Rat der
Europäischen Union

Brüssel, den 6. Dezember 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Betr.:	Schlussfolgerungen des Rates zur ENISA

Die Delegationen erhalten anbei die Schlussfolgerungen des Rates zur ENISA, die der Rat auf seiner Tagung vom 6. Dezember 2024 angenommen hat.

ANLAGE

Entwurf von Schlussfolgerungen des Rates zur ENISA

DER RAT DER EUROPÄISCHEN UNION

1. HEBT HERVOR, dass die Herausforderungen, die sich aus dem globalen Cyberraum ergeben, aufgrund der Komplexität neu aufkommender Cyberbedrohungen, des sich ständig verändernden Sicherheitsumfelds und der derzeitigen geopolitischen Spannungen noch nie so komplex, vielfältig und schwerwiegend waren wie heute. Daher sollten die EU und ihre Mitgliedstaaten ihre Bemühungen fortsetzen, widerstandsfähiger zu werden, um derzeitige und neu aufkommende Bedrohungen und Herausforderungen wirksam zu erkennen und zu bewältigen; STELLT HERAUS, dass die Arbeit an einem höheren Maß an Cyberresilienz gemäß einem gesamtgesellschaftlichen Ansatz fortgesetzt werden sollte; BETONT, dass sich die EU und ihre Mitgliedstaaten in den kommenden Jahren auf die wirksame Umsetzung legislativer und nichtlegislativer Initiativen konzentrieren sollten, die alle bisher in dieser Hinsicht ergriffenen Maßnahmen untermauern und zu ihnen beitragen;

2. VERWEIST darauf, dass die nationale Sicherheit nach wie vor in der alleinigen Verantwortung der einzelnen Mitgliedstaaten liegt, und WÜRDIGT, dass die EU und ihre Mitgliedstaaten in den vergangenen Jahren bei der Schaffung der erforderlichen institutionellen Strukturen und Formen der Zusammenarbeit sowohl auf nationaler als auch auf EU-Ebene im Cyberbereich hervorragend zusammengearbeitet haben; BEGRÜßT die verschiedenen legislativen und nichtlegislativen Initiativen, die der EU und ihren Mitgliedstaaten einen starken und robusten Rahmen in diesem Bereich verschafft haben, der die allgemeine Cyberresilienz der Union erhöht. Dieser Rahmen hat sich dahin gehend entwickelt, dass er mehrere Aspekte des Cyberbereichs abdeckt: Sicherheit, Diplomatie, Strafverfolgung und Verteidigung; WEIST darauf HIN, dass eine große Zahl von Akteuren, darunter die Cybersicherheitsbehörden der Mitgliedstaaten, die NIS-Kooperationsgruppe (NIS CG), das CSIRTs-Netzwerk, das europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das Netzwerk nationaler Koordinierungszentren (NCC), die Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG), die Kommission, der Europäische Auswärtige Dienst (EAD), die Agentur der Europäischen Union für Cybersicherheit (ENISA), das Europäische Kompetenzzentrum für Cybersicherheit (ECCC), CERT-EU, die Europäische Verteidigungsagentur (EDA) und das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Europol, Teil des Cybersicherheitsökosystems der EU sind und alle ihren Teil zur Umsetzung des EU-weiten Cybersicherheitsrahmens beitragen;

3. WÜRDIGT, dass sich die ENISA in den vergangenen zwei Jahrzehnten als unschätzbare Einrichtung im europäischen Cybersicherheitsökosystem erwiesen hat, die eine entscheidende Rolle dabei spielt, die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der EU bei ihrer Umsetzung und Entwicklung von Cybersicherheitsstrategien, bei ihrem Kapazitätsaufbau und ihrer Abwehrbereitschaft, bei ihrer Zusammenarbeit und bei ihrer Förderung des Bewusstseins für Cybersicherheit und der Zertifizierung aktiv zu unterstützen;

