EUROPÄISCHE
KOMMISSION

Brüssel, den 6.9.2023
COM(2023) 526 final

2023/0318 (NLE)

Vorschlag für eine

EMPFEHLUNG DES RATES

für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Im aktuellen geopolitischen Kontext, der von wachsender Instabilität, insbesondere durch den russischen Angriffskrieg gegen die Ukraine und zunehmend komplexere Sicherheitsbedrohungen, sowie von den Folgen des Klimawandels wie der Zunahme ungewöhnlicher Klimaereignisse oder Wasserknappheit gekennzeichnet ist, muss die Union wachsam bleiben und sich ständig anpassen. Bürgerinnen und Bürger, Unternehmen und Behörden in der Union sind auf kritische Infrastrukturen[1] angewiesen, da die Einrichtungen, die solche Infrastrukturen betreiben, wesentliche Dienste erbringen. Solche Dienste sind von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder der Umwelt; sie müssen ungehindert im Binnenmarkt erbracht werden. Da diese wesentlichen Dienste sehr wichtig für den Binnenmarkt sind, müssen kritische Infrastrukturen folglich widerstandsfähiger werden und muss generell die Resilienz kritischer Einrichtungen, die diese Dienste erbringen, gewährleistet werden; daher muss die Union Maßnahmen ergreifen, um diese Resilienz zu verbessern und Störungen bei der Erbringung solcher wesentlichen Dienste zu mindern. Solche Störungen können andernfalls schwerwiegende Folgen für die Bürgerinnen und Bürger in der Union, unsere Volkswirtschaften und das Vertrauen in unsere demokratischen Systeme haben und das reibungslose Funktionieren des Binnenmarkts beeinträchtigen, insbesondere vor dem Hintergrund wachsender Interdependenzen zwischen Sektoren und über Grenzen hinweg.

Die Union hat bereits eine Reihe von Maßnahmen ergriffen, um den Schutz kritischer Infrastrukturen, insbesondere in Bezug auf grenzüberschreitende Infrastrukturen, und die Resilienz kritischer Einrichtungen zu verbessern, um Störungen der von ihnen im Binnenmarkt erbrachten wesentlichen Dienste zu verhindern oder die Folgen abzumildern.

Die Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen[2] (im Folgenden „EKI-Richtlinie“) war das erste Rechtsinstrument, mit dem ein EU-weites Verfahren zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und ein gemeinsames Konzept der Union eingeführt wurden, um zu bewerten, ob der Schutz solcher Infrastrukturen gegen vom Menschen – sowohl vorsätzlich als auch versehentlich – verursachte Bedrohungen sowie gegen Naturkatastrophen verbessert werden muss. Sie konzentrierte sich jedoch nur auf die Sektoren Energie und Verkehr und den Schutz kritischer Infrastrukturen und sah keine umfassenderen Maßnahmen zur Stärkung der Resilienz der Einrichtungen vor, die solche Infrastrukturen betreiben.

Aufgrund des zunehmend vernetzten und grenzüberschreitenden Charakters der Tätigkeiten im Binnenmarkt bestand die Notwendigkeit, mehr als zwei Sektoren abzudecken und über Schutzmaßnahmen für einzelne Anlagen hinauszugehen. Deshalb wurde im Jahr 2022 die

---

[1] Kritische Infrastrukturen sind Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind (Artikel 2 Absatz 4 der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen).

[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).

Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen[3] (im Folgenden „CER-Richtlinie“) zusammen mit der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union[4] (im Folgenden „NIS-2-Richtlinie“) angenommen. Ziel ist es, eine umfassende physische und digitale Resilienz kritischer Einrichtungen zu gewährleisten. Die CER-Richtlinie trat am 16. Januar 2023 in Kraft und soll die Mitgliedstaaten dabei unterstützen, die allgemeine Resilienz kritischer Einrichtungen zu verbessern und gleichzeitig die Koordinierung auf Unionsebene zu verstärken. Sie wird ab dem 18. Oktober 2024 an die Stelle der EKI-Richtlinie treten; bis dahin müssen die Mitgliedstaaten die erforderlichen Maßnahmen ergreifen, um der CER-Richtlinie nachzukommen. Die CER-Richtlinie gilt für elf Sektoren[5]. Der Fokus verlagert sich vom Schutz kritischer Infrastrukturen auf das umfassendere Konzept der Resilienz kritischer Einrichtungen, die eine solche kritische Infrastruktur betreiben; abgedeckt wird der Zeitraum vor, während und nach einem Sicherheitsvorfall. Die NIS-2-Richtlinie trat ebenfalls am 16 Januar 2023 in Kraft und modernisiert den bestehenden Rechtsrahmen mit dem Ziel der Anpassung an die zunehmende Digitalisierung und die sich wandelnde Bedrohungslage im Bereich der Cybersicherheit. Mit der NIS-2-Richtlinie wird auch der Anwendungsbereich der Cybersicherheitsvorschriften auf neue Sektoren und Einrichtungen ausgeweitet und die Resilienz und Reaktionsfähigkeit von öffentlichen und privaten Einrichtungen, zuständigen Behörden und der Union insgesamt verbessert.

Die CER-Richtlinie enthält Bestimmungen über die Meldung von Sicherheitsvorfällen durch die kritische Einrichtung an die zuständige nationale Behörde, die Meldung anderer (potenziell) betroffener Mitgliedstaaten durch die zuständige nationale Behörde und die Meldung an die Kommission, wenn der Sicherheitsvorfall sechs oder mehr Mitgliedstaaten betrifft. In der CER-Richtlinie werden bestimmte Pflichten zur Meldung von Sicherheitsvorfällen festgelegt, wenn der Sicherheitsvorfall erhebliche Auswirkungen auf kritische Einrichtungen und die Kontinuität der Erbringung wesentlicher Dienste für einen oder mehrere andere Mitgliedstaaten oder in einem oder mehreren anderen Mitgliedstaaten hat oder haben könnte[6].

Wie die Sabotage der Nord-Stream-Gasfernleitungen im September 2022 zeigt, hat sich das sicherheitspolitische Umfeld, in dem kritische Infrastrukturen betrieben werden, erheblich verändert, und es bedarf zusätzlicher dringender Maßnahmen auf Unionsebene, um die Widerstandsfähigkeit kritischer Infrastrukturen nicht nur im Hinblick auf die Vorsorge, sondern auch im Hinblick auf eine koordinierte Reaktion zu verbessern.

In diesem Zusammenhang wurde am 8. Dezember 2022 auf Vorschlag der Kommission eine Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur[7] (im Folgenden „Empfehlung für die Resilienz kritischer Infrastruktur“) angenommen. In dieser Empfehlung wird unter anderem hervorgehoben, dass eine koordinierte und wirksame Reaktion auf aktuelle und künftige Risiken für die

---

[3] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

[4] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80).

[5] Energie, Verkehr, Banken, Finanzmarktinfrastruktur, digitale Infrastruktur, öffentliche Verwaltung, Weltraum, Gesundheit, Trinkwasser, Abwasser, Produktion, Verarbeitung und Vertrieb von Lebensmitteln.

[6] Im Einklang mit Artikel 15 Absätze 1 und 3 der CER-Richtlinie.

[7] Empfehlung des Rates vom 8. Dezember 2022 für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur 2023/C 20/01 (ABl. C 20 vom 20.1.2023, S. 1).

Erbringung wesentlicher Dienste auf Unionsebene sichergestellt werden muss. Insbesondere forderte der Rat die Kommission zur Ausarbeitung „eines Konzeptentwurfs für eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung“ auf. In der Empfehlung wird darauf hingewiesen, dass der Konzeptentwurf mit dem EU-Protokoll zur Abwehr hybrider Bedrohungen[8] im Einklang stehen, der Empfehlung 2017/1584 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen[9] („Cyber Blueprint“) Rechnung tragen und die Integrierte Regelung für die politische Reaktion auf Krisen[10] (IPCR) einhalten sollte.

Vor diesem Hintergrund enthält der vorliegende Vorschlag für eine zusätzliche Empfehlung des Rates einen solchen Konzeptentwurf. Mit dem Vorschlag soll der derzeitige Rechtsrahmen ergänzt werden, indem die koordinierte Reaktion auf Unionsebene bei Störungen kritischer Infrastrukturen mit erheblicher grenzüberschreitender Bedeutung beschrieben wird, wobei die bestehenden Regelungen auf Unionsebene genutzt werden. Konkret werden in dem Vorschlag der Umfang und die Ziele des Konzeptentwurfs sowie die Akteure, Verfahren und bestehenden Instrumente beschrieben, die eingesetzt werden könnten, um auf Unionsebene in koordinierter Weise auf eine Störung kritischer Infrastrukturen mit erheblichen grenzüberschreitenden Auswirkungen zu reagieren, und die Modalitäten der Zusammenarbeit zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union in derartigen Situationen skizziert.

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

Dieser Vorschlag für eine Empfehlung des Rates steht im Einklang mit dem derzeitigen Rechtsrahmen für den Schutz kritischer Infrastrukturen und die Resilienz kritischer Einrichtungen – der EKI-Richtlinie bzw. der CER-Richtlinie sowie der Empfehlung für die Resilienz kritischer Infrastruktur – und ergänzt diesen; der Entwurf zielt darauf ab, die Koordinierung der Mitgliedstaaten untereinander sowie der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der Union bei der Reaktion auf Sicherheitsvorfälle, die Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung verursachen, und die Erbringung wesentlicher Dienste ergänzend zu gewährleisten. Der Vorschlag stützt sich auf bestehende Strukturen und Mechanismen auf Unionsebene, einschließlich der durch die CER-Richtlinie geschaffenen, nämlich die Zusammenarbeit zwischen den zuständigen Behörden und der Gruppe für die Resilienz kritischer Einrichtungen, die durch die CER-Richtlinie eingerichtet wurde, um die Kommission zu unterstützen und die Zusammenarbeit zwischen den Mitgliedstaaten sowie den Informationsaustausch im Zusammenhang mit der CER-Richtlinie zu erleichtern.

Dieser Vorschlag für eine Empfehlung des Rates steht auch im Einklang mit dem in der NIS-2-Richtlinie festgelegten Unionsrahmen für Cybersicherheit und ergänzt diesen.

Mit dem vorliegenden Vorschlag soll im Bereich der Resilienz kritischer Einrichtungen und des Schutzes kritischer Infrastrukturen ein Konzeptentwurf für kritische Infrastrukturen nach dem Vorbild des Cyber Blueprint vorgelegt werden.

In Teil I Nummer 4 Buchstabe b des Anhangs werden ferner die Verknüpfungen mit dem Cyber Blueprint erläutert, der für Cybersicherheitsvorfälle großen Ausmaßes gilt, die so

---

[8] Gemeinsame Arbeitsunterlage – EU-Protokoll zur Abwehr hybrider Bedrohungen (SWD(2023)116 final).

[9] 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).

[10] Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die integrierte EU-Regelung für die politische Reaktion auf Krisen (ABl. L 320 vom 17.12.2018, S. 28).

weitreichende Störungen verursachen, dass der betroffene Mitgliedstaat sie nicht allein bewältigen kann, oder die so weitreichende und beträchtliche Auswirkungen von technischer oder politischer Tragweite auf zwei oder mehr Mitgliedstaaten oder Unions-Organe haben, dass rasch koordinierte Maßnahmen zu treffen sind und auf Unionsebene politisch reagiert werden muss. Ein Sicherheitsvorfall ist in der NIS-2-Richtlinie definiert als „ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt" („Cybersicherheitsvorfall").

