Rat der
Europäischen Union

Brüssel, den 9. Dezember 2022
(OR. en)

15623/22

Interinstitutionelles Dossier:
2022/0338(NLE)

PROCIV 149	**ATO 102**
ENV 1248	**CSC 561**
JAI 1617	**ECOFIN 1279**
SAN 650	**CSCI 189**
COSI 315	**DATAPROTECT 346**
CHIMIE 100	**MI 912**
ENFOPOL 619	**CODEC 1916**
RECH 645	**COPS 581**
CT 220	**JAIEX 103**
DENLEG 93	**COPEN 430**
COTER 297	**IND 533**
RELEX 1657	**POLMIL 297**
ENER 654	**IPCR 116**
HYBRID 116	**DIGIT 231**
TRANS 768	**DISINFO 102**
CYBER 397	**CSDP/PSDC 848**
TELECOM 512	**MARE 71**
ESPACE 125	**POLMAR 78**

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	13713/22, 15454/22
Betr.:	EMPFEHLUNG DES RATES für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur

Die Delegationen erhalten in der Anlage die Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur, die vom Rat auf seiner 3920. Tagung vom 8. Dezember 2022 angenommen worden ist.

ANLAGE

EMPFEHLUNG (EU) 2022/… DES RATES

vom [...]

für eine unionsweite koordinierte Vorgehensweise 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 Artikel 114 und Artikel 292 Sätze 1 und 2

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Es liegt im Interesse aller Mitgliedstaaten und der Union als Ganzes, relevante kritische Infrastrukturen, die wesentliche Dienste im Binnenmarkt erbringen, insbesondere in Schlüsselsektoren wie Energie, digitale Infrastruktur, Verkehr und Raumfahrt, sowie kritische Infrastrukturen von erheblicher grenzüberschreitender Bedeutung[1], deren Störung sich erheblich auf andere Mitgliedstaaten auswirken könnte, eindeutig zu ermitteln und zu schützen, um das Funktionieren des Binnenmarkts zu gewährleisten.

[1] Die Mitgliedstaaten sollten diese Relevanz im Einklang mit ihren nationalen Verfahren bewerten und können dies unter anderem auf der Grundlage der Risikobewertung, der Auswirkungen des Ereignisses oder der Art des Ereignisses tun.

(2) Diese Empfehlung, bei der es sich um ein nicht verbindliches Instrument handelt, zeigt den politischen Willen der Mitgliedstaaten zur Zusammenarbeit und ihr Engagement für die empfohlenen Maßnahmen, die in einem Fünf-Punkte-Plan der Präsidentin der Europäischen Kommission hervorgehoben werden, wobei die Zuständigkeiten der Mitgliedstaaten uneingeschränkt geachtet werden. Diese Empfehlung berührt nicht den Schutz der wesentlichen Interessen der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung der Mitgliedstaaten, und von keinem Mitgliedstaat sollte erwartet werden, dass er Informationen weitergibt, die diesen Interessen schaden.

(3) Während die Hauptverantwortung für die Gewährleistung der Sicherheit kritischer Infrastrukturen und die Erbringung wesentlicher Dienste durch kritische Infrastrukturen weiter bei den Mitgliedstaaten und ihren Betreibern kritischer Infrastrukturen liegt, ist eine stärkere Koordinierung auf Unionsebene angezeigt, insbesondere im Lichte sich weiterentwickelnder Bedrohungen, die möglicherweise mehrere Mitgliedstaaten gleichzeitig betreffen, wie etwa Russlands Angriffskrieg gegen die Ukraine und hybride Kampagnen gegen Mitgliedstaaten, oder die die Resilienz und das Funktionieren der Wirtschaft der Union, des Binnenmarkts und der Gesellschaft als Ganzes beeinträchtigen können. Besonderes Augenmerk sollte auf kritische Infrastrukturen außerhalb des Hoheitsgebiets der Mitgliedstaaten gelegt werden, wie z. B. kritische Untersee-Infrastrukturen oder Offshore-Energieinfrastrukturen.

(4) Der Europäische Rat hat in seinen Schlussfolgerungen vom 20. und 21. Oktober 2022 die Sabotage kritischer Infrastruktur, etwa der Nord-Stream-Pipelines, nachdrücklich verurteilt und erklärt, dass die Union jeder vorsätzlichen Beschädigung kritischer Infrastruktur oder anderen hybriden Handlungen gemeinsam und entschlossen begegnen wird.

(5) Angesichts der sich rasch wandelnden Bedrohungslandschaft sollten in Schlüsselsektoren wie beispielsweise Energie, digitale Infrastruktur, Verkehr und Raumfahrt und in anderen von den Mitgliedstaaten ermittelten relevanten Sektoren vorrangig Maßnahmen zur Stärkung der Resilienz ergriffen werden. Diese Maßnahmen sollten sich auf die Stärkung der Resilienz kritischer Infrastrukturen konzentrieren, wobei die einschlägigen Risiken, insbesondere Kaskadeneffekte, Unterbrechungen der Lieferkette, Abhängigkeit, Auswirkungen des Klimawandels, unzuverlässige Anbieter und Partner sowie hybride Bedrohungen und Kampagnen, einschließlich ausländischer Informationsmanipulation und -einmischung, zu berücksichtigen sind. In Bezug auf nationale kritische Infrastrukturen sollten kritische Infrastrukturen mit großer grenzüberschreitender Bedeutung in Anbetracht der möglichen Folgen Vorrang erhalten. Die Mitgliedstaaten werden dazu angehalten, erforderlichenfalls dringend solche Maßnahmen zur Stärkung der Resilienz zu ergreifen und dabei den Ansatz beizubehalten, der in dem sich weiterentwickelnden Rechtsrahmen dargelegt ist.

(6) Der Schutz kritischer europäischer Infrastrukturen im Energie- und Verkehrssektor wird derzeit durch die Richtlinie 2008/114/EG des Rates[2] geregelt, und die auf Cyberbedrohungen ausgerichtete Sicherheit von Netz- und Informationssystemen in der gesamten Union wird durch die Richtlinie 2016/1148 des Europäischen Parlaments und des Rates[3] gewährleistet. Um ein höheres gemeinsames Niveau der Resilienz und des Schutzes kritischer Infrastrukturen, der Cybersicherheit und des Finanzmarkts zu gewährleisten, wird der bestehende Rechtsrahmen geändert und ergänzt, indem neue Vorschriften für kritische Einrichtungen („CER-Richtlinie"), strengere Vorschriften für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union („NIS-2-Richtlinie") und neue Vorschriften über die Betriebsstabilität digitaler Systeme des Finanzsektors („DORA") erlassen werden.