ALLGEMEINE POLITIKEMPFEHLUNGEN

4. ERSUCHT die Kommission, die **Evaluierung der Cybersicherheitsverordnung** als Gelegenheit zu nutzen, um zu prüfen, wie er zur Vereinfachung des komplexen Cyberökosystems beitragen und so die Wirksamkeit und effiziente Nutzung von Ressourcen verbessern kann; FORDERT die Kommission daher AUF, sicherzustellen, dass das Mandat der ENISA zur Unterstützung der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU zielgerichtet und klar definiert ist, mit konkreten strategischen Zielen und priorisierten Aufgaben sowie einer genaueren Aufteilung der Aufgaben und Zuständigkeiten im Verhältnis zu anderen Akteuren; ERSUCHT die Kommission in diesem Zusammenhang, die Rolle der ENISA bei der Unterstützung der operativen Zusammenarbeit auf EU-Ebene und zwischen den Mitgliedstaaten zur Verbesserung der Cyberresilienz zu prüfen und weiter zu stärken und dabei die Zuständigkeiten der Mitgliedstaaten in diesem Bereich zu berücksichtigen; FORDERT die Kommission außerdem AUF, die beratende Rolle der ENISA im Hinblick darauf zu stärken, fachkundige und evidenzbasierte Leitlinien und Empfehlungen für die Umsetzung laufender und künftiger legislativer und nichtlegislativer Initiativen der EU bereitzustellen und zugleich einen kohärenten EU-Rahmen für die Cybersicherheit sicherzustellen;

5. ERMUTIGT die Kommission in diesem Sinne, eine Straffung der Rolle der ENISA in Bezug auf Aufgaben zu erwägen, die nicht zum Kern ihres Auftrags gehören; UNTERSTREICHT die **erhebliche Ausweitung der Verantwortlichkeiten** der ENISA durch jüngste Gesetzgebungsinitiativen, darunter NIS 2, die Cyberresilienzverordnung und die Cybersolidaritätsverordnung; WEIST darauf HIN, dass die ENISA infolge einiger dieser Initiativen zusätzliche Ressourcen erhalten hat, HEBT jedoch HERVOR, dass die Ausweitung der Verantwortlichkeiten der ENISA und die zunehmende Komplexität der Cyberbedrohungen und -herausforderungen zu einer beträchtlichen Zunahme ihrer Aufgaben geführt haben, die sich in **angemessenen Ressourcen** – personeller, finanzieller und technischer Art – niederschlagen sollte, um die Agentur vollständig in die Lage zu versetzen, alle in ihre Zuständigkeit fallenden Aufgaben auszuführen, ohne den Verhandlungen über den mehrjährigen Finanzrahmen vorzugreifen; FORDERT die Kommission zu diesem Zweck AUF, bei der Ausarbeitung des Entwurfs des Gesamthaushaltsplans der Union Maßnahmen zu priorisieren und Aufgaben im Zusammenhang mit der Unterstützung der Mitgliedstaaten bei der Verbesserung ihrer Cyberresilienz, ihrer operativen Zusammenarbeit und der Entwicklung und Umsetzung des Unionsrechts Vorrang einzuräumen;

UNTERSTÜTZUNG DER ENISA FÜR DIE POLITIKENTWICKLUNG UND -UMSETZUNG

6. VERWEIST darauf, dass die ENISA nach dem derzeitigen Rechtsrahmen für die Cybersicherheit mit mehreren wichtigen Unterstützungs- und Beratungsaufgaben in der gesamten EU betraut ist; BEGRÜßT in diesem Zusammenhang die Rolle der ENISA bei der **Unterstützung der Mitgliedstaaten** im Hinblick auf die wirksame Umsetzung legislativer und nichtlegislativer Initiativen; FORDERT die ENISA AUF, in enger Zusammenarbeit mit der NIS CG und der Kommission weiterhin allgemeine Erkenntnisse und Analysen zum derzeitigen rechtlichen Umfeld im Bereich der Cybersicherheit bereitzustellen; ERMUTIGT die ENISA, technische Leitlinien und bewährte Verfahren regelmäßig und strukturiert auszutauschen und aktiv zu fördern, um die Mitgliedstaaten bei der Umsetzung der Politik und der Rechtsvorschriften im Bereich der Cybersicherheit zu unterstützen;

