Rat der
Europäischen Union

Brüssel, den 17. Mai 2021
(OR. en)

8640/21

Interinstitutionelles Dossier:
2020/0359(COD)

LIMITE

CYBER 138
JAI 523
DATAPROTECT 125
TELECOM 194
MI 332
CSC 190
CSCI 78

VERMERK

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Betr.:	Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 – Fortschrittsbericht

Der vorliegende Bericht wurde unter Verantwortung des Vorsitzes erstellt; er soll speziellen Fragen oder weiteren Beiträgen einzelner Mitgliedstaaten nicht vorgreifen. In dem Bericht wird dargelegt, welche Arbeit in den Vorbereitungsgremien des Rates bereits geleistet worden ist und wie weit die Prüfung des eingangs genannten Vorschlags fortgeschritten ist. Der Rat wird ersucht, den Bericht zur Kenntnis zu nehmen.

I. EINLEITUNG

1. Am 16. Dezember 2020 hat die Kommission den Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (überarbeitete NIS-Richtlinie oder „NIS 2“)[1] angenommen, um die derzeitige Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie)[2] zu ersetzen. Der Vorschlag war eine der Maßnahmen, die in der Mitteilung „Die Cybersicherheitsstrategie der EU für die digitale Dekade“[3] angekündigt wurden, um die Abwehrfähigkeit gegenüber Cyberbedrohungen zu stärken und zu gewährleisten, dass Bürgerinnen und Bürger sowie Unternehmen von vertrauenswürdigen digitalen Technologien profitieren können.

2. Ziel des Vorschlags ist es, die Resilienz und die Kapazitäten zur Reaktion auf Sicherheitsvorfälle öffentlicher und privater Einrichtungen, zuständiger Behörden und der Union als Ganzer auf der Grundlage von Artikel 114 AEUV weiter zu verbessern. Mit dem Vorschlag wird der Anwendungsbereich der derzeitigen NIS-Richtlinie erheblich erweitert; so wird die Sicherheit von Lieferketten angegangen, werden die Anforderungen an die Cybersicherheit erhöht und Meldepflichten vereinheitlicht und gleichzeitig strengere Aufsichts- und Durchsetzungsmaßnahmen eingeführt. Er enthält ferner Bestimmungen zum Informationsaustausch und zum Cybersicherheitskrisenmanagement auf nationaler Ebene und auf Unionsebene. Im Vorschlag ist auch die Regulierung der Datenbanken der Domänenregistrierungsstellen vorgesehen.

---

1 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (COM(2020) 823 final).

2 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

3 Dok. 14133/20.

3. Im Europäischen Parlament ist der Ausschuss für Industrie, Forschung und Energie (ITRE) für den Vorschlag zuständig; dem Ausschuss für auswärtige Angelegenheiten (AFET), dem Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO), dem Ausschuss für Verkehr und Tourismus (TRAN) und dem Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (Liebe) wird er zur Stellungnahme vorgelegt. Berichterstatter für das Dossier ist Bart Groothuis (Renew, Niederlande). Der portugiesische Vorsitz hat am 29. Januar 2021 mit dem Berichterstatter des ITRE-Ausschusses einen informellen Gedankenaustausch über das Dossier geführt. Am 12. April 2021 hat der Vorsitz Gespräche mit Vertretern des Verfassers der IMCO-Stellungnahme, Morten Lokkegaard (Renew, Dänemark), aufgenommen. Am 16. April hat der portugiesische Vorsitz mit dem Leiter und anderen Mitgliedern des ITRE-Ausschusses einen informellen Gedankenaustausch über das Dossier geführt. Der Berichterstatter hat seinen Berichtsentwurf am 3. Mai 2021 im ITRE-Ausschuss vorgelegt[4].

