



Brüssel, den 12.9.2018
SWD(2018) 404 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

**VORSCHLAG FÜR EINE VERORDNUNG DES EUROPÄISCHEN PARLAMENTS
UND DES RATES**

**zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in
Industrie, Technologie und Forschung und des Netzes nationaler
Koordinierungszentren**

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Zusammenfassung

Folgenabschätzung zum Vorschlag zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit und des Netzes nationaler Koordinierungszentren

A. Handlungsbedarf

Warum? Um welche Problematik geht es?

Die EU verfügt heute nach wie vor über keine ausreichenden technischen und industriellen Kapazitäten, um ihre Wirtschaft und ihre kritischen Infrastrukturen selbst zu sichern und weltweit eine Führungsrolle auf dem Gebiet der Cybersicherheit zu übernehmen. Die vorliegende Initiative zielt darauf ab, die folgenden Probleme und ihre Ursachen anzugehen:

Problem 1: Unzureichende strategische und nachhaltige Koordinierung und Zusammenarbeit zwischen Industrie, Cybersicherheitsforschung und Behörden, um unsere Wirtschaft, Gesellschaft und Demokratie mit leistungsfähigen europäischen Cybersicherheitslösungen zu schützen.

Problem 2: Unzureichende Investitionen und begrenzter Zugang zu Know-how, Kompetenzen und Einrichtungen im Bereich der Cybersicherheit in ganz Europa.

Problem 3: Nur wenige europäische Forschungs- und Innovationsergebnisse im Bereich der Cybersicherheit werden in marktfähige Lösungen umgewandelt und kommen in der gesamten Wirtschaft zum Einsatz.

Diese Probleme haben mehrere Ursachen, darunter mangelndes Vertrauen zwischen den verschiedenen Akteuren des Cybersicherheitsmarktes, inhärente Beschränkungen bestehender Mechanismen für die Zusammenarbeit und die Bündelung von Mitteln, das Fehlen eines Rahmens für gemeinsame Vergabeverfahren für kostspielige Cybersicherheitsinfrastrukturen und Cybersicherheitsprodukte/-lösungen sowie das ungenutzte Potenzial von Push-Pull-Marktmechanismen.

Was soll mit dieser Initiative erreicht werden?

Mit dieser Initiative soll sichergestellt werden, dass die EU die wesentlichen (technischen und industriellen) Kapazitäten wahrt und weiterentwickelt, um ihre digitale Wirtschaft, Gesellschaft und Demokratie selbst zu sichern, und dass die Mitgliedstaaten von den fortschrittlichsten Cybersicherheitslösungen und Cyberabwehrkapazitäten profitieren. Die Initiative zielt auch darauf ab, die internationale Wettbewerbsfähigkeit der Cybersicherheitsunternehmen in der EU zu steigern und dafür zu sorgen, dass die europäische Industrie über verschiedene Sektoren hinweg Zugang zu den nötigen Kapazitäten und Ressourcen hat, um die Cybersicherheit in einen Wettbewerbsvorteil zu verwandeln. Dies sollte durch die Entwicklung wirksamer Mechanismen für eine langfristige strategische Zusammenarbeit aller relevanten Akteure (Behörden, Industrie, Forschung im zivilen wie militärischen Bereich), die Bündelung von Wissen und Ressourcen für die Bereitstellung von Spitzenkapazitäten und -infrastrukturen, die Förderung der breiten Einführung europäischer Cybersicherheitsprodukte und -lösungen in der gesamten Wirtschaft und im öffentlichen Sektor, die Unterstützung von Start-ups und KMU im Bereich der Cybersicherheit sowie die Schließung der Qualifikationslücke im Bereich der Cybersicherheit erreicht werden.

Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene?

