EUROPÄISCHE
KOMMISSION

Brüssel, den 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Vorschlag für eine

EMPFEHLUNG DES RATES

für eine koordinierte Vorgehensweise der Union zur Stärkung der Resilienz kritischer Infrastruktur

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Sicherheit stellt ein wesentliches Ziel der Europäischen Union dar. Während die Hauptverantwortung für den Schutz der Bürgerinnen und Bürger bei den Mitgliedstaaten liegt, leisten kollektive Maßnahmen auf Unionsebene einen wichtigen Beitrag zur Sicherheit der gesamten EU. Die Koordinierung trägt zur Stärkung der Resilienz, zur Erhöhung der Wachsamkeit und zur Verbesserung unserer gemeinsamen Reaktion bei. Im Rahmen der EU-Sicherheitsunion wurden wichtige Schritte unternommen, um Fähigkeiten und Kapazitäten für die Prävention, Erkennung und rasche Reaktion auf viele Sicherheitsbedrohungen aufzubauen und Akteure des öffentlichen und des privaten Sektors in einer gemeinsamen Anstrengung miteinander zu vernetzen.

Die Befähigung der EU, auf die sich ständig wandelnde Bedrohungslage zu reagieren, erfordert ständige Wachsamkeit und Anpassung. Russlands Angriffskrieg gegen die Ukraine hat neue Risiken mit sich gebracht, die oft kombiniert als hybride Bedrohung auftreten. Dazu zählt auch das Risiko einer Unterbrechung der Erbringung wesentlicher Dienste durch Einrichtungen, die kritische Infrastrukturen in Europa betreiben. Dies ist durch die offensichtliche Sabotage der Gas-Pipelines Nord Stream 1 und 2 und weitere jüngste Vorfälle noch deutlicher geworden. Die Gesellschaft hängt in hohem Maße sowohl von physischen als auch von digitalen Infrastrukturen ab, und die Unterbrechung wesentlicher Dienste, sei es durch konventionelle physische Angriffe oder Cyberangriffe oder eine Kombination aus beidem, kann schwerwiegende Folgen für das Wohlergehen der Bürgerinnen und Bürger, unsere Wirtschaft und das Vertrauen in unsere demokratischen Systeme haben.

Ein reibungslos funktionierender Binnenmarkt ist ein weiteres zentrales Ziel der EU, auch in Bezug auf die wesentlichen Dienste, die von Betreibern kritischer Infrastrukturen erbracht werden. Die EU hat daher bereits eine Reihe von Maßnahmen ergriffen, um Schwachstellen zu verringern und die Widerstandsfähigkeit kritischer Einrichtungen sowohl in Bezug auf cyberbezogene als auch nicht cyberbezogene Risiken zu erhöhen.

Die Fähigkeit der EU, möglichen Angriffen auf kritische Infrastrukturen standzuhalten, muss dringend gestärkt werden – vor allem in der EU selbst, aber gegebenenfalls auch in ihrer unmittelbaren Nachbarschaft.

Die vorgeschlagene Empfehlung des Rates zielt darauf ab, die Unterstützung der EU zur Stärkung der Resilienz kritischer Infrastrukturen zu intensivieren und eine Koordinierung auf EU-Ebene in Bezug auf Abwehrbereitschaft und Reaktion zu gewährleisten. So sollen die Bemühungen zum Schutz der Anlagen, Einrichtungen und Systeme, die für das Funktionieren der Wirtschaft erforderlich sind, maximiert und beschleunigt und grundlegende Dienstleistungen im Binnenmarkt erbracht werden, auf die die Bürgerinnen und Bürger angewiesen sind, sowie die Auswirkungen von Angriffen abgefedert werden, indem für eine möglichst rasche Wiederherstellung der Infrastruktur gesorgt wird. Zwar sollten alle derartigen Infrastrukturen geschützt werden, doch die oberste Priorität liegt derzeit in den Bereichen Energie, digitale Infrastruktur, Verkehr und Raumfahrt, aufgrund ihres speziellen horizontalen Charakters für Gesellschaft und Wirtschaft sowie aufgrund der derzeitigen Risikobewertungen.

Der EU kommt in Bezug auf die Gewährleistung der Resilienz von die Land- oder Seegrenzen überschreitenden Infrastrukturen, die die Interessen mehrerer Mitgliedstaaten berühren, oder Infrastrukturen, über die wesentliche Dienste über Grenzen hinweg erbracht

werden, eine besondere Rolle zu. Kritische Infrastrukturen, die für mehrere Mitgliedstaaten von Bedeutung sind, können auch in nur einem Mitgliedstaat angesiedelt sein oder aber außerhalb des Hoheitsgebiets eines Mitgliedstaats, z. B. im Falle von Unterseekabeln oder Pipelines. Es liegt im Interesse aller Mitgliedstaaten und der EU als Ganzes, die kritischen Infrastrukturen und die sie betreibenden Einrichtungen sowie die Gefahren, die sie bedrohen, klar zu identifizieren und sich gemeinsam zu ihrem Schutz zu verpflichten.

Das Europäische Parlament und der Rat haben bereits eine politische Einigung über den Ausbau des Rechtsrahmens für die EU erzielt, um zur Stärkung der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, beizutragen. Im Sommer 2022 wurden Einigungen über die Richtlinie über die Resilienz kritischer Einrichtungen (im Folgenden „CER-Richtlinie“)[1] und die überarbeitete Richtlinie zur Netz- und Informationssicherheit (im Folgenden „NIS-2-Richtlinie“)[2] erzielt. Diese werden im Vergleich zum bestehenden Rechtsrahmen – der Richtlinie 2008/114/EG vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern („ECI-Richtlinie“)[3], und der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union („NIS-Richtlinie“)[4] – einen erheblichen Aufbau von Kapazitäten gewährleisten. Die neuen Rechtsvorschriften werden voraussichtlich Ende 2022 oder Anfang 2023 in Kraft treten, und die Mitgliedstaaten sollten der Umsetzung und Anwendung im Einklang mit dem Unionsrecht Vorrang einräumen.

Vor diesem Hintergrund und angesichts der möglichen Dringlichkeit, den Bedrohungen, die sich aus dem russischen Angriffskrieg gegen die Ukraine ergeben, zu begegnen, sollten die in den neuen Rechtsvorschriften dargelegten Schritte wenn möglich und angemessen bereits jetzt eingeleitet werden. Eine bereits jetzt intensivere Zusammenarbeit würde auch dazu beitragen, die Dynamik für eine wirksame Umsetzung zu schaffen, sobald die neuen Rechtsvorschriften in vollem Umfang in Kraft sind.

Dies würde dazu führen, dass man bereits über die derzeitigen Rahmenbedingungen hinausgehen könnte, sowohl in Bezug auf die Intensität der Maßnahmen als auch auf die Bandbreite der abgedeckten Sektoren. Die neue CER-Richtlinie enthält einen neuen Rahmen für die Zusammenarbeit sowie Verpflichtungen für die Mitgliedstaaten und kritische Einrichtungen, die auf die Stärkung der physischen nicht cyberbezogenen Resilienz gegenüber natürlichen und vom Menschen verursachten Bedrohungen von Einrichtungen abzielen, die wesentliche Dienste im Binnenmarkt erbringen, wobei elf Sektoren[5] spezifiziert werden. Mit der NIS-2-Richtlinie wird ein breiter sektoraler Geltungsbereich der Cybersicherheitspflichten eingeführt. Dazu gehört eine neue Verpflichtung für die Mitgliedstaaten, Unterseekabel gegebenenfalls in ihre Cybersicherheitsstrategien aufzunehmen.

Die Rechtsvorschriften sehen vor, dass die Kommission eine wesentliche Koordinierungsrolle übernimmt. Im Rahmen der CER-Richtlinie kommt der Kommission eine unterstützende und fördernde Rolle zu; sie sollte mit Unterstützung und Einbeziehung der durch diese Richtlinie eingerichteten Gruppe für die Resilienz kritischer Einrichtungen (CERG) die Tätigkeiten der

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 ABl. L 345 vom 23.12.2008.
4 ABl. L 194 vom 19.7.2016.
5 Energie, Verkehr, digitale Infrastruktur, Banken, Finanzmarktinfrastruktur, Gesundheit, Trinkwasser, Abwasser, öffentliche Verwaltung, Raumfahrt und Lebensmittel.

Mitgliedstaaten durch die Entwicklung bewährter Verfahren, Leitfäden und Methoden ergänzen. Was die Cybersicherheit anbelangt, so hat der Rat die Kommission, den Hohen Vertreter und die NIS-Kooperationsgruppe bereits in seinen Schlussfolgerungen zur Cyberabwehr der EU vom Sommer 2022 ersucht, Risikobewertungen und Szenarien unter dem Gesichtspunkt der Cybersicherheit auszuarbeiten. Eine solche Koordinierung kann als Grundlage für eine Vorgehensweise in Bezug auf andere wichtige kritische Infrastrukturen dienen.

Am 5. Oktober 2022 legte Präsidentin von der Leyen einen Fünf-Punkte-Plan vor, in dem eine koordinierte Vorgehensweise für die notwendigen Arbeiten dargelegt wird. Zu seinen Kernpunkten gehören folgende Aspekte: bessere Abwehrbereitschaft; Zusammenarbeit mit den Mitgliedstaaten im Hinblick auf Stresstests ihrer kritischen Infrastrukturen, beginnend mit dem Energiesektor und anschließend mit anderen Hochrisiko-Sektoren; Ausbau der Reaktionsfähigkeit, insbesondere durch das Katastrophenschutzverfahren der Union; sinnvolle Nutzung der Satellitenkapazitäten zur Erkennung potenzieller Bedrohungen, sowie Stärkung der Zusammenarbeit mit der NATO und wichtigen Partnern im Hinblick auf die Resilienz kritischer Infrastruktur. Im Fünf-Punkte-Plan wurde betont, wie wichtig es ist zu handeln, bevor die Rechtsvorschriften, für die bereits eine politische Einigung besteht, in Kraft treten.