4. Der Europäische Wirtschafts- und Sozialausschuss hat seine Stellungnahme am 28. April 2021 abgegeben[5].

5. Am 3. Februar 2021 hat der Ausschuss der Ständigen Vertreter beschlossen, den Europäischen Ausschuss der Regionen um Stellungnahme zu dem Vorschlag zu ersuchen[6]. Bislang hat der Europäische Ausschuss der Regionen noch keine Stellungnahme abgegeben.

6. Der Europäische Datenschutzbeauftragte hat seine Stellungnahme am 11. März 2021 abgegeben[7].

7. In seiner Erklärung[8] vom 26. Februar 2021 hat der Europäische Rat die beiden gesetzgebenden Organe ersucht, die Arbeit zügig voranzubringen, insbesondere in Bezug auf die überarbeitete Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-2-Richtlinie).

---

4 Dossier 2020/0359(COD).
5 Dok. TEN/730-EESC-2020.
6 Dok. 5573/21.
7 Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie.
8 https://www.consilium.europa.eu/de/press/press-releases/2021/02/26/statement-of-the-members-of-the-european-council-25-26-february-2021/

8. In seinen Schlussfolgerungen[9] vom 22. März 2021 zur Cybersicherheitsstrategie der EU für die digitale Dekade hat der Rat die Bedeutung eines umfassenden und horizontalen Ansatzes für die Cybersicherheit in der Union anerkannt, wobei die Zuständigkeiten und Bedürfnisse der Mitgliedstaaten sowie die Bedeutung der kontinuierlichen Unterstützung der technischen Hilfe und Zusammenarbeit beim Aufbau der Kapazitäten der Mitgliedstaaten uneingeschränkt respektiert werden. Unter Berücksichtigung der Entwicklung der Bedrohungslandschaft hat der Rat den auf der NIS-Richtlinie aufbauenden neuen Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union zur Kenntnis genommen und seine Unterstützung für die Stärkung und Harmonisierung der nationalen Cybersicherheitsrahmen und die nachhaltige Zusammenarbeit zwischen den Mitgliedstaaten bekräftigt. Ferner hat er die Notwendigkeit einer Angleichung und Verknüpfung der sektorspezifischen Rechtsvorschriften in diesem Bereich betont.

II. BERATUNGEN IN DEN VORBEREITUNGSGREMIEN DES RATES

9. Im Rat wird der Vorschlag von der Horizontalen Gruppe „Fragen des Cyberraums“ (im Folgenden „Gruppe“) geprüft. In der informellen Videokonferenz der Gruppe vom 17. Dezember 2020 hat die Kommission die neue Cybersicherheitsstrategie vorgestellt und den Vorschlag für die Überarbeitung der NIS-Richtlinie vorgelegt. Am 12. Januar 2021 hat sie ihn dann ausführlicher erläutert.

10. In der informellen Videokonferenz der Gruppe vom 19. Januar 2021 hat der portugiesische Vorsitz seine Vorgehensweise für die Beratungen über die NIS-2-Richtlinie skizziert. Der Vorsitz hat eine sorgfältige Prüfung des Vorschlags vorgesehen, um den wichtigen Neuerungen der überarbeiteten Richtlinie Rechnung zu tragen und den Delegationen die Möglichkeit zu geben, schriftlich Stellung zu nehmen und Fragen zu stellen, gefolgt von Klarstellungen seitens der Kommission.

[9] Dok. 6722/21.