Die Initiative würde einen Mehrwert zu den derzeitigen Anstrengungen auf nationaler Ebene darstellen, da sie in Industrie und Forschung zur Schaffung eines europaweiten Cybersicherheitsökosystems beiträgt. Sie soll zu einer besseren Zusammenarbeit der einschlägigen Interessenträger beitragen (auch zwischen zivilem und militärischem Cybersicherheitssektor), um die in ganz Europa vorhandenen Cybersicherheitsressourcen und -kenntnisse bestmöglich zu nutzen. Ferner soll sie der EU und den Mitgliedstaaten helfen, im Bereich der Cybersicherheit eine proaktive, längerfristige und strategische Industriepolitik zu verfolgen, die über die Forschung und Entwicklung hinausgeht. Dieser Ansatz soll nicht nur Durchbrüche bei der Bewältigung der Cybersicherheitsprobleme ermöglichen, vor denen sowohl der private als auch der öffentliche Sektor steht, sondern auch die wirksame Einführung der gefundenen Lösungen unterstützen. Er wird einschlägigen Forschungs- und Industriekreisen wie auch den Behörden Zugang zu Schlüsselkapazitäten verschaffen, z. B. zu Erprobungs- und Versuchseinrichtungen, die wegen mangelnder finanzieller und personeller Mittel häufig für einzelne Mitgliedstaaten unerschwinglich sind. Darüber hinaus wird sie dazu beitragen, die Qualifikationslücke zu schließen und ein Abwandern der fähigsten Fachkräfte zu verhindern, indem sie den besten Talenten Zugang zu europäischen Großprojekten verschafft und ihnen somit interessante berufliche Herausforderungen bietet. All dies wird auch als erforderlich angesehen, damit Europa weltweit eine Führungsrolle auf dem Gebiet der Cybersicherheit in Anspruch nehmen kann.

B. Lösungen

Welche Rechtsetzungs- und sonstigen Maßnahmen wurden erwogen? Wird eine Option bevorzugt? Warum?

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

1. **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 Programms „Horizont Europa“ unterstützt werden;
2. **Option 1:** Cybersicherheitskompetenznetz und Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung mit der Befugnis, Maßnahmen zur Förderung von Industrietechnologien sowie im Bereich Forschung und Innovation zu ergreifen;
3. **Option 2:** Cybersicherheitskompetenznetz und Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung beschränkt auf Forschungs- und Innovationstätigkeiten.

Die bereits in einem frühen Stadium verworfenen Optionen waren: 1) überhaupt keine Maßnahme zu ergreifen, 2) nur bestehende Kompetenzzentren zu vernetzen und 3) eine bestehende Agentur (ENISA, REA oder INEA) zu beauftragen.

Angesichts der allgemeinen Verpflichtung, die die Kommission im Hinblick auf die vorliegende Initiative bereits eingegangen ist, und angesichts der wichtigen Rolle, die die Mitgliedstaaten spielen müssen, liegt der Unterschied zwischen den beiden eingehend analysierten Optionen im Wesentlichen in ihrem Anwendungsbereich, der sich in ihrer Rechtsgrundlage widerspiegelt: Eine Einrichtung, die sich ausschließlich auf Artikel 187 AEUV stützt (Option 2), würde die Initiative auf den Bereich Forschung und Innovation beschränken und würde in der Regel einen Finanzbeitrag privater Akteure voraussetzen. Eine Einrichtung, die auf einer doppelten Rechtsgrundlage – Artikel 187 und 173 AEUV (Option 1) – beruht, würde über ein umfassenderes Mandat verfügen, das u. a. auch die Technologieeinführung und Unterstützung für die Industrie sowie die Schaffung größerer Synergien mit der Cyberabwehr bedeuten würde. Ferner würde den Mitgliedstaaten auch eine wichtigere Rolle eingeräumt – sowohl im Hinblick auf die Leitung als auch auf ihre Rolle als potenzielle Auftraggeber im Bereich der Cybersicherheitstechnik.

Die Analyse zeigte, dass die Option 1 am besten geeignet ist, um die Ziele der Initiative zu erreichen und gleichzeitig die größte wirtschaftliche, gesellschaftliche und ökologische Wirkung zu erzielen sowie die Interessen der Union zu wahren. Für diese Option sprach vor allem Folgendes: die Flexibilität, unterschiedliche Kooperationsmodelle mit der Gemeinschaft und dem Netz von Kompetenzzentren zu ermöglichen, um die Nutzung der vorhandenen Kenntnisse und Ressourcen zu optimieren; die Möglichkeit, die Zusammenarbeit der öffentlichen und privaten Akteure aus allen einschlägigen Bereichen, einschließlich der Verteidigung, zu strukturieren; die Möglichkeit, eine echte Industriepolitik für Cybersicherheit zu schaffen, indem nicht nur Forschung und Entwicklung, sondern auch Tätigkeiten zur Markteinführung gefördert werden. Nicht zuletzt ermöglicht die Option 1 auch eine größere Kohärenz, da sie einen Durchführungsmechanismus für die Finanzierungen im Bereich der Cybersicherheit aus den Programmen „Digitales Europa“ und „Horizont Europa“ schaffen und Synergien zwischen der zivilen und der verteidigungspolitischen Dimension der Cybersicherheit in Bezug auf den Europäischen Verteidigungsfonds fördern würde.

Wer unterstützt welche Option?