In der vorgeschlagenen Empfehlung des Rates wird diese Vorgehensweise – die Unterstützung für die Mitgliedstaaten zu strukturieren und ihre Bemühungen zur Sensibilisierung für Risiken, Abwehrbereitschaft und Reaktion auf die derzeitigen Bedrohungen zu koordinieren – aufgegriffen. In diesem Zusammenhang werden Sachverständigensitzungen einberufen, um die Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, im Vorgriff auf das Inkrafttreten der CER-Richtlinie und der damit geschaffenen CERG zu erörtern.

Eine verstärkte Zusammenarbeit mit wichtigen Partnern sowie benachbarten und anderen relevanten Drittländern im Hinblick auf die Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, wird von entscheidender Bedeutung sein, insbesondere im Rahmen des strukturierten Dialogs über Resilienz zwischen der EU und der NATO.

Der Schwerpunkt dieser Empfehlung liegt auf der Stärkung der Fähigkeit der Union, die neuen Bedrohungen, die sich aus dem Angriffskrieg Russlands gegen die Ukraine ergeben, zu antizipieren, zu verhindern und darauf zu reagieren. Die empfohlenen Maßnahmen konzentrieren sich daher auf die Bewältigung sicherheitsrelevanter Risiken und Bedrohungen für die kritische Infrastruktur. Es sei jedoch darauf hingewiesen, dass die jüngsten Ereignisse auch deutlich gemacht haben, dass den Auswirkungen des Klimawandels auf kritische Infrastrukturen und Dienstleistungen dringend mehr Aufmerksamkeit gewidmet werden muss, beispielsweise im Hinblick auf eine saisonal gefährdete und unvorhersehbare Wasserversorgung für die Kühlung von Kernkraftwerken, für Wasserkraftwerke und die Binnenschifffahrt, oder die Gefahr materieller Schäden an der Verkehrsinfrastruktur, die zu erheblichen Störungen bei den wesentlichen Diensten führen können. Diesen Bedenken wird weiterhin durch einschlägige Rechtsvorschriften und Koordinierung Rechnung getragen.

- **Kohärenz mit den bestehenden Vorschriften in diesem Politikbereich**

Dieser Vorschlag für eine Empfehlung des Rates steht voll und ganz im Einklang mit dem derzeitigen und dem künftigen Rechtsrahmen für die Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, der ECI-Richtlinie bzw. der CER-Richtlinie, da er unter anderem darauf abzielt, die Zusammenarbeit zwischen den Mitgliedstaaten in diesem Bereich zu erleichtern und konkrete Maßnahmen zur Stärkung der Resilienz gegenüber den

derzeitigen unmittelbaren Bedrohungen für Einrichtungen, die kritische Infrastrukturen in der EU betreiben, zu unterstützen.

Darüber hinaus ergänzt und antizipiert er die CER-Richtlinie, da die Mitgliedstaaten bereits aufgefordert werden, der fristgerechten Umsetzung der Richtlinie Vorrang einzuräumen, indem sie im Rahmen des von der Kommission angekündigten 5-Punkte-Plans in Sachverständigensitzungen zusammenarbeiten und indem sie sich die Koordinierung des Weges zu einer gemeinsamen Vorgehensweise für die Durchführung von Stresstests für kritische Infrastrukturen in der EU zum Ziel setzen.

Der Vorschlag steht auch im Einklang mit der NIS-Richtlinie und der künftigen NIS-2-Richtlinie, mit der die NIS-Richtlinie aufgehoben wird, da ein frühzeitiger Beginn der Durchführungs- und Umsetzungsarbeiten gefordert wird. Er spiegelt auch den gemeinsamen Aufruf im Rahmen der Tagung in Nevers vom März 2022 sowie die Schlussfolgerungen des Rates zur Cyberabwehr der EU vom Mai 2022 in Bezug auf die Aufforderung der Mitgliedstaaten an die Kommission, Risikobewertungen und Risikoszenarien zu entwickeln, wider.

Der Vorschlag steht auch im Einklang mit der Katastrophenschutzpolitik der EU, im Zuge derer die Mitgliedstaaten und Drittländer im Falle einer massiven Störung des Betriebs kritischer Infrastrukturen/Einrichtungen über das Zentrum für die Koordination von Notfallmaßnahmen (ERCC) im Rahmen des Katastrophenschutzverfahrens der Union (UCPM) um Hilfe ersuchen können. Im Falle einer Aktivierung des UCPM kann das ERCC den Einsatz der in den Mitgliedstaaten (teilweise im Rahmen des Europäischen Katastrophenschutz-Pools) und im Rahmen von rescEU verfügbaren wesentlichen Ausrüstungsgegenstände, Materialien und Fachkenntnisse für das betroffene Land koordinieren und kofinanzieren. Die Hilfe, die auf Anfrage bereitgestellt werden kann, umfasst beispielsweise Brennstoff, Generatoren, Strominfrastruktur, Schutz-, Wasseraufbereitungs- und medizinische Notfallkapazitäten.

Der Vorschlag steht auch im Einklang mit dem EU-Besitzstand im Bereich der Energieversorgungssicherheit.

Der Kernenergiesektor ist in der vorgeschlagenen Empfehlung des Rates nicht ausdrücklich enthalten, mit Ausnahme z. B. damit verbundener Infrastruktur (wie Übertragungsleitungen zu Kernkraftwerken), die die Versorgungssicherheit beeinträchtigen könnte. Bestimmte nukleare Elemente fallen unter die einschlägigen Rechtsvorschriften im Nuklearbereich im Rahmen des Euratom-Vertrags und/oder nationale Rechtsvorschriften.[6] Auf der Grundlage der Lehren aus dem Unfall in Fukushima wurden die europäischen Rechtsvorschriften für nukleare Sicherheit verschärft, weshalb die nationalen Behörden regelmäßige Sicherheitsüberprüfungen für jede Anlage durchführen müssen, um die kontinuierliche Einhaltung der höchsten Sicherheitsanforderungen sicherzustellen und weitere Sicherheitsverbesserungen zu ermitteln; dazu kommen sechs jährliche themenbezogene Peer-Reviews auf EU-Ebene.

In der EU-Strategie für maritime Sicherheit[7] und ihrem Aktionsplan[8] wird der Wandel der Bedrohungen im maritimen Bereich hervorgehoben und ein erneutes Engagement für den Schutz kritischer maritimer Infrastruktur, einschließlich der Infrastruktur unter Wasser und insbesondere der maritimen Infrastruktur in den Bereichen Verkehr, Energie und

6 Erwägungsgrund 9 der Richtlinie 2008/114/EG des Rates (ECI-Richtlinie).
7 11205/14.
8 10494/18.

Kommunikation gefordert, auch durch eine Verbesserung der maritimen Lageerfassung durch bessere Interoperabilität und einen optimierten Informationsaustausch.

Der Vorschlag steht auch im Einklang mit anderen einschlägigen sektorspezifischen Rechtsvorschriften. Daher sollte die Umsetzung dieser Empfehlung mit spezifischen Maßnahmen, mit denen bestimmte Aspekte der Resilienz von Einrichtungen, die in betroffenen Sektoren wie z. B. dem Verkehrssektor tätig sind, geregelt werden oder künftig geregelt werden können, übereinstimmen. Dazu gehören auch andere einschlägige Initiativen wie der Notfallplan für den Verkehr[9] oder der Notfallplan für Lebensmittelversorgung und Ernährungssicherheit in Krisenzeiten[10] und der Europäische Vorsorge- und Reaktionsmechanismus für Ernährungssicherheit. Ganz allgemein sollte die Empfehlung natürlich unter uneingeschränkter Achtung aller geltenden Vorschriften des EU-Rechts umgesetzt werden, einschließlich derjenigen, die in der ECI-Richtlinie und der NIS-Richtlinie festgelegt sind.

Der Vorschlag steht auch im Einklang mit dem Strategischen Kompass für Sicherheit und Verteidigung, in dem betont wurde, dass die Resilienz und die Fähigkeit zur Abwehr von hybriden Bedrohungen und Cyberangriffen erheblich verbessert werden müssen, und dass die Resilienz der Partnerländer und die Zusammenarbeit mit der NATO gestärkt werden müssen. Er steht außerdem im Einklang mit dem Rahmen für eine koordinierte Reaktion der EU auf gegen die EU, ihre Mitgliedstaaten und ihre Partner gerichtete hybride Bedrohungen und Kampagnen.[11]

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Der Vorschlag stützt sich auf Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der die Angleichung der Rechtsvorschriften zur Verbesserung des Binnenmarkts vorsieht, in Verbindung mit Artikel 292 AEUV. Dies ist dadurch gerechtfertigt, dass mit der vorgeschlagenen Empfehlung des Rates in erster Linie Maßnahmen vorgezogen werden sollen, die in der neuen CER-Richtlinie und der NIS-2-Richtlinie festgelegt sind, die beide ebenfalls auf Artikel 114 AEUV beruhen. Im Einklang mit der Logik, die die Verwendung dieses Artikels als Rechtsgrundlage für diese Richtlinien rechtfertigt, ist ein Tätigwerden der EU erforderlich, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, insbesondere angesichts des grenzüberschreitenden Charakters und des grenzüberschreitenden Umfangs der betreffenden Dienste und der potenziellen Folgen im Falle von Störungen sowie der tatsächlichen und sich abzeichnenden nationalen Maßnahmen zur Stärkung der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, welche zur Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Ein weiteres Vorgehen auf europäischer Ebene im Bereich der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, ist angesichts der voneinander abhängigen und grenzüberschreitenden Beziehungen zwischen dem Betrieb kritischer Infrastrukturen und den

9 COM(2022) 211.
10 COM(2021) 689.
11 Rat der Europäischen Union, 10016/22, 21. Juni 2022.

erbrachten wesentlichen Diensten und der Notwendigkeit einer gemeinsamen und besser koordinierten europäischen Vorgehensweise gerechtfertigt, damit sichergestellt wird, dass die betreffenden Einrichtungen im derzeitigen geopolitischen Kontext über eine ausreichende Resilienz verfügen. Viele der gemeinsamen Herausforderungen, wie die offensichtliche Sabotage der Gaspipelines Nord Stream 1 und 2, werden zwar in erster Linie durch nationale Maßnahmen oder durch Einrichtungen, die kritische Infrastrukturen betreiben, angegangen; die Unterstützung durch die EU, gegebenenfalls mithilfe einschlägiger Agenturen, ist jedoch erforderlich, um die Resilienz zu stärken, die Wachsamkeit zu erhöhen und die gemeinsame Reaktion der EU zu verbessern.