11. Darüber hinaus hat die Gruppe über die Wechselwirkungen zwischen der überarbeiteten NIS-Richtlinie und den sektorspezifischen Rechtsvorschriften beraten, insbesondere mit der Richtlinie über die Resilienz kritischer Einrichtungen (Resilienzrichtlinie) und der Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA). Die Kommission (DG HOME) hat den neuen Vorschlag für die Resilienzrichtlinie vorgelegt und hervorgehoben, welche Elemente der Wechselwirkungen mit der NIS-2-Richtlinie besonders relevant sind. Die Gruppe hat sich in ihren Sitzungen ferner mit den Verbindungen zur vorgeschlagenen Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors („DORA-Verordnung“) befasst und dabei auf ein Diskussionspapier des Vorsitzes der (für die Verhandlungen über DORA zuständigen) Gruppe „Finanzdienstleistungen“ gestützt, ebenso wie mit einem Non-Paper zum Thema „Korrelation zwischen NIS-Behörden und zuständigen nationalen Behörden im Rahmen von DORA“, das im Rahmen einer Sitzung der Gruppe „Finanzdienstleistungen“ von drei Mitgliedstaaten vorgelegt wurde. Ferner hat der Vorsitzende in einer Sitzung der Gruppe „Katastrophenschutz“ über den Stand der Beratungen über die NIS-2-Richtlinie berichtet. Umgekehrt hat der Vorsitz seine Gruppe regelmäßig über den Fortgang der einschlägigen Beratungen in der Gruppe „Katastrophenschutz“ und der Gruppe „Finanzdienstleistungen“ über ihre jeweiligen Dossiers informiert und bekräftigt, dass die verschiedenen federführenden Ministerien auf nationaler Ebene eng zusammenarbeiten müssen.

12. Auf den informellen Videokonferenzen vom 2. und 9. Februar 2021 hat die Gruppe mit der Prüfung der ersten beiden Artikel („Gegenstand“ und „Anwendungsbereich“) und der Anhänge I und II der Vorschläge begonnen. Auf ihrem Treffen vom 2. Februar wurde die Gruppe von der Kommission und dem Vorsitz der NIS-Kooperationsgruppe über den Stand der Arbeit in der Kooperationsgruppe unterrichtet, auch über ihre Rolle bei der Erleichterung der Umsetzung der NIS-Richtlinie. Bei dieser Gelegenheit hat der Exekutivdirektor der ENISA das Arbeitsprogramm der Agentur vorgestellt, einschließlich Informationen über die NIS-Investitionsstudie der ENISA und ihre Rolle bei der Unterstützung der Mitgliedstaaten und der EU-Organe bei der Umsetzung von politischen Maßnahmen und Empfehlungen im Zusammenhang mit der NIS-Richtlinie. Während dieser Treffen wurden inhaltliche Beratungen über den Anwendungsbereich geführt und Fragen zur Verhältnismäßigkeit gestellt.

13. In der Sitzung der Gruppe vom 22. Februar 2021 hat die Kommission die Folgenabschätzung für die Überarbeitung der NIS-Richtlinie vorgelegt, und die Beratungen über den Vorschlag wurden mit den Artikeln 3 und 4 („Mindestharmonisierung“ und „Begriffsbestimmungen“) fortgesetzt.

14. Am 2. März 2021 wurde die Erstbewertung des Vorschlags in der Sitzung der Gruppe fortgeführt, wobei Artikel 5 und 6 („nationale Cybersicherheitsstrategie“ und „koordinierte Offenlegung von Schwachstellen und europäisches Schwachstellenregister“) umfassend erörtert wurden und die Kommission das Thema „koordinierte Offenlegung von Schwachstellen und europäisches Schwachstellenregister“ ausführlich erläutert hat.

15. Die Beratungen wurden in der Sitzung der Gruppe vom 9. März 2021 in Bezug auf die Artikel 7 bis 11 weitergeführt. Sie betreffen die nationalen Rahmen für das Cybersicherheitskrisenmanagement, die nationalen zuständigen Behörden und zentralen Anlaufstellen gemäß der überarbeiteten NIS-Richtlinie und die Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs), einschließlich ihrer Anforderungen, Aufgaben und Zusammenarbeit auf nationaler Ebene.