Die gemäß der CER-Richtlinie und der NIS-2-Richtlinie zuständigen Behörden sind verpflichtet, zusammenzuarbeiten und Informationen über Cybersicherheitsvorfälle und Sicherheitsvorfälle, die kritische Einrichtungen betreffen, auszutauschen, auch im Hinblick auf die einschlägigen Maßnahmen, die ergriffen wurden. In einer Situation, in der ein erheblicher Sicherheitsvorfall bei kritischen Infrastrukturen und ein Cybersicherheitsvorfall großen Ausmaßes dieselbe Einrichtung betreffen, sollten die einschlägigen Akteure die möglichen Reaktionen koordinieren.

Der Vorschlag steht im Einklang mit dem EU-Protokoll zur Abwehr hybrider Bedrohungen, das für hybride Sicherheitsvorfälle gilt. In Teil I Nummer 4 Buchstabe a des Anhangs werden die Verknüpfungen mit dem EU-Protokoll erläutert, einschließlich des Instruments, das bei einem erheblichen Sicherheitsvorfall bei kritischer Infrastruktur mit hybrider Dimension Anwendung findet.

Der Vorschlag steht auch im Einklang mit anderen bestehenden Krisenbewältigungsmechanismen auf Unionsebene, wie der IPCR-Regelung des Rates, dem internen Krisenkoordinierungsprozess der Kommission, ARGUS[11], und dem Katastrophenschutzverfahren der Union[12] (UCPM), das von seinem Zentrum für die Koordination von Notfallmaßnahmen (ERCC) unterstützt wird, sowie dem Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes.

Der Vorschlag steht auch im Einklang mit anderen einschlägigen sektoralen Rechtsvorschriften, insbesondere mit den darin enthaltenen spezifischen Maßnahmen, die bestimmte Aspekte der Reaktion auf Störungen durch in den betroffenen Sektoren tätige Einrichtungen regeln.

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, in dem die einschlägigen Vorschriften für die Annahme von Empfehlungen festgelegt sind.

Die Wahl von Artikel 114 AEUV als materielle Rechtsgrundlage ist dadurch gerechtfertigt, dass mit der vorgeschlagenen Empfehlung des Rates eine koordinierte Reaktion auf

[11] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Bestimmungen der Kommission zum allgemeinen Frühwarnsystem „ARGUS" (COM(2005) 662 final).

[12] Verordnung (EU) 2021/836 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Änderung des Beschlusses Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union (ABl. L 185 vom 26.5.2021, S. 1).

Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung sichergestellt werden soll. Solche Störungen betreffen mehrere Mitgliedstaaten und könnten das Funktionieren des Binnenmarkts aufgrund wachsender Interdependenzen zwischen Infrastrukturen und Sektoren in einer immer stärker verwobenen Wirtschaft in der Union beeinträchtigen. Eine bessere Reaktion auf Störungen wird wiederum Störungen des Funktionierens des Binnenmarkts verhindern, da diese kritischen Infrastrukturen und die von ihnen erbrachten wesentlichen Dienste für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen, wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit sowie der Umwelt von entscheidender Bedeutung sind.

Der Vorschlag würde die EKI-Richtlinie und die CER-Richtlinie ergänzen, die sich ebenfalls auf Artikel 114 AEUV stützen. Die Empfehlung für die Resilienz kritischer Infrastruktur stützt sich, wie die nun vorgeschlagene Empfehlung, ebenfalls auf die Artikel 114 und 292 AEUV.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

In der Erwägung, dass die Reaktion auf Störungen kritischer Infrastrukturen oder der von den kritischen Einrichtungen, die diese kritischen Infrastrukturen betreiben, erbrachten Dienstleistungen in erster Linie in die Zuständigkeit der Mitgliedstaaten fällt, kommt der Union bei einer Störung kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung eine wichtige Rolle zu, da sich diese Störung auf mehrere oder sogar alle Bereiche der Wirtschaftstätigkeit innerhalb des Binnenmarkts, die Sicherheit und die internationalen Beziehungen der Union auswirken kann. Um das Funktionieren des Binnenmarkts zu gewährleisten, ist die Koordinierung auf Unionsebene im Falle von Störungen kritischer Infrastrukturen mit erheblichen grenzüberschreitenden Auswirkungen nicht nur angemessen, sondern auch notwendig, da eine solche koordinierte Reaktion auf Unionsebene die Reaktion der Mitgliedstaaten auf die Störung durch eine gemeinsame Lageerfassung, eine koordinierte öffentliche Unterrichtung der Öffentlichkeit und die Abmilderung der Folgen der Störung auf den Binnenmarkt unterstützen wird.

- **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; diese konzentrieren sich auf die Gewährleistung einer koordinierten Reaktion auf Unionsebene bei Störungen kritischer Infrastrukturen oder der von den kritischen Einrichtungen, die diese kritischen Infrastrukturen betreiben, erbrachten Dienstleistungen mit erheblicher grenzüberschreitender Bedeutung. Die vorgeschlagene koordinierte Reaktion steht in einem angemessenen Verhältnis zu den Vorrechten und Pflichten der Mitgliedstaaten nach nationalem Recht. Sicherheitsvorfälle, die kritische Infrastrukturen oder die Erbringung wesentlicher Dienste durch kritische Einrichtungen stören, liegen häufig unterhalb der Schwelle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen und können wirksam auf nationaler Ebene angegangen werden. Daher beschränkt sich die Anwendung des in diesem Vorschlag vorgesehenen Mechanismus auf größere Störungen von erheblicher grenzüberschreitender Bedeutung, die mehrere Mitgliedstaaten betreffen.

- **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. Empfehlungen sind gemäß Artikel 288 AEUV nicht verbindlich. Eine Empfehlung des Rates ist in diesem Fall ein geeignetes Instrument, da sie das Engagement der Mitgliedstaaten für die darin enthaltenen Maßnahmen signalisiert und eine solide Grundlage für die Zusammenarbeit im Bereich der koordinierten Reaktion bei erheblichen Störungen kritischer Infrastrukturen bietet. Auf diese Weise würde die vorgeschlagene Empfehlung den verbindlichen Rechtsrahmen (insbesondere die CER-Richtlinie) und auch die zuvor angenommene Empfehlung für die Resilienz kritischer Infrastruktur ergänzen, in der solche ergänzenden Maßnahmen gefordert werden, wobei die Zuständigkeiten der Mitgliedstaaten in dem betreffenden Bereich uneingeschränkt geachtet werden.

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

- **Konsultation der Interessenträger**

Bei der Ausarbeitung dieses Vorschlags wurden die Mitgliedstaaten, die EU-Organe und Agenturen konsultiert. Außerdem wurden die Standpunkte der Sachverständigen der Mitgliedstaaten berücksichtigt, die sowohl beim Workshop vom 24. April 2023 vorgebracht als auch nach diesem Workshop schriftlich übermittelt wurden.

Es gab einen allgemeinen Konsens, dass eine stärkere Koordinierung auf Unionsebene bei der Reaktion auf Störungen kritischer Infrastrukturen mit erheblicher grenzüberschreitender Bedeutung angesichts der derzeitigen Bedrohungslage sinnvoll ist, wobei die Zuständigkeit der Mitgliedstaaten in diesem Bereich und die Vertraulichkeit sensibler Informationen zu wahren sind. Ebenfalls bestand auch Einigkeit darüber, dass Doppelungen bei den Instrumenten vermieden und die auf Unionsebene bestehenden Mechanismen für die Koordinierung, den Informationsaustausch und die Reaktion sinnvoll genutzt werden müssen.

Während einige Mitgliedstaaten den breiteren Anwendungsbereich des Konzeptentwurfs für kritische Infrastrukturen positiv beurteilten, vertraten andere die Auffassung, dass der in der CER-Richtlinie vorgesehene Schwellenwert von sechs oder mehr Mitgliedstaaten für die Ermittlung kritischer Einrichtungen von besonderer Bedeutung für Europa ausreichend und es nicht erforderlich sei, eine zweite Art von Sicherheitsvorfällen in den Anwendungsbereich aufzunehmen. Einige Mitgliedstaaten wiesen darauf hin, dass die Betreiber kritischer Infrastrukturen, die wesentliche Dienste erbringen, gegebenenfalls einbezogen werden sollten, da sie über Fachwissen verfügen und der Relevanz der Cyberdimension Rechnung getragen werden sollte.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Der Vorschlag für eine Empfehlung des Rates besteht aus einem Hauptteil und einem Anhang.

Der Hauptteil besteht aus den folgenden elf Punkten:

In Nummer 1 wird die Notwendigkeit einer verstärkten Zusammenarbeit bei der Reaktion auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen im Einklang mit dem in der vorliegenden Empfehlung enthaltenen Konzeptentwurf für kritische Infrastrukturen einschließlich der entsprechenden Teile des Anhangs dargelegt.

In Nummer 2 wird der Anwendungsbereich des Konzeptentwurfs für kritische Infrastrukturen spezifiziert, der sich auf zwei Arten von Störfällen bezieht, die die Anwendung dieses Konzeptentwurfs auslösen würden: Der Sicherheitsvorfall hat entweder erhebliche störende Auswirkungen auf die Erbringung wesentlicher Dienste für oder in sechs oder mehr Mitgliedstaaten, oder er hat erhebliche störende Auswirkungen in zwei oder mehr Mitgliedstaaten, und die dort genannten einschlägigen Akteure sind sich einig, dass aufgrund der erheblichen Auswirkungen des Vorfalls eine Koordinierung auf Unionsebene erforderlich ist.

Nummer 3 bezieht sich auf die Ermittlung der einschlägigen Akteure, die am Konzeptentwurf für kritische Infrastrukturen beteiligt werden sollen, und der Ebenen, auf denen der Entwurf für kritische Infrastrukturen (operationell, strategisch/politisch) zur Anwendung kommt. Dies wird im Anhang der Empfehlung näher erläutert.

In Nummer 4 wird empfohlen, den Konzeptentwurf für kritische Infrastrukturen im Einklang mit anderen einschlägigen Instrumenten anzuwenden, wie im Anhang beschrieben.

In Nummer 5 wird den Mitgliedstaaten angeraten, auf erhebliche Störungen kritischer Infrastrukturen auf nationaler Ebene wirksam zu reagieren.

Nummer 6 empfiehlt die Einrichtung oder Benennung von Kontaktstellen durch die einschlägigen Akteure, die die Nutzung des Konzeptentwurfs für kritische Infrastrukturen unterstützen sollen. Diese Kontaktstellen sollten nach Möglichkeit die gleichen sein wie die zentralen Anlaufstellen gemäß der CER-Richtlinie.

Nummer 7 bezieht sich auf den Informationsfluss im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen.

In Ziffer 8 wird erläutert, wie der Informationsaustausch ablaufen soll.

In Nummer 9 wird empfohlen, die Funktionsweise des Konzeptentwurfs für kritische Infrastrukturen durch Übungen zu testen.

In Nummer 10 wird angeraten, die ermittelten Erkenntnisse in der Gruppe für die Resilienz kritischer Einrichtungen zu erörtern; diese sollte dann einen Bericht mit Empfehlungen ausarbeiten. Der Bericht sollte von der Kommission angenommen werden.

Nummer 11 empfiehlt den Mitgliedstaaten die Erörterung des Berichts im Rat.

Im Anhang werden die Ziele, Grundsätze, zentralen Akteure, das Zusammenspiel mit bestehenden Krisenreaktionsmechanismen und die Funktionsweise des Konzeptentwurfs für kritische Infrastrukturen mit seinen beiden Formen der Zusammenarbeit beschrieben: Informationsaustausch und Reaktion.

2023/0318 (NLE)

Vorschlag für eine

EMPFEHLUNG DES RATES

für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung

(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) Für das Funktionieren des Binnenmarkts und der Gesellschaft insgesamt ist es von grundlegender Bedeutung, dass widerstandsfähige kritische Infrastrukturen und widerstandsfähige kritische Einrichtungen, die für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen, wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit sowie der Umwelt unerlässliche Dienste erbringen, zur Verfügung stehen.