- **Verhältnismäßigkeit**

Der vorliegende Vorschlag steht im Einklang mit dem in Artikel 5 Absatz 4 des Vertrags über die Europäische Union (EUV) verankerten Grundsatz der Verhältnismäßigkeit.

Weder Inhalt noch Form der vorgeschlagenen Empfehlung des Rates gehen über das hinaus, was zur Erreichung ihrer Ziele notwendig ist. Die vorgeschlagenen Maßnahmen stehen in einem angemessenen Verhältnis zu den verfolgten Zielen, da sie die Vorrechte und Pflichten der Mitgliedstaaten nach nationalem Recht achten.

Schließlich wird in dem Vorschlag ein möglicher differenzierter Ansatz berücksichtigt, der den unterschiedlichen internen Gegebenheiten der Mitgliedstaaten in Bezug auf die Abwehrbereitschaft und Reaktion auf physische Bedrohungen kritischer Infrastrukturen Rechnung trägt.

- **Wahl des Instruments**

Um die oben genannten Ziele zu erreichen, sieht der AEUV insbesondere in Artikel 292 vor, dass der Rat Empfehlungen auf der Grundlage eines Vorschlags der Kommission annimmt. Eine Empfehlung des Rates ist in diesem Fall ein geeignetes Instrument, auch unter Berücksichtigung des derzeitigen oben erläuterten rechtlichen Kontexts. Als Rechtsakt – wenn auch nicht verbindlich – signalisiert eine Empfehlung des Rates das Engagement der Mitgliedstaaten für die darin enthaltenen Maßnahmen und bietet eine solide politische Grundlage für die Zusammenarbeit in diesen Bereichen, wobei die Befugnisse der Mitgliedstaaten in vollem Umfang gewahrt bleiben.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Konsultation der Interessenträger**

Bei der Ausarbeitung dieses Vorschlags wurden die in der Sitzung vom 12. Oktober 2022 geäußerten Ansichten der Sachverständigen der Mitgliedstaaten berücksichtigt. Es bestand ein breiter Konsens darüber, dass eine stärkere Koordinierung auf Unionsebene in Bezug auf Abwehrbereitschaft und Reaktion angesichts der derzeitigen Bedrohungslage sinnvoll ist und bestimmte Elemente der CER-Richtlinie bereits vor ihrer förmlichen Annahme umgesetzt werden sollten. Die Mitgliedstaaten erklärten sich bereit, Erfahrungen und bewährte Verfahren in Bezug auf Maßnahmen und Methoden zur Stärkung der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, auszutauschen. Die Mitgliedstaaten zeigten sich auch offen für eine koordinierte Vorgehensweise in Bezug auf Stresstests von Einrichtungen, die kritische Infrastrukturen betreiben – auf freiwilliger Basis und auf der Grundlage gemeinsamer Grundsätze. Die Mitgliedstaaten wiesen darauf hin, dass Einrichtungen, die kritische Infrastrukturen in den Bereichen Energie, digitale Infrastruktur und Verkehr betreiben, für die Zwecke dieser Empfehlung als prioritär betrachtet werden

sollten, insbesondere solche, die für mehrere Mitgliedstaaten von Bedeutung sind. Die Mitgliedstaaten begrüßten ferner die Absicht der Kommission, in den kommenden Wochen weitere Sitzungen von Sachverständigen der Mitgliedstaaten einzuberufen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Der Vorschlag für eine Empfehlung des Rates enthält Folgendes:

– In Kapitel I werden das Ziel des Vorschlags, sein Inhalt und die Priorisierung der empfohlenen Maßnahmen dargelegt.

– Kapitel II konzentriert sich auf Maßnahmen, die sowohl auf Ebene der Union als auch auf Ebene der Mitgliedstaaten zur Verbesserung der Abwehrbereitschaft ergriffen werden sollten.

– Kapitel III befasst sich mit der verstärkten Reaktion sowohl auf EU-Ebene als auch auf Ebene der Mitgliedstaaten.

– Kapitel IV bezieht sich auf die internationale Zusammenarbeit und die Maßnahmen, die zur Stärkung der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, ergriffen werden sollten.

2022/0338 (NLE)

Vorschlag für eine

EMPFEHLUNG DES RATES

für eine koordinierte Vorgehensweise der Union zur Stärkung der Resilienz kritischer Infrastruktur

(Text von Bedeutung für den EWR)

DER RAT DER EUROPÄISCHEN UNION

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 114 und 292,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Der Union kommt in Bezug auf grenzüberschreitende Infrastruktur, die die Interessen mehrerer Mitgliedstaaten berührt, oder Infrastruktur, die von Einrichtungen zur Bereitstellung wesentlicher Dienste über Grenzen hinweg genutzt wird, eine besondere Rolle zu. Die zu erbringenden Dienste und die kritische Infrastruktur, die für mehrere Mitgliedstaaten von Bedeutung sind, können auch in einem einzigen Mitgliedstaat angesiedelt sein oder aber außerhalb der Hoheitsgebiete der Mitgliedstaaten, z. B. im Falle von Unterseekabeln oder Pipelines. Es liegt im Interesse aller Mitgliedstaaten und der Union insgesamt, diese Infrastruktur und Einrichtungen eindeutig zu identifizieren, ihre Bedrohungen zu ermitteln und sich gemeinsam zu ihrem Schutz zu verpflichten.

(2) Die Richtlinie 2008/114/EG des Rates[12] regelt derzeit den Schutz kritischer Infrastruktur in zwei Sektoren. Um die Menschen besser zu schützen, werden in dieser Richtlinie ein Verfahren zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen sowie ein gemeinsamer Ansatz für die Bewertung der Notwendigkeit, den Schutz derartiger Infrastrukturen zu verbessern, festgelegt. Die Richtlinie betrifft den Energiesektor und den Verkehrssektor. Um die Resilienz kritischer Einrichtungen und der von ihnen erbrachten wesentlichen Dienste sowie der kritischen Infrastruktur, auf die sie hierbei angewiesen sind, zu verbessern, befindet sich derzeit eine neue Richtlinie über die Resilienz kritischer Einrichtungen[13] (im Folgenden „CER-Richtlinie“) im Annahmeverfahren der Gesetzgebungsorgane der Union, die die Richtlinie 2008/114/EG ersetzen soll und sich auf mehr Sektoren, einschließlich der digitalen Infrastruktur, erstrecken wird.

(3) Daneben stellt die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen

[12] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

[13] COM(2020) 829.

Sicherheitsniveaus von Netz- und Informationssystemen in der Union[14] auf Cyberbedrohungen ab. Diese Richtlinie soll durch eine neue Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union[15] (im Folgenden „NIS-2-Richtlinie“) ersetzt werden, die sich derzeit ebenfalls im Annahmeverfahren der Gesetzgebungsorgane der Union befindet.

(4) Angesichts der sich rasch ändernden Bedrohungslage, insbesondere im Kontext der offensichtlichen Sabotage der Gasinfrastruktur Nord Stream 1 und Nord Stream 2, stehen Einrichtungen, die kritische Infrastrukturen betreiben, vor besonderen Herausforderungen in Bezug auf ihre Widerstandsfähigkeit gegen feindliche Handlungen und andere von Menschen verursachte Bedrohungen, während die Gefahren aufgrund natürlicher Faktoren und des Klimawandels zunehmen und mit diesen feindlichen Handlungen zusammenwirken können. Daher müssen diese Einrichtungen mit Unterstützung der Mitgliedstaaten geeignete Maßnahmen zur Stärkung ihrer Resilienz ergreifen. Diese Maßnahmen und diese Unterstützung sollten über das in den Richtlinie 2008/114/EG und (EU) 2016/1148 vorgesehene Maß hinausgehen und noch vor der Annahme, dem Inkrafttreten und der Umsetzung der neuen CER- und NIS-2-Richtlinien ergriffen und geleistet werden.

(5) Die Union und die Mitgliedstaaten werden aufgefordert, bis zur Annahme, dem Inkrafttreten und der Umsetzung dieser neuen Richtlinien im Einklang mit dem Unionsrecht alle verfügbaren Instrumente zu nutzen, um Fortschritte zu erzielen und einen Beitrag zu leisten zur Stärkung der physischen Resilienz und Cyberresilienz dieser Einrichtungen und der von ihnen betriebenen kritischen Infrastruktur, mit der wesentliche Dienste im Binnenmarkt erbracht werden, d. h. Dienstleistungen, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit, der Sicherheit oder für die Umwelt von entscheidender Bedeutung sind. In diesem Zusammenhang bezeichnet der Ausdruck „Resilienz“ die Fähigkeit einer Einrichtung, Ereignisse, die die Erbringung der betreffenden wesentlichen Dienste erheblich stören oder stören könnten, zu verhindern, sich davor zu schützen, darauf zu reagieren, sie abzuwehren, ihre Folgen zu begrenzen, sie aufzufangen, zu bewältigen und sich von ihnen zu erholen.

(6) Um eine Vorgehensweise zu gewährleisten, die sowohl wirksam ist als auch so weit wie möglich mit der neuen CER-Richtlinie im Einklang steht, sollten die in dieser Empfehlung enthaltenen Maßnahmen Infrastruktur betreffen, die von einem Mitgliedstaat als kritische Infrastruktur eingestuft wird, sowohl nationale kritische Infrastruktur als auch europäische kritische Infrastruktur, unabhängig davon, ob die Einrichtung, die die kritische Infrastruktur betreibt, bereits im Rahmen dieser neuen Richtlinie als kritische Einrichtung ausgewiesen wurde. Für die Zwecke dieser Empfehlung wird der Ausdruck „kritische Infrastruktur“ mit dieser Bedeutung verwendet.

(7) Angesichts der bestehenden Bedrohungen sollten Maßnahmen zur Stärkung der Resilienz vorrangig in den Schlüsselsektoren Energie, digitale Infrastruktur, Verkehr und Weltraum ergriffen werden, und der Schwerpunkt dieser Maßnahmen sollte auf der Stärkung der Resilienz der kritische Infrastrukturen betreibenden Einrichtungen

[14] 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).