16. Im Rahmen ihrer außerordentlichen Sitzung vom 17. März 2021 hat die Gruppe die Artikel 12 bis 16 erörtert (Kapitel III über die „Zusammenarbeit“); diese betreffen die NIS-Kooperationsgruppe, das CSIRT-Netzwerk, das europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), den Bericht über den Stand der Cybersicherheit in der Union und die Frage der Peer Reviews. Insbesondere zu diesen Artikeln wurde eine Reihe von Fragen und Klarstellungen geäußert. Ferner wurde während dieser Sitzung Artikel 17 über „Governance“ behandelt. Darüber hinaus erläuterte der Leiter des Teams Prävention und Öffentlichkeitsarbeit des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3) der Europol den Standpunkt der Strafverfolgungsbehörden zur überarbeiteten NIS-Richtlinie.

17. In ihrer Sitzung vom 24. März 2021 hat sich die Gruppe mit Kapitel IV zum Risikomanagement und den Meldepflichten im Bereich Cybersicherheit befasst, und dabei insbesondere mit den Artikeln 18 („Risikomanagementmaßnahmen im Bereich der Cybersicherheit“), 19 („EU-weit koordinierte Risikobewertungen kritischer Lieferketten“) und 20 („Meldepflichten“). Letzterer gilt als eine der Kernbestimmungen der NIS-2-Richtlinie.

18. Im Rahmen ihrer Sitzung vom 14. April hat die Gruppe die Artikel 21 („Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung“), 22 („Normung“) und 23 („Datenbanken der Domänennamen und Registrierungsdaten“) sowie die nachfolgenden Artikel 24 und 25 („Gerichtliche Zuständigkeit und Registrierung“) erörtert. In dieser Sitzung wurde auch über die Kapitel V und VI („Informationsaustausch“ bzw. „Aufsicht und Durchsetzung“) beraten. Aufgrund des Umfangs und der Ausführlichkeit der Artikel 29 und 30 über die Aufsicht und Durchsetzung in Bezug auf wesentliche bzw. wichtige Einrichtungen haben die Mitgliedstaaten zahlreiche Bemerkungen abgegeben und Fragen gestellt. Ebenso wurden substanzielle Bemerkungen und Fragen zu den Artikeln 31, 32 und 33 über Geldbußen, Verstöße mit Verletzungen des Schutzes personenbezogener Daten und Sanktionen geäußert. Ferner haben die Mitgliedstaaten weitere Klarstellungen im Zusammenhang mit Artikel 34 über Amtshilfe erbeten.

19. Die Gruppe hat sich in ihrer Sitzung vom 19. April mit Kapitel VII über Übergangs- und Schlussbestimmungen (Artikel 35 bis 43) befasst, womit die Prüfung der Artikel abgeschlossen wurde.

20. In ihrer Sitzung vom 28. April 2021 hat die Gruppe die Erwägungsgründe erörtert und damit die vollständige Prüfung der Vorschlags abgeschlossen. Dies war die erste Präsenzsitzung der Gruppe, die während des portugiesischen Vorsitzes zur NIS-2-Richtlinie stattfand. Eine Entsprechungstabelle zwischen den Erwägungsgründen und den entsprechenden Artikeln des Wortlauts war bereits am 15. Februar 2021 von der Kommission übermittelt worden.

21. In ihrer Sitzung vom 5. Mai 2021 hat die Gruppe einen ersten Gedankenaustausch geführt, um mit der Ausarbeitung der Stellungnahme zu dem Dossier zu beginnen. Um Fortschritte bei dem Dossier zu erzielen, hat der Vorsitz beschlossen, den Ausarbeitungsprozess mit der Frage der Wechselwirkungen zwischen der überarbeiteten NIS-Richtlinie und den einschlägigen sektorspezifischen Rechtsvorschriften zu beginnen. Dieser Beschluss wurde auf der Grundlage der Beratungen im Rahmen der Prüfung des Dossiers in der Gruppe und der Tatsache getroffen, dass diese Frage von den Mitgliedstaaten bereits als wichtig eingestuft worden war, wie der spezifische diesbezügliche Verweis in den Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade vom 22. März zeigt. Die Mitgliedstaaten wurden aufgefordert, bis zum 14. Mai 2021 konkrete Textvorschläge zu dieser Frage vorzulegen.