Nach den Ergebnissen des Konsultationsprozesses und der Faktenermittlung ist sowohl aus Sicht der Industrials als auch der Forschungskreise klar ein Mechanismus erforderlich, der es der EU ermöglicht, über Forschungs- und Entwicklungstätigkeiten hinaus eine kohärente Industriepolitik im Bereich der Cybersicherheit zu betreiben, wenn Europa weltweit eine Führungsrolle im Bereich der Cybersicherheit einnehmen soll. Gleichzeitig betonten die Interessenträger, dass für den Erfolg des Zentrums von entscheidender Bedeutung sein wird, dass seine Rolle bei der Unterstützung und Erleichterung der Bemühungen des Netzes und der einschlägigen Fachkreise genau definiert und mit dem Netz ein inklusiver, kooperativer Ansatz verfolgt wird, um neue Abschottungen zu vermeiden. Die Struktur sollte ferner so flexibel sein, dass sie leicht angepasst werden kann, da es sich bei der Cybersicherheit um ein sich rasch wandelndes Umfeld handelt. Während des gesamten Prozesses betonten die Mitgliedstaaten die Notwendigkeit, dass alle Mitgliedstaaten und ihre bestehenden Exzellenz- und Kompetenzzentren einbezogen werden müssen und dass der Komplementarität der Maßnahmen besondere

Aufmerksamkeit zukommen muss. Insbesondere im Hinblick auf das Zentrum hoben die Mitgliedstaaten die Bedeutung seiner koordinierenden Rolle bei der Unterstützung des Netzes hervor. Daher muss eine etwaige Initiative der Kommission das richtige Gleichgewicht bei den Leitungs- und Durchführungsstrukturen finden und dieses Gleichgewicht darin widerspiegeln, um eine wirksame Koordinierung auf europäischer Ebene unter Berücksichtigung der Entwicklungen auf nationaler Ebene zu gewährleisten.

C. Auswirkungen der bevorzugten Option

Worin bestehen die Vorteile der bevorzugten Option bzw. der wesentlichen Optionen?

Die bevorzugte Option wird es den Behörden und Unternehmen der Mitgliedstaaten ermöglichen, Cyberbedrohungen wirksamer zu verhüten und abzuwehren, indem sicherere Produkte und Lösungen zur Ausstattung bereitstehen. Dies ist insbesondere für den Schutz des Zugangs zu wesentlichen Dienstleistungen (z. B. Verkehr, Gesundheit, Banken und Finanzdienstleistungen) von Bedeutung. Sie würde außerdem positive Auswirkungen auf die Wettbewerbsfähigkeit der EU und die hier ansässigen KMU haben, da bei dieser Option von der Schaffung eines Mechanismus ausgegangen wird, mit dem die industriellen Kapazitäten der Mitgliedstaaten und der Union im Bereich der Cybersicherheit aufgebaut werden und die europäische wissenschaftliche Exzellenz in marktfähige Lösungen umgesetzt wird, die in der gesamten Wirtschaft eingesetzt werden könnten. Diese Option ermöglicht es, Ressourcen zu bündeln, um auf der Ebene der Mitgliedstaaten in die notwendigen Kapazitäten zu investieren und öffentliche europäische Werte und Anlagen aufzubauen, wobei gleichzeitig Größenvorteile erzielt werden. Dies wird wahrscheinlich dazu führen, dass KMU, die Industrie und Forscher besseren Zugang zu solchen Einrichtungen erhalten, wodurch Innovationen gefördert und Entwicklungsprozesse verkürzt werden können. Dies wird auch die Kosten für einige nachfrageseitige Unternehmen senken und ihnen helfen, die Cybersicherheit in einen Wettbewerbsvorteil zu verwandeln. Die Option ermöglicht es, Marktchancen für Produkte mit doppeltem Verwendungszweck zu nutzen, indem militärische und zivile Fachkreise zusammen an gemeinsamen Herausforderungen arbeiten können. Sie dürfte auch einen Mehrwert zu den nationalen Anstrengungen zur Schließung der Qualifikationslücke im Bereich der Cybersicherheit schaffen. Auf EU-Ebene ermöglicht diese Option auch die Verbesserung der Kohärenz und der Synergien zwischen den verschiedenen Finanzierungsmechanismen.

Eine indirekte positive Auswirkung auf die Umwelt könnte dadurch erreicht werden, dass besondere Cybersicherheitslösungen für Sektoren entwickelt werden, die potenziell enorme Umweltauswirkungen haben (z. B. Kernkraftwerke), um sie dabei zu unterstützen, potenziell verheerende Folgen von Cyberangriffen auf diese Art von Infrastruktur zu vermeiden.