[15] COM(2020) 823.

gegenüber vom Menschen verursachten Risiken liegen. In Bezug auf nationale kritische Infrastruktur sollte Infrastruktur von grenzüberschreitender Bedeutung in Anbetracht der möglichen Folgen eines Eintritts von Risikoereignissen Vorrang genießen.

(8) Dementsprechend zielen die in dieser Empfehlung enthaltenen Maßnahmen in erster Linie darauf ab, die neuen CER- und NIS-2-Richtlinien, die sich auf Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) stützen, zu erweitern, indem sie die in diesen neuen Richtlinien vorgesehenen Maßnahmen vorziehen und ergänzen. Angesichts des grenzüberschreitenden Charakters und der Bedeutung der betreffenden kritischen Infrastruktur und wesentlichen Dienste und in Anbetracht der bereits bestehenden und möglicherweise noch entstehenden Unterschiede zwischen den nationalen Rechtsvorschriften, die den Binnenmarkt verzerren, ist es daher angezeigt, diese Empfehlung auch auf Artikel 114 AEUV in Verbindung mit Artikel 292 AEUV zu stützen.

(9) Die Umsetzung der vorliegenden Empfehlung lässt die bestehenden und zukünftigen Anforderungen des Unionsrechts in Bezug auf bestimmte Aspekte der Resilienz der betreffenden Einrichtungen unberührt und sollte stets mit diesen Anforderungen im Einklang stehen. Diese Anforderungen sind in allgemeinen Instrumenten wie der Richtlinie 2008/114/EG, der Richtlinie (EU) 2016/1148 und den diese ersetzenden neuen CER- und NIS-2-Richtlinien festgelegt, und auch in bestimmten sektorspezifischen Instrumenten, wie etwa im Verkehrsbereich, wo die Kommission unter anderem einen „Notfallplan für den Verkehr“[16] angenommen hat. Im Einklang mit dem Grundsatz der loyalen Zusammenarbeit sollte diese Empfehlung mit uneingeschränkter gegenseitiger Achtung und Unterstützung umgesetzt werden.

(10) Am 5. Oktober 2022 kündigte die Kommission einen Fünf-Punkte-Plan an, in dem eine koordinierte Vorgehensweise zur Bewältigung der künftigen Herausforderungen dargelegt wird und der vorsieht, die Abwehrbereitschaft voranzubringen, indem auf der neuen CER-Richtlinie aufgebaut wird, ohne auf deren Annahme und Inkrafttreten zu warten; der Plan sieht zudem vor, in Zusammenarbeit mit den Mitgliedstaaten auf der Grundlage gemeinsamer Grundsätze und beginnend mit dem Energiesektor Einrichtungen, die kritische Infrastrukturen betreiben, Stresstests zu unterziehen. Die vorliegende Empfehlung soll zu diesem Plan beitragen; sie greift die dort vorgeschlagene Vorgehensweise auf und präzisiert konkrete Umsetzungsmaßnahmen dazu.

(11) Vor dem Hintergrund einer sich rasch ändernden Bedrohungslage und des derzeitigen durch vom Menschen verursachte Risiken gekennzeichneten Risikoumfelds ist es insbesondere in Bezug auf kritische Infrastruktur von grenzüberschreitender Bedeutung entscheidend, ein genaues, aktuelles und vollständiges Bild der wichtigsten Risiken zu erhalten, die sich für Einrichtungen, die kritische Infrastrukturen betreiben, ergeben. Die Mitgliedstaaten sollten daher die erforderlichen Maßnahmen treffen, um ihre Bewertungen dieser Risiken vorzunehmen oder zu aktualisieren. Obgleich der Schwerpunkt der vorliegenden Empfehlung auf Sicherheitsrisiken liegt, sollten zusätzlich die Anstrengungen zur Bewältigung des Klimawandels und der Umweltrisiken fortgesetzt werden, insbesondere zumal Naturereignisse die vom Menschen verursachten Risiken weiter verschärfen können.

---

16 COM(2022) 211.

(12) Angesichts dieser Bedrohungslage sollten die Mitgliedstaaten aufgefordert werden, so bald wie möglich geeignete Maßnahmen zur Stärkung der Resilienz kritischer Infrastruktur zu ergreifen, die gegebenenfalls auch über die genannten Risikobewertungen hinausgehen, die nach der neuen CER-Richtlinie in Zukunft erforderlich sein werden.

(13) Zur Umsetzung des von der Kommission angekündigten Fünf-Punkte-Plans ist ein koordiniertes Arbeiten erforderlich, sodass noch vor der Einsetzung der in der neuen CER-Richtlinie vorgesehenen Gruppe für die Resilienz kritischer Einrichtungen nationale Sachverständige zusammengerufen werden sollten, um die Zusammenarbeit zwischen den Mitgliedstaaten und den Informationsaustausch in Bezug auf die Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, zu ermöglichen. Darunter fallen die Zusammenarbeit und der Informationsaustausch bei Tätigkeiten wie der Ermittlung kritischer Einrichtungen und Infrastruktur, der Vorbereitung der Ausarbeitung und Förderung gemeinsamer Grundsätze für die Durchführung von Stresstests und der gemeinsamen Auswertung der Ergebnisse dieser Stresstests, bei denen Schwachstellen sowie mögliche Kapazitäten ermittelt werden. Diese Prozesse dürften auch die Widerstandsfähigkeit der kritische Infrastrukturen betreibenden Einrichtungen gegen Klima- und Umweltrisiken verbessern. Auch würde diese Arbeit eine gemeinsame Priorisierung der Stresstestarbeiten mit einem Schwerpunkt auf den Sektoren Energie, digitale Infrastruktur, Verkehr und Weltraum ermöglichen. Die Kommission hat bereits begonnen, Sachverständige zu versammeln und deren Arbeit zu unterstützen, und sie beabsichtigt, diese Arbeit fortzuführen. Sobald die neue CER-Richtlinie in Kraft getreten und die Gruppe für die Resilienz kritischer Einrichtungen eingerichtet ist, sollte die Gruppe diese Vorarbeit im Rahmen ihrer in dieser Richtlinie festgelegten Aufgaben fortsetzen.

(14) Die Stresstestreihe sollte durch die Ausarbeitung eines Konzeptpapiers zu Sicherheitsvorfällen und Krisen bei kritischer Infrastruktur ergänzt werden, in dem die Ziele und Formen der Zusammenarbeit zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU bei der Reaktion auf Anschläge auf kritische Infrastruktur beschrieben und festgelegt werden, insbesondere wenn diese erhebliche Störungen bei der Bereitstellung von für den Binnenmarkt wesentlichen Diensten verursachen. In diesem Konzeptpapier sollten die bestehende Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) für die Koordinierung der Reaktion berücksichtigt, auf Kohärenz und Komplementarität mit dem Konzeptentwurf für eine koordinierte Reaktion auf Cybersicherheitsvorfälle und -krisen großen Ausmaßes geachtet und gemeinsam abgestimmte Kernbotschaften für die Öffentlichkeit festgelegt werden, da die Krisenkommunikation bei der Folgenbegrenzung von Sicherheitsvorfällen und Krisen im Zusammenhang mit kritischer Infrastruktur eine wichtige Rolle spielt.

(15) Um eine koordinierte und wirksame Reaktion auf aktuelle und zu erwartende Bedrohungen zu gewährleisten, wird die Kommission die Mitgliedstaaten bei der Stärkung ihrer Resilienz gegenüber diesen Bedrohungen zusätzlich unterstützen, indem sie ihnen insbesondere mit Briefings, Handbüchern und Leitlinien einschlägige Informationen liefert, die Übernahme von Ergebnissen von mit Unionsmitteln finanzierten Forschungs- und Innovationsprojekten fördert, die erforderlichen Maßnahmen vorzieht und dafür sorgt, dass die Überwachungsinstrumente der Union optimal eingesetzt werden. Der EAD sollte Bedrohungsanalysen vorlegen, die insbesondere von seinem EU-Zentrum für Informationsgewinnung und Lageerfassung erstellt werden können.

(16) Auch die sektorrelevanten Agenturen und Stellen der Union und andere einschlägige Einrichtungen sollten, soweit ihre in den einschlägigen Instrumenten des Unionsrechts festgelegten Mandate dies zulassen, in Resilienzfragen Unterstützung leisten. Insbesondere könnte die Agentur der Europäischen Union für Cybersicherheit (ENISA) in Fragen der Cybersicherheit Unterstützung leisten, die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) könnte ihr Fachwissen bereitstellen und dank ihres Meeresüberwachungsdienstes den Mitgliedstaaten in puncto maritime Sicherheit und Gefahrenabwehr zur Seite stehen, die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (EUROPOL) könnte bei der Informationssammlung und bei grenzüberschreitenden strafrechtlichen Ermittlungen behilflich sein, und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA) sowie das Satellitenzentrum der Europäischen Union (SatCen) könnten mittels Maßnahmen im Rahmen des Weltraumprogramms der Union Unterstützung leisten.

(17) Während die Hauptverantwortung für die Gewährleistung der Sicherheit kritischer Infrastruktur und der betreffenden Einrichtungen weiter bei den Mitgliedstaaten liegt, ist eine stärkere Koordinierung auf Unionsebene angezeigt, insbesondere in Bezug auf Bedrohungen, die möglicherweise mehrere Mitgliedstaaten gleichzeitig betreffen, wie etwa Russlands Angriffskrieg gegen die Ukraine, oder Bedrohungen, die die Resilienz und das Funktionieren der Wirtschaft der Union, des Binnenmarkts und unserer Gesellschaften beeinträchtigen können.

(18) Die vorliegende Empfehlung umfasst nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderläuft.

(19) Angesichts der zunehmenden wechselseitigen Abhängigkeiten zwischen physischer und digitaler Infrastruktur können zum einen auf kritische Bereiche gerichtete böswillige Cyberaktivitäten zu Störungen oder Schäden an physischer Infrastruktur führen, und kann zum anderen die Sabotage physischer Infrastruktur digitale Dienste unzugänglich machen. Da die Bedrohung durch komplexe hybride Angriffe zunimmt, sollten die Mitgliedstaaten bei ihrer Arbeit zur Umsetzung der vorliegenden Empfehlung auch solche Erwägungen berücksichtigen. In Anbetracht der Verflechtungen zwischen Cybersicherheit und physischer Sicherheit bei den Betreibern ist es wichtig, dass die Vorbereitungen für die Umsetzung und Anwendung der neuen NIS-2-Richtlinie so bald wie möglich beginnen und dass solche Vorbereitungen gleichzeitig auch in Bezug auf die neue CER-Richtlinie anlaufen.