22. Unter portugiesischem Vorsitz hat die Gruppe der Vorlage und der Prüfung des Vorschlags bisher 17 Sitzungen gewidmet. In den Beratungen haben einige Mitgliedstaaten Prüfungsvorbehalte zum gesamten Vorschlag oder Teilen davon eingelegt.

23. Der Vorsitz ist der Überzeugung, dass die Mitgliedstaaten durch die sorgfältige Prüfung der NIS-2-Richtlinie die Möglichkeit hatten, ausführliche Erläuterungen der Kommission zu den grundlegenden Änderungen der überarbeiteten Richtlinie zu erhalten und gleichzeitig ihre wichtigsten Anliegen in Bezug auf den Vorschlag zu äußern, wodurch die künftige Arbeit erleichtert und gestrafft wird, um rechtzeitig eine allgemeine Ausrichtung zu erreichen.

III. SACHFRAGEN

24. In den Beratungen der Gruppe haben die Mitgliedstaaten die überarbeitete NIS-Richtlinie im Großen und Ganzen begrüßt, jedoch eine Reihe von wichtigen Fragen und Bedenken vorgebracht, die in den Verhandlungen über den Vorschlag berücksichtigt werden sollten.

25. Eine der Fragen, die in den Beratungen immer wieder aufgeworfen wurde, betrifft die Frage der Wechselwirkungen zwischen der überarbeiteten NIS-Richtlinie und den sektorspezifischen Rechtsvorschriften. Während der bislang geführten Beratungen hat eine deutliche Mehrheit der Mitgliedstaaten erklärt, dass der überarbeitete Vorschlag unbedingt als horizontaler Rahmen für die Cybersicherheit in der EU betrachtet werden und als Grundnorm für die Mindestharmonisierung aller einschlägigen sektorspezifischen Rechtsvorschriften in diesem Bereich dienen sollte.

26. Zweitens wurden zahlreiche Bedenken in Bezug auf die erhebliche Ausweitung des Anwendungsbereichs der überarbeiteten NIS-Richtlinie geäußert, und zwar: die Frage, in welchem Umfang wesentliche und wichtige Einrichtungen in den Anwendungsbereich der Richtlinie fallen; die Zuständigkeiten der Mitgliedstaaten, wesentliche und wichtige Einrichtungen zu ermitteln; die Auswirkungen auf die Fähigkeit der zuständigen nationalen Behörden, diese Listen der Einrichtungen zu überwachen; die Besonderheiten der Anhänge, in denen die wesentlichen und wichtigen Einrichtungen, die in den Anwendungsbereich fallen, aufgeführt werden, beispielweise die umfassende Einbeziehung des Lebensmittel- und des Verkehrssektors ungeachtet ihrer Bedeutung für den jeweiligen Sektor; die Beschränkungen der Einführung eines Schwellenwerts für die Größe, insbesondere im Zusammenhang mit Einrichtungen, die mehr als eine Dienstleistung erbringen, oder mit Klein- und Kleinsteinrichtungen, die sehr stark von anderen Dienstleistungen abhängen, was zu Kaskadeneffekten führen könnte.

27. Drittens wurde der Schwellenwert als alleiniges Kriterium für die Ermittlung wesentlicher und wichtiger Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen sollen, von einigen Mitgliedstaaten zur Sprache gebracht, die einen kumulativ risikobasierten Ansatz oder zusätzliche, auf nationaler Ebene einzuführende qualitative Kriterien vorziehen würden. Die Kommission hat deutlich gemacht, dass das Kriterium des Schwellenwerts das geeignetste, wenn vielleicht auch nicht perfekte Maß ist, um den ineffizienten Ermittlungsprozess der derzeitigen NIS-Richtlinie anzugehen und somit eine Fragmentierung bei der Anwendung des künftigen Instruments zu vermeiden.

