in der Union niedergelassen sind, können als Mitglieder der Kompetenzgemeinschaft für Cybersicherheit akkreditiert werden. Sie müssen nachweisen, dass sie über Fachkompetenz auf dem Gebiet der Cybersicherheit in mindestens einem der folgenden Bereiche verfügen:

a) Forschung,

b) industrielle Entwicklung,

c) Schulung und Bildung.

(4) Das Kompetenzzentrum akkreditiert Einrichtungen, die nach nationalem Recht eingerichtet sind, als Mitglieder der Kompetenzgemeinschaft für Cybersicherheit, nachdem das nationale Koordinierungszentrum des Mitgliedstaats, in dem die Einrichtung niedergelassen ist, geprüft hat, ob diese Einrichtung die in Absatz 3 genannten Kriterien erfüllt. Eine Akkreditierung gilt unbefristet, kann jedoch vom Kompetenzzentrum jederzeit widerrufen werden, wenn es oder die zuständige nationale Koordinierungsstelle der Auffassung ist, dass die Einrichtung die in Absatz 3 genannten Kriterien nicht erfüllt oder unter die einschlägigen Bestimmungen des Artikels 136 der Verordnung XXX [neue Haushaltsordnung] fällt.

(5) Das Kompetenzzentrum akkreditiert einschlägige Stellen, Agenturen und Ämter der Union als Mitglieder der Kompetenzgemeinschaft für Cybersicherheit, nachdem es geprüft hat, ob diese die in Absatz 3 genannten Kriterien erfüllen. Eine Akkreditierung gilt unbefristet, kann jedoch vom Kompetenzzentrum jederzeit widerrufen werden, wenn es der Auffassung ist, dass die Einrichtung die in Absatz 3

genannten Kriterien nicht erfüllt oder unter die einschlägigen Bestimmungen des Artikels 136 der Verordnung XXX [neue Haushaltsordnung] fällt.

(6) Die Vertreter der Kommission können sich an der Arbeit der Gemeinschaft beteiligen.

Artikel 9

Aufgaben der Mitglieder der Kompetenzgemeinschaft für Cybersicherheit

Die Mitglieder der Kompetenzgemeinschaft für Cybersicherheit

1. unterstützen das Kompetenzzentrum bei der Erfüllung seines Auftrags und der in den Artikeln 3 und 4 festgelegten Ziele und arbeiten hierzu eng mit dem Kompetenzzentrum und den zuständigen nationalen Koordinierungszentren zusammen;
2. beteiligen sich an vom Kompetenzzentrum und den nationalen Koordinierungszentren geförderten Tätigkeiten;
3. beteiligen sich gegebenenfalls an Arbeitsgruppen, die vom Verwaltungsrat des Kompetenzzentrums eingerichtet wurden, um bestimmte, im Arbeitsplan des Kompetenzzentrums vorgesehene Tätigkeiten durchzuführen;
4. unterstützen das Kompetenzzentrum und die nationalen Koordinierungszentren gegebenenfalls bei der Förderung bestimmter Projekte;
5. fördern und verbreiten die einschlägigen Ergebnisse der in der Gemeinschaft durchgeführten Tätigkeiten und Projekte.

Artikel 10

Zusammenarbeit des Kompetenzzentrums mit den Organen, Einrichtungen und sonstigen Stellen der Union

(1) Das Kompetenzzentrum arbeitet mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zusammen, einschließlich der Agentur der Europäischen Union für Netz- und Informationssicherheit, des IT-Notfallteams der EU (CERT-EU), des Europäischen Auswärtigen Dienstes, der Gemeinsamen Forschungsstelle der Kommission, der Exekutivagentur für Forschung, Innovation und Netze, des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität bei Europol sowie der Europäischen Verteidigungsagentur.

(2) Diese Zusammenarbeit findet im Rahmen von Arbeitsvereinbarungen statt. Diese Vereinbarungen bedürfen der vorherigen Zustimmung der Kommission.

KAPITEL II

ORGANISATION DES KOMPETENZZENTRUMS

Artikel 11

Zusammensetzung und Struktur

(1) Die Mitglieder des Kompetenzzentrums sind die Union, vertreten durch die Kommission, und die Mitgliedstaaten.

(2) Die Struktur des Kompetenzzentrums umfasst

a) einen Verwaltungsrat, der die in Artikel 13 vorgesehenen Aufgaben wahrnimmt;

b) einen Exekutivdirektor, der die in Artikel 16 vorgesehenen Aufgaben wahrnimmt;

c) einen wissenschaftlich-technischen Beirat, der die in Artikel 20 genannten Funktionen ausübt.

ABSCHNITT I

VERWALTUNGSRAT

Artikel 12

Zusammensetzung des Verwaltungsrats

(1) Der Verwaltungsrat besteht aus je einem Vertreter pro Mitgliedstaat und fünf Kommissionsvertretern, die im Namen der Union handeln.

(2) Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter, der das Mitglied im Fall seiner Abwesenheit vertritt.

(3) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter werden aufgrund ihrer technischen Sachkenntnis sowie ihrer einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen ernannt. Die Kommission und die Mitgliedstaaten bemühen sich, die Fluktuation bei ihren Vertretern im Verwaltungsrat gering zu halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen. Die Kommission und die Mitgliedstaaten setzen sich für eine ausgewogene Vertretung von Frauen und Männern im Verwaltungsrat ein.

(4) Die Amtszeit der Mitglieder des Verwaltungsrats und ihrer Stellvertreter beträgt vier Jahre. Sie kann verlängert werden.

(5) Die Mitglieder des Verwaltungsrats handeln im Interesse des Kompetenzzentrums und setzen sich in aller Unabhängigkeit in transparenter Weise für dessen Ziele, Aufgaben, Identität, Eigenständigkeit und Kohärenz ein.

(6) Die Kommission kann Beobachter einladen, die gegebenenfalls an den Sitzungen des Verwaltungsrats teilnehmen, darunter Vertreter der einschlägigen Einrichtungen, Ämter, Agenturen und sonstigen Stellen der Union.

(7) Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) ist ein ständiger Beobachter im Verwaltungsrat.

Artikel 13

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat trägt die Gesamtverantwortung für die strategische Ausrichtung und die Geschäfte des Kompetenzzentrums und beaufsichtigt die Durchführung seiner Tätigkeiten.

(2) Der Verwaltungsrat gibt sich eine Geschäftsordnung. Diese Geschäftsordnung beinhaltet spezielle Verfahren zur Ermittlung und Vermeidung von Interessenkonflikten und zur Gewährleistung der Vertraulichkeit sensibler Informationen.

(3) Der Verwaltungsrat trifft die erforderlichen strategischen Entscheidungen, insbesondere:

a) Annahme eines mehrjährigen Strategieplans mit einer Aufstellung der wichtigsten Prioritäten und geplanten Initiativen des Kompetenzzentrums, einschließlich einer Schätzung des Finanzierungsbedarfs und der Finanzierungsquellen;

b) Annahme des Arbeitsplans, des Jahresabschlusses und der Bilanz sowie des jährlichen Tätigkeitsberichts des Kompetenzzentrums auf der Grundlage eines Vorschlags des Exekutivdirektors;

c) Annahme der eigenen Finanzordnung des Kompetenzzentrums gemäß [Artikel 70 der Haushaltsordnung];

d) Annahme eines Verfahrens zur Ernennung des Exekutivdirektors;

e) Annahme von Kriterien und Verfahren zur Prüfung und Akkreditierung von Einrichtungen als Mitglieder der Kompetenzgemeinschaft für Cybersicherheit;

f) Ernennung und Abberufung des Exekutivdirektors, Verlängerung seiner Amtszeit, Vorgabe von Leitlinien für den Exekutivdirektor und Beaufsichtigung seiner Tätigkeit sowie Ernennung des Rechnungsführers;

g) Annahme des jährlichen Haushaltsplans des Kompetenzzentrums, einschließlich des entsprechenden Stellenplans mit Angabe der Anzahl der Planstellen auf Zeit nach Funktions- und Besoldungsgruppen sowie der Anzahl der Vertragsbediensteten und abgeordneten nationalen Sachverständigen (in Vollzeitäquivalenten);

h) Annahme von Vorschriften über Interessenkonflikte;

i) Einrichtung von Arbeitsgruppen mit Mitgliedern der Kompetenzgemeinschaft für Cybersicherheit

j) Ernennung der Mitglieder des wissenschaftlich-technischen Beirats;

k) Einrichtung einer internen Auditstelle gemäß der Delegierten Verordnung (EU) Nr. 1271/2013 der Kommission[28];

l) weltweite Bekanntmachung des Kompetenzzentrums, um seine Attraktivität zu erhöhen und es zu einem internationalen Exzellenzzentrum für Cybersicherheit zu machen;

m) Festlegung der Kommunikationspolitik des Kompetenzzentrums auf Empfehlung des Exekutivdirektors;

n) Wahrnehmung der Zuständigkeit für die Überwachung der angemessenen Weiterverfolgung der Schlussfolgerungen aus den nachträglichen Bewertungen;

o) gegebenenfalls Festlegung von Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen nach Artikel 31 Absatz 3;

[28] Delegierte Verordnung (EU) Nr. 1271/2013 der Kommission vom 30. September 2013 über die Rahmenfinanzregelung für Einrichtungen gemäß Artikel 208 der Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates (ABl. L 328 vom 7.12.2013, S. 42).

p) gegebenenfalls Festlegung von Bestimmungen über die Abstellung nationaler Sachverständiger zum Kompetenzzentrum und über den Einsatz von Praktikanten nach Artikel 32 Absatz 2;

q) Annahme von Sicherheitsvorschriften für das Kompetenzzentrum;

r) Annahme einer Betrugsbekämpfungsstrategie, die den diesbezüglichen Risiken entspricht und auf einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen beruht;

s) Festlegung der Methode zur Berechnung des Finanzbeitrags der Mitgliedstaaten;

t) Wahrnehmung der Zuständigkeit für alle Aufgaben, die nicht ausdrücklich einem bestimmten Organ des Kompetenzzentrums übertragen wurden; Zuweisung solcher Aufgaben an ein Mitglied des Kompetenzzentrums.

Artikel 14

Vorsitz und Sitzungen des Verwaltungsrates

(1) Der Verwaltungsrat wählt aus dem Kreis seiner stimmberechtigten Mitglieder für einen Zeitraum von zwei Jahren einen Vorsitzenden und einen stellvertretenden Vorsitzenden. Die Amtszeit des Vorsitzenden und des stellvertretenden Vorsitzenden kann einmal auf Beschluss des Verwaltungsrates verlängert werden. Endet jedoch ihre Mitgliedschaft im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch am selben Tag. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle. Der Vorsitzende nimmt an den Abstimmungen teil.

(2) Der Verwaltungsrat hält mindestens dreimal jährlich ordentliche Sitzungen ab. Außerordentliche Sitzungen können auf Antrag der Kommission, auf Antrag eines Drittels aller Mitglieder des Verwaltungsrats, auf Antrag des Vorsitzes oder auf Antrag des Exekutivdirektors in Wahrnehmung seiner Aufgaben einberufen werden.

(3) Der Exekutivdirektor beteiligt sich an den Beratungen, sofern der Verwaltungsrat nichts anderes beschließt, verfügt jedoch über kein Stimmrecht. Der Verwaltungsrat kann im Einzelfall andere Personen einladen, um an den Sitzungen als Beobachter teilzunehmen.