(20) Neben der Verbesserung der Abwehrbereitschaft ist es auch wichtig, die Kapazitäten für eine rasche und wirksame Reaktion auf Ereignisse zu verbessern, die die Erbringung wesentlicher Dienste durch Einrichtungen, die kritische Infrastrukturen betreiben, gefährden können. Daher sollte die vorliegende Empfehlung Maßnahmen enthalten, die von den Mitgliedstaaten und auf Unionsebene ergriffen werden sollten, darunter eine stärkere Zusammenarbeit und einen intensiveren Informationsaustausch im Rahmen des Katastrophenschutzverfahrens der Union und der Einsatz der einschlägigen Instrumente des Weltraumprogramms der Union.

(21) Gemäß der Aufforderung des Rates in seinen Schlussfolgerungen zur Cyberabwehr der EU[17] führen die Kommission, der Hohe Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) und die mit der Richtlinie

[17] Cyber posture: Council approves conclusions - Consilium (europa.eu)

(EU) 2016/1148 eingesetzte Kooperationsgruppe (im Folgenden „NIS-Kooperationsgruppe“) in Abstimmung mit den einschlägigen zivilen und militärischen Stellen und Einrichtungen und den etablierten Netzwerken, darunter EU-CyCLONe, eine Risikobewertung durch und erstellen Risikoszenarien aus der Perspektive der Cybersicherheit für Bedrohungssituationen oder mögliche Angriffe auf Mitgliedstaaten oder Partnerländer. Bei diesem Arbeitsstrang liegt der Schwerpunkt auf kritischen Sektoren wie Energie, digitale Infrastruktur, Verkehr und Weltraum.

(22) Im gemeinsamen Aufruf der Minister auf der Tagung in Nevers[18] und in den Schlussfolgerungen des Rates zur Cyberabwehr der EU wurde zudem dazu aufgerufen, die Widerstandsfähigkeit der Kommunikationsinfrastruktur und -netze in der Union zu stärken und hierfür basierend auf einer Risikobewertung Empfehlungen an die Mitgliedstaaten und die Kommission zu richten. Diese Risikobewertung wird derzeit von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA sowie in Zusammenarbeit mit dem Gremium europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt. Die Risikobewertung und die Lückenanalyse befassen sich mit den Risiken von Cyberangriffen für die verschiedenen Teilsektoren der Kommunikationsinfrastruktur, darunter Festnetz- und Mobilnetzinfrastruktur, Satelliten, Unterseekabel, Internet-Routing usw., und bilden somit eine Grundlage für die Arbeit im Rahmen dieser Empfehlung. Die Ergebnisse dieser Risikobewertung werden in die laufende sektorübergreifende Cyberrisikobewertung und in die einschlägigen Szenarien einfließen, die der Rat in seinen Schlussfolgerungen vom 23. Mai 2022 gefordert hat.

(23) Diese beiden Arbeitsstränge werden aufeinander abgestimmt sein und auch mit der Arbeit an Katastrophenschutzszenarien koordiniert werden – Szenarien bei denen ein breites Spektrum von Naturkatastrophen und vom Menschen verursachten Katastrophen und unter anderem auch Cybersicherheitsvorfälle und deren reale Auswirkungen berücksichtigt werden und die derzeit von der Kommission und den Mitgliedstaaten gemäß dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates[19] erstellt werden. Aus Gründen der Effizienz, Wirksamkeit und Kohärenz sollten die Ergebnisse dieser Arbeiten bei der Umsetzung der vorliegenden Empfehlung berücksichtigt werden.

(24) Das EU-Instrumentarium für 5G-Sicherheit[20] umfasst einschlägige Maßnahmen und Risikominderungspläne zur Stärkung der Sicherheit von 5G-Netzen. Da viele wesentliche Dienste auf 5G-Netzen beruhen und die digitalen Ökosysteme eng verflochten sind, ist es von entscheidender Bedeutung, dass alle Mitgliedstaaten die in diesem Instrumentarium empfohlenen Maßnahmen so schnell wie möglich umsetzen und insbesondere auf Hochrisikoanbieter von wichtigen Anlagen, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft wurden, die einschlägigen Beschränkungen anwenden.

(25) Um die Abwehrbereitschaft und Reaktionsfähigkeit bei schwerwiegenden Cybersicherheitsvorfällen umgehend zu stärken, hat die Kommission ein kurzfristiges Unterstützungsprogramm für die Mitgliedstaaten eingerichtet und ENISA zusätzliche Mittel zugewiesen. Die Unterstützungsdienste im Rahmen des Programms umfassen

---

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924).

20 https://digital-strategy.ec.europa.eu/de/library/eu-toolbox-5g-security

Vorsorgemaßnahmen, wie Penetrationstests kritischer Einrichtungen zur Ermittlung von Schwachstellen. Außerdem sieht der Plan zusätzliche Möglichkeiten vor, um Mitgliedstaaten im Falle eines schwerwiegenden Sicherheitsvorfalls bei einer kritischen Einrichtung zu unterstützen. Dies ist ein erster Schritt gemäß den Schlussfolgerungen des Rates zur Cyberabwehr der EU, in denen die Kommission aufgefordert wurde, einen Vorschlag für einen Notfallfonds für Cybersicherheit vorzulegen. Die Mitgliedstaaten sollten diese Möglichkeiten im Einklang mit den geltenden Anforderungen in vollem Umfang nutzen.

(26) Das Unterseekabelnetz für Daten- und elektronische Kommunikation, das die ganze Welt umspannt, ist für die globale und innereuropäische Konnektivität von entscheidender Bedeutung. Wegen der erheblichen Länge der Kabel und ihres Verlaufs am Meeresboden ist eine visuelle Überwachung unter Wasser für die meisten Kabelabschnitte äußerst schwierig. Die geteilte Zuständigkeit und andere Fragen der Zuständigkeit im Zusammenhang mit diesen Kabeln stellen für die europäische und internationale Zusammenarbeit beim Schutz und der Wiederherstellung der Infrastruktur eine besondere Herausforderung dar. Die Risikobewertungen, die für digitale und physische Infrastruktur, die digitalen Diensten zugrunde liegt, derzeit laufen und noch geplant sind, müssen daher durch besondere, auf Unterseekabel abzielende Risikobewertungen und Optionen für Risikominderungsmaßnahmen ergänzt werden. Die Kommission wird zu diesem Zweck Studien durchführen und die Mitgliedstaaten über ihre Ergebnisse informieren.

(27) Die in der vorliegenden Empfehlung als vorrangig eingestuften Bereiche Energie und Verkehr können auch Risiken im Zusammenhang mit digitaler Infrastruktur ausgesetzt sein. Solche Risiken können beispielsweise bei Energietechnologien bestehen, die digitale Komponenten beinhalten. Für die Aufrechterhaltung der Erbringung wesentlicher Dienste und für die strategische Kontrolle der von Einrichtungen im Energiesektor betriebenen kritischen Infrastruktur ist auch die Sicherheit der einschlägigen Lieferketten von Belang. Diesen Umständen sollte Rechnung getragen werden, wenn zur Stärkung der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, gemäß dieser Empfehlung Maßnahmen ergriffen werden.

(28) Die zunehmende Bedeutung von Weltrauminfrastruktur und weltraumgestützter Dienste für sicherheitsbezogene Maßnahmen macht es unerlässlich, die Resilienz und den Schutz der Weltraumressourcen und -dienste der Union in der EU zu gewährleisten, und zwar auch im Rahmen der vorliegenden Empfehlung, um weltraumgestützte Daten und Dienste, die von Weltraumsystemen und -programmen für die Überwachung und den Schutz kritischer Infrastruktur in anderen Sektoren bereitgestellt werden, systematischer einzusetzen. In der neuen EU-Weltraumstrategie für Sicherheit und Verteidigung werden diesbezüglich geeignete Maßnahmen vorgeschlagen, die bei der Umsetzung der vorliegenden Empfehlung berücksichtigt werden sollten.

(29) Um Risiken für die Resilienz von Einrichtungen, die kritische Infrastrukturen in der Union oder in einschlägigen Drittländern oder in internationalen Gewässern betreiben, wirksam anzugehen, ist auch Zusammenarbeit auf internationaler Ebene erforderlich. Daher sollten die Mitgliedstaaten aufgefordert werden, mit der Kommission und dem Hohen Vertreter zusammenzuarbeiten, um zu diesem Zweck bestimmte Schritte zu unternehmen, wobei solche Schritte nur im Einklang mit ihren im Unionsrecht und insbesondere in den Bestimmungen der EU-Verträge zu den Außenbeziehungen festgelegten Aufgaben und Zuständigkeiten unternommen werden dürfen.

(30) Wie in der Mitteilung „Beitrag der Kommission zur europäischen Verteidigung“[21] dargelegt wurde, wird die Kommission in Zusammenarbeit mit dem Hohen Vertreter und den Mitgliedstaaten zur Unterstützung des „Strategischen Kompasses für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt“[22] in Bezug auf hybride Bedrohungen die sektorspezifischen Referenzwerte für die Resilienz bewerten und dazu bis 2023 Lücken, Bedarf und Lösungsschritte ermitteln. Diese Initiative dürfte die Arbeit im Rahmen der vorliegenden Empfehlung zur Stärkung der Resilienz, einschließlich der Resilienz kritischer Infrastruktur, unterstützen, indem sie dazu beiträgt, den Informationsaustausch und die Koordinierung der Maßnahmen zu verbessern.

(31) In der Strategie der Europäischen Union für maritime Sicherheit aus dem Jahr 2014 und dem zugehörigen Aktionsplan wurde ein erhöhter Schutz kritischer maritimer Infrastruktur, einschließlich der Unterseeinfrastruktur und insbesondere der maritimen Infrastruktur in den Bereichen Verkehr, Energie und Kommunikation, gefordert, indem unter anderem die maritime Lageerfassung durch eine bessere Interoperabilität und einen optimierten (verpflichtenden und freiwilligen) Informationsaustausch verbessert wird. Die Strategie und der Aktionsplan werden derzeit aktualisiert und um verstärkte Maßnahmen zum Schutz kritischer maritimer Infrastruktur erweitert. Diese Maßnahmen sollten in die vorliegende Empfehlung einfließen und sie ergänzen.