28. Einige Mitgliedstaaten haben die Frage aufgeworfen, ob es nach der Rechtsgrundlage für den Binnenmarkt (Artikel 114 AEUV) zulässig ist, die öffentliche Verwaltung in den Anwendungsbereich der überarbeiteten Richtlinie einzubeziehen. Drei Mitgliedstaaten haben ihr Interesse an einer schriftlichen Stellungnahme des Juristischen Dienstes des Rates zu dieser Angelegenheit bekundet. Darüber hinaus wurden die Kriterien für die Ermittlung von Einrichtungen der öffentlichen Verwaltung (Systematik der Gebietseinheiten für die Statistik – NUTS) in Frage gestellt.

29. In den Beratungen wurde von mehreren Mitgliedstaaten ein fünftes Thema hervorgehoben: Sie äußerten Bedenken im Zusammenhang mit der nationalen Sicherheit und der Umsetzung der Bestimmung in der Praxis, nach der öffentliche Einrichtungen, die an der Aufrechterhaltung der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit beteiligt sind, vom Anwendungsbereich der überarbeiteten Richtlinie ausgeschlossen sein sollen.

30. Sonstige Fragen von Interesse, die von den Mitgliedstaaten angesprochen wurden, betrafen die Verbindungen und möglichen Überschneidungen mit anderen Strukturen, Netzen und Mechanismen im Bereich der Cybersicherheit auf EU-Ebene, insbesondere im Zusammenhang mit der Einführung von EU-CyCLONe, jedoch auch mit Blick auf bevorstehende Vorschläge und/oder Initiativen wie die Einrichtung eines Netzes von Sicherheitseinsatzzentren (SOC) oder den Vorschlag für eine gemeinsamen Cyberstelle.

31. Was die Einführung von Peer Reviews betrifft, haben einige Mitgliedstaaten den zwingenden Charakter ihrer Durchführung und den Mechanismus zur Festlegung der jeweiligen Methodik in Frage gestellt, nach der Vertraulichkeit und Verfügbarkeit der ausgetauschten Informationen gefragt und betont, dass für die Durchführung der Peer Reviews nur begrenzte Ressourcen zur Verfügung stehen, insbesondere in kleineren Mitgliedstaaten.

32. In Bezug auf die Sicherheit der Lieferkette, insbesondere im Zusammenhang mit den Risikomanagementmaßnahmen im Bereich der Cybersicherheit nach Artikel 18 und den EU-weit koordinierten Risikobewertungen kritischer Lieferketten nach Artikel 19 des überarbeiteten Richtlinienvorschlags, hat die Kommission darauf hingewiesen, dass sie derzeit einen umfassenden Ansatz in Erwägung zieht, einschließlich der Möglichkeit neuer horizontaler Vorschriften zur Verbesserung der Cybersicherheit aller vernetzten Produkte und zugehörigen Dienste im Binnenmarkt.

33. Wie bereits erwähnt, haben die Mitgliedstaaten mehrere Fragen zur koordinierten Offenlegung von Sicherheitslücken und zur Einrichtung eines europäischen Schwachstellenregisters durch die ENISA gestellt. Die Kommission hat beide Fragen umfassend erläutert und angekündigt, sich bei ihrer Entwicklung auf national und international bewährte Vorgehensweisen und Verfahren in diesem Bereich zu stützen.

34. Was die Meldung betrifft, äußerten sich die Mitgliedstaaten zum Verwaltungsaufwand, den sich daraus ergebenden Auswirkungen auf die Haftung, zur Meldefrist von 24 Stunden und zur Meldung von erheblichen Cyberbedrohungen und Beinahe-Vorfällen.

35. Mehrere Mitgliedstaaten thematisierten auch die Bezugnahme auf praktische und rechtliche Erwägungen im Hinblick auf die Aufhebung der relevanten Bestimmungen der eIDAS-Verordnung und des europäischen Kodex für die elektronische Kommunikation und baten die Europäische Kommission um zusätzliche Erläuterungen zu diesen Punkten.