(4) Mitglieder des wissenschaftlich-technischen Beirats können auf Einladung des Vorsitzes an den Sitzungen des Verwaltungsrats ohne Stimmrecht teilnehmen.

(5) Die Mitglieder des Verwaltungsrates und ihre Stellvertreter können sich nach Maßgabe seiner Geschäftsordnung in den Sitzungen von Beratern oder Sachverständigen unterstützen lassen.

(6) Die Sekretariatsgeschäfte des Verwaltungsrats werden vom Kompetenzzentrum wahrgenommen.

Artikel 15

Abstimmungsregeln des Verwaltungsrates

(1) Die Union verfügt über 50 % der Stimmrechte. Die Stimmrechte der Union sind unteilbar.

(2) Jeder beteiligte Mitgliedstaat hat eine Stimme.

(3) Der Verwaltungsrat fasst seine Beschlüsse mit einer Mehrheit von mindestens 75 % aller Stimmen, einschließlich der Stimmen der abwesenden Mitglieder, auf die mindestens 75 % der gesamten Finanzbeiträge zum Kompetenzzentrum entfallen. Der Finanzbeitrag wird auf der Grundlage der veranschlagten Ausgaben, die von den Mitgliedstaaten gemäß Artikel 17 Absatz 2 Buchstabe c vorgeschlagen werden, und auf der Grundlage des in Artikel 22 Absatz 5 genannten Berichts über den Wert der Beiträge der beteiligten Mitgliedstaaten berechnet.

(4) Nur die Vertreter der Kommission und die Vertreter der beteiligten Mitgliedstaaten sind stimmberechtigt.

(5) Der Vorsitzende nimmt an den Abstimmungen teil.

ABSCHNITT II

EXEKUTIVDIREKTOR

Artikel 16

Ernennung und Abberufung des Exekutivdirektors, Verlängerung seiner Amtszeit

(1) Der Exekutivdirektor ist eine Person mit Fachwissen und hohem Ansehen auf den Gebieten, auf denen das Kompetenzzentrum tätig ist.

(2) Der Exekutivdirektor wird als Zeitbediensteter des Kompetenzzentrums nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen für die sonstigen Bediensteten eingestellt.

(3) Der Exekutivdirektor wird vom Verwaltungsrat aus einer Liste von Bewerbern ernannt, die die Kommission im Anschluss an ein offenes und transparentes Auswahlverfahren vorschlägt.

(4) Für den Abschluss des Vertrags mit dem Exekutivdirektor wird das Kompetenzzentrum durch den Vorsitzenden des Verwaltungsrats vertreten.

(5) Die Amtszeit des Exekutivdirektors beträgt vier Jahre. Zum Ende dieses Zeitraums nimmt die Kommission eine Bewertung vor, bei der die Leistung des Exekutivdirektors und die künftigen Aufgaben und Herausforderungen des Kompetenzzentrums berücksichtigt werden.

(6) Der Verwaltungsrat kann auf Vorschlag der Kommission unter Berücksichtigung der Bewertung nach Absatz 5 die Amtszeit des Exekutivdirektors einmal um höchstens vier Jahre verlängern.

(7) Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, darf nicht an einem anderen Auswahlverfahren für dieselbe Stelle teilnehmen.

(8) Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission seines Amtes enthoben werden.

Artikel 17

Aufgaben des Exekutivdirektors

(1) Der Exekutivdirektor ist für den Tagesbetrieb und die Geschäftsführung des Kompetenzzentrums verantwortlich und ist dessen gesetzlicher Vertreter. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig und nimmt seine Aufgaben im Rahmen der ihm übertragenen Befugnisse völlig unabhängig wahr.

(2) Der Exekutivdirektor erfüllt insbesondere folgende Aufgaben in unabhängiger Weise:

a) Durchführung der vom Verwaltungsrat gefassten Beschlüsse;

b) Unterstützung des Verwaltungsrats bei seiner Arbeit, Bereitstellung des Sekretariats für seine Sitzungen sowie aller zur Erfüllung seiner Aufgaben erforderlichen Informationen;

c) Ausarbeitung und Vorlage des Entwurfs des mehrjährigen Strategieplans und des Entwurfs des jährlichen Arbeitsplans des Kompetenzzentrums zur Annahme, unter anderem mit Angaben zum Umfang der Aufforderungen zur Einreichung von Vorschlägen, der Aufforderungen zur Interessenbekundung und der Ausschreibungen, die für die Durchführung des Arbeitsplans erforderlich sind, sowie mit den entsprechenden von den beteiligten Mitgliedstaaten und der Kommission vorgelegten Ausgabenvoranschlägen nach Anhörung des Verwaltungsrates und der Kommission;

d) Ausarbeitung und Vorlage des Entwurfs des jährlichen Haushaltsplans zur Annahme durch den Verwaltungsrat, einschließlich des entsprechenden Stellenplans mit Angabe der Anzahl der Planstellen auf Zeit je Besoldungs- und Funktionsgruppe sowie der Anzahl der Vertragsbediensteten und abgeordneten nationalen Sachverständigen (in Vollzeitäquivalenten);

e) Durchführung des Arbeitsplans und Berichterstattung darüber an den Verwaltungsrat;

f) Ausarbeitung des Entwurfs des jährlichen Tätigkeitsberichts des Kompetenzzentrums mit den Angaben über die entsprechenden Ausgaben;

g) Gewährleistung der Durchführung wirksamer Überwachungs- und Bewertungsverfahren in Bezug auf die Leistung des Kompetenzzentrums;

h) Ausarbeitung eines Aktionsplans mit Folgemaßnahmen zu den Schlussfolgerungen aus den nachträglichen Bewertungen und alle zwei Jahre Berichterstattung an die Kommission über die erzielten Fortschritte;

i) Ausarbeitung, Aushandlung und Abschluss der Vereinbarungen mit den nationalen Koordinierungszentren;

j) Zuständigkeit für Verwaltungs-, Finanz- und Personalangelegenheiten, einschließlich der Ausführung des Haushaltsplans des Kompetenzzentrums, wobei die Beratung durch die interne Auditstelle im Rahmen der Vorgaben der Befugnisübertragung durch den Verwaltungsrat gebührend zu berücksichtigen ist;

k) Genehmigung und Verwaltung der Einleitung von Aufforderungen zur Einreichung von Vorschlägen entsprechend dem Arbeitsplan und Verwaltung der Finanzhilfevereinbarungen und -beschlüsse;

l) Genehmigung der Liste der Maßnahmen, die auf der Grundlage der von einer unabhängigen Sachverständigengruppe erstellten Rangliste für eine Finanzierung ausgewählt wurden;

m) Genehmigung und Verwaltung der Einleitung von Ausschreibungen entsprechend dem Arbeitsplan und Verwaltung der Verträge;

n) Genehmigung der Angebote, die für eine Finanzierung ausgewählt wurden;

o) Vorlage des Entwurfs des Jahresabschlusses und der Bilanz bei der internen Auditstelle und anschließend beim Verwaltungsrat,

p) Gewährleistung einer Risikobewertung und eines Risikomanagements;

q) Unterzeichnung einzelner Finanzhilfevereinbarungen, Beschlüsse und Verträge;

r) Unterzeichnung der Verträge über öffentliche Aufträge;

s) Ausarbeitung eines Aktionsplans mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte sowie der Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und alle zwei Jahre Berichterstattung über die erzielten Fortschritte an die Kommission sowie regelmäßig an den Verwaltungsrat;

t) Ausarbeitung des Entwurfs der für das Kompetenzzentrum geltenden Finanzordnung;

u) Einrichtung eines wirksamen und effizienten internen Kontrollsystems und Sicherstellung seines ordnungsgemäßen Funktionierens sowie Meldung bedeutsamer diesbezüglicher Änderungen an den Verwaltungsrat;

v) Gewährleistung einer wirksamen Kommunikation mit den Organen der Union;

w) Ergreifung sonstiger Maßnahmen, die zur Beurteilung der Fortschritte des Kompetenzzentrums mit Blick auf die Erfüllung seines Auftrags und der in den Artikeln 3 und 4 dieser Verordnung festgelegten Ziele erforderlich sind;

x) Ausführung der ihm vom Verwaltungsrat übertragenen sonstigen Aufgaben.

ABSCHNITT III

WISSENSCHAFTLICH-TECHNISCHER BEIRAT

Artikel 18

Zusammensetzung des wissenschaftlich-technischen Beirats

(1) Der wissenschaftlich-technische Beirat besteht aus höchstens 16 Mitgliedern. Die Mitglieder werden vom Verwaltungsrat aus dem Kreis der Vertreter der Einrichtungen in der Kompetenzgemeinschaft für Cybersicherheit ernannt.

(2) Die Mitglieder des wissenschaftlich-technischen Beirats verfügen über Fachwissen in der Forschung, industriellen Entwicklung, gewerblichen Dienstleistungen oder deren Einführung im Bereich der Cybersicherheit. Die Anforderungen in Bezug auf solches Fachwissen werden vom Verwaltungsrat genauer festgelegt.

(3) Die Verfahren für die Ernennung seiner Mitglieder durch den Verwaltungsrat und die Arbeitsweise des Beirats werden in der Geschäftsordnung des Kompetenzzentrums festgelegt und veröffentlicht.

(4) Die Amtszeit der Mitglieder des wissenschaftlich-technischen Beirats beträgt drei Jahre. Sie kann verlängert werden.

(5) Vertreter der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit können sich an den Arbeiten des wissenschaftlich-technischen Beirats beteiligen und diese unterstützen.

Artikel 19

Arbeitsweise des wissenschaftlich-technischen Beirats

(1) Der wissenschaftlich-technische Beirat tritt mindestens zweimal im Jahr zusammen.

(2) Der wissenschaftlich-technische Beirat kann den Verwaltungsrat bei der Einsetzung von Arbeitsgruppen zu bestimmten Fragen beraten, die für die Arbeit des Kompetenzzentrums von Bedeutung sind, gegebenenfalls im Rahmen der Gesamtkoordinierung durch eines oder mehrere Mitglieder des wissenschaftlich-technischen Beirats.

(3) Der wissenschaftlich-technische Beirat wählt seinen Vorsitzenden.

(4) Der wissenschaftlich-technische Beirat gibt sich eine Geschäftsordnung, in der er gegebenenfalls auch die Ernennung der Vertreter des Beirats sowie die Dauer ihrer Ernennung regelt.

Artikel 20

Aufgaben des wissenschaftlich-technischen Beirats

Der wissenschaftlich-technische Beirat berät das Kompetenzzentrum bei der Durchführung seiner Tätigkeiten und

1. bietet dem Exekutivdirektor und dem Verwaltungsrat strategische Beratung und leistet Beiträge zur Ausarbeitung des Arbeitsplans und des mehrjährigen Strategieplans innerhalb der vom Verwaltungsrat festgelegten Fristen;
2. organisiert öffentliche Konsultationen, an denen alle öffentlichen und privaten Akteure teilnehmen können, die ein Interesse im Bereich der Cybersicherheit haben, um Beiträge für die in Absatz 1 genannte strategische Beratung zu sammeln;
3. fördert und erfasst Rückmeldungen zum Arbeitsplan und zum mehrjährigen Strategieplan des Kompetenzzentrums.