(7) Die Mitgliedstaaten sollten im Einklang mit dem Unionsrecht und dem nationalen Recht alle verfügbaren Instrumente nutzen, um Fortschritte zu erzielen und einen Beitrag zur Stärkung der physischen Resilienz und Cyberresilienz zu leisten. In diesem Zusammenhang sollten „kritische Infrastrukturen" relevante kritische Infrastrukturen, die von einem Mitgliedstaat auf nationaler Ebene ermittelt oder gemäß der Richtlinie 2008/114/EG als europäische kritische Infrastrukturen ausgewiesen wurden, wie auch kritische Einrichtungen, die gemäß der CER-Richtlinie zu ermitteln sind, oder gegebenenfalls Einrichtungen gemäß der NIS-2-Richtlinie umfassen. Der Ausdruck „Resilienz" sollte verstanden werden als die Fähigkeit einer kritischen Infrastruktur, Ereignisse, die die Erbringung wesentlicher Dienste im Binnenmarkt erheblich stören oder erheblich stören könnten, d. h. Dienste, die für die Aufrechterhaltung wichtiger gesellschaftlicher und wirtschaftlicher Funktionen, der öffentlichen Sicherheit und Gesundheit oder für die Umwelt von entscheidender Bedeutung sind, zu verhindern, sich davor zu schützen, darauf zu reagieren, sie abzuwehren, ihre Folgen zu begrenzen, sie aufzufangen, sie zu bewältigen oder sich von ihnen zu erholen.

---

2 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).

3 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).

(8) Nationale Experten sollten zusammengebracht werden, um die Arbeit an der Erreichung eines höheren gemeinsamen Maßes an Resilienz und Schutz kritischer Infrastrukturen zu koordinieren, das durch die neuen Vorschriften für kritische Einrichtungen eingeführt werden soll. Dieses koordinierte Arbeiten würde eine Zusammenarbeit zwischen den Mitgliedstaaten und die gemeinsame Nutzung von Informationen über Tätigkeiten wie die Ausarbeitung von Methoden zur Ermittlung wesentlicher Dienste, die von kritischen Infrastrukturen erbracht werden, ermöglichen. Die Kommission hat bereits begonnen, diese Experten zusammenzubringen und ihre Arbeit zu unterstützen, und sie beabsichtigt, weiter auf diese Weise vorzugehen. Sobald die CER-Richtlinie in Kraft getreten und eine Gruppe für die Resilienz kritischer Einrichtungen im Rahmen dieser Richtlinie eingerichtet ist, sollte die Gruppe diese Vorarbeit im Rahmen ihrer Aufgaben fortsetzen.

(9) Angesichts der veränderten Bedrohungslage sollte das Potenzial zur Durchführung von Stresstests für kritische Infrastrukturen auf nationaler Ebene weiterentwickelt werden, da diese Tests für die Stärkung der Resilienz kritischer Infrastrukturen nützlich sein könnten. Im Hinblick auf die besondere Bedeutung des Energiesektors und die unionsweiten Folgen einer möglichen Störung könnte dieser Sektor am meisten von der Durchführung von Stresstests auf der Grundlage gemeinsam vereinbarter Grundsätze profitieren. Diese Tests fallen in die Zuständigkeit der Mitgliedstaaten, die die Betreiber kritischer Infrastrukturen ermutigen und unterstützen sollten, diese Tests durchzuführen, sofern dies als vorteilhaft bewertet wird und im Einklang mit ihrem nationalen Rechtsrahmen steht.

(10) Um eine koordinierte und wirksame Reaktion auf aktuelle und zu erwartende Bedrohungen zu gewährleisten, wird die Kommission dazu angehalten, die Mitgliedstaaten zusätzlich zu unterstützen, indem sie ihnen insbesondere mit Briefings, nicht verbindlichen Handbüchern und Leitlinien einschlägige Informationen liefert. Der Europäische Auswärtige Dienst (EAD) sollte insbesondere über sein EU-Zentrum für Informationsgewinnung und Lageerfassung und dessen Analyseeinheit für hybride Bedrohungen – mit Unterstützung der Abteilung „Aufklärung“ des Militärstabs der Europäischen Union (EUMS) im Rahmen des Einheitlichen Analyseverfahrens (SIAC) – Bedrohungsanalysen erstellen. Die Kommission wird ferner ersucht, in Zusammenarbeit mit den Mitgliedstaaten die Übernahme von von der Union finanzierten Forschungs- und Innovationsprojekten zu fördern.

(11) Angesichts der zunehmenden wechselseitigen Abhängigkeiten zwischen physischer und digitaler Infrastruktur ist es möglich, dass auf kritische Bereiche gerichtete böswillige Cyberaktivitäten zu Störungen oder Schäden an physischer Infrastruktur führen, oder dass die Sabotage physischer Infrastruktur digitale Dienste unzugänglich macht. Die Mitgliedstaaten werden ersucht, die Vorbereitungsarbeiten für die Umsetzung in Rechtsvorschriften und die Anwendung des neuen Rechtsrahmens für kritische Einrichtungen und des gestärkten Rechtsrahmens für die Cybersicherheit zu beschleunigen und dabei so bald wie möglich auf den Erfahrungen der mit der Richtlinie (EU) 2016/1148 eingerichteten Kooperationsgruppe („NIS-Kooperationsgruppe“) aufzubauen, wobei die Fristen für die Umsetzung in Rechtsvorschriften zu berücksichtigen sind, und diese Vorbereitungsarbeiten parallel und kohärent voranschreiten sollten.

(12) Neben der Verbesserung der Abwehrbereitschaft ist es auch wichtig, die Kapazitäten für eine rasche und wirksame Reaktion auf die Unterbrechung der Erbringung wesentlicher Dienste durch kritische Infrastrukturen zu stärken. Daher enthält diese Empfehlung Maßnahmen auf Unionsebene und auf nationaler Ebene, einschließlich durch Betonung der Unterstützungsrolle und des Mehrwerts, der dadurch erreicht werden kann, dass eine stärkere Zusammenarbeit und ein intensiverer Informationsaustausch im Rahmen des mit dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates[4] eingerichteten Katastrophenschutzverfahrens der Union (UCPM) eingeführt werden und dass die einschlägigen Instrumente des im Rahmen der Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates[5] eingerichteten Weltraumprogramms der Union eingesetzt werden.