(32) Die Mitgliedstaaten sollten das gesamte Potenzial des Sicherheitsforschungsprogramms der Union und vor allem seine spezifische Priorität in Bezug auf kritische Infrastruktur nutzen, insbesondere im Rahmen der aus dem Fonds für die innere Sicherheit finanzierten Programme und anderer potenzieller Finanzierungsmöglichkeiten auf Unionsebene, wie des Europäischen Fonds für regionale Entwicklung, soweit die spezifischen Maßnahmen dessen Kriterien erfüllen. Auch REPowerEU bietet möglicherweise Finanzierungsoptionen für den Bereich der Resilienz. Unionsmittel müssen stets im Einklang mit den geltenden rechtlichen Anforderungen eingesetzt werden.

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

KAPITEL I: ZIEL, ANWENDUNGSBEREICH UND PRIORITÄTEN

1. Mit dieser Empfehlung werden die Mitgliedstaaten aufgefordert, dringend wirksame Maßnahmen zu ergreifen sowie miteinander, mit der Kommission und anderen einschlägigen Behörden und den betreffenden Einrichtungen loyal, effizient, solidarisch und koordiniert zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die zur Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu verbessern.

2. Die in dieser Empfehlung dargelegten Maßnahmen beziehen sich auf Infrastrukturen, die von einem Mitgliedstaat als kritische Infrastruktur, auch als europäische kritische Infrastruktur, ausgewiesen wurden.

---

[21] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52022DC0060&qid=1666001839847

[22] Rat der Europäischen Union, 7371/22, 21. März 2022 (https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/de/pdf).

3. Bei der Umsetzung dieser Empfehlung sollte der Stärkung der Resilienz von Einrichtungen, die in den Bereichen Energie, digitale Infrastruktur, Verkehr und Weltraum tätig sind, und der von diesen Einrichtungen betriebenen kritischen Infrastrukturen, die von grenzüberschreitender Bedeutung sind, Vorrang in Bezug auf vom Menschen verursachten Risiken eingeräumt werden.

KAPITEL II: BESSERE ABWEHRBEREITSCHAFT

Maßnahmen auf Ebene der Mitgliedstaaten

4. Die Mitgliedstaaten werden aufgefordert, Risikobewertungen in Bezug auf die Resilienz von Einrichtungen, die gemäß der Richtlinie 2008/114/EG im Verkehrs- und Energiesektor ausgewiesene europäische kritische Infrastrukturen betreiben, durchzuführen oder zu aktualisieren und die Zusammenarbeit bei solchen Risikobewertungen und den sich daraus ergebenden Maßnahmen zur Stärkung der Resilienz gegebenenfalls und im Einklang mit der genannten Richtlinie fortzusetzen.

5. Um ein hohes Maß an Resilienz der Einrichtungen, die kritische Infrastrukturen betreiben, zu erreichen, sollten die Mitgliedstaaten zudem die Vorbereitungsarbeiten beschleunigen, um die neue CER-Richtlinie so bald wie möglich umzusetzen und anzuwenden, insbesondere durch:

a) Beschleunigung der Annahme oder Aktualisierung nationaler Strategien zur Stärkung der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, als Reaktion auf die derzeitige Bedrohung. Die einschlägigen Teile dieser Strategie sollten der Kommission mitgeteilt werden;

b) Durchführung oder Aktualisierung von Risikobewertungen entsprechend der Entwicklung der derzeitigen Bedrohungen in Bezug auf die Resilienz von Einrichtungen, die kritische Infrastrukturen in relevanten Sektoren über Energie, digitale Infrastruktur, Verkehr und Weltraum hinaus betreiben, und, wenn möglich, in den Sektoren, die in den Anwendungsbereich der neuen CER-Richtlinie fallen, d. h. Banken, Finanzmarktinfrastruktur, digitale Infrastruktur, Gesundheit, Trinkwasser, Abwasser, öffentliche Verwaltung, Weltraum und Lebensmittelerzeugung, -verarbeitung und -verteilung, wobei der potenzielle hybride Charakter relevanter Bedrohungen, darunter Kaskadeneffekte und die Auswirkungen des Klimawandels, zu berücksichtigen ist;

c) Unterrichtung der Kommission über die nach Sektoren und Teilsektoren ermittelten Arten von Risiken und über die Ergebnisse der Risikobewertungen; dies kann anhand eines von der Kommission in Zusammenarbeit mit den Mitgliedstaaten entwickelten gemeinsamen Meldeformulars erfolgen;

d) Beschleunigung des Verfahrens zur Ermittlung und Ausweisung kritischer Einrichtungen, wobei die Priorität auf kritischen Einrichtungen liegen sollte, die

a) kritische Infrastrukturen nutzen, die physisch zwischen zwei oder mehr Mitgliedstaaten verbunden sind;

b) Teil von Unternehmensstrukturen sind, die mit kritischen Einrichtungen in anderen Mitgliedstaaten verbunden oder an diese angeschlossen sind;

c) in einem Mitgliedstaat als solche identifiziert wurden und wesentliche Dienste in oder für sechs oder mehr Mitgliedstaaten erbringen und daher von besonderer europäischer Bedeutung sind, und die Kommission entsprechend unterrichten;

d) Zusammenarbeit untereinander, vor allem in Bezug auf kritische Einrichtungen, wesentliche Dienste und kritische Infrastrukturen von grenzüberschreitender Bedeutung, insbesondere durch gegenseitige Konsultationen für die Zwecke von Nummer 5 Buchstabe d und durch gegenseitige Unterrichtung im Falle eines Sicherheitsvorfalls mit erheblichen oder potenziell erheblichen grenzüberschreitenden Störungen, wobei die Kommission gegebenenfalls auf dem Laufenden gehalten wird;

e) Verstärkung der Unterstützung für ausgewiesene kritische Einrichtungen zur Verbesserung ihrer Resilienz, wozu auch die Bereitstellung von Leitfäden und Methoden, die Organisation von Übungen zur Prüfung ihrer Resilienz, die Bereitstellung von Beratung und die Schulung ihres Personals gehören können, sowie die Ermöglichung von Zuverlässigkeitsüberprüfungen von Personen mit sensiblen Funktionen im Einklang mit den Rechtsvorschriften der Union und den nationalen Rechtsvorschriften im Rahmen der die Mitarbeiter betreffenden Maßnahmen für das Sicherheitsmanagement der kritischen Einrichtungen;

f) Beschleunigung der Benennung oder Einrichtung einer zentralen Anlaufstelle in der zuständigen Behörde, die zum Zwecke der grenzüberschreitenden Zusammenarbeit mit den zentralen Anlaufstellen anderer Mitgliedstaaten in Bezug auf die Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, eine Verbindungsfunktion wahrnehmen soll.

6. Die Mitgliedstaaten werden aufgefordert, Stresstests für Einrichtungen durchzuführen, die kritische Infrastrukturen betreiben. Insbesondere werden die Mitgliedstaaten aufgefordert, ihre Abwehrbereitschaft und die der betroffenen Einrichtungen im Energiesektor zu erhöhen und Stresstests in diesem Sektor durchzuführen, soweit möglich nach den auf Unionsebene gemeinsam vereinbarten Grundsätzen, und dabei eine wirksame Kommunikation mit den betreffenden Einrichtungen zu gewährleisten. Stresstests in anderen vorrangigen Sektoren, nämlich digitale Infrastruktur, Verkehr und Weltraum, könnten erforderlichenfalls später in Erwägung gezogen werden, wobei Inspektionen in den Teilsektoren Luft- und Seeverkehr gemäß dem Unionsrecht und unter Berücksichtigung der einschlägigen Bestimmungen der sektorspezifischen Rechtsvorschriften gebührend zu berücksichtigen sind.

7. Die Mitgliedstaaten werden aufgefordert, gegebenenfalls und im Einklang mit dem Unionsrecht in Bezug auf die Resilienz von Einrichtungen, die kritische Infrastrukturen von grenzüberschreitender Bedeutung betreiben, mit einschlägigen Drittländern zusammenzuarbeiten.

8. Die Mitgliedstaaten werden aufgefordert, im Einklang mit den geltenden Anforderungen potenzielle Finanzierungsmöglichkeiten auf Unionsebene und auf nationaler Ebene zu nutzen, um die Resilienz von Einrichtungen, die kritische Infrastrukturen in der Union betreiben, beispielsweise entlang transeuropäischer Netze, gegenüber dem gesamten Spektrum erheblicher Bedrohungen zu verbessern, insbesondere im Rahmen der aus dem Fonds für die innere Sicherheit und dem Europäischen Fonds für regionale Entwicklung finanzierten Programme, sofern die jeweiligen Förderkriterien erfüllt sind, sowie der Fazilität „Connecting Europe“; dies schließt Bestimmungen über die Sicherung der Klimaresilienz mit ein. Die im Rahmen des Katastrophenschutzverfahrens der Union bereitgestellten Mittel können im Einklang mit den geltenden Anforderungen auch zu diesem Zweck verwendet werden, insbesondere für Projekte im Zusammenhang mit Risikobewertungen,

Investitionsplänen oder -studien, dem Aufbau von Kapazitäten oder der Verbesserung der Wissensbasis. Auch REPowerEU bietet möglicherweise Finanzierungsoptionen für den Bereich der Resilienz.

9. Im Hinblick auf die Kommunikations- und Netzinfrastruktur in der Union sollte die NIS-Kooperationsgruppe – stets nach Artikel 11 der Richtlinie (EU) 2016/1148 und dann Artikel 14 der NIS-2-Richtlinie handelnd – ihre laufende Arbeit an einer gezielten Risikobewertung beschleunigen und Anfang 2023 erste Empfehlungen vorlegen. Dabei sollten Kohärenz und Komplementarität mit der Arbeit der NIS-Kooperationsgruppe zur Sicherheit der Lieferkette der Informations- und Kommunikationstechnologie sowie anderer einschlägiger Gruppen wie der gemäß der neuen CER-Richtlinie einzurichtenden Gruppe für die Resilienz kritischer Einrichtungen und dem im Rahmen des neuen Rechtsakts über die digitale Betriebsstabilität (DORA)[23] einzurichtenden Aufsichtsforum sichergestellt werden.