KAPITEL III

FINANZVORSCHRIFTEN

Artikel 21

Finanzbeitrag der Union

(1) Der Beitrag der Union zur Deckung der Verwaltungs- und Betriebskosten des Kompetenzzentrums besteht aus

a) 1 981 668 000 EUR aus dem Programm „Horizont Europa“, davon höchstens 23 746 000 EUR für Verwaltungskosten;

b) einem Betrag aus dem Programm „Horizont Europa“, auch für Verwaltungskosten, der unter Berücksichtigung des strategischen Planungsprozesses gemäß Artikel 6 Absatz 6 der Verordnung XXX [Verordnung über „Horizont Europa“] festzulegen ist.

(2) Der Höchstbeitrag der Union wird aus den Mitteln des Gesamthaushaltsplans der Union für das [Programm „Digitales Europa“] und das mit dem Beschluss XXX

festgelegte Spezifische Programm zur Durchführung von Horizont Europa bereitgestellt.

(3) Das Kompetenzzentrum führt die Cybersicherheitsmaßnahmen im Rahmen des [Programms „Digitales Europa“] und des [Programms „Horizont Europa“] im Einklang mit Artikel 62 Buchstabe c Ziffer iv der Verordnung (EU, Euratom) XXX[29] [Haushaltsordnung] durch.

(4) Der Finanzbeitrag der Union deckt nicht die in Artikel 4 Absatz 8 Buchstabe b genannten Aufgaben.

Artikel 22

Beiträge der beteiligten Mitgliedstaaten

(1) Die beteiligten Mitgliedstaaten leisten einen Gesamtbeitrag zu den Betriebs- und Verwaltungskosten des Kompetenzzentrums, der mindestens den in Artikel 21 Absatz 1 dieser Verordnung genannten Beträgen entspricht.

(2) Für die Zwecke der Beurteilung der Beiträge nach Absatz 1 und Artikel 23 Absatz 3 Buchstabe b Ziffer ii werden die Kosten nach den üblichen Kostenrechnungsverfahren der betreffenden Mitgliedstaaten, den geltenden Rechnungslegungsgrundsätzen des Mitgliedstaats und den relevanten internationalen Rechnungslegungsstandards (*International Accounting Standards* und *International Financial Reporting Standards*) bestimmt. Die Kosten werden von einem unabhängigen externen Rechnungsprüfer bestätigt, der von dem jeweiligen Mitgliedstaat benannt wird. Die Bewertungsmethode kann vom Kompetenzzentrum überprüft werden, falls hinsichtlich der Zertifizierung Unklarheiten bestehen.

(3) Der Exekutivdirektor weist die beteiligten Mitgliedstaaten, die ihren Verpflichtungen zur Leistung ihrer Finanzbeiträge nicht nachgekommen sind, schriftlich auf ihr Versäumnis hin und setzt ihnen eine angemessene Frist für die Beseitigung dieses Versäumnisses. Wird das Versäumnis nicht innerhalb dieser Frist beseitigt, beruft der Exekutivdirektor eine Sitzung des Verwaltungsrats ein, in der darüber entschieden wird, ob dem säumigen beteiligten Mitgliedstaat das Stimmrecht zu entziehen ist oder ob andere Maßnahmen zu treffen sind, bis der Mitgliedstaat seinen Verpflichtungen nachgekommen ist. Das Stimmrecht des säumigen Mitgliedstaats wird ausgesetzt, bis es seine Verpflichtungen erfüllt hat.

(4) Die Kommission kann den Finanzbeitrag der Union zum Kompetenzzentrum aufkündigen, anteilsmäßig kürzen oder aussetzen, wenn die beteiligten Mitgliedstaaten die in Absatz 1 genannten Beiträge nicht, nur teilweise oder verspätet leisten.

(5) Die beteiligten Mitgliedstaaten melden jährlich bis zum 31. Januar dem Verwaltungsrat die Höhe der in Absatz 1 genannten Beiträge, die in jedem der vorangegangenen Haushaltsjahre geleistet wurden.

Artikel 23

Kosten und Mittelausstattung des Kompetenzzentrums

(1) Das Kompetenzzentrum wird von der Union und den Mitgliedstaaten gemeinsam durch in Tranchen gezahlte Finanzbeiträge sowie durch Beiträge finanziert, die aus

[29] [Vollständigen Titel und ABl.-Fundstelle einfügen]

den Kosten bestehen, die den nationalen Koordinierungszentren und den Begünstigten bei der Durchführung von Maßnahmen entstehen und vom Kompetenzzentrum nicht erstattet werden.

(2) Die Verwaltungskosten des Kompetenzzentrums belaufen sich auf höchstens [Zahl] EUR und werden durch Finanzbeiträge gedeckt, die jährlich zu gleichen Teilen von der Union und den beteiligten Mitgliedstaaten geleistet werden. Wird ein Teil des Beitrags zu den Verwaltungskosten nicht in Anspruch genommen, so kann er zur Deckung von Betriebskosten des Kompetenzzentrums bereitgestellt werden.

(3) Die Betriebskosten des Kompetenzzentrums werden gedeckt durch

a) den Finanzbeitrag der Union,

b) Beiträge der beteiligten Mitgliedstaaten in Form von

i) Finanzbeiträgen und

ii) gegebenenfalls Sachbeiträgen der beteiligten Mitgliedstaaten, die aus den Kosten bestehen, die den nationalen Koordinierungszentren und den Begünstigten bei der Durchführung indirekter Maßnahmen entstehen, abzüglich des Beitrags des Kompetenzzentrums und etwaiger sonstiger Beiträge der Union zu diesen Kosten.

(4) Die in den Haushalt des Kompetenzzentrums eingestellten Mittel setzen sich aus den folgenden Beiträgen zusammen:

a) den Finanzbeiträgen der beteiligten Mitgliedstaaten zu den Verwaltungskosten;

b) den Finanzbeiträgen der beteiligten Mitgliedstaaten zu den Betriebskosten;

c) etwaigen Einnahmen des Kompetenzzentrums;

d) sämtlichen sonstigen Finanzbeiträgen, Mitteln und Einnahmen.

(5) Zinserträge aus den von den beteiligten Mitgliedstaaten an das Kompetenzzentrum gezahlten Beiträgen gelten als Einnahmen des Kompetenzzentrums.

(6) Alle Mittel des Kompetenzzentrums und seine Tätigkeiten sind darauf ausgerichtet, die in Artikel 4 festgelegten Ziele zu erreichen.

(7) Das Kompetenzzentrum ist Eigentümer aller Vermögenswerte, die es selbst erwirtschaftet hat oder die ihm zum Zweck der Verfolgung seiner Ziele übertragen wurden.

(8) Sofern sich das Kompetenzzentrum nicht in Abwicklung befindet, werden etwaige Einnahmeüberschüsse nicht an die am Kompetenzzentrum beteiligten Mitglieder ausgezahlt.

Artikel 24

Finanzielle Verpflichtungen

Die finanziellen Verpflichtungen des Kompetenzzentrums dürfen den Betrag der ihm zur Verfügung stehenden oder seinem Haushalt von seinen Mitgliedern zugewiesenen Finanzmittel nicht übersteigen.

Artikel 25

Haushaltsjahr

Das Haushaltsjahr beginnt am 1. Januar und endet am 31. Dezember.

Artikel 26

Aufstellung des Haushaltsplans

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben des Kompetenzzentrums für das folgende Haushaltsjahr und legt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans vor. Einnahmen und Ausgaben müssen ausgeglichen sein. Die Ausgaben des Kompetenzzentrums umfassen die Personal-, Verwaltungs-, Infrastruktur- und Betriebsausgaben. Die Verwaltungsausgaben bleiben auf ein Mindestmaß beschränkt.

(2) Der Verwaltungsrat erstellt jedes Jahr auf der Grundlage des nach Absatz 1 erstellten Entwurfs des Voranschlags der Einnahmen und Ausgaben einen Voranschlag der Einnahmen und Ausgaben des Kompetenzzentrums für das folgende Haushaltsjahr.

(3) Der Verwaltungsrat übermittelt jedes Jahr bis zum 31. Januar der Kommission den in Absatz 2 genannten Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments ist.

(4) Die Kommission setzt aufgrund dieses Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan und den Betrag des Zuschusses aus dem Gesamthaushaltsplan in den Haushaltsplanentwurf der Union ein, den sie nach den Artikeln 313 und 314 AEUV dem Europäischen Parlament und dem Rat vorlegt.

(5) Das Europäische Parlament und der Rat bewilligen die Mittel für den Beitrag für das Kompetenzzentrum.

(6) Das Europäische Parlament und der Rat legen den Stellenplan des Kompetenzzentrums fest.

(7) Der Haushaltsplan des Zentrums wird zusammen mit dem Arbeitsplan vom Verwaltungsrat angenommen. Er wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Gegebenenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans des Kompetenzzentrums und des Arbeitsplans entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 27

Rechnungslegung des Kompetenzzentrums und Entlastung

Für die vorläufigen und endgültigen Rechnungsabschlüsse des Kompetenzzentrums sowie für die Entlastung gelten die Regeln und der Zeitplan der Haushaltsordnung und seiner im Einklang mit Artikel 29 angenommenen Finanzordnung.

Artikel 28

Tätigkeitsberichte und Finanzberichterstattung

(1) Der Exekutivdirektor erstattet dem Verwaltungsrat jährlich Bericht über die Erfüllung seiner Pflichten gemäß der Finanzordnung des Kompetenzzentrums.

(2) Binnen zwei Monaten nach Abschluss jedes Haushaltsjahres legt der Exekutivdirektor dem Verwaltungsrat den jährlichen Tätigkeitsbericht über die Fortschritte des Kompetenzzentrums im vorangegangenen Kalenderjahr zur

Billigung vor; darin wird insbesondere auf den für jenes Jahr geltenden Arbeitsplan Bezug genommen. Dieser Bericht enthält unter anderem Informationen über folgende Aspekte:

a) durchgeführte operative Maßnahmen mit den entsprechenden Ausgaben;

b) die eingereichten Maßnahmen mit einer Aufschlüsselung nach Art der Teilnehmer (einschließlich KMU) und nach Mitgliedstaat;

c) die für eine Finanzierung ausgewählten Maßnahmen mit einer Aufschlüsselung nach Art der Teilnehmer (einschließlich KMU) und nach Mitgliedstaat unter Angabe des vom Kompetenzzentrum für die einzelnen Teilnehmer und Maßnahmen zur Verfügung gestellten Beitrags;

d) die Fortschritte bei der Erreichung der in Artikel 4 aufgeführten Ziele und Vorschläge für weitere Arbeiten, die zur Erreichung dieser Ziele erforderlich sind.

(3) Der jährliche Tätigkeitsbericht wird nach seiner Billigung durch den Verwaltungsrat veröffentlicht.

Artikel 29

Finanzordnung

Das Kompetenzzentrum beschließt eine eigene Finanzordnung gemäß Artikel 70 der Verordnung XXX [neuen Haushaltsordnung].

Artikel 30

Schutz der finanziellen Interessen

(1) Das Kompetenzzentrum gewährleistet bei der Durchführung der nach dieser Verordnung finanzierten Maßnahmen den Schutz der finanziellen Interessen der Union durch geeignete Präventivmaßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und – bei Feststellung von Unregelmäßigkeiten – durch Rückforderung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch wirksame, verhältnismäßige und abschreckende verwaltungsrechtliche Sanktionen.