(13) Die Kommission, der Hohe Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) und die NIS-Kooperationsgruppe sollen in Zusammenarbeit mit einschlägigen zivilen und militärischen Stellen und Einrichtungen und den etablierten Netzwerken, darunter das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), eine Risikobewertung durchführen und Risikoszenarien erstellen. Nach dem gemeinsamen Ministeraufruf von Nevers wird derzeit eine Risikobewertung von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie in Zusammenarbeit mit dem Gremium europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt. Diese beiden Arbeitsstränge werden aufeinander abgestimmt sein und auch mit der Erstellung von Szenarien im Rahmen des UCPM koordiniert werden, einschließlich Cybersicherheitsvorfällen und deren reale Auswirkungen, wie derzeit von der Kommission und den Mitgliedstaaten entwickelt. Aus Gründen der Effizienz, Wirksamkeit und Kohärenz und im Hinblick auf die gute Anwendung dieser Empfehlung sollten sich die Ergebnisse dieser Arbeiten auf nationaler Ebene widerspiegeln.

---

4 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).

5 Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm und zur Aufhebung der Verordnungen (EU) Nr. 912/2010, (EU) Nr. 1285/2013 und (EU) Nr. 377/2014 sowie des Beschlusses Nr. 541/2014/EU (ABl. L 170 vom 12.5.2021, S. 69).

(14) Um die Abwehrbereitschaft und Reaktionsfähigkeit bei großen Cybersicherheitsvorfällen umgehend zu stärken, hat die Kommission ein kurzfristiges Unterstützungsprogramm für die Mitgliedstaaten eingerichtet und ENISA zusätzliche Mittel zugewiesen. Zu den vorgeschlagenen Unterstützungsdiensten gehören unter anderem Vorsorgemaßnahmen wie Penetrationstests von Einrichtungen zur Ermittlung von Schwachstellen. Außerdem können im Programm zusätzliche Möglichkeiten vorgesehen werden, um Mitgliedstaaten im Falle eines großen Sicherheitsvorfalls bei einer kritischen Einrichtung zu unterstützen. Dies ist ein erster Schritt gemäß den Schlussfolgerungen des Rates vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union („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 und werden ermutigt, die Arbeit im Bereich des Cyberkrisenmanagements der Union fortzusetzen, insbesondere durch regelmäßige Überwachung und Bestandsaufnahme der Fortschritte bei der Umsetzung des kürzlich im Rat entwickelten Fahrplans für das Cyberkrisenmanagement. Dieser Fahrplan ist ein dynamisches Dokument und sollte bei Bedarf überprüft und aktualisiert werden.

(15) Die weltweiten Unterseekommunikationskabel sind für die globale und innereuropäische Konnektivität von entscheidender Bedeutung. Wegen der erheblichen Länge dieser 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 spezifische Herausforderung dar. Die Risikobewertungen, die für digitale und physische Infrastruktur, die digitalen Diensten zugrunde liegt, derzeit laufen und noch geplant sind, müssen daher durch spezifische, auf Unterseekommunikationskabel abzielende Risikobewertungen und Optionen für Risikominderungsmaßnahmen ergänzt werden. Die Mitgliedstaaten ersuchen die Kommission, zu diesem Zweck Studien durchzuführen und die Mitgliedstaaten über ihre Ergebnisse zu informieren.

(16) Die Bereiche Energie und Verkehr können auch Bedrohungen im Zusammenhang mit digitaler Infrastruktur ausgesetzt sein, beispielsweise im Zusammenhang mit Energietechnologien, die digitale Komponenten beinhalten. Für die Aufrechterhaltung der Erbringung wesentlicher Dienste und für die strategische Kontrolle der kritischen Infrastrukturen im Energiesektor ist auch die Sicherheit der einschlägigen Lieferketten von Belang. Diesen Umständen sollte Rechnung getragen werden, wenn zur Stärkung der Resilienz von kritischen Infrastrukturen gemäß dieser Empfehlung Maßnahmen ergriffen werden.

(17) Die zunehmende Bedeutung von Weltrauminfrastrukturen, weltraumbezogener Bodenbetriebsmittel einschließlich Produktionsstätten und weltraumgestützter Dienste für sicherheitsbezogene Maßnahmen macht es unerlässlich, die Resilienz und den Schutz des Weltraums der Union und seiner bodengestützten Betriebsmittel und Dienste in der Union zu gewährleisten. Aus denselben Gründen ist es auch von wesentlicher Bedeutung, im Rahmen dieser Empfehlung weltraumgestützte Daten und Dienste, die von Weltraumsystemen und programmen für die Beobachtung und Verfolgung und für 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.

(18) Um Risiken für kritische Infrastrukturen unter anderem in internationalen Gewässern wirksam anzugehen, ist auch Zusammenarbeit auf internationaler Ebene erforderlich. Daher sind die Mitgliedstaaten aufgefordert, mit der Kommission und dem Hohen Vertreter zusammenzuarbeiten, um auf dem Weg zur Verwirklichung dieser Zusammenarbeit bestimmte Schritte zu unternehmen, wobei solche Schritte nur im Einklang mit ihren im Unionsrecht und insbesondere in den Bestimmungen der Verträge zu den Außenbeziehungen festgelegten Aufgaben und Zuständigkeiten unternommen werden dürfen.

(19) Wie in der Mitteilung der Kommission vom 15. Februar 2022 mit dem Titel „Beitrag der Kommission zur europäischen Verteidigung“ 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“ 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.

(20) In der Strategie der Europäischen Union für maritime Sicherheit aus dem Jahr 2014 und dem zugehörigen überarbeiteten 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. Diese Strategie und dieser Aktionsplan werden derzeit aktualisiert und um verstärkte Maßnahmen zum Schutz kritischer maritimer Infrastruktur erweitert. Diese Maßnahmen sollten die vorliegende Empfehlung ergänzen.