(2) In der sich derzeit wandelnden Risikolage und angesichts zunehmender Interdependenzen zwischen Infrastruktur und Sektoren sowie weitergehender sektor- und grenzübergreifender Verflechtungen ist es ein umfassendes und koordiniertes Vorgehen erforderlich, um den Schutz kritischer Infrastrukturen und die Resilienz kritischer Einrichtungen, die solche Infrastrukturen betreiben, zu verbessern.

(3) Ein Sicherheitsvorfall, der den Betrieb kritischer Infrastrukturen stört und dadurch die Erbringung wesentlicher Dienste verhindert oder erheblich behindert, kann beträchtliche grenzüberschreitende Folgen haben und sich negativ auf den Binnenmarkt auswirken. Um einen zielgenauen, verhältnismäßigen und wirksamen Ansatz zu gewährleisten, sollten Maßnahmen ergriffen werden, um insbesondere erheblichen Sicherheitsvorfällen bei kritischen Infrastrukturen im Sinne dieser Empfehlung zu begegnen, die sich beispielsweise auf Situationen erstrecken, in denen die durch den Sicherheitsvorfall verursachte Störung lang anhaltend ist oder signifikante Kaskadeneffekte in demselben oder anderen Sektoren oder Mitgliedstaaten auslösen kann.

(4) Eine koordinierte Reaktion auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen ist von wesentlicher Bedeutung, um größere Störungen im Binnenmarkt zu verhindern und die schnellstmögliche Wiederherstellung der Erbringung dieser wesentlichen Dienste sicherzustellen, da solche Sicherheitsvorfälle schwerwiegende Folgen für die Wirtschaft und die Bürgerinnen und Bürger in der Union haben können. Um auf Unionsebene zeitnah und wirksam auf derartige Vorfälle reagieren zu können, sind eine rasche und effektive Zusammenarbeit aller

einschlägigen Akteure sowie von der Union unterstützte, abgestimmte Maßnahmen erforderlich. Daher ist es unabdingbar, dass im Voraus festgelegte und, soweit möglich, eingespielte Verfahren und Mechanismen der Zusammenarbeit mit genau definierten Rollen und Zuständigkeiten der wichtigsten Akteure auf nationaler und auf Unionsebene existieren.

(5) Während für die Gewährleistung einer Reaktion auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen in erster Linie die Mitgliedstaaten und die Einrichtungen, die kritische Infrastrukturen betreiben und wesentliche Dienste erbringen, verantwortlich sind, ist im Falle von Störungen von erheblicher grenzüberschreitender Bedeutung eine stärkere Koordinierung auf Unionsebene angezeigt. Eine zeitnahe und wirksame Reaktion hängt nicht nur von der Einführung nationaler Mechanismen durch die Mitgliedstaaten ab, sondern auch von unionsweit abgestimmten Maßnahmen und einer raschen und wirksamen einschlägigen Zusammenarbeit.

(6) Der Schutz kritischer europäischer Infrastrukturen wird derzeit durch die Richtlinie 2008/114/EG des Rates[1] geregelt, die nur die beiden Bereiche Verkehr und Energie abdeckt. Mit dieser Richtlinie werden ein Verfahren zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen sowie ein gemeinsamer Ansatz für die Bewertung der Notwendigkeit eines besseren Schutzes derartiger Infrastrukturen eingeführt. Sie ist die zentrale Säule des von der Kommission im Jahr 2006 angenommenen Europäischen Programms für den Schutz kritischer Infrastrukturen[2] (EPKIP), mit dem auf europäischer Ebene ein Rahmen für den Schutz kritischer Infrastrukturen vor Gefahren aller Art festgelegt wurde.

(7) Um über den Schutz kritischer Infrastrukturen hinaus auch generell die Resilienz kritischer Einrichtungen zu gewährleisten, die solche Infrastrukturen zur Erbringung wesentlicher Dienste im Binnenmarkt betreiben, wird mit Wirkung vom 18. Oktober 2024 die Richtlinie 2008/114/EG durch die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates[3] ersetzt. Die Richtlinie (EU) 2022/2557 deckt elf Sektoren ab und beinhaltet Verpflichtungen der Mitgliedstaaten und kritischen Einrichtungen zur Verbesserung der Resilienz und Regeln für die Zusammenarbeit zwischen den Mitgliedstaaten und mit der Kommission sowie für die Unterstützung der nationalen Behörden und kritischen Einrichtungen durch die Kommission und die Unterstützung der kritischen Einrichtungen durch die Mitgliedstaaten.

(8) Nach der Sabotage der Nord-Stream-Gasfernleitungen gilt es, auf Unionsebene weitere Maßnahmen zur Verbesserung der Resilienz kritischer Infrastrukturen anzunehmen. Daher hat der Rat auf der Grundlage eines Vorschlags der Kommission die Empfehlung für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur (im Folgenden „Empfehlung 2023/C 20/01“)[4] angenommen, mit der die Vorsorge, Reaktion und internationale Zusammenarbeit in

---

[1] 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).

[2] KOM(2006) 786 endgültig vom 12. Dezember 2006 – Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen.

[3] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

[4] Empfehlung des Rates vom 8. Dezember 2022 für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur 2023/C 20/01 (ABl. C 20 vom 20.1.2023, S. 1).

diesem Bereich verbessert werden sollen. In dieser Empfehlung wird vor allem hervorgehoben, dass eine koordinierte und wirksame Reaktion auf Risiken für die Erbringung wesentlicher Dienste auf Unionsebene sichergestellt werden muss.

(9) Daher ist es erforderlich, den bestehenden Rechtsrahmen durch eine zusätzliche Ratsempfehlung für einen Konzeptentwurf für eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung („Konzeptentwurf für kritische Infrastrukturen“) zu ergänzen und dabei auf bestehende Regelungen auf Unionsebene zurückzugreifen.

(10) Diese Empfehlung sollte zur Gewährleistung der Kohärenz und zur Vermeidung von Doppelarbeit an die Empfehlung 2023/C 20/01 angepasst werden. Daher sollte diese Empfehlung als solche keine anderen Elemente des Krisenmanagementzyklus wie Prävention, Vorsorge und Folgenbewältigung abdecken.

(11) Diese Empfehlung sollte die Richtlinie (EU) 2022/2557 insbesondere im Hinblick auf eine koordinierte Reaktion ergänzen und unter Gewährleistung der Kohärenz mit dieser Richtlinie und anderen geltenden Vorschriften des Unionsrechts umgesetzt werden. Daher sollte sich diese Empfehlung so weit als möglich auch auf die Begriffe, Instrumente und Verfahren der genannten Richtlinie stützen und diese nutzen, wie etwa die Gruppe für die Resilienz kritischer Einrichtungen, die im Rahmen ihrer in der Richtlinie festgelegten Aufgaben handelt, und die Anlaufstellen. Darüber hinaus sollte der in dieser Empfehlung verwendete Begriff „kritische Infrastrukturen“ im Sinne des Erwägungsgrunds 7 der Empfehlung 2023/C 20/01 verstanden werden, d. h. dass er relevante kritische Infrastrukturen umfasst, die von einem Mitgliedstaat auf nationaler Ebene ermittelt oder gemäß der Richtlinie 2008/114/EG als europäische kritische Infrastruktur ausgewiesen wurden, sowie kritische Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 zu ermitteln sind. Um Kohärenz mit der Richtlinie (EU) 2022/2557 zu gewährleisten, sollten die in dieser Empfehlung verwendeten Begriffe daher bedeutungsgleich zu der genannten Richtlinie ausgelegt werden. Der Ausdruck „Resilienz“ sollte beispielsweise im Sinne des Artikels 2 Nummer 2 der Richtlinie verstanden werden als die Fähigkeit einer kritischen Infrastruktur, Ereignisse, die die Erbringung wesentlicher Dienste im Binnenmarkt – 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 – erheblich stören oder erheblich stören könnten, 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.

(12) Darüber hinaus sollte der Begriff der „erheblichen Störung“ im Lichte der Kriterien in Artikel 7 Absatz 1 der Richtlinie (EU) 2022/2557 verstanden werden, die Folgendes berücksichtigen: i) die Zahl der Nutzer, die den von der betreffenden Einrichtung erbrachten wesentlichen Dienst in Anspruch nehmen; ii) das Ausmaß der Abhängigkeit anderer im Anhang der Richtlinie festgelegter Sektoren und Teilsektoren von dem betreffenden wesentlichen Dienst; iii) die möglichen Auswirkungen von Sicherheitsvorfällen – hinsichtlich Ausmaß und Dauer – auf wirtschaftliche und gesellschaftliche Tätigkeiten, die Umwelt, die öffentliche Ordnung und Sicherheit oder die Gesundheit der Bevölkerung; iv) den Marktanteil der Einrichtung auf dem Markt für wesentliche Dienste oder für die betreffenden wesentlichen Dienste; v) das geografische Gebiet, das von einem Sicherheitsvorfall betroffen sein könnte, einschließlich etwaiger grenzüberschreitender Auswirkungen, unter Berücksichtigung der Schwachstellen, die mit dem Grad der Isolierung bestimmter Arten geografischer Gebiete – zum Beispiel Inselregionen, abgelegene

Regionen oder Berggebiete – verbunden sind; vi) die Bedeutung der Einrichtung für die Aufrechterhaltung des wesentlichen Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Erbringung des betreffenden wesentlichen Dienstes.

(13) Im Interesse der Effizienz und Wirksamkeit sollte der Konzeptentwurf für kritische Infrastrukturen mit dem überarbeiteten operativen Protokoll der Union zur Abwehr hybrider Bedrohungen[5] vollständig kohärent und interoperabel sein, dem bestehenden Konzept für eine koordinierte Reaktion auf große grenzüberschreitende Cybersicherheitsvorfälle und -krisen gemäß der Empfehlung (EU) 2017/1584 der Kommission[6] („Cyber Blueprint“) und dem in der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[7] festgelegten Mandat für das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) Rechnung tragen und eine Doppelung von Strukturen und Tätigkeiten vermeiden. Darüber hinaus sollte bei der Koordinierung der Reaktion die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) des Rates[8] vollumfänglich beachtet werden.

(14) Diese Empfehlung baut auf den bestehenden Krisenbewältigungsmechanismen der Union auf, entspricht ihnen und ergänzt sie; dabei handelt es sich insbesondere um die IPCR-Regelung des Rates, den internen Krisenkoordinierungsprozess der Kommission ARGUS[9] und das Katastrophenschutzverfahren der Union (UCPM)[10], unterstützt durch das Zentrum für die Koordination von Notfallmaßnahmen (ERCC)[11], den Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) sowie das Notfallinstrument für den Binnenmarkt[12] – und damit um Instrumente, die bei der Reaktion auf eine größere Störung des Betriebs kritischer Infrastrukturen eine Rolle spielen können.

(15) In Reaktion auf einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen können die oben genannten Instrumente oder Mechanismen auf Unionsebene im Einklang mit den für sie geltenden Vorschriften und Verfahren eingesetzt werden, die durch diese Empfehlung zwar ergänzt, aber unberührt bleiben sollten. So bleibt die IPCR-Regelung des Rates das wichtigste Instrument für die Koordinierung der Reaktion auf Ebene der Unionspolitik zwischen den Mitgliedstaaten. Die interne

---

5 Gemeinsame Arbeitsunterlage – EU-Protokoll zur Abwehr hybrider Bedrohungen (SWD(2023)116 final).

6 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).

7 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80).

8 Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die integrierte EU-Regelung für die politische Reaktion auf Krisen (ABl. L 320 vom 17.12.2018, S. 28).

9 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Bestimmungen der Kommission zum allgemeinen Frühwarnsystem „ARGUS“ (COM(2005) 662 final).