10. Die NIS-Kooperationsgruppe, die ihre Aufgaben nach Artikel 11 der Richtlinie (EU) 2016/1148 und dann Artikel 14 der NIS-2-Richtlinie wahrnehmen soll, wird ersucht, mit Unterstützung der Kommission und der ENISA ihrer Arbeit zur Sicherheit der digitalen Infrastruktur und des Weltraumsektors Vorrang einzuräumen, unter anderem durch die Ausarbeitung politischer Leitlinien sowie Methoden und Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit; Grundlage hierfür sind ein gefahrenübergreifender Ansatz in Bezug auf Untersee-Kommunikationskabel im Vorgriff auf das Inkrafttreten der NIS-2-Richtlinie sowie die Ausarbeitung von Leitlinien für Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit für Betreiber im Weltraumsektor mit dem Ziel, die Resilienz bodengestützter Infrastrukturen zur Unterstützung der Bereitstellung weltraumgestützter Dienste zu erhöhen.

11. Die Mitgliedstaaten sollten die Dienste für die Abwehrbereitschaft im Bereich der Cybersicherheit, die im Rahmen des mit der ENISA durchgeführten kurzfristigen Unterstützungsprogramms der Kommission angeboten werden, in vollem Umfang nutzen, insbesondere Penetrationstests zur Ermittlung von Schwachstellen; sie werden in diesem Zusammenhang ersucht, Einrichtungen, die kritische Infrastrukturen in den Bereichen Energie, digitale Infrastruktur und Verkehr betreiben, Vorrang einzuräumen.

12. Die Mitgliedstaaten sollten dringend die im EU-Instrumentarium für die 5G-Cybersicherheit[24] empfohlenen Maßnahmen umsetzen. Mitgliedstaaten, die noch keine Beschränkungen für Hochrisikoanbieter erlassen haben, sollten dies unverzüglich tun, da Zeitverluste die Anfälligkeit der Netze in der Union erhöhen können. Sie sollten auch den physischen und nicht physischen Schutz kritischer und sensibler Teile von 5G-Netzen verstärken, unter anderem durch strenge Zugangskontrollen. Darüber hinaus sollten die Mitgliedstaaten in Zusammenarbeit mit der Kommission prüfen, ob ergänzende Maßnahmen, einschließlich rechtsverbindlicher Anforderungen auf Unionsebene, notwendig sind, um so ein einheitliches Maß an Sicherheit und Resilienz der 5G-Netze zu gewährleisten.

13. Die Mitgliedstaaten sollten den anstehenden Netzkodex für Aspekte der Cybersicherheit bei grenzüberschreitenden Stromflüssen so bald wie möglich umsetzen und dabei auf den Erfahrungen bei der Umsetzung der NIS-Richtlinie und

---

23 COM(2020) 595 final.

24 https://digital-strategy.ec.europa.eu/de/library/eu-toolbox-5g-security

den einschlägigen Leitlinien der NIS-Kooperationsgruppe aufbauen, insbesondere auf ihrem Referenzdokument über Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste.

14. Die Mitgliedstaaten sollten die Nutzung von Galileo und/oder Copernicus für Überwachungszwecke ausbauen und einschlägige Informationen mit den nach Nummer 15 einberufenen Sachverständigen austauschen. Die Fähigkeiten, die die staatliche Satellitenkommunikation (GOVSATCOM) der Union im Rahmen des Weltraumprogramms der Union für die Überwachung kritischer Infrastrukturen und die Unterstützung der Krisenreaktion bietet, sollten sinnvoll genutzt werden.

Maßnahmen auf Unionsebene

15. Die Kommission beabsichtigt, die Zusammenarbeit zwischen den Sachverständigen der Mitgliedstaaten zu verstärken, um die physische, nicht cyberbezogene Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, zu verbessern; dies soll insbesondere über folgende Maßnahmen erfolgen:

a) Vorbereitung der Entwicklung und Förderung gemeinsamer Instrumente zur Unterstützung der Mitgliedstaaten bei der Stärkung dieser Resilienz, einschließlich Methoden und Risikoszenarien;

b) Unterstützung der Entwicklung gemeinsamer Grundsätze für die Durchführung der unter Nummer 6 genannten Stresstests durch die Mitgliedstaaten, beginnend mit Tests, bei denen der Schwerpunkt auf vom Menschen verursachten Risiken im Energiesektor und anschließend in anderen Schlüsselsektoren wie digitale Infrastruktur, Verkehr und Weltraum liegt, Beseitigung anderer erheblicher Risiken und Gefahren sowie gegebenenfalls Unterstützung und Beratung bei der Durchführung solcher Stresstests;

c) Bereitstellung einer sicheren Plattform für die Sammlung, Bestandsaufnahme und den Austausch von bewährten Verfahren, Lehren aus nationalen Erfahrungen und anderen Informationen im Zusammenhang mit einer solchen Resilienz, einschließlich der Durchführung dieser Stresstests und der Umsetzung der Ergebnisse in Protokolle und Notfallpläne.

Die Arbeit dieser Sachverständigen sollte sektorübergreifenden Abhängigkeiten und Einrichtungen, die kritische Infrastrukturen von grenzüberschreitender Bedeutung betreiben, besondere Aufmerksamkeit widmen und von der Gruppe für die Resilienz kritischer Einrichtungen, sobald sie eingerichtet ist, fortgesetzt werden.

16. Die Mitgliedstaaten sollten sich uneingeschränkt an der verstärkten Zusammenarbeit nach Nummer 15 beteiligen, unter anderem durch die Benennung von Kontaktstellen mit einschlägigem Fachwissen und durch den Erfahrungsaustausch über die für die Stresstests verwendeten Verfahren und die auf deren Grundlage entwickelten Protokolle und Notfallpläne. Bei diesem Informationsaustausch sollten die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen kritischer Einrichtungen unter Beachtung der Sicherheit der Mitgliedstaaten geschützt werden. Dies umfasst nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderläuft.

17. Die Kommission wird die Mitgliedstaaten durch die Bereitstellung von Handbüchern und Leitlinien, etwa eines Handbuchs zum Schutz kritischer Infrastruktur und öffentlicher Räume vor unbemannten Luftfahrzeugsystemen, sowie von

Instrumenten für Risikobewertungen unterstützen. Der EAD wird ersucht, insbesondere über das EU-Zentrum für Informationsgewinnung und Lageerfassung und seine Analyseeinheit für hybride Bedrohungen Briefings zu den Bedrohungen für kritische Infrastrukturen in der EU durchzuführen, um das Lagebewusstsein zu verbessern.

18. Die Kommission wird die Übernahme der Ergebnisse von im Rahmen der Forschungs- und Innovationsprogramme der Union finanzierten Projekten zur Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, unterstützen. Die Kommission beabsichtigt, innerhalb des Budgets für Horizont Europa im Rahmen des Mehrjährigen Finanzrahmens 2021-2027 die Mittel für diese Resilienz aufzustocken. Dies sollte es ermöglichen, aktuelle und künftige Herausforderungen in diesem Bereich – wie etwa die Sicherung der Klimaresilienz kritischer Infrastrukturen – anzugehen, ohne dass dadurch die Mittel für sonstige Forschungs- und Innovationsförderung im Bereich der zivilen Sicherheit im Rahmen von Horizont Europa gekürzt werden. Die Kommission wird auch ihre Bemühungen um die Verbreitung der Ergebnisse einschlägiger von der Union finanzierter Forschungsprojekte intensivieren.

19. Die NIS-Kooperationsgruppe wird ersucht, in Zusammenarbeit mit der Kommission und dem Hohen Vertreter im Einklang mit ihren jeweiligen Aufgaben und Zuständigkeiten nach dem Unionsrecht die Zusammenarbeit mit den einschlägigen Netzen und zivilen und militärischen Gremien bei der Durchführung von Risikobewertungen und der Erstellung von Cybersicherheitsrisikoszenarien zu intensivieren, wobei der Schwerpunkt zunächst auf der Energie-, Kommunikations-, Verkehrs- und Weltrauminfrastruktur und den Interdependenzen zwischen Sektoren und Mitgliedstaaten liegen sollte. Dabei sollten die damit verbundenen Risiken für die physische Infrastruktur, auf die diese Sektoren angewiesen sind, berücksichtigt werden. Die Risikobewertungen und -szenarien sollten regelmäßig durchgeführt werden und bestehende oder geplante Risikobewertungen in diesen Sektoren ergänzen, darauf aufbauen und Überschneidungen vermeiden; sie sollten zudem als Grundlage für Diskussionen darüber dienen, wie die Gesamtresilienz von Einrichtungen, die kritische Infrastrukturen betreiben, gestärkt werden kann und Schwachstellen beseitigt werden können.

20. Die Kommission wird ihre Tätigkeiten zur Unterstützung der Abwehrbereitschaft der Mitgliedstaaten und der Reaktion auf große Cybersicherheitsvorfälle beschleunigen; insbesondere wird sie

a) ergänzend zu einschlägigen Risikobewertungen im Zusammenhang mit der Netz- und Informationssicherheit eine umfassende Studie durchführen, in der eine Bestandsaufnahme der Unterseekabelinfrastruktur vorgenommen wird, die die Mitgliedstaaten verbindet und Europa weltweit anbindet, einschließlich einer Kartierung, Kapazitäten und Redundanzen, Schwachstellen, Risiken für die Verfügbarkeit von Diensten und Risikominderung. Die Ergebnisse sollten den Mitgliedstaaten mitgeteilt werden;

b) die Abwehrbereitschaft der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU (EUIBA) bei großen Cybersicherheitsvorfällen unterstützen.

21. Die Kommission wird die Arbeit an zukunftsorientierten vorausschauenden Maßnahmen, auch im Rahmen des Katastrophenschutzverfahrens der Union (UCPM), in Zusammenarbeit mit den Mitgliedstaaten nach den Artikeln 6 und 10 des

Beschlusses 1313/2013/EU und in Form einer Notfallplanung intensivieren, um die Einsatzbereitschaft des Zentrums für die Koordination von Notfallmaßnahmen zu unterstützen.