(2) Das Kompetenzzentrum gewährt Bediensteten der Kommission und sonstigen von der Kommission ermächtigten Personen sowie dem Europäischen Rechnungshof Zugang zu seinen Standorten und Räumlichkeiten sowie zu allen Informationen, einschließlich Informationen in elektronischer Form, die für die Durchführung der Rechnungsprüfungen erforderlich sind.

(3) Das Europäische Amt für Betrugsbekämpfung (OLAF) kann nach den in der Verordnung (Euratom, EG) Nr. 2185/96 des Rates[30] und der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates[31] festgelegten

[30] Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. L 292 vom 15.11.1996, S. 2).

[31] Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung

Bestimmungen und Verfahren Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob es im Zusammenhang mit Finanzhilfevereinbarungen oder Verträgen, die gemäß dieser Verordnung direkt oder indirekt finanziert werden, zu Betrug, Korruption oder anderen rechtswidrigen Handlungen zum Nachteil der finanziellen Interessen der Union gekommen ist.

(4) Unbeschadet der Absätze 1, 2 und 3 ist in Verträgen und Finanzhilfevereinbarungen, die sich aus der Durchführung dieser Verordnung ergeben, der Kommission, dem Kompetenzzentrum, dem Rechnungshof und OLAF ausdrücklich die Befugnis zu erteilen, entsprechend ihren Zuständigkeiten derartige Rechnungsprüfungen und Untersuchungen durchzuführen. Wenn die Durchführung einer Maßnahme ganz oder teilweise weitervergeben oder weiterdelegiert wird oder wenn sie die Vergabe eines öffentlichen Auftrags oder finanzieller Unterstützung an einen Dritten erfordert, müssen der Vertrag bzw. die Finanzhilfevereinbarung die Pflicht des Auftragnehmers oder des Begünstigten einschließen, von beteiligten Dritten die ausdrückliche Anerkennung dieser Befugnisse der Kommission, des Kompetenzzentrums, des Rechnungshofs und des OLAF zu verlangen.

KAPITEL IV

PERSONAL DES KOMPETENZZENTRUMS

Artikel 31

PERSONAL

(1) Für das Personal des Kompetenzzentrums gelten das Statut der Beamten der Europäischen Union und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union, festgelegt durch die Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates[32] (im Folgenden „Statut der Beamten“ und „Beschäftigungsbedingungen“), sowie die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung des Statuts der Beamten und der Beschäftigungsbedingungen.

(2) Der Verwaltungsrat übt in Bezug auf das Personal des Kompetenzzentrums die Befugnisse aus, die der Anstellungsbehörde durch das Statut der Beamten und der zum Abschluss von Dienstverträgen befugten Behörde durch die Beschäftigungsbedingungen übertragen wurden (im Folgenden „Befugnisse der Anstellungsbehörde“).

(3) Der Verwaltungsrat erlässt gemäß Artikel 110 des Statuts der Beamten einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts der Beamten und Artikel 6 der Beschäftigungsbedingungen, durch den dem Exekutivdirektor die entsprechenden Befugnisse der Anstellungsbehörde übertragen und die Bedingungen festgelegt werden, unter denen diese Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse weiter übertragen.

(OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).

[32] Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1).

(4) Ist dies in außergewöhnlichen Fällen erforderlich, so kann der Verwaltungsrat die Übertragung von Befugnissen der Anstellungsbehörde auf den Exekutivdirektor sowie jegliche weitere Übertragung durch Letzteren durch einen Beschluss vorübergehend aussetzen. In solchen Fällen übt der Verwaltungsrat die Befugnisse der Anstellungsbehörde selbst aus oder überträgt sie einem seiner Mitglieder oder einem anderen Bediensteten des Kompetenzzentrums als dem Exekutivdirektor.

(5) Der Verwaltungsrat erlässt im Einklang mit Artikel 110 des Statuts Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen.

(6) Die Personalstärke wird durch den Stellenplan des Kompetenzzentrums unter Angabe der Zahl der Planstellen auf Zeit nach Funktions- und Besoldungsgruppen und der Zahl der Vertragsbediensteten (in Vollzeitäquivalenten) in Übereinstimmung mit seinem jährlichen Haushaltsplan festgelegt.

(7) Das Personal des Kompetenzzentrums besteht aus Bediensteten auf Zeit und Vertragsbediensteten.

(8) Sämtliche Personalausgaben trägt das Kompetenzzentrum.

Artikel 32

Abgeordnete nationale Sachverständige und sonstige Bedienstete

(1) Das Kompetenzzentrum kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht vom Kompetenzzentrum selbst beschäftigt wird.

(2) Der Verwaltungsrat beschließt im Einvernehmen mit der Kommission eine Regelung für die Abordnung nationaler Sachverständiger zum Kompetenzzentrum.

Artikel 33

Vorrechte und Befreiungen

Das dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf das Kompetenzzentrum und sein Personal Anwendung.

KAPITEL V

GEMEINSAME BESTIMMUNGEN

Artikel 34

Sicherheitsvorschriften

(1) Artikel 12 Absatz 7 der Verordnung (EU) XXX [Programm „Digitales Europa“] gilt für die Teilnahme an allen vom Kompetenzzentrum finanzierten Maßnahmen.

(2) Für aus dem Programm „Horizont Europa“ finanzierte Maßnahmen gelten die folgenden besonderen Sicherheitsvorschriften:

a) für die Zwecke von Artikel 34 Absatz 1 [Eigentum und Schutzrechte] der Verordnung (EU) XXX [„Horizont Europa“] kann die Gewährung nicht ausschließlicher Lizenzen, wenn dies im Arbeitsplan vorgesehen ist, auf Dritte

beschränkt werden, die in Mitgliedstaaten niedergelassen sind oder als niedergelassen gelten und von Mitgliedstaaten und/oder Staatsangehörigen der Mitgliedstaaten geführt werden;

b) für die Zwecke von Artikel 36 Absatz 4 Buchstabe b [Übertragung und Lizenzierung] der Verordnung (EU) XXX [„Horizont Europa“] kann gegen die Übertragung von Eigentumsrechten an den Ergebnissen oder gegen die Gewährung einer ausschließlichen Lizenz zur Nutzung der Ergebnisse Einspruch erhoben werden, wenn die Übertragung oder Lizenzierung an einen Rechtsträger erfolgen soll, der zwar seinen Sitz in einem assoziierten Land oder in der Union hat, aber aus Drittländern geführt wird;

c) für die Zwecke von Artikel 37 Absatz 3 Buchstabe a [Zugangsrechte] der Verordnung (EU) XXX [„Horizont Europa“] kann die Gewährung des Zugangs zu Ergebnissen, wenn dies im Arbeitsplan vorgesehen ist, auf Rechtsträger beschränkt werden, die in Mitgliedstaaten niedergelassen sind oder als niedergelassen gelten und von Mitgliedstaaten und/oder Staatsangehörigen der Mitgliedstaaten geführt werden.

Artikel 35

Transparenz

(1) Das Kompetenzzentrum führt seine Tätigkeiten mit einem hohen Maß an Transparenz aus.

(2) Das Kompetenzzentrum stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere über seine eigenen Arbeitsergebnisse, erhalten. Ferner veröffentlicht es die nach Artikel 41 abgegebenen Interessenerklärungen.

(3) Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Arbeiten des Kompetenzzentrums teilnehmen.

(4) Das Kompetenzzentrum legt in seiner Geschäftsordnung die praktischen Einzelheiten für die Anwendung der Transparenzvorschriften der Absätze 1 und 2 fest. Bei Maßnahmen, die aus dem Programm „Horizont Europa“ finanziert werden, wird den Bestimmungen in Anhang III der Verordnung über das Programm „Horizont Europa“ gebührend Rechnung getragen.

Artikel 36

Sicherheitsvorschriften für den Schutz von Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen

(1) Unbeschadet des Artikels 35 gibt das Kompetenzzentrum Informationen, die bei ihm eingehen oder von ihm verarbeitet werden und die auf begründetes Ersuchen ganz oder teilweise vertraulich behandelt werden sollen, nicht an Dritte weiter.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die Mitglieder des wissenschaftlich-technischen Beirats, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal des Zentrums unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 des Vertrags über die Arbeitsweise der Europäischen Union.

(3) Der Verwaltungsrat des Kompetenzzentrums legt nach Genehmigung der Kommission seine Sicherheitsvorschriften auf der Grundlage der in den Sicherheitsvorschriften der Kommission für den Schutz von Verschlusssachen der Europäischen Union und nicht als Verschlusssache eingestuften sensiblen Informationen enthaltenen Grundsätze und Regeln fest, einschließlich unter anderem der Bestimmungen über die Verarbeitung und Speicherung derartiger Informationen gemäß den Beschlüssen (EU, Euratom) 2015/443[33] und 2015/444[34] der Kommission.

(4) Das Kompetenzzentrum kann alle notwendigen Maßnahmen treffen, um den Austausch von Informationen, die für seine Aufgaben von Belang sind, mit der Kommission und den Mitgliedstaaten sowie gegebenenfalls den zuständigen Agenturen der Union zu erleichtern. Jede zu diesem Zweck getroffene Verwaltungsvereinbarung über den Austausch von Verschlusssachen oder, falls keine solche Vereinbarung vorliegt, jede Ad-hoc-Weitergabe von EU-Verschlusssachen in Ausnahmefällen bedarf der vorherigen Genehmigung durch die Kommission.

Artikel 37

Zugang zu Unterlagen

(1) Die Verordnung (EG) Nr. 1049/2001 findet auf die Dokumente des Kompetenzzentrums Anwendung.

(2) Der Verwaltungsrat legt innerhalb von sechs Monaten nach Einrichtung des Kompetenzzentrums Maßnahmen zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

(3) Gegen Entscheidungen des Kompetenzzentrums nach Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe von Artikel 228 des Vertrags über die Arbeitsweise der Europäischen Union bzw. Artikel 263 des Vertrags über die Arbeitsweise der Europäischen Union Beschwerde beim Bürgerbeauftragten eingelegt oder Klage beim Gerichtshof der Europäischen Union erhoben werden.

Artikel 38

Überwachung, Bewertung und Überprüfung

(1) Das Kompetenzzentrum stellt sicher, dass seine Tätigkeiten, einschließlich der über die nationalen Koordinierungszentren und das Netz verwalteten Tätigkeiten, einer kontinuierlichen und systematischen Überwachung und regelmäßigen Bewertung unterzogen werden. Das Kompetenzzentrum stellt sicher, dass die Daten für die Überwachung der Programmdurchführung und der Programmergebnisse effizient, wirksam und zeitnah erhoben und den Empfängern von Fördermitteln der Union und der Mitgliedstaaten verhältnismäßige Vorgaben für die Berichterstattung auferlegt werden. Die Bewertungsergebnisse werden veröffentlicht.

(2) Sobald ausreichende Informationen über die Durchführung dieser Verordnung vorliegen, spätestens jedoch dreieinhalb Jahre nach Beginn der Durchführung dieser

---

33 Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

34 Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

Verordnung, nimmt die Kommission eine Zwischenbewertung des Kompetenzzentrums vor. Die Kommission erstellt einen Bericht über diese Bewertung und leitet ihn bis zum 31. Dezember 2024 dem Europäischen Parlament und dem Rat zu. Das Kompetenzzentrum und die Mitgliedstaaten stellen der Kommission die für die Erstellung des Berichts erforderlichen Informationen zur Verfügung.