10 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).

11 Mit dem Beschluss Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union wird ein Rahmen für alle Gefahren mit Vorkehrungen für Prävention, Vorsorge und Reaktion auf Unionsebene geschaffen, um alle Arten von Naturkatastrophen und vom Menschen verursachten Katastrophen oder drohenden Katastrophen innerhalb und außerhalb der EU zu bewältigen.

12 Verordnung .../... des Europäischen Parlaments und des Rates zur Schaffung eines Notfallinstruments für den Binnenmarkt und zur Aufhebung der Verordnung (EG) Nr. 2679/98 des Rates (COM(2022) 459 final).

Koordinierung innerhalb der Kommission erfolgt im Rahmen des sektorübergreifenden Krisenkoordinierungprozesses ARGUS. Berührt die Krise eine externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), so kann der Krisenreaktionsmechanismus des EAD ausgelöst werden. Im Einklang mit dem Beschluss Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union (UCPM) werden im Rahmen dieses Verfahrens operative Reaktionen auf eingetretene oder unmittelbar bevorstehende Naturkatastrophen und vom Menschen verursachte Katastrophen innerhalb und außerhalb der Union (einschließlich solcher, die die kritische Infrastruktur betreffen) vom Zentrum für die Koordination von Notfallmaßnahmen (ERCC) organisiert, der einzigen rund um die Uhr einsatzbereiten operativen Plattform der Kommission zur Krisenbewältigung. In solchen Fällen kann das ERCC Frühwarnungen, Meldungen und Analysen gewährleisten und den Informationsaustausch sowie im Falle einer Aktivierung des Katastrophenschutzverfahrens durch einen Mitgliedstaat die Entsendung von operativer Hilfe und Expertinnen und Experten in die betroffenen Gebiete unterstützen. Das ERCC kann darüber hinaus die sektorale und sektorübergreifende Koordinierung sowohl auf Unionsebene als auch zwischen der Union und den zuständigen nationalen Behörden, einschließlich der für den Katastrophenschutz und die Resilienz kritischer Infrastrukturen zuständigen Behörden, erleichtern.

(16) Die in dieser Empfehlung festgelegten Verfahren sollten einerseits gegebenenfalls in Verbindung mit diesen anderen Instrumenten oder Mechanismen, sofern diese zum Einsatz kommen, in Erwägung gezogen werden; darüber hinaus sollten in dieser Empfehlung Maßnahmen dargelegt werden, die auf Unionsebene mit Blick auf die gemeinsame Lageerfassung, eine koordinierte Unterrichtung der Öffentlichkeit und eine wirksame Reaktion jenseits des Rahmens dieser Krisenkoordinierungsmechanismen der Union in dem Fall ergriffen werden könnten, dass die genannten Mechanismen nicht eingesetzt werden.

(17) Um die Reaktion auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen besser zu koordinieren, sollte die Zusammenarbeit zwischen den Mitgliedstaaten und den Organen der Union sowie den einschlägigen Agenturen, Einrichtungen und sonstigen Stellen der Union im Rahmen bestehender Vereinbarungen und im Einklang mit dem Konzeptentwurf für kritische Infrastrukturen verbessert werden. Der Konzeptentwurf für kritische Infrastrukturen sollte daher angewendet werden, wenn der in der Richtlinie (EU) 2022/2557 festgelegte Schwellenwert von sechs oder mehr Mitgliedstaaten in Bezug auf die Ermittlung kritischer Einrichtungen von besonderer Bedeutung für Europa erreicht wird, und ebenso, wenn sich Vorfälle ereignen, die weniger Mitgliedstaaten betreffen, da solche Vorfälle aufgrund von grenzüberschreitenden Kaskadeneffekten ebenfalls weitreichende Auswirkungen haben könnten und daher eine Koordinierung der Reaktion auf Unionsebene von Vorteil wäre.

(18) Zwar wird ein Rahmen für die Zusammenarbeit auf Unionsebene für eine koordinierte Reaktion auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen für notwendig erachtet, doch sollte dies nicht dazu führen, dass den kritischen Einrichtungen und den zuständigen Behörden Ressourcen für die – als vorrangig zu betrachtende – Bewältigung von Sicherheitsvorfällen entzogen werden.

(19) Die einschlägigen an der Umsetzung des Konzeptentwurfs für kritische Infrastrukturen beteiligten Akteure sollten klar benannt werden, damit es einen klaren und umfassenden Überblick über die Organe, Einrichtungen, sonstigen Stellen und

Behörden gibt, die auf einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen reagieren könnten.

(20) Die Reaktion auf Sicherheitsvorfälle bei kritischen Infrastrukturen, einschließlich erheblicher Sicherheitsvorfälle, liegt in erster Linie in der Verantwortung der zuständigen Behörden der Mitgliedstaaten. Diese Empfehlung sollte im Einklang mit dem Unionsrecht die Zuständigkeit der Mitgliedstaaten für den Schutz der nationalen Sicherheit und Verteidigung sowie ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, insbesondere in Bezug auf die öffentliche Sicherheit, die territoriale Unversehrtheit und die Aufrechterhaltung der öffentlichen Ordnung unberührt lassen. Darüber hinaus sollte diese Empfehlung keine Auswirkungen auf nationale Verfahren wie die Kommunikation und die Verbindung der Betreiber kritischer Infrastrukturen mit den zuständigen nationalen Behörden haben. Diese Empfehlung sollte unbeschadet einschlägiger bilateraler oder multilateraler Vereinbarungen zwischen Mitgliedstaaten Anwendung finden.

(21) Für eine wirksame und zeitnahe Zusammenarbeit im Rahmen des Konzeptentwurfs für kritische Infrastrukturen ist es wesentlich, dass von den beteiligten Akteuren Anlaufstellen benannt oder eingerichtet werden. Im Interesse der Kohärenz sollten die Mitgliedstaaten die Möglichkeit in Erwägung ziehen, die nach der Richtlinie (EU) 2022/2557 zu benennenden oder einzurichtenden zentralen Anlaufstellen auch als Anlaufstellen für die Zwecke dieses Konzeptentwurfs zu benennen oder einzurichten.

(22) Um ein wirksames Vorgehen zu ermöglichen, gilt es, unter Beteiligung der einschlägigen Akteure die Verfahren des Konzeptentwurfs für kritische Infrastrukturen zu erproben und zu trainieren sowie darüber Bericht zu erstatten und die in der Praxis gewonnenen Erkenntnisse auszuwerten, damit für den Fall erheblicher Sicherheitsvorfälle bei kritischen Infrastrukturen eine hohe Einsatzbereitschaft sichergestellt ist und rasch und koordiniert reagiert werden kann.

(23) Angesichts der Struktur des Krisenreaktionsmechanismus des Rates IPCR und unter Berücksichtigung der möglichen Aktivierung der auf Unionsebene bereits bestehenden Koordinierungsmechanismen zur Krisenbewältigung sollte der Konzeptentwurf für kritische Infrastrukturen zwei Formen der Zusammenarbeit umfassen, mit denen auf einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen reagiert werden kann. Die erste sollte den Informationsaustausch unter Einbeziehung aller einschlägigen Akteure, die Koordinierung der Unterrichtung der Öffentlichkeit und, sofern dies genutzt wird, die Koordinierung über bereits bestehende Mechanismen wie die IPCR-Regelung im Rat oder die – durch die rund um die Uhr einsatzbereite ERCC-Kontaktstelle unterstützte – ARGUS-Koordinierung innerhalb der Kommission und den EAD-Krisenreaktionsmechanismus umfassen. Die zweite sollte entsprechend dem Ausmaß des Vorfalls weitere Reaktionsmaßnahmen beinhalten. Diese Zusammenarbeit sollte ein Engagement auf operativer und auf strategisch/politischer Ebene umfassen, das den Ebenen in der Empfehlung 2017/1584 und im Protokoll der Union zur Abwehr hybrider Bedrohungen entspricht, damit Maßnahmen koordiniert und auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen wirksam und effizient reagiert werden kann. Auf der Grundlage der Grundsätze der Verhältnismäßigkeit, der Subsidiarität, der Vertraulichkeit von Informationen und der Komplementarität und um eine wirksame Zusammenarbeit zu gewährleisten, sollte in dem Konzeptentwurf für kritische Infrastrukturen beschrieben werden, wie die gemeinsame Lageerfassung durch die einschlägigen Akteure sowie eine koordinierte Unterrichtung der Öffentlichkeit und eine wirksame Reaktion erfolgen.

(24) Durch den Informationsaustausch gemäß dieser Empfehlung sollten die nationale Sicherheit bzw. die Sicherheit und die geschäftlichen Interessen der Einrichtungen, die kritische Infrastrukturen betreiben, nicht gefährdet werden. Daher sollten der Zugang zu sensiblen Informationen, ihr Austausch und der Umgang mit ihnen im Einklang mit den geltenden Vorschriften und mit besonderem Augenmerk auf die verwendeten Übertragungskanäle und Speicherkapazitäten umsichtig erfolgen —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

(1) Die Mitgliedstaaten, der Rat, die Kommission und gegebenenfalls der Europäische Auswärtige Dienst (EAD) und die einschlägigen Einrichtungen und sonstigen Stellen der Union sollten im Rahmen des in dieser Empfehlung niedergelegten Konzepts für kritische Infrastrukturen zusammenarbeiten, um die in Teil I Abschnitt 1 des Anhangs festgelegten Ziele zu erreichen und unter Berücksichtigung der in Teil I Abschnitt 2 des Anhangs dargelegten Grundsätze in koordinierter Weise auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen zu reagieren.

(2) Die Mitgliedstaaten, der Rat, die Kommission und gegebenenfalls der EAD sowie die einschlägigen Einrichtungen und sonstigen Stellen der Union sollten den Konzeptentwurf für kritische Infrastrukturen unverzüglich anwenden, wenn ein erheblicher Sicherheitsvorfall bei kritischen Infrastrukturen eintritt, d. h. ein Vorfall, der die kritische Infrastruktur betrifft und eine der folgenden Auswirkungen hat:

a) eine erhebliche Störung der Bereitstellung wesentlicher Dienste für oder in sechs oder mehr Mitgliedstaaten, darunter auch Vorfälle, die eine kritische Einrichtung von besonderer Bedeutung für Europa im Sinne des Artikels 17 der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen[13] betreffen, oder

b) erhebliche störende Auswirkungen auf die Bereitstellung wesentlicher Dienste in zwei oder mehr Mitgliedstaaten, wenn der den turnusmäßig wechselnden Ratsvorsitz innehabende Mitgliedstaat im Einvernehmen mit den betroffenen Mitgliedstaaten und in Abstimmung mit der Kommission der Auffassung ist, dass aufgrund der großen Tragweite und der erheblichen technischen oder politischen Auswirkungen des Vorfalls eine zügige Koordinierung der Reaktion auf Unionsebene erforderlich ist.

(3) Die einschlägigen Akteure des Konzeptentwurfs für kritische Infrastrukturen, die im Einklang mit Teil I Abschnitt 3 des Anhangs auf operativer und strategischer/politischer Ebene ermittelt wurden, sollten sich darum bemühen, dass das Zusammenwirken und die Zusammenarbeit komplementär erfolgen. Sie sollten einen angemessenen und raschen Informationsaustausch, einschließlich der Koordinierung der Unterrichtung der Öffentlichkeit, und die koordinierte Reaktion gemäß Teil II des Anhangs gewährleisten.

(4) Der Konzeptentwurf für kritische Infrastrukturen sollte gemäß Teil I Abschnitt 4 des Anhangs unter Berücksichtigung der anderen einschlägigen Instrumente und im Einklang mit ihnen Anwendung finden. Sollte ein Sicherheitsvorfall sowohl physische

[13] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

Aspekte als auch die Cybersicherheit kritischer Infrastrukturen betreffen, sollten Synergien mit entsprechenden, im Cyber Blueprint festgelegten Verfahren gewährleistet werden.