7. WÜRDIGT die entscheidende Rolle der ENISA bei der Entwicklung **europäischer Systeme für die Cybersicherheitszertifizierung**, die das Vertrauen in IKT-Produkte, -Dienste und -Prozesse und außerdem in die verwalteten Sicherheitsdienste vor dem Hintergrund der bevorstehenden gezielten Änderung der Cybersicherheitsverordnung untermauern; BETONT, dass die Mitgliedstaaten und die Industrie über das langwierige Verfahren der Auswahl, Ausarbeitung und Annahme von Systemen für die Cybersicherheitszertifizierung besorgt sind; HÄLT die Kommission daher AN, die Gelegenheit der Evaluierung der Cybersicherheitsverordnung zu nutzen, um Wege für einen schlankeren, risikobasierten sowie transparenteren und schnelleren Ansatz bei der Entwicklung von EU-Systemen für die Cybersicherheitszertifizierung zu finden, und BETONT die wichtige Rolle der Mitgliedstaaten in diesem Prozess; HEBT außerdem HERVOR, wie wichtig es ist, die Verantwortung für die Pflege eines jeden Zertifizierungssystems ausdrücklich zuzuweisen; VERWEIST ferner darauf, dass die ENISA alle einschlägigen Interessenträger bei der Ausarbeitung infrage kommender Systeme zügig mittels eines förmlichen, offenen, transparenten und inklusiven Verfahrens konsultieren sollte und dass die Kommission bei der Bewertung der Effizienz und Nutzung der angenommenen Systeme offene, transparente und inklusive Konsultationen durchführen sollte; ERMUTIGT die ENISA, die Zusammenarbeit mit der Datenschutzgemeinschaft, vor allem mit dem Europäischen Datenschutzausschuss, soweit relevant, und den zuständigen nationalen Behörden, weiter zu verstärken, insbesondere im Hinblick auf die Förderung von Synergien im Zusammenhang mit der Entwicklung künftiger europäischer Systeme für die Cybersicherheitszertifizierung;

8. FORDERT die ENISA AUF, den Austausch mit den Mitgliedstaaten über die praktischen Aspekte, die Vereinfachung und die Straffung des Meldeverfahrens in Zusammenarbeit mit der Kommission fortzusetzen, um den unnötigen Verwaltungsaufwand zu vermeiden, der sich aus einem komplexen Melderahmen ergeben könnte; VERWEIST ferner auf sein Ersuchen an die Kommission, mit Unterstützung der ENISA und anderer einschlägiger EU-Einrichtungen eine Bestandsaufnahme der in den jeweiligen EU-Gesetzgebungsakten in Bezug auf Cyber- und digitale Angelegenheiten festgelegten einschlägigen Meldepflichten zu erstellen; VERWEIST darauf, dass der Informationsaustausch zwischen der ENISA und den Mitgliedstaaten auf einem Vertrauensverhältnis beruht, in dem Sicherheit und Vertraulichkeit im Einklang mit der Cybersicherheitsverordnung und den einschlägigen Vorschriften und Protokollen gewährleistet sind, und dass er auf das beschränkt werden sollte, was für den Zweck des Austauschs relevant und verhältnismäßig ist; STELLT HERAUS, dass Daten und Informationen mit der gebotenen Sorgfalt behandelt werden müssen;

9. HEBT HERVOR, dass die ENISA für die Einrichtung und Pflege der **einheitlichen Meldeplattform im Rahmen der Cyberresilienzverordnung** verantwortlich ist, die einen konkreten operativen Mehrwert bieten wird, insbesondere in Bezug auf aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle, die die Sicherheit von Produkten mit digitalen Elementen beeinträchtigen. Angesichts des breiten Anwendungsbereichs dieser horizontalen Verordnung sollte die einheitliche Meldeplattform ein wirksames und sicheres Instrument zur Erleichterung des Informationsaustauschs zwischen nationalen CSIRTs und der ENISA sein; HÄLT die ENISA daher AN, neben der Bereitstellung ausreichender personeller Ressourcen die Einrichtung der Plattform als Schlüsselpriorität zu beschleunigen, um ihre Einsatzbereitschaft innerhalb der in der Cyberresilienzverordnung festgelegten Frist sicherzustellen;

10. WÜRDIGT die Rolle der ENISA bei der Einrichtung einer **europäischen Datenbank für Schwachstellen**, die für mehr Transparenz bei der Offenlegung von Schwachstellen sorgen und zugleich einen angemessenen Umgang mit sensiblen Daten sicherstellen soll; HÄLT die ENISA angesichts des Ablaufs der Umsetzungsfrist der NIS-2-Richtlinie AN, alle erforderlichen Arbeiten zu intensivieren, um das reibungslose Funktionieren dieser Datenbank sicherzustellen; ERSUCHT zugleich die NIS CG, mit Unterstützung der ENISA weiterhin Leitlinien, Strategien und Verfahren für die Offenlegung von Schwachstellen zu veröffentlichen;