(3) Die in Absatz 2 genannte Bewertung umfasst ebenfalls eine Bewertung der vom Kompetenzzentrum erzielten Ergebnisse im Hinblick auf die Ziele, den Auftrag und die Aufgaben des Zentrums. Ist die Kommission der Ansicht, dass das Fortbestehen des Kompetenzzentrums vor dem Hintergrund der Ziele, des Auftrags und der Aufgaben, die dem Kompetenzzentrum übertragen wurden, gerechtfertigt ist, kann sie vorschlagen, dass die in Artikel 46 festgelegte Bestehensdauer des Kompetenzzentrums verlängert wird.

(4) Auf der Grundlage der Schlussfolgerungen der Zwischenbewertung nach Absatz 2 kann die Kommission Maßnahmen gemäß [Artikel 22 Absatz 5] oder sonstige geeignete Maßnahmen ergreifen.

(5) Die Überwachung, Bewertung, stufenweise Beendigung und Erneuerung des Beitrags aus dem Programm „Horizont Europa“ erfolgen nach Maßgabe der Artikel 8, 45 und 47 sowie des Anhangs III der Verordnung über das Programm „Horizont Europa“ und der vereinbarten Durchführungsmodalitäten.

(6) Die Überwachung, Berichterstattung und Bewertung des Beitrags aus dem Programm „Digitales Europa“ erfolgen nach Maßgabe der Artikel 24 und 25 des Programms „Digitales Europa“.

(7) Im Falle einer Abwicklung des Kompetenzzentrums nimmt die Kommission innerhalb von sechs Monaten, spätestens jedoch zwei Jahre nach Einleitung des Abwicklungsverfahrens gemäß Artikel 46 dieser Verordnung eine abschließende Bewertung des Kompetenzzentrums vor. Die Ergebnisse dieser abschließenden Bewertung werden dem Europäischen Parlament und dem Rat vorgelegt.

Artikel 39

Haftung des Kompetenzzentrums

(1) Die vertragliche Haftung des Kompetenzzentrums bestimmt sich nach dem für die betreffende Vereinbarung bzw. den betreffenden Vertrag oder Beschluss geltenden Recht.

(2) Im Bereich der außervertraglichen Haftung leistet das Kompetenzzentrum für die von seinem Personal in Wahrnehmung seiner Aufgaben verursachten Schäden Schadenersatz nach den allgemeinen Rechtsgrundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

(3) Etwaige Schadenersatzzahlungen des Kompetenzzentrums aufgrund der Haftung gemäß den Absätzen 1 und 2 sowie die damit zusammenhängenden Kosten und Ausgaben gelten als Ausgaben des Kompetenzzentrums und werden aus seinen Mitteln geleistet.

(4) Für die Erfüllung seiner Verpflichtungen haftet ausschließlich das Kompetenzzentrum.

Artikel 40

Zuständigkeit des Gerichtshofs der Europäischen Union und anwendbares Recht

(1) Der Gerichtshof der Europäischen Union ist zuständig

1. aufgrund von Schiedsklauseln in Vereinbarungen, Beschlüssen oder Verträgen, die das Kompetenzzentrum geschlossen hat;
2. für Entscheidungen in Schadenersatzstreitigkeiten aufgrund eines durch das Personal des Kompetenzzentrums in Wahrnehmung seiner Aufgaben verursachten Schadens;
3. für alle Streitsachen zwischen dem Kompetenzzentrum und seinem Personal im Rahmen und unter den Bedingungen des Statuts der Beamten.

(2) In Angelegenheiten, die nicht durch diese Verordnung oder sonstige Rechtsakte der Union geregelt sind, gilt das Recht des Mitgliedstaats, in dem das Kompetenzzentrum seinen Sitz hat.

Artikel 41

Haftung der Mitglieder und Versicherung

(1) Die finanzielle Haftung der Mitglieder für die Schulden des Kompetenzzentrums ist auf deren bereits zu den Verwaltungsausgaben geleistete Finanzbeiträge beschränkt.

(2) Das Kompetenzzentrum schließt angemessene Versicherungsverträge und erhält diese aufrecht.

Artikel 42

Interessenkonflikt

Der Verwaltungsrat des Kompetenzzentrums nimmt in Bezug auf dessen Mitglieder, dessen Gremien und Personal Regeln zur Vermeidung von Interessenkonflikten und Regeln für den Umgang mit solchen Konflikten an. In diesen Regeln sind Bestimmungen vorzusehen, durch die im Einklang mit der Verordnung XXX [neue Haushaltsordnung] Interessenkonflikte bei den Vertretern der Mitglieder, die einen Sitz im Verwaltungsrat sowie im wissenschaftlich-technischen Beirat haben, vermieden werden.

Artikel 43

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch das Kompetenzzentrum unterliegt der Verordnung (EU) XXX/2018 des Europäischen Parlaments und des Rates.

(2) Der Verwaltungsrat beschließt die in Artikel xx Absatz 3 der Verordnung (EU) xxx/2018 vorgesehenen Durchführungsbestimmungen. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) xxx/2018 durch das Kompetenzzentrum erforderlich sind, festlegen.

Artikel 44

Unterstützung seitens des Sitzmitgliedstaats

Zwischen dem Kompetenzzentrum und dem Mitgliedstaat [Belgien], in dem es seinen Sitz hat, kann eine Verwaltungsvereinbarung über die Vorrechte und Befreiungen und die sonstige Unterstützung des Kompetenzzentrums seitens dieses Mitgliedstaats geschlossen werden.

KAPITEL VII

SCHLUSSBESTIMMUNGEN

Artikel 45

Erste Maßnahmen

(1) Die Kommission ist für die Einrichtung und die Aufnahme der Tätigkeit des Kompetenzzentrums verantwortlich, bis dieses über die operativen Fähigkeiten zur Ausführung seines eigenen Haushaltsplans verfügt. Die Kommission führt im Einklang mit dem Unionsrecht alle notwendigen Maßnahmen unter Einbeziehung der zuständigen Gremien des Kompetenzzentrums durch.

(2) Für die Zwecke von Absatz 1 kann die Kommission einen Interims-Exekutivdirektor benennen, der die Aufgaben des Exekutivdirektors wahrnimmt und von einer begrenzten Zahl von Kommissionsbeamten unterstützt werden kann, bis der Exekutivdirektor nach seiner Ernennung durch den Verwaltungsrat gemäß Artikel 16 die Amtsgeschäfte aufnimmt. Die Kommission kann hierzu eine begrenzte Zahl eigener Beamter übergangsweise einsetzen.

(3) Der Interims-Exekutivdirektor kann alle Zahlungen genehmigen, für die im Jahreshaushaltsplan des Kompetenzzentrums Mittel zur Verfügung stehen und die Genehmigung des Verwaltungsrats vorliegt, und Vereinbarungen und Verträge – nach Annahme des Stellenplans des Kompetenzzentrums auch Arbeitsverträge – schließen sowie Beschlüsse fassen.

(4) Der Interims-Exekutivdirektor bestimmt im Einvernehmen mit dem Exekutivdirektor des Kompetenzzentrums und vorbehaltlich der Zustimmung des Verwaltungsrats den Tag, an dem das Kompetenzzentrum über die Fähigkeit zur Ausführung seines eigenen Haushaltsplans verfügt. Ab diesem Tag nimmt die Kommission für die Tätigkeiten des Kompetenzzentrums keine Mittelbindungen mehr vor und führt keine Zahlungen mehr aus.

Artikel 46

Bestehensdauer

(1) Das Kompetenzzentrum wird für den Zeitraum vom 1. Januar 2021 bis zum 31. Dezember 2029 eingerichtet.

(2) Nach Ablauf dieses Zeitraums wird – sofern im Rahmen einer Überprüfung dieser Verordnung nicht anders beschlossen – das Abwicklungsverfahren eingeleitet. Das Abwicklungsverfahren wird automatisch eingeleitet, wenn die Union oder alle beteiligten Mitgliedstaaten ihre Mitgliedschaft im Kompetenzzentrum kündigen.

(3) Zur Abwicklung des Kompetenzzentrums ernennt der Verwaltungsrat einen oder mehrere Abwicklungsbeauftragte, die seinen Beschlüssen nachkommen.

(4) Bei der Abwicklung des Kompetenzzentrums werden seine Vermögenswerte zur Deckung seiner Verbindlichkeiten und der Kosten seiner Abwicklung verwendet. Etwaige Überschüsse werden proportional zu ihren Finanzbeiträgen auf die Union und die beteiligten Mitgliedstaaten umgelegt, die zum Zeitpunkt der Abwicklung am Kompetenzzentrum beteiligt sind. Etwaige auf die Union umgelegte Überschüsse fließen in den Unionshaushalt zurück.

Artikel 47

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

FINANZBOGEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1 Bezeichnung des Vorschlags/der Initiative

1.2 Politikbereich(e) in der ABM-/ABB-Struktur

1.3 Art des Vorschlags/der Initiative

1.4 Ziel(e)

1.5 Begründung des Vorschlags/der Initiative

1.6 Laufzeit der Maßnahme(n) und Dauer ihrer finanziellen Auswirkungen

1.7 Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMASSNAHMEN

2.1 Überwachung und Berichterstattung

2.2 Verwaltungs- und Kontrollsystem

2.3 Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1 Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

3.2 Geschätzte Auswirkungen auf die Ausgaben

3.2.1 Übersicht über die geschätzten Auswirkungen auf die Ausgaben

3.2.2 Geschätzte Auswirkungen auf operative Mittel

3.2.3 Geschätzte Auswirkungen auf die Verwaltungsmittel

3.2.4 Vereinbarkeit mit dem mehrjährigen Finanzrahmen

3.2.5 Finanzierungsbeteiligung Dritter

3.3 Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung

1.2. Politikbereich(e) in der ABM-/ABB-Struktur[35]

Forschung und Innovation

Europäische strategische Investitionen

1.3. Art des Vorschlags/der Initiative

☒ Der Vorschlag/Die Initiative betrifft eine **neue Maßnahme**

☐ Der Vorschlag/Die Initiative betrifft **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[36]

☐ Der Vorschlag/Die Initiative betrifft **die Verlängerung einer bestehenden Maßnahme**

☐ Der Vorschlag/Die Initiative betrifft **eine neu ausgerichtete Maßnahme**

1.4. Ziel(e)

1.4.1. Mit dem Vorschlag/der Initiative verfolgte mehrjährige strategische Ziele der Kommission

1. Ein vernetzter digitaler Binnenmarkt

2. Neue Impulse für Arbeitsplätze, Wachstum und Investitionen

1.4.2. Betreffende spezifische Ziele

Spezifische Ziele

1.3 Die digitale Wirtschaft kann ihr volles Potenzial entfalten mit Unterstützung von Initiativen, die ein uneingeschränktes Wachstum der Digital- und Datentechnologien ermöglichen.

2.1 Europa hält an seiner weltweit führenden Position in der digitalen Wirtschaft fest, in der europäische Unternehmen aufbauend auf starkem digitalen Unternehmertum und leistungsstarken Start-ups weltweit wachsen können und in der die Industrie und die öffentlichen Dienste den digitalen Wandel meistern.