(5) Die Mitgliedstaaten sollten auf nationaler Ebene und im Einklang mit dem Unionsrecht eine wirksame Reaktion auf Störungen bei kritischen Infrastrukturen infolge erheblicher Sicherheitsvorfälle gewährleisten.

(6) Die Mitgliedstaaten, der Rat, der EAD, die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und die anderen einschlägigen Agenturen der Union sollten ebenso wie die Kommission eine Anlaufstelle für Fragen im Zusammenhang mit dem Konzeptentwurf für kritische Infrastrukturen benennen oder einrichten. Die Anlaufstellen sollten die Anwendung des Konzeptentwurfs für kritische Infrastrukturen unterstützen, indem sie in Reaktion auf einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen die erforderlichen Informationen bereitstellen und Koordinierungsmaßnahmen erleichtern. In den Mitgliedstaaten sollten diese Anlaufstellen nach Möglichkeit dieselben sein wie die gemäß Artikel 9 Absatz 2 der Richtlinie (EU) 2022/2557 zu benennenden oder einzurichtenden zentralen Anlaufstellen. Für die Kommission sorgt das ERCC rund um die Uhr für Kontaktmöglichkeiten und Kapazitäten und koordiniert, beobachtet und unterstützt in Echtzeit die Reaktion auf Notfälle auf Unionsebene, zugleich dient es den Mitgliedstaaten und der Kommission als operative Plattform für die Krisenreaktion und fördert einen sektorübergreifenden Ansatz beim Katastrophenmanagement.

(7) Der den turnusmäßig wechselnden Vorsitz im Rat innehabende Mitgliedstaat sollte im Einvernehmen mit den betroffenen Mitgliedstaaten alle einschlägigen Akteure über die in Nummer 6 genannten Anlaufstellen darüber informieren, wenn ein erheblicher Sicherheitsvorfall bei kritischen Infrastrukturen eintritt und der Konzeptentwurf für kritische Infrastrukturen Anwendung findet. Der Informationsaustausch zu erheblichen Vorfällen bei kritischen Infrastrukturen sollte über geeignete Kommunikationskanäle erfolgen, gegebenenfalls einschließlich der Plattform für die Integrierte Regelung für die politische Reaktion auf Krisen[14] (IPCR) und des ERCC über das Gemeinsame Kommunikations- und Informationssystem für Notfälle (CECIS), eine webbasierte Warn- und Benachrichtigungsanwendung, die einen Informationsaustausch in Echtzeit ermöglicht.

(8) Erforderlichenfalls sollte die Übertragung über gesicherte Kanäle erfolgen, damit die nationale Sicherheit und die geschäftlichen Interessen der betreffenden Einrichtungen nicht gefährdet werden. Der in Teil II Abschnitt 1 des Anhangs dieser Empfehlung dargelegte Informationsaustausch sollte ferner die nationale Sicherheit bzw. die Sicherheit und die geschäftlichen Interessen der kritischen Einrichtungen nicht gefährden und im Einklang mit dem Unionsrecht, insbesondere der Verordnung (EU).../... des Europäischen Parlaments und des Rates[15], erfolgen. Insbesondere sollten sensible Informationen mit Umsicht zugänglich gemacht, ausgetauscht und behandelt werden. Für den Umgang mit und den Austausch von Verschlusssachen sollten die

[14] Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die Integrierte EU-Regelung für die politische Reaktion auf Krisen, ST/13422/2018/INIT (ABl. L 320 vom 17.12.2018, S. 28).

[15] Verordnung (EU) .../... über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union, COM(2022) 119 final.

verfügbaren akkreditierten Instrumente verwendet und angemessene Sicherheitsmaßnahmen getroffen werden.

(9) Die einschlägigen Akteure sollten den Konzeptentwurf für kritische Infrastrukturen regelmäßig anwenden und ihre koordinierte Reaktion auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen auf nationaler, regionaler und Unionsebene trainieren und erproben, beispielsweise im Rahmen von Übungen. Bei diesen Trainings und Erprobungen können gegebenenfalls auch privatwirtschaftliche Einrichtungen einbezogen werden. Bis zum [*Datum der Annahme dieser Empfehlung + 12 Monate*] sollte eine Übung auf Unionsebene stattfinden, bei der physische Aspekte und Cyberaspekte berücksichtigt werden.

(10) Nach der Anwendung des Konzeptentwurfs für kritische Infrastrukturen in Bezug auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen sollte die in Artikel 19 der Richtlinie (EU) 2022/2557 genannte Gruppe für die Resilienz kritischer Einrichtungen die gewonnenen Erkenntnisse zeitnah mit den einschlägigen Akteuren erörtern, die auf Lücken und verbesserungsbedürftige Bereiche hindeuten können, und anschließend einen Bericht mit Empfehlungen für entsprechende Verbesserungen verfassen. Die Erstellung dieses Berichts sollte von den einschlägigen und an der Anwendung des Konzeptentwurfs für kritische Infrastrukturen beteiligten Akteuren unterstützt werden. Der Bericht sollte von der Kommission angenommen werden.

(11) Die Mitgliedstaaten sollten den unter Nummer 10 genannten Bericht in den zuständigen Vorbereitungsgremien des Rates oder im Rat erörtern.

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident /// Die Präsidentin

EUROPÄISCHE
KOMMISSION

Brüssel, den 6.9.2023
COM(2023) 526 final

ANNEX

ANHANG

des

Vorschlags für eine Empfehlung des Rates

für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung

ANHANG

In diesem Anhang werden die Grundsätze, Ziele, die zentralen Akteure, das Zusammenspiel mit bestehenden Krisenreaktionsmechanismen und die Funktionsweise eines Konzeptentwurfs für eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen („Konzeptentwurf für kritische Infrastrukturen“) und eine bessere Zusammenarbeit zwischen den Mitgliedstaaten und den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union in Bezug auf solche Vorfälle im Einklang mit den geltenden Vorschriften und Verfahren beschrieben. Dieser Konzeptentwurf lässt die Rolle und Funktionsweise anderer Regelungen unberührt.

TEIL I: ZIELE, GRUNDSÄTZE, AKTEURE UND ANDERE INSTRUMENTE

1. Ziele

Mit dem Konzeptentwurf für kritische Infrastrukturen sollen die folgenden drei wichtigsten Ziele bei einer Reaktion auf einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen erreicht werden:

a) **eine gemeinsame Lageerfassung**, da ein fundiertes Verständnis des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen in den Mitgliedstaaten, seines Ursprungs und seiner möglichen Folgen für alle relevanten Akteure auf operativer und strategischer/politischer Ebene für eine angemessene koordinierte Reaktion unabdingbar ist;

b) **eine koordinierte Unterrichtung der Öffentlichkeit**, da sie dazu beiträgt, negative Auswirkungen eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen abzumildern und Diskrepanzen bei den Informationen, die der Öffentlichkeit in den Mitgliedstaaten und zwischen den Mitgliedstaaten vermittelt werden, so gering wie möglich zu halten. Eine klare Unterrichtung der Öffentlichkeit ist auch wichtig, um die Folgen von Desinformation einzudämmen;

c) **eine wirksame Reaktion**, da eine verbesserte Reaktionsfähigkeit der Mitgliedstaaten und eine verstärkte Zusammenarbeit der Mitgliedstaaten und einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union dazu beiträgt, die Auswirkungen eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen abzufedern und eine rasche Wiederherstellung wesentlicher Dienste ermöglicht, sodass die Anfälligkeit für weitere erhebliche Sicherheitsvorfälle reduziert wird.

2. Grundsätze

Verhältnismäßigkeit

Sicherheitsvorfälle, die kritische Infrastrukturen und/oder die Erbringung wesentlicher Dienste beeinträchtigen, liegen häufig unterhalb der Schwelle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen wie in Abschnitt 2 dieser Empfehlung dargelegt. Daher können sie grundsätzlich auf nationaler Ebene wirksam angegangen werden. So beschränkt sich die Anwendung des Konzeptentwurfs für kritische Infrastrukturen auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen.

Subsidiarität

Im Einklang mit dem Unionsrecht sind vorrangig die Mitgliedstaaten dafür verantwortlich, auf Störungen bei kritischen Infrastrukturen oder bei den von kritischen Einrichtungen erbrachten wesentlichen Dienste zu reagieren. Den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union und dem Europäischen Auswärtigen Dienst (EAD) fällt eine

wichtige ergänzende Rolle im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen von erheblicher grenzüberschreitender Bedeutung zu, da ein solcher Vorfall mehrere oder sogar alle Bereiche des Wirtschaftslebens innerhalb des Binnenmarkts, das Leben der in der Union lebenden Bürgerinnen und Bürger, die Sicherheit und die internationalen Beziehungen der Union beeinträchtigen kann.

Komplementarität

Der Konzeptentwurf für kritische Infrastrukturen berücksichtigt und spiegelt die Funktionsweise der bestehenden Krisenbewältigungsmechanismen auf Unionsebene wider, darunter die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) des Rates, den internen Krisenkoordinierungsprozess der Kommission ARGUS, das Katastrophenschutzverfahren der Union (UCPM), das vom Zentrum für die Koordination von Notfallmaßnahmen (ERCC) unterstützt wird, und das Krisenreaktionsverfahren des EAD. Er stützt sich ferner auf sektorbezogene Vereinbarungen, einschließlich der Bestimmungen für das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes gemäß der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[1] und des Rahmens, der im Konzeptentwurf zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes („Cyber Blueprint“)[2] festgelegt ist, sowie auf das Netz der nationalen Anlaufstellen für den Verkehr[3] und das Krisenkoordinierungsgremium für die Europäische Luftfahrt[4].

Darüber hinaus baut der Konzeptentwurf für kritische Infrastrukturen auf den gemäß der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates[5] eingerichteten Strukturen und Mechanismen auf und ist im Einklang damit anzuwenden, insbesondere was die Zusammenarbeit zwischen den zuständigen Behörden und mit der Kommission und innerhalb der Gruppe für die Resilienz kritischer Einrichtungen anbelangt. Er trägt auch den Zuständigkeiten der einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union gemäß dem für diese geltenden Rechtsrahmen Rechnung. Die Krisenreaktionsmaßnahmen für kritische Infrastrukturen ergänzen andere Krisenmanagementmechanismen auf Unionsebene sowie auf nationaler und sektoraler Ebene, die die sektorübergreifende Koordinierung unterstützen.

Vertraulichkeit von Informationen

Der Konzeptentwurf für kritische Infrastrukturen berücksichtigt, wie wichtig es ist, dass die Vertraulichkeit von als Verschlusssache eingestuften und nicht als Verschlusssache eingestuften sensiblen Informationen in Bezug auf kritische Infrastrukturen und kritische Einrichtungen gewahrt bleibt.

---

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80).

2 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).

3 Mitteilung der Kommission „Ein Notfallplan für den Verkehr“ (COM(2022) 211 final).

4 Eingerichtet nach Artikel 19 der Durchführungsverordnung (EU) 2019/123 der Kommission vom 24. Januar 2019 zur Festlegung detaillierter Durchführungsbestimmungen für die Netzfunktionen des Flugverkehrsmanagements.