11. WÜRDIGT die Vorteile der von der ENISA durchgeführten **Maßnahme zur Unterstützung der Cybersicherheit**, die als Pool von Cybersicherheitsdiensten fungiert, welche den Mitgliedstaaten zur Ergänzung ihrer Bemühungen zur Verfügung stehen, sowie die von der ENISA bei der Durchführung der Maßnahme gesammelten Erfahrungen; HEBT in diesem Zusammenhang HERVOR, dass die ENISA eine zentrale Rolle bei der Verwaltung und dem Betrieb der EU-Cybersicherheitsreserve spielen sollte; ERSUCHT die ENISA, unmittelbar nach Inkrafttreten der Cybersolidaritätsverordnung mit der Bestandsaufnahme der benötigten Dienste und ihrer Verfügbarkeit zu beginnen, damit die EU-Cybersicherheitsreserve in allen Mitgliedstaaten so nützlich und auf die Bedürfnisse der Nutzer zugeschnitten wie möglich ist; ERSUCHT die ENISA, nach ihrer Betrauung die Mitgliedstaaten in einem frühen Stadium des Verfahrens zur Einrichtung der EU-Cybersicherheitsreserve einzubeziehen, insbesondere durch die Einholung von Beiträgen zu den erforderlichen Kriterien und die Unterrichtung über bevorstehende Ausschreibungen; ERSUCHT die ENISA, nach ihrer Betrauung sicherzustellen, dass das Auswahlverfahren für vertrauenswürdige Anbieter verwalteter Sicherheitsdienste transparent, offen und fair ist und die Teilnahme von Anbietern aus allen Mitgliedstaaten unabhängig von ihrer Größe ermöglicht; VERWEIST zudem darauf, dass die ENISA verpflichtet ist, die Interoperabilitätsleitlinien für die grenzübergreifenden Cyberknotenpunkte unverzüglich herauszugeben;

12. UNTERSTREICHT, dass die **Beobachtung von Trends in Bezug auf neu aufkommende Technologien** in einem sich schnell wandelnden Bereich wie dem Cyberraum von entscheidender Bedeutung für die Aufrechterhaltung und weitere Stärkung unserer Cyberabwehr ist; WÜRDIGT die Arbeit, die die ENISA geleistet hat, um die Öffentlichkeit auf die Risiken und Möglichkeiten von Technologien wie etwa künstlicher Intelligenz und Quanteninformatik aufmerksam zu machen und so ein besseres Verständnis der derzeitigen Herausforderungen zu fördern; ERMUTIGT die ENISA, weiter zu diesen Aufgaben beizutragen, sich aktiv für die Umsetzung ihrer Empfehlungen einzusetzen und gegebenenfalls das ECCC zu beraten und mit ihm zusammenzuarbeiten;

UNTERSTÜTZUNG DER ENISA FÜR DIE MITGLIEDSTAATEN BEI DER VERBESSERUNG DER CYBERRESILIENZ UND DER OPERATIVEN ZUSAMMENARBEIT

13. BETONT, dass die ENISA eine wichtige Rolle **als Sekretariat der beiden von den Mitgliedstaaten geleiteten Kooperationsnetze auf EU-Ebene für den Cyberbereich, dem CSIRTs-Netzwerk und EU-CyCLONe** spielt; BEKRÄFTIGT, wie wertvoll die Teilnahme der ENISA an der NIS CG ist, insbesondere durch ihre aktive Einbeziehung in die verschiedenen Arbeitsbereiche und ihre fachlichen Beiträge dazu; ERMUTIGT die ENISA, das Funktionieren und die Zusammenarbeit dieser Netze auch in Zukunft zu unterstützen, da sie den Mitgliedstaaten grundlegende Kanäle für die Zusammenarbeit auf verschiedenen Ebenen bieten;