(21) Die Stärkung der Resilienz kritischer Infrastrukturen trägt zu umfassenderen Bemühungen um die Abwehr hybrider Bedrohungen und Kampagnen gegen die Union und ihre Mitgliedstaaten bei. Diese Empfehlung baut auf der Gemeinsamen Mitteilung an das Europäische Parlament und den Rat mit dem Titel „Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union“ auf. Maßnahme 1 des Gemeinsamen Rahmens, nämlich die Untersuchung über hybride Risiken, spielt eine Schlüsselrolle bei der Ermittlung von Schwachstellen, von denen die nationalen und gesamteuropäischen Strukturen und Netze betroffen sein könnten. Darüber hinaus wird die Umsetzung der Schlussfolgerungen des Rates vom 21. Juni 2022 über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen ein stärkeres koordiniertes Vorgehen durch die Anwendung des EU-Instrumentariums zur Abwehr hybrider Bedrohungen in allen betroffenen Bereichen ermöglichen —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

KAPITEL I: ZIEL, ANWENDUNGSBEREICH UND PRIORITÄTEN

1. Diese Empfehlung enthält eine Reihe gezielter Maßnahmen auf Unionsebene und auf nationaler Ebene, um die Resilienz kritischer Infrastrukturen auf freiwilliger Basis zu fördern und zu verbessern, wobei der Schwerpunkt auf kritischen Infrastrukturen von erheblicher grenzüberschreitender Bedeutung und in bestimmten Schlüsselsektoren wie Energie, digitale Infrastruktur, Verkehr und Weltraum liegt. Bei diesen gezielten Maßnahmen geht es um bessere Abwehrbereitschaft, verstärkte Reaktion und internationale Zusammenarbeit.

2. Informationen, die gemeinsam genutzt werden, um die Ziele dieser Empfehlung zu erreichen, und die gemäß den Vorschriften der Union und der Mitgliedstaaten sowie den Vorschriften über Betriebsgeheimnisse vertraulich sind, sollten mit der Kommission und anderen einschlägigen Stellen nur ausgetauscht werden, wenn dieser Austausch für die gute Anwendung dieser Empfehlung erforderlich ist. Diese Empfehlung berührt nicht den Schutz der wesentlichen Interessen der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung der Mitgliedstaaten, und von keinem Mitgliedstaat sollte erwartet werden, dass er Informationen weitergibt, die diesen Interessen zuwiderlaufen.

KAPITEL II: BESSERE ABWEHRBEREITSCHAFT

Maßnahmen auf Ebene der Mitgliedstaaten

3. Die Mitgliedstaaten sollten bei der Aktualisierung ihrer Risikobewertungen oder ihrer bestehenden gleichwertigen Analysen im Einklang mit der sich wandelnden Art der derzeitigen Bedrohungen für ihre kritischen Infrastrukturen, insbesondere in bestimmten Schlüsselsektoren und – soweit möglich – in allen Sektoren, die unter den künftigen neuen Rechtsrahmen für kritische Einrichtungen fallen, einen gefahrenübergreifenden Ansatz in Erwägung ziehen.

4. Die Mitgliedstaaten werden ersucht, nach Möglichkeit die Vorbereitungsarbeiten zu beschleunigen und Maßnahmen zur Stärkung der Resilienz zu ergreifen, wie es der künftige Rechtsrahmen für kritische Einrichtungen vorschreibt, wobei ein besonderer Schwerpunkt auf der Zusammenarbeit und dem Austausch einschlägiger Informationen zwischen den Mitgliedstaaten und mit der Kommission, auf der Ermittlung kritischer Einrichtungen von erheblicher grenzüberschreitender Bedeutung und auf der Verstärkung der Unterstützung ermittelter kritischer Einrichtungen zur Verbesserung ihrer Resilienz liegen soll.

5. Die Mitgliedstaaten sollten die Ausbildung von Experten und Übungen sowie den Austausch bewährter Verfahren und gewonnener Erkenntnisse zwischen Experten unterstützen Die Mitgliedstaaten sollten Experten dazu anhalten, sich an bestehenden nationalen und internationalen Ausbildungsplattformen, beispielsweise im Rahmen des UCPM, zu beteiligen.

6. Die Mitgliedstaaten sollten die Betreiber kritischer Infrastrukturen zumindest im Energiesektor dazu anhalten und dabei unterstützen, Stresstests nach den auf Unionsebene gemeinsam vereinbarten Grundsätzen durchzuführen, sofern dies nutzbringend ist. Im Rahmen von Stresstests sollte die Resilienz kritischer Infrastrukturen gegen vom Menschen verursachte feindliche Bedrohungen bewertet werden. Daher sollten die Mitgliedstaaten darauf abzielen, relevante kritische Infrastrukturen zu ermitteln, die getestet werden sollen, und die Betreiber der relevanten kritischen Infrastrukturen so bald wie möglich, spätestens jedoch bis zum Ende des ersten Quartals 2023, konsultieren. Darüber hinaus sollten die Mitgliedstaaten die Betreiber kritischer Infrastrukturen dabei unterstützen, diese Tests im Einklang mit dem nationalen Recht so bald wie möglich durchzuführen, und bestrebt sein, sie bis Ende 2023 abzuschließen. Der Rat beabsichtigt, den Stand der Stresstests bis Ende April 2023 zu bewerten.

7. Angesichts der sich rasch wandelnden Bedrohungen für kritische Infrastrukturen ist die Aufrechterhaltung des hohen Schutzniveaus für diese Infrastrukturen von entscheidender Bedeutung. Die Mitgliedstaaten werden aufgefordert, ausreichende Finanzmittel bereitzustellen, um die Kapazitäten ihrer zuständigen nationalen Behörden zu stärken, und sie zu unterstützen, damit sie die Resilienz kritischer Infrastrukturen verbessern können. Die Mitgliedstaaten werden zudem ermutigt, den für die Bewältigung großer Cybersicherheitsvorfälle zuständigen Behörden ausreichende Finanzmittel zuzuweisen, um sie zu unterstützen, und sicherzustellen, dass ihre Reaktionsteams für Computersicherheitsverletzungen (CSIRTs) und die zuständigen Behörden in vollem Umfang im CSIRTs-Netz bzw. im EU-CyCLONe mobilisiert werden.

8. Die Mitgliedstaaten werden aufgefordert, im Einklang mit den geltenden Anforderungen potenzielle Finanzierungsmöglichkeiten auf Unionsebene und auf nationaler Ebene zu nutzen, um die Resilienz kritischer Infrastrukturen in der Union für sich selbst zu verbessern, und überdies die Betreiber kritischer Infrastrukturen dazu anzuhalten, diese Finanzierungsmöglichkeiten, einschließlich beispielsweise transeuropäischer Netze, für die Bewältigung des gesamten Spektrums erheblicher Bedrohungen zu nutzen, insbesondere im Rahmen der Programme die aus dem mit der Verordnung (EU) 2021/1149 des Europäischen Parlaments und des Rates[6] eingerichteten Fonds für die innere Sicherheit, aus dem mit der Verordnung (EU) Nr. 1301/2013 des Europäischen Parlaments und des Rates[7] eingerichteten Europäischen Fonds für regionale Entwicklung, aus dem Katastrophenschutzverfahren der Union (UCPM) und aus dem RePowerEU-Plan der Kommission finanziert werden. Die Mitgliedstaaten werden zudem ermutigt, die Ergebnisse einschlägiger Projekte im Rahmen von Forschungsprogrammen, wozu beispielsweise das mit der Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates[8] eingerichtete Programm „Horizont Europa" zählt, bestmöglich zu nutzen.