2.2 Die europäische Forschung bietet Investitionsmöglichkeiten für potenzielle technologische Durchbrüche und in Leitinitiativen, insbesondere im Rahmen des Programms „Horizont 2020/Horizont Europa“ und mithilfe öffentlich-privater Partnerschaften.

35 ABM: maßnahmenbezogenes Management; ABB: maßnahmenbezogene Budgetierung.

36 Im Sinne des Artikels 54 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken dürfte.

Das Kompetenzzentrum soll zusammen mit dem Netz und der Gemeinschaft folgende Ziele erreichen:

1) Beitrag zur Umsetzung der Cybersicherheitskomponente des mit der Verordnung (EU) XXX eingerichteten Programms „Digitales Europa“, insbesondere zu den Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) XXX [Programm „Digitales Europa“], und des mit der Verordnung (EU) XXX eingerichteten Programms „Horizont Europa“ sowie insbesondere des Anhangs I Abschnitt 2.2.6 des Beschlusses XXX über das Spezifische Programm zur Durchführung von Horizont Europa – Rahmenprogramm für Forschung und Innovation – und anderer Unionsprogramme, sofern dies in den Rechtsakten der Union vorgesehen ist];

2) Verbesserung der Kapazitäten, des Wissens und der Infrastrukturen im Bereich der Cybersicherheit, die der Industrie, dem öffentlichen Sektor und der Forschung zur Verfügung stehen;

3) Beitrag zur umfassenden Einführung modernster Cybersicherheitsprodukte und -lösungen in der gesamten Wirtschaft;

4) Verbesserung des Verständnisses der Cybersicherheit und Beitrag zur Verringerung des Qualifikationsdefizits im Zusammenhang mit der Cybersicherheit in der Union;

5) Beitrag zur Stärkung der Cybersicherheitsforschung und -entwicklung in der Union;

6) Verbesserung der Zusammenarbeit zwischen zivilen und militärischen Fachkreisen in Bezug auf Technologien und Anwendungen mit doppeltem Verwendungszweck;

7) bessere Synergien zwischen der zivilen und der verteidigungspolitischen Dimension der Cybersicherheit;

8) Unterstützung der Koordinierung und Erleichterung der Arbeiten des Netzes nationaler Koordinierungszentren (im Folgenden das „Netz“) gemäß Artikel 10 und der Kompetenzgemeinschaft für Cybersicherheit gemäß Artikel 12.

1.4.4. Leistungs- und Erfolgsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

· Anzahl der gemeinsam angeschafften Cybersicherheitsinfrastrukturen/-werkzeuge;

· Zugang zu Erprobungs- und Versuchszeit für europäische Forscher und Unternehmen im gesamten Netz und im Zentrum. Sofern die Einrichtungen bereits vorhanden sind, sollte diesen Fachkreisen mehr Zeit gegenüber den derzeit verfügbaren Stunden gewährt werden;

· Zunahme der Zahl der bedienten Nutzergruppen und der Wissenschaftler, die Zugang zu europäischen Cybersicherheitseinrichtungen erhalten, im Vergleich zu Wissenschaftlern, die solche Ressourcen außerhalb Europas nutzen müssen;

· beginnende Zunahme der Wettbewerbsfähigkeit europäischer Hersteller, gemessen als weltweiter Marktanteil (Ziel: 25 % Marktanteil bis 2027) und als Anteil der von der Industrie übernommenen europäischen FuE-Ergebnisse;

· Beitrag zur Cybersicherheitstechnik, gemessen in Form von Urheberrechten sowie als Zahl der Patente, wissenschaftlichen Veröffentlichungen und vermarkteten Produkte;

· Zahl der bewerteten und angepassten Lehrpläne im Bereich der Cybersicherheit, Zahl der bewerteten professionellen Zertifizierungsprogramme im Bereich der Cybersicherheit;

· Zahl der aus-/weitergebildeten Wissenschaftler, Studierenden und Nutzer (in Industrie und öffentlichen Verwaltungen).

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf

Erreichen einer kritischen Masse von Investitionen, die industrielle Entwicklung im Bereich der Cybersicherheit und Überwindung der Fragmentierung der einschlägigen Kapazitäten in der gesamten EU.

1.5.2. Mehrwert aufgrund des Tätigwerdens der EU

Die Cybersicherheit ist ein Thema von gemeinsamem Interesse der Union, wie in den genannten Schlussfolgerungen des Rates bestätigt wurde. Der Umfang und der grenzüberschreitende Charakter von Vorfällen wie „WannaCry“ oder „NonPetya“ sind typische Beispiele hierfür. Art und Umfang der technischen Herausforderungen im Bereich der Cybersicherheit sowie die unzureichende Koordinierung der Anstrengungen innerhalb der Industrie, des öffentlichen Sektors und der Forschung machen es erforderlich, dass die EU die Koordinierungsbemühungen weiter unterstützt, um eine kritische Masse an Ressourcen zu bilden und bessere Kenntnisse und eine bessere Verwaltung der Ressourcen zu gewährleisten. Dies ist erforderlich angesichts des Ressourcenbedarfs im Zusammenhang mit bestimmten Kapazitäten für Forschung, Entwicklung und Einführung im Bereich der Cybersicherheit, angesichts der Notwendigkeit, Zugang zu interdisziplinärem Fachwissen im Bereich der Cybersicherheit zwischen verschiedenen Fachgebieten zu ermöglichen (häufig nur teilweise auf nationaler Ebene gegeben), und angesichts des globalen Charakters der industriellen Wertschöpfungsketten sowie der Aktivitäten globaler Wettbewerber, die märkteübergreifend tätig sind.

Hierzu sind Ressourcen und Fachwissen in einer Größenordnung nötig, die durch die Maßnahmen eines einzelnen Mitgliedstaats kaum erreicht werden können. So könnte beispielsweise ein gesamteuropäisches Quantenkommunikationsnetz eine EU-Investition in Höhe von 900 Mio. EUR erfordern, je nach den Investitionen der Mitgliedstaaten (zu vernetzen/ergänzen) und je nachdem, in welchem Umfang bestehende Infrastrukturen weiterverwendet werden können.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

In der Zwischenbewertung des Programms Horizont 2020 wurde die anhaltende Bedeutung der EU-Unterstützung für FuE und gesellschaftliche Herausforderungen (darunter „Sichere Gesellschaften“, in deren Rahmen FuE im Bereich der Cybersicherheit gefördert wird) bestätigt. Gleichzeitig bestätigt die Bewertung, dass die Stärkung der führenden Rolle der Industrie nach wie vor eine Herausforderung

darstellt und dass weiterhin eine Innovationslücke besteht, sodass die EU bei bahnbrechenden Innovationen, die neue Märkte schaffen, hinterherhinkt.

Die Zwischenbewertung der Fazilität „Connecting Europe“ (CEF) scheint den Mehrwert der EU-Intervention über FuE hinaus zu bestätigen, wenngleich die Cybersicherheit im Rahmen der CEF einen etwas anderen Schwerpunkt (auf Betriebssicherheit) und eine andere Interventionslogik aufwies. Gleichzeitig äußerten die meisten Empfänger der CEF-Finanzhilfen im Bereich der Cybersicherheit – die nationalen Computer-Notfallteams – ihren Wunsch nach einem maßgeschneiderten Unterstützungsprogramm im nächsten mehrjährigen Finanzrahmen.

Die Gründung der öffentlich-privaten Partnerschaft für Cybersicherheit („cPPP“) in der EU im Jahr 2016 war ein erster konkreter Schritt, um die Fachkreise in Forschung, Industrie und öffentlichem Sektor zusammenzubringen, um Forschung und Innovation im Bereich der Cybersicherheit zu erleichtern, und sollte innerhalb der Grenzen des Finanzrahmens 2014–2020 zu guten, stärker zielgerichteten Ergebnissen in Forschung und Innovation führen. Die cPPP ermöglichte es den Partnern aus der Industrie, eigene Zusagen in Bezug auf ihre Ausgaben in den in der strategischen Forschungs- und Innovationsagenda der Partnerschaft festgelegten Bereiche zu machen.

1.5.4. Vereinbarkeit mit anderen geeigneten Instrumenten sowie mögliche Synergieeffekte

Das Cybersicherheitskompetenznetz und das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung werden als zusätzliche Unterstützung für bestehende Bestimmungen und Akteure im Bereich der Cybersicherheit dienen. Der Auftrag des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung wird die Arbeit der ENISA ergänzen, hat jedoch einen anderen Schwerpunkt und erfordert ein anderes Spektrum an Kompetenzen. Während die ENISA eine beratende Funktion in Bezug auf Forschung und Innovation im Bereich der Cybersicherheit in der EU hat, konzentriert sich das für das Kompetenzzentrum vorgeschlagene Mandat in erster Linie auf andere Aufgaben, die für die Stärkung der Abwehrfähigkeit der EU in Cybersicherheitsfragen von entscheidender Bedeutung sind. Das Zentrum sollte die Entwicklung und Verbreitung von Cybersicherheitstechnik fördern und die Bemühungen um den Aufbau von Kapazitäten in diesem Bereich auf EU-Ebene und auf nationaler Ebene ergänzen.

Das Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung wird mit dem Cybersicherheitskompetenznetz ebenfalls gemeinsam darauf hinarbeiten, die Forschung zu erleichtern und Normungs- und Zertifizierungsverfahren zu beschleunigen, insbesondere im Zusammenhang mit Zertifizierungssystemen für Cybersicherheit im Sinne des Rechtsakts zur Cybersicherheit.

Das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung wird als einheitliche Durchführungsstelle für zwei europäische Programme zur Förderung der Cybersicherheit (Programm „Digitales Europa“ und Programm „Horizont Europa“) dienen und die Verbesserung der Kohärenz und der Synergien zwischen beiden fördern.

Diese Initiative ermöglicht es, die Anstrengungen der Mitgliedstaaten zu ergänzen, indem sie geeignete Zuarbeiten für bildungspolitische Entscheidungen liefert, um die Cybersicherheit zu verbessern (z. B. durch die Entwicklung von

Cybersicherheitslehrplänen in zivilen und militärischen Bildungssystemen, aber auch durch Beiträge zur grundlegenden Ausbildung im Bereich der Cybersicherheit). Sie würde es auch ermöglichen, die Angleichung und kontinuierliche Bewertung der professionellen Zertifizierungsprogramme im Bereich der Cybersicherheit zu unterstützen – alle notwendigen Maßnahmen, um die Lücke im Bereich der Cybersicherheit zu schließen und den Zugang von Unternehmen und anderen Gruppen zu Cybersicherheitsspezialisten zu erleichtern. Die Angleichung der Bildung und der Kompetenzen wird zum Aufbau qualifizierter Arbeitskräfte im Bereich der Cybersicherheit in der EU beitragen – ein wichtiges Gut für Cybersicherheitsunternehmen sowie andere Branchen, für die die Cybersicherheit von Bedeutung ist.

1.6. Laufzeit der Maßnahme(n) und Dauer ihrer finanziellen Auswirkungen

☒ Vorschlag/Initiative mit **befristeter Laufzeit**

– ☒ Laufzeit: 1.1.2021 bis 31.12.2029

– ☒ Finanzielle Auswirkungen: von 2021 bis 2027 für Mittel für Verpflichtungen und von 2021 bis 2031 für Mittel für Zahlungen.