36. Ferner stellten die Mitgliedstaaten die umfassenden Befugnisse in Frage, die die Kommission nach der überarbeiteten NIS-Richtlinie beim Erlass von delegierten Rechtsakten und Durchführungsrechtsakten erhalten soll. Dazu gehörten auch Fragen nach den Verbindungen zum Rechtsakt zur Cybersicherheit, was die Zertifizierung betrifft.

IV. FAZIT

37. Der Vorsitz bedankt sich ausdrücklich für das große Engagement, mit dem die Kommission während der gründlichen Prüfung auf die Fragen und Bemerkungen eingegangen ist, die die Mitgliedstaaten im Rahmen der Beratungen vorgebracht haben.

38. Darüber hinaus würdigt der Vorsitz das Engagement der Mitgliedstaaten in diesem Verfahren, das sie mit den zahlreichen ausführlichen Bemerkungen und Fragen während der Beratungen unter Beweis gestellt haben. Der Vorsitz ist sich voll und ganz bewusst. dass die Mitgliedstaaten große Anstrengungen bei der interministeriellen Koordinierung des Dossiers auf nationaler Ebene unternommen haben.

39. Auf der Grundlage der oben beschriebenen Beratungen ist der Vorsitz der Überzeugung, dass bestimmte wesentliche Elemente des überarbeiteten Vorschlags für die NIS-Richtlinie noch nicht ausgereift genug sind, um erfolgreiche Fortschritte bei den Beratungen der Mitgliedstaaten über deren Formulierung erzielen zu können. Der Vorsitz ist daher der Auffassung, dass die Lösung der Frage der Wechselwirkungen zwischen der überarbeiteten NIS-Richtlinie und den einschlägigen sektorspezifischen Rechtsvorschriften Fortschritte bei diesem Dossier ermöglichen und zur notwendigen Klarstellung der einschlägigen entsprechenden Bestimmungen der NIS 2 und anderer Rechtsakte beitragen wird, die derzeit und/oder demnächst in den Vorbereitungsgremien des Rates erörtert werden (unter anderem die DORA-Verordnung und die Resilienzrichtlinie). Bei den Wechselwirkungen muss auch berücksichtigt werden, dass sich die betreffenden Rechtsakte jeweils in verschiedenen Phasen der Verhandlungen in den zuständigen Vorbereitungsgremien des Rates befinden. Wird die Frage der Wechselwirkungen mit einschlägigen sektorspezifischen Rechtsvorschriften bereits zu Beginn des Ausarbeitungsprozesses der NIS-2-Richtlinie gelöst, sollte dies reibungslose, unabhängige und auf einer soliden Grundlage geführte Verhandlungen über die verschiedenen Rechtsakte ermöglichen.

40. Nach der derzeitigen Planung des portugiesischen Vorsitzes wird die Gruppe bis Ende Juni 2021 insgesamt 19 Sitzungen zur überarbeiteten NIS-Richtlinie abgehalten haben. Der Vorsitz ist der Auffassung, dass der Rat durch den Abschluss der gründlichen und – aus unserer Sicht – erforderlichen Prüfung der überarbeiteten Richtlinie und durch die anschließende Einleitung des Ausarbeitungsprozesses dem Ersuchen des Europäischen Rates vom 26. Februar, die Arbeit in Bezug auf die überarbeitete Richtlinie über die Sicherheit von Netz- und Informationssystemen zügig voranzubringen, umfassend nachkommt.

41. Der portugiesische Vorsitz ist entschlossen, eng mit dem bevorstehenden slowenischen Vorsitz zusammenzuarbeiten, um die Fortsetzung der Beratungen in der Gruppe zu erleichtern und für reibungslose Fortschritte bei diesem Dossier im Rat zu sorgen.

42. Vor diesem Hintergrund werden der Ausschuss der Ständigen Vertreter und der Rat ersucht, die bei der Prüfung des Richtlinienvorschlags erzielten Fortschritte zur Kenntnis zu nehmen.