Insbesondere wird die Kommission

a) im Zentrum für die Koordination von Notfallmaßnahmen weiter an der Antizipation und sektorübergreifenden Präventions-, Vorsorge- und Reaktionsplanung arbeiten, um Störungen bei der Erbringung wesentlicher Dienste durch Einrichtungen, die kritische Infrastrukturen betreiben, zu antizipieren und sich darauf vorzubereiten;

b) die Investitionen in präventive Ansätze und Vorkehrungen für die Bevölkerung im Falle solcher Störungen erhöhen, wobei ein besonderer Schwerpunkt auf chemischen, biologischen, radiologischen und nuklearen explosiven Stoffen oder anderen vom Menschen verursachten Bedrohungen liegt;

c) den Austausch von einschlägigem Wissen und bewährten Verfahren verstärken und die Konzeption und Durchführung von Maßnahmen zum Aufbau von Kapazitäten – so etwa Schulungen und Übungen mit den Einrichtungen, die kritische Infrastrukturen betreiben – durch bestehende Strukturen und Expertise, beispielsweise das EU-Wissensnetz für Katastrophenschutz, verbessern.

22. Die Kommission wird die Nutzung der EU-Überwachungsmittel (Copernicus und Galileo) fördern, um die Mitgliedstaaten bei der Überwachung kritischer Infrastrukturen und gegebenenfalls ihrer unmittelbaren Umgebung zu unterstützen und andere im Weltraumprogramm der Union vorgesehene Überwachungsoptionen zu unterstützen.

23. Gegebenenfalls werden die Agenturen der Union und andere einschlägige Stellen ersucht, im Einklang mit ihren jeweiligen Mandaten Unterstützung in Fragen betreffend die Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, zu leisten; dies betrifft insbesondere:

a) Europol im Zusammenhang mit der Sammlung von Informationen, der kriminalpolizeilichen Analyse und der Unterstützung von Ermittlungen bei grenzüberschreitenden Strafverfolgungsmaßnahmen;

b) EMSA im Zusammenhang mit der maritimen Sicherheit und Gefahrenabwehr in der Union, einschließlich Seeverkehrsüberwachungsdiensten zur maritimen Sicherheit und Gefahrenabwehr;

c) EUSPA in Bezug auf Tätigkeiten im Rahmen des Weltraumprogramms der Union;

d) ENISA in Bezug auf Tätigkeiten betreffend die Cybersicherheit.

KAPITEL III: VERSTÄRKTE REAKTION

Maßnahmen auf Ebene der Mitgliedstaaten

24. Die Mitgliedstaaten sollten

a) ihre Reaktion abstimmen und den Überblick über die sektorübergreifende Reaktion auf erhebliche Störungen der Erbringung wesentlicher Dienste durch Einrichtungen, die kritische Infrastrukturen betreiben, bewahren, und zwar im Rahmen des Krisenmechanismus (IPCR) des Rates, wenn es um kritische Infrastrukturen mit grenzüberschreitender Bedeutung geht, des Konzeptentwurfs zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen

Ausmaßes oder im Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen im Falle einer hybriden Kampagne;

b) den Informationsaustausch im Rahmen des Katastrophenschutzverfahrens der Union intensivieren, um die Frühwarnung zu verbessern und ihre Reaktion im Rahmen des Verfahrens bei solchen erheblichen Störungen zu koordinieren und so bei Bedarf eine schnellere unionsgestützte Reaktion zu gewährleisten;

c) ihre Bereitschaft erhöhen, im Rahmen des Katastrophenschutzverfahrens der Union auf solche erheblichen Störungen zu reagieren, insbesondere, wenn sie voraussichtlich erhebliche grenzüberschreitende oder sogar gesamteuropäische sowie sektorübergreifende Auswirkungen haben werden;

d) mit der Kommission beim Ausbau der einschlägigen Reaktionskapazitäten im Europäischen Katastrophenschutz-Pool (ECPP) und in rescEU zusammenarbeiten;

e) die Einrichtungen, die kritische Infrastrukturen betreiben, und die zuständigen nationalen Behörden auffordern, die Kapazitäten dieser Einrichtungen aufzustocken, um bei der Erbringung wesentlicher Dienste rasch eine Grundversorgung wiederherzustellen;

f) sicherstellen, dass – sollte der Wiederaufbau kritischer Infrastruktur erforderlich sein – eine solche wiederaufgebaute Infrastruktur allen erdenklichen erheblichen Risiken standhält, und zwar auch in ungünstigen Klimaszenarien.

25. Die Mitgliedstaaten werden aufgefordert, die Vorbereitungsarbeiten für die Umsetzung und Anwendung der NIS-2-Richtlinie zu beschleunigen, indem sie unverzüglich beginnen, die Kapazitäten der nationalen Reaktionsteams für Computersicherheitsverletzungen (Computer Security Incident Response Teams – CSIRT) angesichts der neuen Aufgaben der CSIRT und der größeren Zahl von Einrichtungen aus neuen Sektoren aufzustocken und dabei ihre Cybersicherheitsstrategien rasch zu aktualisieren und schnellstmöglich nationale Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen anzunehmen.

Maßnahmen auf Unionsebene

26. Die Reaktion auf erhebliche Störungen der Erbringung wesentlicher Dienste durch Einrichtungen, die kritische Infrastrukturen betreiben, sollte in Bezug auf die Resilienz dieser Einrichtungen und die Reaktionen auf solche Störungen, die zum Funktionieren des Krisenmechanismus des Rates (IPCR) beitragen können, unter den Sachverständigen der Mitgliedstaaten koordiniert werden.

27. Die Kommission wird eng mit den Mitgliedstaaten zusammenarbeiten, um einsatzfähige Notfallabwehrkapazitäten, einschließlich Sachverständige und rescEU-Bestände im Rahmen des Katastrophenschutzverfahrens der Union, auszubauen und so die Einsatzbereitschaft zur Bewältigung der unmittelbaren und indirekten Auswirkungen erheblicher Störungen der Erbringung wesentlicher Dienste durch Einrichtungen, die kritische Infrastrukturen betreiben, zu verbessern.

28. Unter Berücksichtigung der sich wandelnden Risikolandschaft und in Zusammenarbeit mit den Mitgliedstaaten wird die Kommission im Rahmen des Katastrophenschutzverfahrens der Union

a) die Angemessenheit und Einsatzbereitschaft bestehender Reaktionskapazitäten kontinuierlich analysieren und testen;

b) den potenziellen Bedarf an einer Entwicklung neuer Reaktionskapazitäten auf EU-Ebene durch rescEU regelmäßig überprüfen;

c) die sektorübergreifende Zusammenarbeit weiter intensivieren, um eine angemessene Reaktion auf EU-Ebene zu gewährleisten, und regelmäßige Übungen organisieren, um diese Zusammenarbeit zu testen;

d) das Zentrum für die Koordination von Notfallmaßnahmen (ERCC) als sektorübergreifendes Krisenzentrum auf EU-Ebene für die Koordinierung der Unterstützung der betroffenen Mitgliedstaaten ausbauen.

29. Die Kommission wird in Zusammenarbeit mit dem Hohen Vertreter und in enger Abstimmung mit den Mitgliedstaaten sowie mit der Unterstützung der einschlägigen Agenturen der Union ein Konzeptpapier zu Vorfällen und Krisen bei kritischer Infrastruktur ausarbeiten, in dem die Ziele und Formen der Zusammenarbeit zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU bei der Reaktion auf Anschläge auf kritische Infrastruktur beschrieben und festgelegt werden, insbesondere wenn diese erhebliche Störungen bei der Bereitstellung von für den Binnenmarkt wesentlichen Diensten verursachen. In diesem Konzept sollte auf die bestehende Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) für die Koordinierung der Reaktion zurückgegriffen werden.

30. Die Kommission wird mit Interessenträgern und Sachverständigen an Plänen für mögliche Wiederherstellungsmaßnahmen nach Sicherheitsvorfällen in Bezug auf die Infrastruktur für Unterseekabel arbeiten, die in Verbindung mit der unter Nummer 20 Buchstabe a genannten Bestandsaufnahme vorzulegen sind, und die Notfallplanung und Risikoszenarien weiter ausarbeiten sowie die Arbeit zur Katastrophenresilienz der Union im Rahmen des Katastrophenschutzverfahrens der Union fortsetzen.

KAPITEL IV INTERNATIONALE ZUSAMMENARBEIT

31. Die Kommission und der Hohe Vertreter werden gegebenenfalls und im Einklang mit ihren jeweiligen Aufgaben und Zuständigkeiten nach dem Unionsrecht Partnerländer dabei unterstützen, die Resilienz von Einrichtungen, die in ihrem Hoheitsgebiet kritische Infrastrukturen betreiben, zu verbessern.

32. Die Kommission und der Hohe Vertreter werden im Einklang mit ihren jeweiligen Aufgaben und Zuständigkeiten nach dem Unionsrecht die Koordinierung mit der NATO in Bezug auf die Resilienz kritischer Infrastrukturen im Rahmen des strukturierten Dialogs zwischen der EU und der NATO über Resilienz verstärken und zu diesem Zweck eine Taskforce einsetzen.

33. Die Mitgliedstaaten werden ersucht, in Zusammenarbeit mit der Kommission und dem Hohen Vertreter zur beschleunigten Entwicklung und Umsetzung des Instrumentariums zur Abwehr hybrider Bedrohungen der EU und der Durchführungsleitlinien, auf die in den Schlussfolgerungen des Rates über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen[25] Bezug genommen wird, beizutragen und diese anschließend zu nutzen, um dem Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen insbesondere bei der

[25] Schlussfolgerungen des Rates über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen – Consilium (europa.eu)

Prüfung und Vorbereitung umfassender und koordinierter Reaktionen der EU auf hybride Kampagnen und hybride Bedrohungen, die unter anderem auf Einrichtungen abzielen, die kritische Infrastrukturen betreiben, volle Wirkung zu verleihen.

34. Die Kommission wird die Teilnahme von Vertretern von Drittländern – soweit angezeigt und angemessen – im Rahmen der Zusammenarbeit und des Informationsaustauschs zwischen Sachverständigen der Mitgliedstaaten im Bereich der Resilienz von Einrichtungen, die kritische Infrastrukturen betreiben, in Erwägung ziehen.

[…]

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident /// Die Präsidentin