5 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

3. Einschlägige Akteure

Jeder Mitgliedstaat und die unter den Buchstaben a bis e genannten einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union entscheiden im Einklang mit den jeweils geltenden Vorschriften und Verfahren je nach betroffenem Sektor und Art des Vorfalls über die einschlägigen Akteure für jeden erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen.

a) Mitgliedstaaten

- zuständige Behörden (z. B. für kritische Infrastrukturen zuständige Behörden, einschlägige sektorale Behörden, gemäß Artikel 9 Absatz 2 der Richtlinie (EU) 2022/2557 benannte oder errichtete zentrale Anlaufstellen, gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2557 benannte oder eingerichtete Behörden);

- gegebenenfalls das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) gemäß Artikel 16 der Richtlinie (EU) 2022/2555;

- die in Artikel 14 der Richtlinie (EU) 2022/2555 genannte Kooperationsgruppe;

- gegebenenfalls andere Interessenträger einschließlich Einrichtungen oder Personen des Privatsektors, z. B. Betreiber kritischer Infrastrukturen, einschließlich der als kritisch eingestuften Einrichtungen;

- für die Resilienz kritischer Infrastrukturen zuständige Minister und/oder Minister, die für die Sektoren zuständig sind, die am stärksten von dem betreffenden erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffen sind.

b) der Rat

- der turnusmäßig wechselnde Vorsitz;

- die einschlägigen Arbeitsgruppen wie die Gruppe „Katastrophenschutz“ einschließlich der Untergruppe „Resilienz kritischer Einrichtungen“ (PROCIV-CER) und des Vorsitzes der einschlägigen Arbeitsgruppe(n) je nach betroffenem Sektor und Art des Vorfalls, wie die Horizontale Gruppe „Fragen des Cyberraums“ und die Horizontale Gruppe „Stärkung der Resilienz und Abwehr hybrider Bedrohungen“;

- AStV, das Politische und Sicherheitspolitische Komitee und die IPCR-Regelung, die alle vom Generalsekretariat des Rates unterstützt werden.

c) die Kommission, einschließlich Expertengruppen der Kommission

- benannte federführende Dienststelle (je nach betroffenem Sektor), die vom ERCC als rund um die Uhr operierendes Zentrum für die Krisenbewältigung und von der Generaldirektion Migration und Inneres als der in diesem Bereich zuständigen Dienststelle unterstützt wird, und bei einem sektorübergreifenden Vorfall die Generaldirektion Migration und Inneres sowie andere einschlägige Dienststellen der Kommission;

- die Generaldirektion Kommunikation und der Sprecherdienst;

- die Generaldirektion HERA, Europäische Behörde für die Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen;

- die durch die Richtlinie (EU) 2022/2557 eingesetzte Gruppe für die Resilienz kritischer Einrichtungen unter dem Vorsitz eines Vertreters der Kommission (Generaldirektion

Migration und Inneres) und gegebenenfalls anderer einschlägiger Expertengruppen und -ausschüsse;

- das im Rahmen des Katastrophenschutzverfahrens der Union (UCPM) durch den Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates[6] eingerichtete ERCC (rund um die Uhr operierende Plattform für das Management von Notsituationen im Rahmen des Katastrophenschutzverfahrens der Union in der Generaldirektion Europäischer Katastrophenschutz und humanitäre Hilfe);

- die in Artikel 14 der Richtlinie (EU) 2022/2555 genannte Kooperationsgruppe;

- das Zentrum für Cyberlageerfassung und -analyse;

- der in Artikel 4 der Richtlinie (EU) 2022/2371 genannte Gesundheitssicherheitsausschuss[7];

- das Generalsekretariat der Kommission (ARGUS-Sekretariat) und der (stellvertretende) Generalsekretär (ARGUS-Verfahren), Generaldirektion Humanressourcen (Direktion Sicherheit);

- andere einschlägige Expertengruppen der Kommission, die die Kommission bei der Koordinierung von Maßnahmen in Not- oder Krisensituationen unterstützen;

- andere Krisenmanagementnetze, einschließlich sektoraler Netze (z. B. Netz der von der Generaldirektion Mobilität und Verkehr verwalteten nationaler Verkehrskontaktstellen, der interinstitutionelle Krisenstab für Cybersicherheit[8], das Krisenkoordinierungsgremium für die Europäische Luftfahrt);

- die Präsidentin und/oder der/die zuständige Vizepräsident/in bzw. das bevollmächtigte Kommissionsmitglied.

d) EAD

- Single Intelligence Analysis Capability (Einheitliches Analyseverfahren, SIAC), bestehend aus dem Zentrum der Europäischen Union für Informationsgewinnung und Lageerfassung (IntCen) und die Abteilung Aufklärung des Militärstabs der EU (EUMS Int);

- das Krisenreaktionszentrum (CRC);

- der Hohe Vertreter der Union für Außen- und Sicherheitspolitik/Vizepräsident der Europäischen Kommission.

e) relevante Einrichtungen und Stellen der Union sowie einschlägige Agenturen der Union wie Europol, je nach betroffenem Bereich[9].

---

[6] 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).

[7] Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26).

[8] Eine informelle Gruppe, in der die zuständigen Kommissionsdienststellen, der EAD, die Agentur der Europäischen Union für Cybersicherheit (ENISA), das CERT-EU und Europol unter dem gemeinsamen Vorsitz der Generaldirektion Kommunikationsnetze, Inhalte und Technologien und des EAD vertreten sind.

[9] Wie Europol; Bereich Verkehr: die Agentur der Europäischen Union für Flugsicherheit (EASA), die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA), die Europäische Eisenbahnagentur (ERA); Bereich Gesundheit: das Europäisches Zentrum für die Prävention und die Kontrolle von Krankheiten (ECDC) und die Europäische Arzneimittel-Agentur (EMA); Bereich Energie: die Agentur für die Zusammenarbeit der

4. Zusammenspiel mit anderen einschlägigen Krisenbewältigungsmechanismen und -instrumenten

Der Konzeptentwurf für kritische Infrastrukturen ist ein flexibles Instrument, mit dem verschiedene Maßnahmen erfasst werden, die teilweise oder vollständig unter Rückgriff auf unterschiedliche bestehende Regelungen erfolgen könnten, je nach Art und Schwere des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen und der Notwendigkeit einer operativen, strategischen/politischen Koordinierung.

a) das Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen[10] (im Folgenden „EU-Protokoll“)

Das EU-Protokoll gilt im Falle hybrider Bedrohungen[11] und enthält eine Übersicht über die Verfahren und Instrumente, die im Falle solcher Bedrohungen oder Kampagnen Anwendung finden.

Im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen mit hybrider Dimension gilt das EU-Protokoll gegebenenfalls ergänzend zum Konzeptentwurf für kritische Infrastrukturen, z. B. für spezifische Informationen, Analysen oder die Kommunikation über hybride Aspekte des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen und in Bezug auf die Zusammenarbeit mit externen Partnern.

b) Konzeptentwurf zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes

Dieser Konzeptentwurf beschäftigt sich mit Sicherheitsvorfällen großen Ausmaßes, die so große Störungen hervorrufen, dass der betroffene Mitgliedstaat sie allein nicht bewältigen kann, oder die so weitreichende und beträchtliche Auswirkungen von technischer oder politischer Tragweite auf zwei oder mehr Mitgliedstaaten oder EU-Organe haben, dass rasch koordinierte Maßnahmen zu treffen sind und auf Unionsebene politisch reagiert werden muss.

Im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen, der mit einem Cybersicherheitsvorfall großen Ausmaßes zusammenfällt oder damit in Zusammenhang zu stehen scheint, legen die zuständigen Arbeitsgruppen des Rates eine angemessene Koordinierung auf operativer Ebene fest, beispielsweise mit EU-CyCLONe oder durch eine gemeinsame Sitzung der Gruppe für die Resilienz kritischer Einrichtungen mit der Kooperationsgruppe. Zweck der Koordinierung ist festzustellen, welche Akteure, Instrumente oder Mechanismen am wirksamsten dazu beitragen könnten, auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen zu reagieren, wobei Doppelarbeit und parallele Arbeit zu vermeiden sind.

Energieregulierungsbehörden (ACER) Bereich Weltraum: die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), Lebensmittelsektor: Europäische Behörde für Lebensmittelsicherheit (EFSA) Auf See: Europäische Fischereiaufsichtsagentur (EFCA) Bereich Cybervorfälle: die Agentur der Europäischen Union für Cybersicherheit (ENISA), Computer Security Incident Response Teams (Reaktionsteam für Computersicherheitsverletzungen, CSIRT), das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU).

[10] Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

[11] Hybride Bedrohungen können als Mischung von Zwang und Unterwanderung und von konventionellen und unkonventionellen Methoden beschrieben werden, auf die staatliche oder nichtstaatliche Akteure in koordinierter Weise zurückgreifen können, um bestimmte Ziele zu verfolgen, ohne dabei die Schwelle eines offiziell erklärten Kriegs zu erreichen, siehe EU-Protokoll über hybride Bedrohungen.

c) Katastrophenschutzverfahren der Union und Zentrum für die Koordination von Notfallmaßnahmen

Im Einklang mit dem Beschluss Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union werden operative Reaktionen im Rahmen des Katastrophenschutzverfahrens der Union auf eingetretene oder unmittelbar bevorstehende Naturkatastrophen und vom Menschen verursachte Katastrophen innerhalb und außerhalb der Union (einschließlich die kritische Infrastruktur betreffende) vom ERCC, dem Zentrum für die Koordination von Notfallmaßnahmen, geleitet, der einzigen rund um die Uhr einsatzbereiten operativen Plattform der Kommission zur Krisenbewältigung. In solchen Fällen kann das ERCC Frühwarnungen, Meldungen, Analysen erstellen und den Informationsaustausch sowie im Falle einer Aktivierung des Katastrophenschutzverfahrens der Union durch einen Mitgliedstaat die Entsendung von operativer Hilfe und Experten in die betroffenen Gebiete unterstützen. Das ERCC kann darüber hinaus die sektorale und sektorübergreifende Koordinierung sowohl auf Unionsebene als auch zwischen der Union und den zuständigen nationalen Behörden, einschließlich der für den Katastrophenschutz und die Resilienz kritischer Infrastrukturen zuständigen Behörden, erleichtern.

d) andere sektorale oder sektorübergreifende Mechanismen und Instrumente

Der Konzeptentwurf für kritische Infrastrukturen überschneidet sich nicht mit anderen sektoralen oder sektorübergreifenden Krisenbewältigungsinstrumenten oder Koordinierungsmechanismen. Sind solche Instrumente oder Mechanismen in dem betroffenen Sektor bereits vorhanden, kann dieser Konzeptentwurf für kritische Infrastrukturen innerhalb seines Anwendungsbereichs als ergänzendes Instrument zu den sektoralen oder sektorübergreifenden Instrumenten oder Mechanismen verwendet werden, ersetzt diese jedoch nicht. Es gilt, die notwendige Koordinierung zwischen den verschiedenen Akteuren sicherzustellen, um solche Überschneidungen zu vermeiden. Dies könnte beispielsweise im Rahmen des internen Krisenkoordinierungsprozesses der Kommission ARGUS, unterstützt durch das ERCC, und/oder IPCR-Koordinierungssitzungen erreicht werden.

TEIL II: INFORMATIONSAUSTAUSCH UND KOORDINIERTE REAKTION

Die nachstehend beschriebenen Maßnahmen umfassen Formen der Zusammenarbeit, d. h. den Informationsaustausch, die koordinierte Kommunikation und Reaktion. Diese Struktur entspricht den Modalitäten der Integrierten EU-Regelung für die politische Reaktion auf Krisen (IPCR) und berücksichtigt im weiteren Sinne den potenziellen Einsatz der auf EU-Ebene bereits bestehenden Krisenkoordinierungsmechanismen. Diese Struktur zeigt, wie sich diese Formen der Zusammenarbeit integrieren würden, sofern sie genutzt werden. Die meisten dieser Maßnahmen können jedoch auch eigenständig ergriffen werden: Sie hängen nicht von der Anwendung dieser Regelung ab, sondern ergänzen sie. Die Maßnahmen werden in chronologischer Reihenfolge dargestellt, wobei zu berücksichtigen ist, dass in einem Krisenfall großen Ausmaßes, die einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen darstellt, mehrere Maßnahmen gleichzeitig und durchgängig durchgeführt werden können.