14. WEIST ERNEUT darauf HIN, dass das **gemeinsame Lagebewusstsein** auf EU-Ebene, das zur Cyber-Abwehr der EU beiträgt, verbessert werden muss, und zwar im Zusammenhang mit der Erkennung und der Prävention von Cybersicherheitsvorfällen sowie der Reaktion darauf; BETONT in diesem Zusammenhang, wie wichtig die vorausschauenden Tätigkeiten, regelmäßigen Berichte und Bedrohungsanalysen der ENISA sind, die alle zur Verbesserung des gemeinsamen Lagebewusstseins beitragen; ERMUTIGT die ENISA, eng mit den Mitgliedstaaten zusammenzuarbeiten, um zur Entwicklung eines Lagebewusstseins auf EU-Ebene beizutragen; WÜRDIGT in diesem Zusammenhang die bedeutende Rolle der ENISA – zusammen mit CERT-EU und Europol –, wenn es um die Unterstützung des Rates mit lagebezogenen Briefings im Kontext der Cyber-Diplomacy-Toolbox zur Ergänzung der vom Einheitlichen Analyseverfahren (SIAC) bereitgestellten Lageerfassung geht, und BETONT, dass ein umfassendes Bild der Bedrohungslage aus verschiedenen Quellen, einschließlich des Privatsektors, erstellt werden muss; REGT in diesem Zusammenhang AN, die Zusammenarbeit der ENISA mit dem EAD und insbesondere mit dem INTCEN unter uneingeschränkter Achtung ihrer jeweiligen Mandate weiter auszubauen;

15. HEBT HERVOR, dass das Cyber-Lage- und Analysezentrum der Kommission eine interne Funktion innerhalb der Kommission wahrnimmt und durch deren Zusammenarbeit mit der ENISA und dem CERT-EU unterstützt wird; ERSUCHT die Kommission – um ein größtmögliches Potenzial für Synergien zu schaffen und die Komplexität des Cyber-Ökosystems der EU zu verringern –, die Ergebnisse der Bewertung der Cybersicherheitsverordnung sowie die Beratungen über die Bewertung des Cyber-Blueprint zu berücksichtigen, um die Aufgaben des Cyber-Lage- und Analysezentrums der Kommission und die damit verbundenen Aufgaben der ENISA zu straffen; ERMUTIGT die Kommission, unnötige Doppelarbeit zu vermeiden und gleichzeitig die zentrale Rolle der ENISA bei der Entwicklung eines gemeinsamen Lagebewusstseins auf Unionsebene zur Unterstützung der Mitgliedstaaten – unter gebührender Achtung ihrer nationalen Zuständigkeiten – zu wahren;

16. BETONT, dass die Entwicklung eines gemeinsamen Lagebewusstseins eine Voraussetzung für ein rechtzeitiges und wirksames Krisenmanagement der Union insgesamt ist; UNTERSTREICHT, dass auf EU-Ebene eine Vielzahl wichtiger Akteure in die **Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes** eingebunden sind und dass im Falle solcher Vorfälle die wirksame Zusammenarbeit zwischen den Mitgliedstaaten hauptsächlich durch das CSIRTs-Netz und EU-CyCLONe untermauert wird. Die ENISA spielt beim Cyberkrisenmanagement eine wichtige Rolle als Sekretariat für das CSIRTs-Netz und EU-CyCLONe; ERSUCHT die Kommission, die Bewertung des Cyber-Blueprint zu nutzen, um die zusätzlichen Aufgaben und Zuständigkeiten für einen Beitrag zur Entwicklung einer gemeinsamen Reaktion auf grenzüberschreitende Cybervorfälle oder -krisen großen Ausmaßes sowie die Rolle, die der ENISA als Sekretariat des CSIRTs-Netzes und von EU-CyCLONe sowie aufgrund der jüngsten Rechtsakte zur Cybersicherheit zukommt, ordnungsgemäß abzubilden;

17. UNTERSTREICHT, wie wichtig es ist, regelmäßige **Cybersicherheitsübungen** zu organisieren, die die Abwehrbereitschaft der EU zur Reaktion auf Vorfälle und Krisen erheblich verbessern; ERKENNT AN, dass die ENISA wertvolle und umfassende Erfahrungen in diesem Bereich zur Unterstützung der Mitgliedstaaten gesammelt hat; WÜRDIGT die wichtige Rolle der ENISA bei der Planung, Vorbereitung, Ausführung und Bewertung von Cybersicherheitsübungen und BEKRÄFTIGT, dass sie einer der zentralen Akteure auf EU-Ebene bleiben sollte, wobei zu berücksichtigen ist, dass solche Übungen auf der Grundlage strukturierter Rahmenbedingungen und gemeinsamer Terminologien durchgeführt werden sollten; ERSUCHT die ENISA, das CSIRTs-Netz und EU-CyCLONe, die bestehenden regelmäßigen Übungen so effizient wie möglich zu nutzen, um den EU-Rahmen für die Reaktion auf Cybersicherheitskrisen zu erproben und zu verbessern, und dafür zu sorgen, dass die gewonnenen Erkenntnisse bestmöglich genutzt werden;