☐ Vorschlag/Initiative mit **unbefristeter Laufzeit**

– Anlaufphase von JJJJ bis JJJJ,

– anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[37]

☐ **Direkte Verwaltung** durch die Kommission

– ☐ durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union

– ☐ durch Exekutivagenturen

☐ **Geteilte Verwaltung** mit Mitgliedstaaten

☒

Indirekte Verwaltung durch Übertragung von Haushaltsvollzugsaufgaben an

– ☐ Drittländer oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die EIB und den Europäischen Investitionsfonds

– ☒ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende Finanzsicherheiten bieten

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende Finanzsicherheiten bieten

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind

– *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen“ näher zu erläutern.*

[37] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. VERWALTUNGSMASSNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Artikel 28 enthält ausführliche Bestimmungen über die Überwachung und Berichterstattung.

2.2. Verwaltungs- und Kontrollsystem

2.2.1. Ermittelte Risiken

Um Risiken im Zusammenhang mit der Tätigkeit des Kompetenzzentrums nach dessen Einrichtung und Verzögerungen zu vermeiden, wird die Kommission das Kompetenzzentrum in dieser Phase unterstützen, um eine rasche Einstellung von Personal in Schlüsselpositionen und die Einrichtung eines effizienten internen Kontrollsystems und solider Verfahren zu gewährleisten.

2.2.2. Angaben zum Aufbau des Systems der internen Kontrolle

Der Exekutivdirektor ist für den Tagesbetrieb und die Geschäftsführung des Kompetenzzentrums verantwortlich und ist dessen gesetzlicher Vertreter. Er ist dem Verwaltungsrat rechenschaftspflichtig, dem er kontinuierlich über die Entwicklung der Tätigkeit des Kompetenzzentrums Bericht erstattet.

Der Verwaltungsrat trägt die Gesamtverantwortung für die strategische Ausrichtung und die Geschäfte des Kompetenzzentrums und beaufsichtigt die Durchführung seiner Tätigkeiten.

Der Verwaltungsrat erlässt nach Anhörung der Kommission die für das Kompetenzzentrum geltende Finanzordnung. Die Finanzordnung darf von der Delegierten Verordnung (EU) Nr. 1271/2013 nur abweichen, wenn dies für den Betrieb des Kompetenzzentrums eigens erforderlich ist und die Kommission vorab ihre Zustimmung erteilt hat.

Der Interne Prüfer der Kommission sollte gegenüber dem Kompetenzzentrum die gleichen Befugnisse ausüben wie gegenüber der Kommission. Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel vom Kompetenzzentrum erhalten haben, Rechnungsprüfungen anhand von Unterlagen und vor Ort durchzuführen.

2.2.3. Abschätzung der Kosten und des Nutzens der Kontrollen sowie Bewertung des voraussichtlichen Fehlerrisikos

Kosten und Nutzen von Kontrollen

Die Kontrollkosten für das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung ergeben sich aus den Kosten der Beaufsichtigung auf Kommissionsebene und den Kosten für die operativen Kontrollen auf Ebene der Durchführungsstelle.

Die Kontrollkosten auf der Ebene des Kompetenzzentrums werden auf etwa 1,19 % der operativen Mittel für Zahlungen geschätzt, die auf der Ebene des Kompetenzzentrums ausgeführt werden.

Die Kosten der Beaufsichtigung auf Kommissionsebene werden auf etwa 1,20 % der operativen Mittel für Zahlungen geschätzt, die auf der Ebene des Kompetenzzentrums ausgeführt werden.

Unter der Annahme, dass die Tätigkeiten ohne Unterstützung durch die Durchführungsstelle vollständig von der Kommission verwaltet würden, lägen die Kontrollkosten wesentlich höher bei rund 7,7 % der Mittel für Zahlungen auf Programmebene.

Die vorgesehenen Kontrollen sollen eine reibungslose und wirksame Beaufsichtigung der Durchführungsstellen durch die Kommission und den erforderlichen Grad an Sicherheit auf Kommissionsebene gewährleisten.

Die Kontrollen bringen den folgenden Nutzen:

- Vermeidung der Auswahl schwächerer oder unzureichender Vorschläge;
- Optimierung der Planung und der Verwendung von EU-Mitteln zum Erhalt des EU-Mehrwerts;
- Gewährleistung der Qualität der Finanzhilfevereinbarungen, Vermeidung von Fehlern bei der Identifizierung von Rechtsträgern, Gewährleistung der korrekten Berechnung der EU-Beiträge und Sicherung der erforderlichen Garantien für eine ordnungsgemäße Abwicklung der Finanzhilfen;
- Erkennung nicht förderfähiger Kosten zum Zeitpunkt der Zahlung;
- Erkennung von Fehlern, die die Rechtmäßigkeit und Ordnungsmäßigkeit der Vorgänge beeinträchtigen, zum Zeitpunkt der Prüfung.

Geschätzte Fehlerquote

Das Ziel besteht darin, die Restfehlerquote für das gesamte Programm unter der Schwelle von 2 % zu halten und gleichzeitig den Kontrollaufwand für die Begünstigten und die Kontrollkosten zu begrenzen, um das richtige Gleichgewicht zwischen der Recht- und Ordnungsmäßigkeit und anderen Zielen wie der Attraktivität des Programms, insbesondere für KMU, zu erzielen.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen vorhanden oder vorgesehen sind.

Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates und der Verordnung (Euratom, EG) Nr. 2185/9640 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Union vor Betrug und anderen Unregelmäßigkeiten Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit vom Kompetenzzentrum gewährten Finanzhilfen oder von ihr finanzierten Aufträgen ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

In Vereinbarungen, Beschlüssen und Verträgen, die sich aus der Durchführung dieser Verordnung ergeben, ist der Kommission, dem Kompetenzzentrum, dem Rechnungshof und OLAF ausdrücklich die Befugnis zu erteilen, entsprechend ihren Zuständigkeiten derartige Rechnungsprüfungen und Untersuchungen durchzuführen.

Das Kompetenzzentrum stellt sicher, dass die finanziellen Interessen seiner Mitglieder angemessen geschützt und hierzu geeignete interne und externe Kontrollen durchgeführt werden.

Das Kompetenzzentrum tritt der Interinstitutionellen Vereinbarung vom 25. Mai 1999 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei. Das Kompetenzzentrum beschließt die notwendigen Maßnahmen, um die durch OLAF durchgeführten internen Untersuchungen zu erleichtern.

Das Kompetenzzentrum nimmt eine Betrugsbekämpfungsstrategie an, die sich auf eine Betrugsrisikoanalyse und eine Kosten-Nutzen-Analyse stützt. Es schützt die finanziellen Interessen der Union durch vorbeugende Maßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und, falls Unregelmäßigkeiten festgestellt werden, durch Einziehung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch Verhängung wirksamer, verhältnismäßiger und abschreckender verwaltungsrechtlicher und finanzieller Sanktionen.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

- Neu zu schaffende Haushaltslinien

  In der Reihenfolge der Rubriken des mehrjährigen Finanzrahmens und der Haushaltslinien:

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM [38]	von EFTA-Ländern[39]	von Kandidaten-ländern[40]	von Drittländern	nach Artikel [21 Absatz 2 Buchstabe b] der Haushaltsordnung
Rubrik 1: Binnenmarkt, Innovation und Digitales	01 02 XX XX Horizont Europa – Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung – Unterstützungsausgaben 01 02 XX XX Horizont Europa – Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung 02 06 01 XX Digitales Europa – Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung – Unterstützungsausgaben 02 06 01 XX Digitales Europa Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung	GM/NGM	JA	JA (falls im jährlichen Arbeitsprogramm festgelegt)	JA (auf einen Teil des Programms beschränkt)	NEIN

[38] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.

[39] EFTA: Europäische Freihandelsassoziation.

[40] Kandidatenländer und gegebenenfalls potenzielle Kandidatenländer des Westbalkans.

- Die Beiträge zu diesen Haushaltslinien werden voraussichtlich aus folgenden Haushaltslinien stammen:

in Mio. EUR (3 Dezimalstellen)

Haushaltslinie	Jahr 2021	Jahr 2022	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	**Gesamt**
01 01 01 01 Ausgaben für Beamte und Bedienstete auf Zeit – Horizont Europa	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 02 Forschungsprogramme (Programm „Horizont Europa“) – Ausgaben für externes Personal	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 03 Sonstige Verwaltungsausgaben für den Forschungsbereich (Programm „Horizont Europa“)	pm	pm	pm	pm	pm	pm	pm	pm
01 02 02 Globale Herausforderungen und industrielle Wettbewerbsfähigkeit	pm	pm	pm	pm	pm	pm	pm	pm
02 01 04 Verwaltungsunterstützung (Programm „Digitales Europa“)	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
02 06 01 Cybersicherheit (Programm „Digitales Europa“)	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
Gesamtausgaben	286,130	325,274	331,320	252,200	257,189	262,186	267,368	1 981,668

Der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft“ des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit“ des Programms „Horizont Europa“ (insgesamt 2 800 000 000 EUR) gemäß Artikel 21 Absatz 1 Buchstabe b wird von der Kommission im Laufe des Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen. Der Vorschlag stützt sich auf das Ergebnis des strategischen Planungsprozesses gemäß Artikel 6 Absatz 6 der Verordnung XXX [Rahmenprogramm „Horizont Europa“].

Die genannten Beträge umfassen nicht die Beiträge der Mitgliedstaaten zu den Betriebs- und Verwaltungskosten des Kompetenzzentrums, die dem Finanzbeitrag der Union entsprechen sollen.

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht über die geschätzten Auswirkungen auf die Ausgaben

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	**1**	Binnenmarkt, Innovation und Digitales

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Nach 2027***	**INSGE-SAMT**
Titel 1 (Personalausgaben)	Verpflichtungen = Zahlungen	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
Titel 2 (Infrastruktur- und Betriebsausgaben)	Verpflichtungen = Zahlungen	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
Titel 3 (operative Ausgaben)	Verpflichtungen	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		1 957,922
	Zahlungen	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	1 957,922
Mittel für die Finanzausstattung des Programms INSGESAMT[42]	Verpflichtungen	=1+2+3	286,130	325,274	331,320	252,200	257,189	262,186	267,368		1 981,668
	Zahlungen	=1+2+4	22,459	105,795	153,954	171,154	160,369	154,096	152,126	1 061,715	1 981,668

41 Im Jahr 2021 werden Personalmittel nur für ein halbes Jahr berechnet.

42 Die festgelegten Gesamtmittel beziehen sich ausschließlich auf die EU-Finanzmittel, die im Zusammenhang mit der Cybersicherheit im Rahmen des Programms „Digitales Europa“ bereitgestellt werden. Der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft“ des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit“ des Programms „Horizont Europa“ (insgesamt 2 800 000 000 EUR) gemäß Artikel 5 Absatz 1 Buchstabe b wird von der Kommission im Laufe des Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen. Der Vorschlag stützt sich auf das Ergebnis des strategischen Planungsprozesses gemäß Artikel 6 Absatz 6 der Verordnung XXX [Rahmenprogramm „Horizont Europa“].