Welche Kosten entstehen bei der bevorzugten Option bzw. den wesentlichen Optionen?

Die Kosten im Zusammenhang mit der bevorzugten Option bestehen hauptsächlich aus den Betriebskosten des Kompetenzzentrums und der nationalen Koordinierungszentren. Die Kosten für die Durchführung der verschiedenen Förderprogramme (Programm „Digitales Europa“ und Programm „Horizont Europa“) sind Gegenstand gesonderter Folgenabschätzungen.

Worin bestehen die Auswirkungen auf Unternehmen, KMU und Kleinstunternehmen?

Europäische Unternehmen auf der Angebots- und der Nachfrageseite im Bereich der Cybersicherheit – einschließlich KMU und Kleinstunternehmen, die auf diesem Gebiet tätig sind – zählen zu den Interessenträgergruppen, die die Auswirkungen am stärksten spüren werden. Durch die Einrichtung des Kompetenzzentrums und des Netzes werden ihnen zwar keine rechtlichen Verpflichtungen auferlegt, doch dürften sie dadurch die Kosten für die Gestaltung neuer Produkte senken, einen einfacheren Zugang zu Kapitalgebern erhalten und leichter die notwendigen Mittel für die Einführung marktfähiger Lösungen mobilisieren können. Im Falle von KMU und Kleinstunternehmen ist der Zugang zu öffentlich finanzierten Erprobungs- und Versuchseinrichtungen noch wichtiger, da es ihnen an Ressourcen fehlt, um die notwendige Infrastruktur außerhalb ihres Marktes (und oft auch außerhalb der EU) zu finden. Ferner besteht die Hoffnung, dass diese Initiative neue Märkte für europäische KMU und Kleinstunternehmen eröffnen würde, die im Bereich der Cybersicherheit tätig sind. Darüber hinaus wird der gewählte Mechanismus für die Koordinierung zwischen Forschung und Industrie sorgen und damit die Forschungsanstrengungen auf einen konkreten industriellen Bedarf ausrichten helfen. Die Bereitstellung spitzentechnologischer Kenntnisse und Instrumente im Bereich der Cybersicherheit wird die Wirtschaftsteilnehmer indirekt bei der Einhaltung der NIS-Richtlinie unterstützen.

Wird es nennenswerte Auswirkungen auf die nationalen Haushalte und Behörden geben?

Die Initiative wird es den Mitgliedstaaten ermöglichen, Investitionen in die erforderliche Infrastruktur für Cybersicherheit auf nationaler und europäischer Ebene zu koordinieren. Durch den Mechanismus können Ressourcen für Instrumente und Infrastrukturen gebündelt werden, die sonst für einzelne Mitgliedstaaten kostspieliger oder nicht erschwinglich wären. Ein solches Vorgehen würde Größenvorteile und Einsparungen ermöglichen. Der Finanzbeitrag der Mitgliedstaaten zum Kompetenzzentrum und den einschlägigen Maßnahmen sollte dem Beitrag der Union angemessen sein.

Wird es andere nennenswerte Auswirkungen geben?

Ja, die Initiative hat eindeutig positive Auswirkungen, da sie die Fähigkeit der Mitgliedstaaten, ihre Wirtschaft selbst zu sichern, u. a. durch den Schutz kritischer Sektoren, erheblich steigern sowie die Wettbewerbsfähigkeit europäischer Cybersicherheitsunternehmen und verschiedener Industriesektoren stärken wird, sodass sie ihre vorhandenen Werte und Anlagen angemessen schützen und sichere innovative Produkte und Dienste entwickeln können, während die Kosten für FuE im Zusammenhang mit der Sicherheit sinken werden. Dadurch dürfte es der EU letztlich möglich sein, bei der Digital- und Cybersicherheitstechnik der nächsten Generation eine Führungsrolle zu übernehmen.

D. Folgemaßnahmen**Wann wird die Maßnahme überprüft?**

Eine explizite Klausel in Bezug auf die Überwachung der zentralen Leistungsindikatoren (*Key Performance Indicators*, KPI) sowie eine Bewertungs- und Überprüfungs-klausel, wonach die Europäische Kommission eine Zwischenbewertung durchführen wird, um die Wirkung und den Mehrwert des Instruments zu beurteilen, ist im Rechtsinstrument vorgesehen. Die Europäische Kommission wird dem Europäischen Parlament und dem Rat anschließend Bericht erstatten. Im Anschluss an diese Bewertung kann die Kommission eine Überprüfung und Verlängerung des Mandats des Kompetenzzentrums und des Netzes vorschlagen.