1. INFORMATIONSAUSTAUSCH

a) Operative Ebene

Die von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten wenden ihre eigenen Notfallmaßnahmen an, sorgen für die Koordinierung mit

den einschlägigen nationalen Krisenmanagementmechanismen und beziehen gegebenenfalls alle einschlägigen nationalen, regionalen und lokalen Akteure ein.

Soweit dies für die Katastrophenschutzhilfe erforderlich ist, wird die Koordinierung zwischen den Mitgliedstaaten und der Kommission über das ERCC im Rahmen des Katastrophenschutzverfahrens der Union sichergestellt.

i) Informationsaustausch und Meldung durch die zuständigen nationalen Behörden

Zusätzlich zu den Melde- und Informationspflichten gemäß Artikel 15 der Richtlinie (EU) 2022/2557 teilen die für kritische Infrastrukturen zuständigen nationalen Behörden in den von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten den turnusmäßig wechselnden Vorsitz des Rates und der Kommission über ihre zentralen Anlaufstellen unverzüglich die einschlägigen Informationen mit, die sie von Betreibern kritischer Infrastrukturen, von kritischen Einrichtungen oder aus anderen Quellen erhalten haben, und unterrichten sie über aktivierte Krisenmanagementmechanismen. Das ERCC gewährleistet für die Kommission rund um die Uhr eine operierende Kontaktstelle und Kapazitäten und koordiniert, überwacht und unterstützt in Echtzeit die Reaktion auf Notfälle auf Unionsebene und dient den Mitgliedstaaten und der Kommission als operierende Plattform zur Krisenbewältigung und fördert einen sektorübergreifenden Ansatz für das Katastrophenmanagement.

Ein solcher Informationsaustausch betrifft die Art des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen, seine Ursache, die festgestellten oder geschätzten Auswirkungen der Störung auf kritische Infrastrukturen und die Erbringung wesentlicher Dienste, die Folgen des Sicherheitsvorfalls über Sektoren und Grenzen hinweg und die Abhilfemaßnahmen, die auf nationaler Ebene oder mit den jeweiligen Mitgliedstaaten und der Kommission im Rahmen bestehender Vereinbarungen, z. B. die Vereinbarungen über den Informationsaustausch gemäß den Artikeln 9 und 15 der Richtlinie (EU) 2022/2557 geplant sind oder bereits getroffen wurden. Diese Meldung sollte nicht dazu führen, dass Ressourcen kritischer Infrastrukturen oder in einigen Fällen die eines Mitgliedstaats durch Maßnahmen im Zusammenhang mit dem Umgang mit Sicherheitsvorfällen, denen Vorrang einzuräumen ist, abgezweigt werden.

Zur Gewährleistung von Folgemaßnahmen unterrichten das ERCC oder die benachrichtigten Kommissionsdienststellen, die für den jeweiligen Sektor bzw. die Sektoren zuständig sind, in dem/denen der erhebliche Sicherheitsvorfall bei kritischen Infrastrukturen eintrat, die Kontaktstelle in der Generaldirektion Migration und Inneres und das Generalsekretariat der Kommission. Falls nicht bereits geschehen, beginnt das ERCC zwischenzeitlich Beobachtungsmaßnahmen, insbesondere falls das Katastrophenschutzverfahren der Union durch einen oder mehrere der betroffenen Mitgliedstaaten aktiviert wurde.

Wenn die Informationen Cybersicherheitsaspekte betreffen oder sich auf einen Cybersicherheitsvorfall beziehen könnten, tauscht die Kommission einschlägige Informationen mit EU-CyCLONe aus.

Die gemäß der Richtlinie (EU) 2022/2557 zuständigen nationalen Behörden sollten im Zusammenhang mit Cybersicherheitsvorfällen und Sicherheitsvorfällen, die kritische Einrichtungen betreffen, nach Maßgabe der Richtlinie (EU) 2022/2555 mit den zuständigen Behörden unverzüglich zusammenarbeiten und Informationen austauschen, unter anderem auch zu den von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen und physischen Maßnahmen.

Im maritimen Bereich sollten die zuständigen nationalen Behörden die Möglichkeit prüfen, den gemeinsamen Informationsraum (CISE) zu nutzen, um unverzüglich Informationen auszutauschen.

ii) Organisation von Sachverständigensitzungen

Die Kommission beruft so bald als möglich die Gruppe für die Resilienz kritischer Einrichtungen ein, um den Austausch einschlägiger Informationen zwischen den für kritische Infrastrukturen zuständigen nationalen Behörden und den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union über den Vorfall (Art, Ursache, Auswirkungen und Folgen über Sektoren und Grenzen hinweg) und über Reaktionsmaßnahmen, einschließlich Abhilfemaßnahmen und technischer Unterstützung für die betroffenen Mitgliedstaaten, zu erleichtern. Je nach Schwere des Sicherheitsvorfalls werden die zuständigen Kommissionsdienststellen eng in die Sitzung der Gruppe für die Resilienz kritischer Einrichtungen einbezogen, um die im Rahmen bestehender sektoraler Instrumente erfassten Informationen auszutauschen. Bei Sicherheitsvorfällen mit einer Kombination sowohl cyberbezogener als auch physischer, nicht cyberbezogener Aspekte unterrichten und konsultieren und unterrichten sich die zuständigen Kommissionsdienststellen, das CERT-EU und erforderlichenfalls der EAD so bald als möglich im Rahmen des Krisenstabs für Cybersicherheit, ebenso werden die jeweiligen Vorsitzenden der in Artikel 14 der Richtlinie (EU) 2022/2555 genannten Kooperationsgruppe und gegebenenfalls EU-CyCLONe bezüglich der Notwendigkeit von Koordinierungsmaßnahmen informiert. Im Einvernehmen mit den jeweiligen Vorsitzenden kann die Kommission (Generaldirektion Migration und Inneres und Generaldirektion Kommunikationsnetz, Inhalte und Technologien) eine gemeinsame Sitzung der Gruppe für die Resilienz kritischer Einrichtungen mit der Kooperationsgruppe vorschlagen, um eine gemeinsame Lageerfassung und entsprechende Reaktionen zu koordinieren.

Bei einem erheblichen sektorübergreifenden Sicherheitsvorfall bei kritischen Infrastrukturen, der eine Folgenbewältigung auf Unionsebene erfordert oder voraussichtlich erfordern wird, kann die Kommission sektorübergreifende Koordinierungssitzungen mit allen einschlägigen Interessenträgern einberufen.

Ist ein Drittstaat ebenfalls von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffen, so konsultiert die Kommission die zuständige Behörde des betroffenen Drittstaats und kann sie zu einer Sitzung der Gruppe für die Resilienz kritischer Einrichtungen einladen.

iii) Unterstützung durch die Kommission und die Agenturen der Union

Gegebenenfalls legt Europol im Einklang mit seinem Mandat einen Lagebericht über Sicherheitsvorfälle auf Unionsebene vor. Andere Agenturen der Union übermitteln ihrer jeweiligen „Mutter"-Generaldirektion gegebenenfalls und im Einklang mit ihren jeweiligen Mandaten einschlägige Informationen, die zur Lageerfassung in Bezug auf den erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen oder zur koordinierten Reaktion darauf beitragen, die ihrerseits wiederum der Kommission Bericht erstattet (Generaldirektion Migration und Inneres als Vorsitz der Gruppe für die Resilienz kritischer Einrichtungen).

Die Kommission kann gegebenenfalls und im Einklang mit dem geltenden Rechtsrahmen einen Beitrag zur Lageerfassung unter Nutzung der Ressourcen des Weltraumprogramms der Union[12] wie Copernicus, Galileo und EGNOS leisten.

b) Strategische Ebene

i) Erstellung von Berichten zur Lageerfassung

Auf der Grundlage von Informationen, die von den zuständigen nationalen Behörden in einer Sitzung der Gruppe für die Resilienz kritischer Einrichtungen oder gemeinsamen Sitzungen mit einschlägigen Dienststellen, Expertengruppen oder Netzen ausgetauscht werden, erstellt die Kommission auf Basis der Beiträge der zuständigen nationalen Behörden und anderer verfügbarer Informationen einen Bericht zur Lageerfassung.

Dieser Bericht sollten gegebenenfalls den Ergebnissen der einschlägigen Risikobewertungen, -evaluierungen und -szenarien auf EU-Ebene unter dem Gesichtspunkt der Cybersicherheit Rechnung tragen, darunter jenen, die von der Kommission, dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik und der Kooperationsgruppe durchgeführt wurden.

Im Falle der Aktivierung der IPCR-Regelung kann dieser Bericht zur Integrierten Lageerfassungsanalyse (ISAA) beitragen, die von den Kommissionsdienststellen und dem EAD erstellt wird.

Mithilfe des SIAC wird gegebenenfalls eine aktuelle erkenntnisgestützte Bewertung des Sicherheitsvorfalls vorgelegt.

ii) Aktivierung der Krisenkoordinierungsmechanismen der Union und Nutzung von Unionsinstrumenten

Das ERCC beginnt mit der Unterstützung der Lageerfassung im Zusammenhang mit dem Sicherheitsvorfall, sofern dies relevant ist, insbesondere wenn mit dem Ereignis das Katastrophenschutzverfahren der Union ausgelöst wird.[13] Darüber hinaus können die betroffenen Mitgliedstaaten Satellitenbilder ihres Hoheitsgebiets über den Copernicus-Katastrophen- und Krisenmanagementdienst anfordern.

Wenn es für den Informationsaustausch zwischen der Kommission und dem EAD sowie den einschlägigen Agenturen der Union zweckmäßig erscheint, leitet die federführende Generaldirektion oder die Generaldirektion Migration und Inneres in Abstimmung mit dem Generalsekretariat den internen Krisenkoordinierungsprozess der Kommission ARGUS Phase I ein, indem sie ein Ereignis im Argus-IT-Instrument öffnet.

Der turnusmäßig wechselnde Vorsitz des Rates der Union kann die IPCR-Regelung im Informationsaustausch-Modus aktivieren, was dazu führt, dass die Kommission und der EAD ISAA-Berichte mit Beiträgen der zuständigen nationalen Behörden und gegebenenfalls anderer Quellen ausarbeiten. Auch ohne Aktivierung der IPCR-Regelung kann unter bestimmten Bedingungen eine Beobachtungswebsite auf der IPCR-Internet-Plattform vom turnusmäßig wechselnden Ratsvorsitz oder von der Kommission eingerichtet werden.

---

[12] 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).

[13] Wie die Veröffentlichung von Medienbeobachtungsprodukten, Katastrophenschutzmitteilungen, Kurzanalysen, ECHO Daily Maps, ECHO Daily Flashes und anderen maßgeschneiderten Produkten.

Andere (sektorale) Krisenbewältigungsmechanismen und -instrumente der Union können gegebenenfalls nach Maßgabe der jeweiligen Verfahren aktiviert werden. Die Kommission gewährleistet die Koordinierung zwischen diesen Mechanismen und Instrumenten.

Fällt der physische Sicherheitsvorfall mit einem Cybersicherheitsvorfall großen Ausmaßes im Sinne von Artikel 6 Nummer 7 der Richtlinie (EU) 2022/2555 zusammen bzw. scheint damit in Zusammenhang zu stehen, so kann der turnusmäßig wechselnde Ratsvorsitz den Cyber Blueprint dazu nutzen, eine angemessene Koordinierung auf operativer Ebene festzulegen, an der unter anderem EU-CyCLONe und die Gruppe für die Resilienz kritischer Einrichtungen beteiligt sind.

iii) Koordinierung der Unterrichtung der Öffentlichkeit

Die von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten stimmen ihre Unterrichtung der Öffentlichkeit über die Krise so weit wie möglich ab, wobei sie nationale Zuständigkeiten achten. Gegebenenfalls kann das im Rahmen der IPCR-Regelung eingerichtete informelle Krisenkommunikationsnetz einbezogen werden.