---

6 Verordnung (EU) 2021/1149 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Einrichtung des Fonds für die innere Sicherheit (ABl. L 251 vom 15.7.2021, S. 94).

7 Verordnung (EU) Nr. 1301/2013 des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über den Europäischen Fonds für regionale Entwicklung und mit besonderen Bestimmungen hinsichtlich des Ziels „Investitionen in Wachstum und Beschäftigung" und zur Aufhebung der Verordnung (EG) Nr. 1080/2006 (ABl. L 347 vom 20.12.2013, S. 289).

8 Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung von „Horizont Europa", dem Rahmenprogramm für Forschung und Innovation, sowie über dessen Regeln für die Beteiligung und die Verbreitung der Ergebnisse und zur Aufhebung der Verordnungen (EU) Nr. 1290/2013 und (EU) Nr. 1291/2013 (ABl. L 170 vom 12.5.2021, S. 1).

9. Im Hinblick auf die Kommunikations- und Netzinfrastruktur in der Union wird die NIS-Kooperationsgruppe ersucht, ihre laufende Arbeit auf der Grundlage des gemeinsamen Ministeraufrufs von Nevers an einer gezielten Risikobewertung zu beschleunigen und so bald wie möglich erste Empfehlungen vorzulegen und dabei gemäß Artikel 11 der Richtlinie (EU) 2016/1148 zu handeln. Diese Risikobewertung sollte Informationen für die laufende sektorübergreifende Cyberrisikobewertung und die Szenarien erbringen, wie sie der Rat in seinen Schlussfolgerungen zur Cyberabwehr der EU gefordert hat. Dabei sollten darüber hinaus Kohärenz und Komplementarität mit der Arbeit der NIS-Kooperationsgruppe zur Sicherheit der Lieferkette der Informations- und Kommunikationstechnologie sowie anderer einschlägiger Gruppen sichergestellt werden.

10. Die NIS-Kooperationsgruppe wird ferner ersucht, mit Unterstützung der Kommission und der ENISA ihre Arbeit hinsichtlich der Sicherheit der digitalen Infrastruktur – darunter auch bezüglich Untersee-Infrastruktur, d. h. Unterseekommunikationskabeln – fortzusetzen. Sie wird zudem ersucht, ihre Arbeit im Weltraumsektor zu beginnen, unter anderem erforderlichenfalls durch die Ausarbeitung politischer Leitlinien sowie Methoden für das Risikomanagement im Bereich der Cybersicherheit auf der Grundlage eines gefahrenübergreifenden Ansatzes und eines risikobasierten Ansatzes 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, beispielsweise Penetrationstests zur Ermittlung von Schwachstellen; sie werden in diesem Zusammenhang ersucht, Einrichtungen, die kritische Infrastrukturen in den Sektoren Energie, digitale Infrastruktur und Verkehr betreiben, Vorrang einzuräumen.

12. Die Mitgliedstaaten sollten das Europäische Kompetenzzentrums für Cybersicherheitsforschung (ECCC) in vollem Umfang nutzen. Die Mitgliedstaaten sollten ihre nationalen Koordinierungszentren dazu anhalten, proaktiv mit den Mitgliedern der Cybersicherheitsgemeinschaft zusammenzuarbeiten, um Kapazitäten auf Unionsebene und auf nationaler Ebene aufzubauen, damit die Betreiber wesentlicher Dienste besser unterstützt werden.

13. Es ist wichtig, dass die Mitgliedstaaten die im EU-Instrumentarium für die 5G-Cybersicherheit empfohlenen Maßnahmen umsetzen, und insbesondere dass die Mitgliedstaaten Beschränkungen für Hochrisikoanbieter erlassen, da ein Zeitverlust die Anfälligkeit der Netze in der Union erhöhen kann, und 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 notwendig sind, um so ein einheitliches Maß an Sicherheit und Resilienz der 5G-Netze zu gewährleisten.

14. Die Mitgliedstaaten sollten sich gemeinsam mit der Kommission und der ENISA auf die Umsetzung der Schlussfolgerungen des Rates vom 17. Oktober 2022 zur Sicherheit der IKT-Lieferketten konzentrieren.

15. Die Mitgliedstaaten sollten dem anstehenden Netzkodex für Aspekte der Cybersicherheit bei grenzüberschreitenden Stromflüssen Rechnung tragen und dabei auf den Erfahrungen bei der Umsetzung der Richtlinie (EU) 2016/1148 und den einschlägigen Leitlinien der NIS-Kooperationsgruppe aufbauen, insbesondere auf ihrem Referenzdokument über Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste.

16. Die Mitgliedstaaten sollten die Nutzung von Copernicus, von Galileo und der Europäischen Erweiterung des geostationären Navigationssystems (EGNOS) für Überwachungszwecke ausbauen, um einschlägige Informationen mit den nach Nummer 15 einberufenen Experten auszutauschen. Die Fähigkeiten, die die staatliche Satellitenkommunikation (GOVSATCOM) der Union im Rahmen des Weltraumprogramms der Union für die Überwachung kritischer Infrastrukturen und die Unterstützung der Krisenvorhersage und -reaktion bietet, sollten sinnvoll genutzt werden.