Rubrik des mehrjährigen Finanzrahmens	7	„Verwaltungsausgaben“

in Mio. EUR (3 Dezimalstellen)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Nach 2027***	**INSGE-SAMT**
Personalausgaben		3,090	3,233	3,233	3,233	3,233	3,233	3,805		23,060
Sonstige Verwaltungsausgaben		0,105	0,100	0,104	0,141	0,147	0,153	0,159		0,909
Mittel unter der RUBRIK 7 des mehrjährigen Finanzrahmens INSGESAMT	(Verpflichtungen insges. = Zahlungen insges.)	3,195	3,333	3,337	3,374	3,380	3,386	3,964		23,969

in Mio. EUR (3 Dezimalstellen)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Nach 2027***	**INSGE-SAMT**
Mittel INSGESAMT in allen RUBRIKEN des mehrjährigen Finanzrahmens	Verpflichtungen	289,325	328,607	334,657	255,574	260,569	265,572	271,332		2 005,637
	Zahlungen	25,654	109,128	157,291	174,528	163,749	157,482	156,090	1 061,715	2 005,637

3.2.2. Geschätzte Auswirkungen auf die Verwaltungsmittel

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt

– ☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

Jahre	2021	2022	2023	2024	2025	2026	2027	INSGESAMT
RUBRIK 7 des mehrjährigen Finanzrahmens								
Personalausgaben	3,090	3,233	3,233	3,233	3,233	3,233	3,805	23,060
Sonstige Verwaltungsausgaben	0,105	0,100	0,104	0,141	0,147	0,153	0,159	0,909
Zwischensumme RUBRIK 7 des mehrjährigen Finanzrahmens	3,195	3,333	3,337	3,374	3,380	3,386	3,964	23,969
Außerhalb der RUBRIK 7[43] des mehrjährigen Finanzrahmens								
Personalausgaben								
Sonstige Verwaltungsausgaben	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Zwischensumme außerhalb der RUBRIK 7 des mehrjährigen Finanzrahmens	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
INSGESAMT	4,433	6,363	7,079	7,192	7,274	7,358	8,016	47,715

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch der Verwaltung der Maßnahme zugeordnete Mittel der GD oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Der genannte Mittelbedarf für Personal- und sonstige Verwaltungsausgaben außerhalb der Rubrik 7 entspricht den Beträgen, die durch den Finanzbeitrag der Union aus dem Programm „Digitales Europa“ gedeckt werden.

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben außerhalb der Rubrik 7 erhöht sich um die Beträge, die durch den Finanzbeitrag der Union aus dem Programm „Horizont Europa“ gedeckt werden, sobald der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft“ des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit“ des Programms „Horizont Europa“ (insgesamt 2 800 000 000 EUR) gemäß Artikel 21 Absatz 1 Buchstabe b von der Kommission im Laufe des Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen wird.

[43] Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

Der genannte Mittelbedarf für Personal- und sonstige Verwaltungsausgaben außerhalb der Rubrik 7 umfasst nicht die Beiträge der Mitgliedstaaten zu den Betriebs- und Verwaltungskosten des Kompetenzzentrums entsprechend dem Finanzbeitrag der Union.

3.2.2.1. Geschätzter Personalbedarf bei der Kommission

– ☐ Für den Vorschlag/die Initiative werden keine Mittel für Personal benötigt.

– ■ Für den Vorschlag/die Initiative werden die folgenden Mittel für Personal benötigt:

Schätzung in Vollzeitäquivalenten

Jahre		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
Sitz und Vertretungen der Kommission		20	21	21	21	21	21	22
Delegationen								
Forschung								
• Externes Personal (in Vollzeitäquivalenten (VZÄ)) – VB, ÖB, ANS, LAK und JFD[44] Rubrik 7								
Aus der RUBRIK 7 des mehrjährigen Finanzrahmens finanziert	- am Sitz	3	3	3	3	3	3	3
	- in den Delegationen							
Aus der Finanzausstattung des Programms finanziert[45]	- am Sitz							
	- in den Delegationen							
Forschung								
Sonstiges (bitte angeben)								
INSGESAMT		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	Koordinierung, Überwachung und Steuerung der dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung übertragenen Aufgaben, einschließlich Unterstützungs- und Koordinierungskosten. Entwicklung und Koordinierung der Politik im Bereich der Cybersicherheit in Bezug auf die dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung übertragenen Aufgaben, z. B. im Hinblick auf die Festlegung von Prioritäten für die Forschungs- und Industriepolitik, die allgemeine Zusammenarbeit zwischen den Mitgliedstaaten und den Wirtschaftsteilnehmern, die Kohärenz mit dem künftigen EU-Rahmen für die Cybersicherheitszertifizierung, die Übernahme von Haftung und Fürsorgepflicht oder die Koordinierung mit Maßnahmen im Zusammenhang mit Hochleistungsrechnen, künstlicher Intelligenz und digitalen Kompetenzen.
Externes Personal	Koordinierung, Überwachung und Steuerung der dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung übertragenen Aufgaben, einschließlich Unterstützungs- und Koordinierungskosten.

[44] VB = Vertragsbedienstete, ÖB = Örtliche Bedienstete, ANS = Abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, BSD = Beigeordnete Sachverständige in Delegationen.

[45] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

	Entwicklung und Koordinierung der Politik im Bereich der Cybersicherheit in Bezug auf die dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung übertragenen Aufgaben, z. B. im Hinblick auf die Festlegung von Prioritäten für die Forschungs- und Industriepolitik, die allgemeine Zusammenarbeit zwischen den Mitgliedstaaten und den Wirtschaftsteilnehmern, die Kohärenz mit dem künftigen EU-Rahmen für die Cybersicherheitszertifizierung, die Übernahme von Haftung und Fürsorgepflicht oder die Koordinierung mit Maßnahmen im Zusammenhang mit Hochleistungsrechnen, künstlicher Intelligenz und digitalen Kompetenzen.

3.2.2.2. Geschätzter Personalbedarf beim Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung

	2021	2022	2023	2024	2025	2026	2027
Beamte der Kommission							
davon AD							
davon AST							
davon AST-SC							
Zeitbedienstete							
davon AD	10	11	13	13	13	13	13
davon AST							
davon AST-SC							
Vertragsbedienstete	26	32	39	39	39	39	39
Abgeordnete nationale Sachverständige (ANS)	1	1	1	1	1	1	1
Gesamt	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	Operative Umsetzung der dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung gemäß Artikel 4 dieser Verordnung übertragenen Aufgaben, einschließlich Unterstützungs- und Koordinierungskosten.
Externes Personal	Operative Umsetzung der dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung gemäß Artikel 4 dieser Verordnung übertragenen Aufgaben, einschließlich Unterstützungs- und Koordinierungskosten.

Der genannte geschätzte Personalbedarf des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung entspricht dem geschätzten Bedarf für die Ausführung des Finanzbeitrags der Union im Rahmen des Programms „Digitales Europa“.

Der genannte geschätzte Personalbedarf des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung erhöht sich um den geschätzten Bedarf für die Ausführung des Finanzbeitrags der Union im Rahmen des Programms „Horizont Europa“, sobald der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft“ des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit“ des Programms „Horizont Europa“ (insgesamt 2 800 000 000 EUR) gemäß Artikel 21 Absatz 1 Buchstabe b von der Kommission im Laufe des Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen wird.

3.2.2.3. Stellenplan des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung

Funktions- und Besoldungsgruppe	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD insgesamt	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST insgesamt							

AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
AST/SC insgesamt							
ENDSUMME	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Geschätzte personelle Auswirkungen (zusätzliches Personal) – externes Personal des Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung

Vertragsbedienstete	2021	2022	2023	2024	2025	2026	2027
Funktionsgruppe IV	20	22	29	29	29	29	29
Funktionsgruppe III	2	4	4	4	4	4	4
Funktionsgruppe II	4	6	6	6	6	6	6
Funktionsgruppe I							
Gesamt	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Um Kopfzahlneutralität zu gewährleisten, wird das zusätzliche Personal beim Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung zum Teil dadurch ausgeglichen, dass die Zahl der Beamten und des externen Personals (d. h. im Stellenplan und beim gegenwärtig beschäftigten externen Personal) in den einschlägigen Dienststellen der Kommission verringert wird.

Die Personalzahlen des Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung in den Punkten 3.2.2.2–3.2.2.4 werden wie folgt ausgeglichen[46]:

GESAMT	2021	2022	2023	2024	2025	2026	2027
Beamte der Kommission	5	5	6	6	6	6	6
Bedienstete auf Zeit							

[46] Vorbehaltlich des endgültigen Haushaltsbetrags, dessen Ausführung dem Kompetenzzentrum übertragen wird.

Vertragsbedienstete	14	17	20	20	20	20	20
Abgeordnete nationale Sachverständige (ANS)							
VZÄ insgesamt	19	22	26	26	26	26	26
Kopfzahl	19	22	26	26	26	26	26

Der Ausgleich für das Personal des Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung entspricht dem Anteil des Finanzbeitrags der Union, d. h. 50 %.

Der genannte Ausgleich bezieht sich auf den geschätzten Personalbedarf des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung für die Ausführung des Finanzbeitrags der Union im Rahmen des Programms „Digitales Europa".

Der genannte Ausgleich erhöht sich um den geschätzten Bedarf für die Ausführung des Finanzbeitrags der Union im Rahmen des Programms „Horizont Europa", sobald der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft" des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit" des Programms „Horizont Europa" (insgesamt 2 800 000 000 EUR) gemäß Artikel 21 Absatz 1 Buchstabe b von der Kommission im Laufe des Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen wird.

3.2.3. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative:

– ☐ sieht keine Kofinanzierung durch Dritte vor

– ☒ sieht folgende Kofinanzierung durch Dritte[47] vor:

Mittel in Mio. EUR (3 Dezimalstellen)

Jahre	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**INSGE-SAMT**
Mitgliedstaaten – Beitrag zu den Personalausgaben	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Mitgliedstaaten – Beitrag zu den Infrastruktur- und Betriebsausgaben	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Mitgliedstaaten – Beitrag zu den operativen Ausgaben	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
Kofinanzierung INSGESAMT	286,130	325,274	331,320	252,200	257,189	262,186	267,368	1 981,668

[47] Geschätzte Sachbeiträge der Mitgliedstaaten.

Der oben genannte Beitrag Dritter bezieht sich ausschließlich auf die Kofinanzierung in einem angemessenen Verhältnis zu den EU-Finanzmitteln für die Cybersicherheit im Rahmen des Programms „Digitales Europa“. Der genannte Beitrag Dritter erhöht sich, sobald der Beitrag aus der Finanzausstattung des Clusters „Inklusive und sichere Gesellschaft“ des Pfeilers II „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit“ des Programms „Horizont Europa“ (insgesamt 2 800 000 000 EUR) gemäß Artikel 21 Absatz 1 Buchstabe b von der Kommission im Laufe des Gesetzgebungsverfahrens und in jedem Fall vor Erreichen einer politischen Einigung vorgeschlagen wird. Der Vorschlag stützt sich auf das Ergebnis des strategischen Planungsprozesses gemäß Artikel 6 Absatz 6 der Verordnung XXX [Rahmenprogramm „Horizont Europa“].

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☒ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:

☐ auf die Eigenmittel

☐ auf die übrigen Einnahmen

Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind.

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Auswirkungen des Vorschlags/der Initiative[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikel …….							

Bitte geben Sie für die zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

[48] Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.