Auf der Grundlage der gemeinsamen Lageerfassung stimmen die Gruppe für die Resilienz kritischer Einrichtungen und die betroffenen Mitgliedstaaten gegebenenfalls die Ausarbeitung von Informationen zur Unterrichtung der Öffentlichkeit miteinander ab.

Europol und andere einschlägige Agenturen der Union koordinieren ihre Öffentlichkeitsarbeit auf der Grundlage einer gemeinsamen Lageerfassung mit dem Sprecherdienst der Kommission.

Wenn der erhebliche Sicherheitsvorfall bei kritischen Infrastrukturen externe oder hybride Aspekte oder Aspekte der Gemeinsamen Sicherheits- und Verteidigungspolitik umfasst, wird die Unterrichtung der Öffentlichkeit mit dem EAD und dem Sprecherdienst der Kommission im Einklang mit dem Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen[14] koordiniert.

2. REAKTION (UNTER EINBEZIEHUNG DER IM ABSCHNITT INFORMATIONSAUSTAUSCH BESCHRIEBENEN DURCHGÄNGIGEN MAßNAHMEN UND DER ZUSÄTZLICHEN MAßNAHMEN AUF STRATEGISCHER/POLITISCHER EBENE)

a) Strategische Ebene

i) Fortlaufende Erstellung von Lageberichten

Die Ratsgruppe „Katastrophenschutz – Resilienz kritischer Einrichtungen“ (PROCIV-CER) wird über die Erstellung eines politisch-strategischen Lageberichts (z. B. die ISAA im Falle einer Aktivierung der IPCR-Regelung oder den von der Kommission erstellten gemeinsamen Lagebericht) unterrichtet und bereitet die Sitzung des AStV, falls dieser noch nicht einberufen wurde, oder gegebenenfalls die Sitzung des Politischen und Sicherheitspolitischen Komitees vor.

Im Rahmen des SIAC werden die Kontakte zu den Nachrichtendiensten der Mitgliedstaaten intensiviert, die Informationen aus allen Quellen zusammengefasst und eine Analyse und eine Bewertung des Sicherheitsvorfalls sowie erforderlichenfalls regelmäßige Aktualisierungen erstellt.

ii) Vollständige Aktivierung der Krisenkoordinierungsmechanismen der Union und Nutzung von Unionsinstrumenten

[14] Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

Falls die Präsidentin der Kommission den internen Krisenkoordinierungsprozess der Kommission ARGUS Phase II in Gang setzt, werden kurzfristig Sitzungen des Krisenkoordinierungsausschusses, an denen die zuständigen Dienststellen, Agenturen und gegebenenfalls der EAD beteiligt sind, einberufen, um die Koordinierung in Bezug auf alle Aspekte des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen zu gewährleisten.

Sollte die IPCR-Regelung vom Ratsvorsitz vollständig aktiviert werden:

- beruft der turnusmäßig wechselnde Ratsvorsitz ein zeitnahes informelles Rundtischgespräch ein, an dem die einschlägigen nationalen, europäischen und internationalen Akteure teilnehmen, wobei der Vertreter der Kommission, der als Vorsitzender der Gruppe für die Resilienz kritischer Einrichtungen (Generaldirektion Migration und Inneres) fungiert, über die zuvor einberufene(n) Sitzung(en) der Gruppe berichten kann; gegebenenfalls kommen andere Kommissionsdienststellen und der EAD ergänzend hinzu;

- das SIAC und die einschlägigen Agenturen der Union können ersucht werden, im Rahmen der Gespräche aktuelle Informationen über die Lage in Bezug auf den erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen vorzulegen.

Die federführende Dienststelle der ISAA (federführende Dienststelle der Kommission oder der EAD) erstellt den ISAA-Bericht mit Beiträgen der zuständigen Kommissionsdienststellen, der einschlägigen Ämter, Einrichtungen und sonstigen Stellen der Union und der zuständigen nationalen Behörden. Die Mitgliedstaaten werden ersucht, über die IPCR-Internet-Plattform Beiträge zu den ISAA-Berichten zu leisten.

Bei einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen mit internationaler Sicherheitsrelevanz können die Kommissionsdienststellen und der EAD einen strukturierten Dialog zwischen der EU und der NATO über Resilienz einberufen, um zur gemeinsamen Lageerfassung und zum Informationsaustausch über die von der Union bzw. der NATO ergriffenen Maßnahmen beizutragen.

iii) Unterrichtung der Öffentlichkeit

Der Rat arbeitet gemeinsame Botschaften für die Unterrichtung der Öffentlichkeit aus. Dabei kann er von dem im Rahmen der IPCR eingerichteten informellen Krisenkommunikationsnetz unterstützt werden. Der Sprecherdienst der Kommission bereitet gegebenenfalls auch Botschaften für die Unterrichtung der Öffentlichkeit aus.

Wenn der erhebliche Sicherheitsvorfall bei kritischen Infrastrukturen externe oder hybride Aspekte oder Aspekte der Gemeinsamen Sicherheits- und Verteidigungspolitik umfasst, wird die Unterrichtung der Öffentlichkeit mit dem EAD und dem Sprecherdienst der Kommission abgestimmt.

iv) Unterstützung der Mitgliedstaaten und wirksame Reaktion

Der turnusmäßig wechselnde Vorsitz kann eine Sitzung des PROCIV-CER einberufen, um die Tätigkeiten im Rahmen der IPCR-Regelung zu unterstützen, sofern diese Regelung aktiviert ist.

Die von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten können über die Gruppe für die Resilienz kritischer Einrichtungen die technische Unterstützung anderer Mitgliedstaaten oder der einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union anfordern, z. B. spezifisches Fachwissen zur Eindämmung nachteiliger Auswirkungen des erheblichen Sicherheitsvorfalls.

Die von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten können auch die Kommission oder einschlägige Agenturen der Union um

technische und/oder finanzielle Unterstützung ersuchen. In Abstimmung mit den zuständigen Agenturen der Union bewertet die Kommission eine mögliche Unterstützung und aktiviert gegebenenfalls im Einklang mit ihren jeweiligen Verfahren technische Abhilfemaßnahmen auf Unionsebene und koordiniert die technischen Kapazitäten, die erforderlich sind, um die Auswirkungen des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen zu beenden oder zu verringern.

Insbesondere im Rahmen des Katastrophenschutzverfahrens der Union könnten die betroffenen Länder Unterstützung über das Gemeinsame Kommunikations- und Informationssystem für Notfälle (CECIS) anfordern, woraufhin das ERCC die Bereitstellung von Unterstützung durch die Mitgliedstaaten und die Teilnehmerstaaten des Katastrophenschutzverfahrens der Union sowie über rescEU koordinieren würde.

Im Rahmen ihrer jeweiligen Mandate und auf Ersuchen unterstützen Europol und andere einschlägige Agenturen der Union die von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten bei der Untersuchung des Sicherheitsvorfalls.

b) Politische Ebene

Der Ratsvorsitz könnte prüfen, ob es notwendig ist, IPCR-Rundtischgespräche, Sitzungen von Ratsarbeitsgruppen, den AStV, den Ministerrat und/oder Gipfeltreffen einzuberufen, um sich über die mögliche Ursache und die erwarteten Folgen des schwerwiegenden Sicherheitsvorfalls bei kritischen Infrastrukturen für die Mitgliedstaaten und die Union auszutauschen, gemeinsame Leitlinien festzulegen und die erforderlichen Maßnahmen zu ergreifen, um die von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten zu unterstützen und dessen Auswirkungen abzumildern.

Abbildung 1: Schematischer Überblick über den Konzeptentwurf für kritische Infrastrukturen

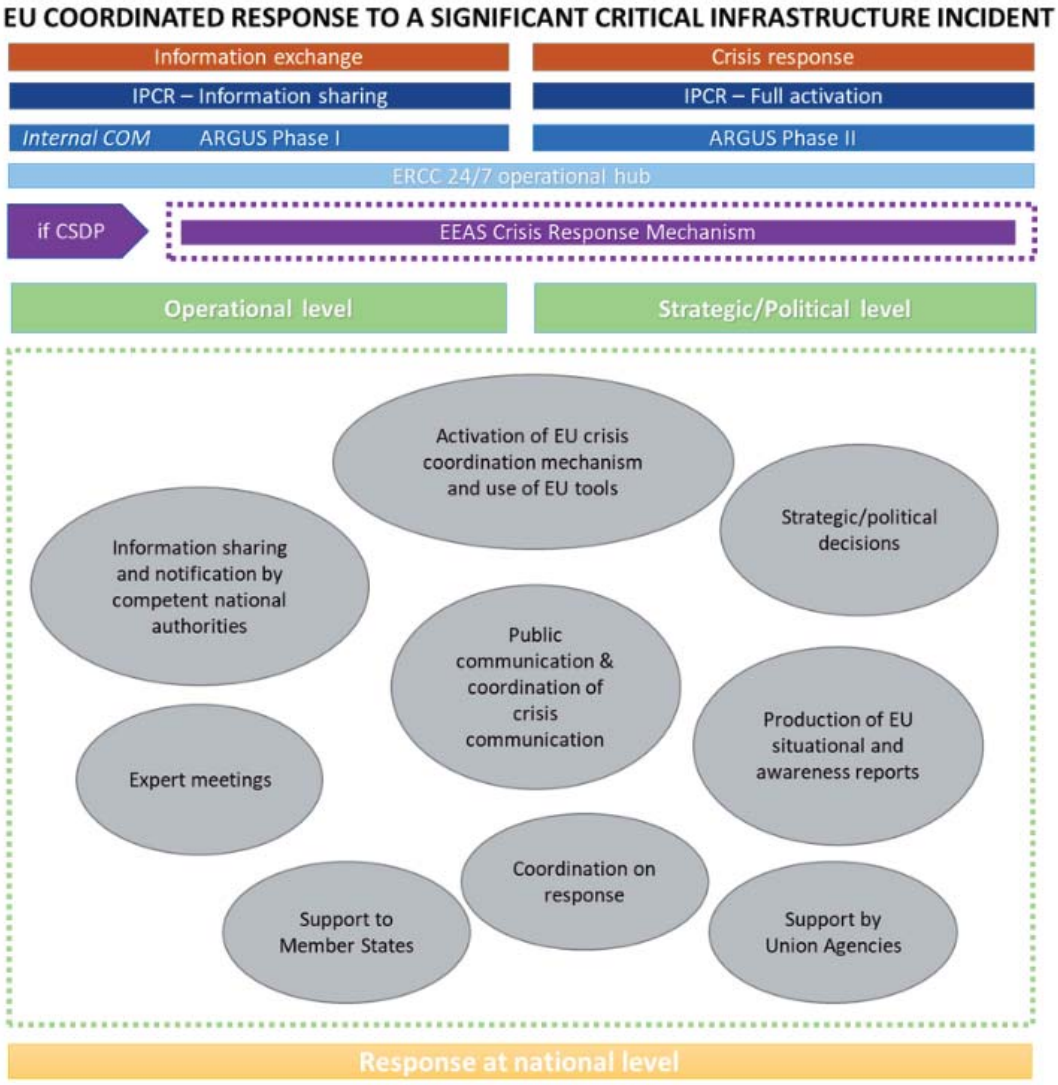

Abbildung 2: Beschluss über den Konzeptentwurf für kritische Infrastrukturen