Maßnahmen auf Unionsebene

17. Der Dialog und die Zusammenarbeit zwischen den benannten Experten der Mitgliedstaaten und mit der Kommission sollten verstärkt werden, um die physische Resilienz kritischer Infrastrukturen zu verbessern; dies soll insbesondere über folgende Maßnahmen erfolgen:

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

b) Unterstützung der Mitgliedstaaten bei der Umsetzung des neuen Rechtsrahmens für kritische Einrichtungen, einschließlich der Ermutigung der Kommission dazu, den delegierten Rechtsakt zeitig anzunehmen;

c) Unterstützung der Durchführung der unter Nummer 6 genannten Stresstests auf der Grundlage gemeinsamer Grundsätze, beginnend mit Tests, bei denen der Schwerpunkt auf vom Menschen verursachten feindlichen Bedrohungen im Energiesektor liegt, und anschließend in anderen Schlüsselsektoren, sowie Unterstützung und Beratung bei der Durchführung solcher Stresstests auf Ersuchen eines Mitgliedstaats;

d) Nutzung einer sicheren Plattform, sobald sie von der Kommission eingerichtet ist, für die Sammlung, Bestandsaufnahme und den Austausch von bewährten Verfahren, Lehren aus nationalen Erfahrungen und anderen Informationen im Zusammenhang mit einer solchen Resilienz auf der Grundlage der Freiwilligkeit.

Bei der Arbeit der betreffenden benannten Experten sollte sektorübergreifenden Abhängigkeiten und kritischen Infrastrukturen von erheblicher grenzüberschreitender Bedeutung besondere Aufmerksamkeit gelten, und sie sollte gegebenenfalls im Rat und von der Kommission weiterverfolgt werden.

18. Die Mitgliedstaaten werden dazu angehalten, jede von der Kommission angebotene Unterstützung, beispielsweise durch die Ausarbeitung von Handbüchern und Leitlinien, wie etwa eines Handbuchs zum Schutz kritischer Infrastruktur und öffentlicher Räume vor unbemannten Luftfahrzeugsystemen, sowie von Instrumenten für Risikobewertungen, in Anspruch zu nehmen. Der EAD wird ersucht, insbesondere über das EU-Zentrum für Informationsgewinnung und Lageerfassung und seine Analyseeinheit für hybride Bedrohungen mit Unterstützung der Abteilung „Aufklärung“ des EUMS innerhalb des SIAC-Rahmens Briefings zu den Bedrohungen für kritische Infrastrukturen in der Union durchzuführen, um das Lagebewusstsein zu verbessern.

19. Die Mitgliedstaaten sollten Maßnahmen unterstützen, die die Kommission im Hinblick auf die Übernahme der Ergebnisse von im Rahmen der Forschungs- und Innovationsprogramme der Union finanzierten Projekten zur Resilienz kritischer Infrastrukturen unternimmt. Der Rat nimmt die Absicht der Kommission zur Kenntnis, innerhalb des Budgets für Horizont Europa im Rahmen des Mehrjährigen Finanzrahmens 2021-2027 die Mittel für diese Resilienz aufzustocken, ohne dass dadurch die Mittel für sonstige Forschungs- und Innovationsprojekte im Bereich der zivilen Sicherheit im Rahmen von Horizont Europa gekürzt werden.

20. Entsprechend den in den Schlussfolgerungen des Rates zur Cyberabwehr der EU festgelegten Aufgaben werden die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe ersucht, im Einklang mit ihren jeweiligen Aufgaben und Zuständigkeiten nach dem Unionsrecht die Zusammenarbeit mit den einschlägigen Netzen und zivilen und militärischen Gremien und Agenturen bei der Durchführung von Risikobewertungen und der Erstellung von Cybersicherheitsrisikoszenarien zu intensivieren und dabei insbesondere die Bedeutung der Energie-, Digital-, Verkehrs- und Weltrauminfrastruktur und der Interdependenzen zwischen Sektoren und Mitgliedstaaten zu berücksichtigen. Dabei sollten die damit verbundenen Risiken für die Infrastruktur, auf die diese Sektoren angewiesen sind, berücksichtigt werden. Die Risikobewertungen und -szenarien könnten, sofern dies nutzbringend ist, regelmäßig durchgeführt werden und bestehende oder geplante Risikobewertungen in diesen Sektoren ergänzen, darauf aufbauen und Überschneidungen mit ihnen 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.

21. Die Kommission wird ersucht, ihre Tätigkeiten im Einklang mit ihren jeweiligen Aufgaben im Rahmen des Cyberkrisenmanagements zur Unterstützung der Abwehrbereitschaft und Reaktion der Mitgliedstaaten auf Cybersicherheitsvorfälle großen Ausmaßes zu beschleunigen und insbesondere

a) ergänzend zu einschlägigen Risikobewertungen im Zusammenhang mit der Netz- und Informationssicherheit eine umfassende Studie[9] durchzuführen, in der eine Bestandsaufnahme der Untersee-Infrastruktur, insbesondere der Unterseekommunikationskabel vorgenommen wird, die die Mitgliedstaaten verbindet und Europa weltweit anbindet, und deren Ergebnisse den Mitgliedstaaten mitgeteilt werden sollten;

b) die Abwehrbereitschaft und Reaktion der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der Union bei Cybersicherheitsvorfällen großen Ausmaßes oder großen Vorfällen im Einklang mit dem verstärkten Rechtsrahmen für Cybersicherheit und sonstigen einschlägigen anzuwendenden Vorschriften zu unterstützen[10];

c) das Hauptkonzept des Cyber-Notfallfonds bei angemessener Erörterung mit den Mitgliedstaaten beschleunigt voranzubringen.

22. Die Kommission wird ermutigt, die Arbeit an zukunftsorientierten vorausschauenden Maßnahmen, einschließlich einer Zusammenarbeit mit den Mitgliedstaaten nach den Artikeln 6 und 10 des Beschlusses 1313/2013/EU, und in Form einer Notfallplanung zu intensivieren, um die Einsatzbereitschaft und die Reaktion des Zentrums für die Koordination von Notfallmaßnahmen (ERCC) auf Störungen kritischer Infrastrukturen zu unterstützen, Investitionen in präventive Ansätze und Vorkehrungen für die Bevölkerung zu erhöhen und die Unterstützung in Bezug auf Kapazitätsaufbau im Rahmen des Wissensnetzes der Union für Katastrophenschutz zu erhöhen..

---

9 Diese Studie sollte eine Bestandsaufnahme ihrer Kapazitäten und redundanten Elemente, Schwachstellen, Bedrohungen und Risiken für die Verfügbarkeit von Diensten, die Auswirkungen der Ausfallzeiten von (transatlantischen) Unterseekabeln auf die Mitgliedstaaten und die Union insgesamt und die Risikominderung umfassen, wobei die Sensibilität dieser Informationen und die Notwendigkeit ihres Schutzes zu berücksichtigen sind.

10 Besondere Aufmerksamkeit sollte auch allen Tätigkeiten gelten, mit denen eine wirksame koordinierte Reaktion auf Unionsebene im Falle eines grenzüberschreitenden schweren Cybervorfalls oder einer damit zusammenhängenden Bedrohung mit etwaigen systemischen Auswirkungen auf den Finanzsektor der Union vorbereitet wird, wie es der neue Rechtsrahmen für die Betriebsstabilität digitaler Systeme vorschreibt.

23. Die Kommission sollte die Nutzung der Überwachungsmittel der Union (Copernicus, Galileo und EGNOS) fördern, um die Mitgliedstaaten bei der Überwachung kritischer Infrastrukturen und gegebenenfalls ihrer unmittelbaren Umgebung zu unterstützen und andere im Weltraumprogramm der Union vorgesehene Überwachungsoptionen wie Weltraumlageerfassung und die Beobachtung und Verfolgung von Objekten im Weltraum zu unterstützen.

24. Sofern relevant werden die Agenturen der Union und andere einschlägige Stellen ersucht, im Einklang mit ihren jeweiligen Mandaten Unterstützung in Fragen betreffend die Resilienz kritischer Infrastrukturen zu leisten; dies betrifft insbesondere

a) die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (EUROPOL) im Zusammenhang mit der Sammlung von Informationen, der kriminalpolizeilichen Analyse und der Unterstützung von Ermittlungen bei grenzüberschreitenden Strafverfolgungsmaßnahmen und – sofern relevant und angebracht – die Weitergabe der Ergebnisse an die Mitgliedstaaten;

b) die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) im Zusammenhang mit der maritimen Sicherheit und Gefahrenabwehr in der Union, einschließlich Seeverkehrsüberwachungsdiensten zur maritimen Sicherheit und Gefahrenabwehr;

c) die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA) sowie das Satellitenzentrum der Europäischen Union (SatCen), die mittels Maßnahmen im Rahmen des Weltraumprogramms der Union Unterstützung leisten könnten;

d) das ECCC im Zusammenhang mit Tätigkeiten bezüglich der Cybersicherheit, die auch in Zusammenarbeit mit der ENISA Innovation und Industriepolitik im Bereich der Cybersicherheit unterstützen könnte.

KAPITEL III: VERSTÄRKTE REAKTION

Maßnahmen auf Ebene der Mitgliedstaaten

25. Die Mitgliedstaaten werden ersucht,

a) ihre Reaktion weiterhin – sofern relevant – abzustimmen und den Überblick über die sektorübergreifende Reaktion auf ernsthafte Störungen wesentlicher Dienste, die durch kritische Infrastrukturen erbracht werden, zu bewahren. Dies könnte geschehen im Rahmen eines künftigen Konzeptentwurfs für eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung, bestehender Regelungen für die Integrierte EU-Regelung für die politische Reaktion auf Krisen (IPCR), wenn es um kritische Infrastrukturen von grenzüberschreitender Bedeutung geht, des Konzeptentwurfs zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes im Rahmen der Empfehlung (EU) 2017/1584 der Kommission[11], von EU-CyCLONe, der Vorgaben für eine koordinierte Reaktion der EU auf hybride Kampagnen und des EU-Instrumentariums zur Abwehr hybrider Bedrohungen und Kampagnen und des Schnellwarnsystems für den Fall von Desinformation;

b) den Informationsaustausch auf operativer Ebene mit dem ERCC im Rahmen des UCPM zu intensivieren, um die Frühwarnung zu verbessern und ihre Reaktion im Rahmen des UCPM bei Störungen kritischer Infrastrukturen mit erheblicher grenzüberschreitender Relevanz zu koordinieren und so bei Bedarf eine schnellere unionsgestützte Reaktion zu gewährleisten;

c) ihre Bereitschaft zu erhöhen, gegebenenfalls über bestehende oder zu entwickelnde Instrumente auf solche unter Buchstabe a genannten erheblichen Störungen zu reagieren;

---

11 Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

d) beim Ausbau der einschlägigen Reaktionskapazitäten im ECPP und in rescEU zusammenzuarbeiten;

e) die Betreiber kritischer Infrastrukturen und die zuständigen nationalen Behörden dazu anzuhalten, ihre Kapazitäten aufzustocken, damit sie imstande sind, bei der Erbringung wesentlicher Dienste durch diese Betreiber kritischer Infrastrukturen rasch eine Grundversorgung wiederherzustellen;

f) die Betreiber kritischer Infrastrukturen beim Wiederaufbau ihrer kritischen Infrastruktur zu ermutigen, diese so resilient wie möglich wiederaufzubauen, wobei die Verhältnismäßigkeit der Maßnahmen in Bezug auf Risikobeurteilungen und Kosten zu berücksichtigen ist, und zwar gegen alle erdenklichen erheblichen Risiken, einschließlich ungünstiger Klimaszenarien.

26. Die Mitgliedstaaten werden aufgefordert, die Vorbereitungsarbeiten nach Möglichkeit gemäß ihrer Aufgaben nach dem verstärkten Rechtsrahmen für Cybersicherheit zu beschleunigen, indem sie darauf abzielen, die Kapazitäten der CSIRTs angesichts der neuen Aufgaben der CSIRTs und der größeren Zahl von Einrichtungen aus neuen Sektoren aufzustocken, und dabei ihre Cybersicherheitsstrategien zeitig zu überprüfen und zu aktualisieren und schnellstmöglich nationale Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen anzunehmen, sofern es noch keine gibt.

27. Die Mitgliedstaaten werden ersucht, auf nationaler Ebene die zweckdienlichsten Mittel in Erwägung zu ziehen, um sicherzustellen, dass sich die einschlägigen Interessenträger der Notwendigkeit bewusst sind, die Resilienz kritischer Infrastrukturen durch Zusammenarbeit mit vertrauenswürdigen Anbietern und Partnern zu verbessern. Es ist wichtig, in zusätzliche Kapazitäten zu investieren, insbesondere in den Sektoren, in denen sich die derzeitige Infrastruktur am Ende ihrer Lebensdauer befindet (z. B. die Infrastruktur von Unterseekommunikationskabeln), um die Kontinuität der Erbringung wesentlicher Dienste im Falle von Störungen gewährleisten und unerwünschte Abhängigkeiten verringern zu können.

28. Die Mitgliedstaaten werden dazu angehalten, auf eine proaktive strategische Kommunikation auf nationaler Ebene im Zusammenhang mit der Abwehr hybrider Bedrohungen und Kampagnen zu achten, und zwar angesichts dessen, dass Gegner bestrebt sein können, ausländische Informationsmanipulation und -einmischung auszuüben, indem sie die Narrative über Vorfälle, die auf kritische Infrastrukturen abzielen, prägen.

Maßnahmen auf Unionsebene

29. Die Kommission wird ersucht, eng mit den Mitgliedstaaten zusammenzuarbeiten, um einschlägige Stellen, Instrumente und Reaktionskapazitäten weiterzuentwickeln und so die Einsatzbereitschaft zur Bewältigung der unmittelbaren und indirekten Auswirkungen erheblicher Störungen relevanter wesentlicher Dienste, die durch kritische Infrastrukturen erbracht werden, zu verbessern, insbesondere durch Experten und Ressourcen, die über den ECPP und rescEU im Rahmen des UCPM oder künftiger Soforteinsatzteams für hybride Bedrohungen zur Verfügung stehen.

30. Die Kommission wird ersucht, unter Berücksichtigung der sich wandelnden Bedrohungslandschaft und in Zusammenarbeit mit den Mitgliedstaaten im Rahmen des UCPM

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

b) potenziell erhebliche Lücken bei den Reaktionskapazitäten des ECPP und den rescEU-Kapazitäten regelmäßig zu überwachen und zu erkennen;

c) die sektorübergreifende Zusammenarbeit weiter intensivieren, um eine angemessene Reaktion auf Unionsebene zu gewährleisten, und regelmäßige Schulungen oder Übungen zu organisieren, um diese Zusammenarbeit zu testen, und zwar in Zusammenarbeit mit einem oder mehreren Mitgliedstaaten;

d) das ERCC als sektorübergreifendes Notfallzentrum auf Unionsebene für die Koordinierung der Unterstützung der betroffenen Mitgliedstaaten auszubauen.

31. Der Rat ist entschlossen, die Arbeit im Hinblick auf die Billigung eines Konzeptentwurfs über eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung auf den Weg zu bringen, in dem die Ziele und die Formen der Zusammenarbeit zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU bei der Reaktion auf Angriffe auf solche kritischen Infrastrukturen beschrieben und festgelegt werden. Der Rat sieht dem Vorschlag der Kommission für einen solchen Konzeptentwurf, der auf der Unterstützung und den Beiträgen einschlägiger Agenturen der Union aufbaut, erwartungsvoll entgegen. Der Konzeptentwurf muss mit dem überarbeiteten operativen Protokoll der Union zur Abwehr hybrider Bedrohungen („EU-Playbook“) vollständig kohärent und interoperabel sein und dem bestehenden Konzeptentwurf für eine koordinierte Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen[12] großen Ausmaßes sowie dem in der NIS-2-Richtlinie festgelegten EU-CyCLONe-Mandat Rechnung tragen und muss die Doppelung von Strukturen und Tätigkeiten vermeiden. In diesem Konzeptentwurf sollte die bestehende Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) bei der Koordinierung der Reaktion vollständig geachtet werden.

[12] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

32. Die Kommission wird ersucht, sich mit einschlägigen Interessenträgern und Experten zu geeigneten Maßnahmen bei etwaigen erheblichen Vorfällen in Bezug auf die Untersee-Infrastruktur abzustimmen, die in Verbindung mit der unter Nummer 20 Buchstabe a genannten Bestandsaufnahme vorzulegen sind, und die Notfallplanung, Risikoszenarien und Katastrophenresilienzziele der Union im Beschluss Nr. 1313/2013/EU weiter auszuarbeiten.

KAPITEL IV: INTERNATIONALE ZUSAMMENARBEIT

Maßnahmen auf Ebene der Mitgliedstaaten

33. Die Mitgliedstaaten sollten, sofern zweckdienlich und im Einklang mit dem Unionsrecht, in Bezug auf die Resilienz kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung mit einschlägigen Drittländern zusammenarbeiten.

34. Die Mitgliedstaaten werden dazu angehalten, mit der Kommission und dem Hohen Vertreter zusammenzuarbeiten, um Risiken für kritische Infrastrukturen in internationalen Gewässern wirksam zu begegnen.

35. 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 vom 21. Juni 2022 über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen Bezug genommen wird, beizutragen und diese anschließend zu nutzen, um dem Rahmen für eine koordinierte Reaktion der Union auf hybride Kampagnen insbesondere bei der Prüfung und Vorbereitung umfassender und koordinierter Reaktionen der Union auf hybride Kampagnen und hybride Bedrohungen, die unter anderem auf Betreiber kritischer Infrastrukturen abzielen, volle Wirkung zu verleihen.

Maßnahmen auf Unionsebene

36. Die Kommission und der Hohe Vertreter werden ersucht, sofern zweckdienlich und im Einklang mit ihren jeweiligen Aufgaben und Zuständigkeiten nach dem Unionsrecht, einschlägige Drittländer bei der Stärkung der Resilienz kritischer Infrastrukturen in ihrem Hoheitsgebiet und insbesondere kritischer Infrastrukturen, die physisch mit ihrem Hoheitsgebiet und dem Hoheitsgebiet eines Mitgliedstaats verbunden sind, zu unterstützen.

37. 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 von gemeinsamem Interesse durch den strukturierten Dialog zwischen der EU und der NATO über Resilienz unter uneingeschränkter Achtung der Zuständigkeiten der Union und der Mitgliedstaaten gemäß den Verträgen und der vom Europäischen Rat vereinbarten zentralen Grundsätze der Zusammenarbeit zwischen der EU und der NATO, insbesondere Gegenseitigkeit, Inklusivität und Beschlussfassungsautonomie, verstärken. In diesem Zusammenhang wird diese Zusammenarbeit im Rahmen des strukturierten Dialogs zwischen der EU und der NATO über Resilienz vorangebracht, der in den bestehenden Mechanismus auf der Arbeitsebene für die Umsetzung der Gemeinsamen Erklärungen eingebettet ist, wobei für vollständige Transparenz und Einbeziehung aller Mitgliedstaaten zu sorgen ist.

38. Die Kommission wird ersucht, die Teilnahme von Vertretern einschlägiger Drittländer – soweit erforderlich und zweckdienlich – im Rahmen der Zusammenarbeit und des Informationsaustauschs zwischen Mitgliedstaaten im Bereich der Resilienz kritischer Infrastrukturen, die physisch mit dem Hoheitsgebiet eines Mitgliedstaats und dem Hoheitsgebiet eines Drittlands verbunden sind, in Erwägung zu ziehen.

Geschehen zu … am … .

Im Namen des Rates

Der Präsident / Die Präsidentin