ZUSAMMENARBEIT DER ENISA MIT ANDEREN AKTEUREN DES CYBERSICHERHEITSÖKOSYSTEMS

18. WEIST ERNEUT darauf HIN, dass die **Zusammenarbeit zwischen allen Akteuren auf Ebene der Mitgliedstaaten und der Union** aufgrund des horizontalen Charakters der Cybersicherheit von entscheidender Bedeutung ist, und UNTERSTREICHT daher, dass es zur Stärkung der allgemeinen Cyberresilienz auf europäischer Ebene auch der Zusammenarbeit zwischen der ENISA und anderen einschlägigen Einrichtungen im Cyberbereich bedarf;

19. UNTERSTREICHT, dass die Fähigkeit der Organe, Einrichtungen und sonstigen Stellen der EU, ihre Cybersicherheit zu wahren, von Bedeutung für die allgemeine Cyberresilienz auf EU-Ebene ist, bei der die Rolle von CERT-EU von unschätzbarem Wert ist, BEGRÜßT in diesem Zusammenhang die etablierte strukturierte Zusammenarbeit zwischen CERT-EU und der ENISA und ERMUTIGT sie dazu, ihre enge Zusammenarbeit auch in Zukunft fortzusetzen.

20. Sobald die finanzielle Autonomie des ECCC hergestellt ist, wird das Kompetenzzentrum einen wesentlichen Beitrag zur Entwicklung eines starken europäischen Forschungs-, Industrie- und Technologieökosystems für den Cyberbereich leisten, einschließlich Kompetenzen für die Arbeitskräfteentwicklung im Einklang mit seinem Mandat; ERMUTIGT die ENISA und das ECCC, ihre enge Zusammenarbeit fortzusetzen, insbesondere in Bezug auf den Bedarf und die Prioritäten im Bereich Forschung und Innovation sowie auf Cyberkompetenzen, um die Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union zu steigern; ERSUCHT die Kommission, zu prüfen, wie Synergien in der Arbeit der ENISA und des ECCC weiter optimiert werden können und wie die Tätigkeiten entsprechend ihren jeweiligen Mandaten besser gestrafft werden können;

21. UNTERSTREICHT, dass regelmäßige Aktualisierungen der Bedrohungslage dazu beitragen, genauer zu ermitteln, welche Maßnahmen und Instrumente für eine wirksame Bekämpfung der Cyberkriminalität erforderlich sind; HEBT den Mehrwert der Berichte über die Gemeinsame Cyberbewertung der EU HERVOR, die das Ergebnis der Zusammenarbeit zwischen der ENISA, dem EC3 von Europol und CERT-EU sind und bereits wertvolle Beiträge zur Bewältigung der verschiedenen Herausforderungen, einschließlich der Bekämpfung der Cyberkriminalität, geleistet haben; ERSUCHT die ENISA und Europol, ihre strukturierte Zusammenarbeit auch in Zukunft fortzusetzen;

22. BETONT, dass die Cyberabwehr ein wichtiger und sich ständig weiterentwickelnder Teil der Bewältigung von Bedrohungen, die sich aus dem Cyberraum ergeben, ist; HEBT HERVOR, dass die ENISA sich in den Fällen, in denen sie eine unterstützende Rolle bei der Umsetzung der EU-Cyberabwehrpolitik spielt, mit dem EAD und der Kommission abstimmen muss, und zwar in enger Zusammenarbeit mit der EDA, dem ECCC und der Cyberabwehrgemeinschaft; BEKRÄFTIGT die Rolle der ENISA als zivile Agentur; UNTERSTREICHT, wie wichtig es ist, die zivil-militärische Zusammenarbeit im Cyberbereich innerhalb der EU zu vertiefen und zu straffen, mit einer klaren Aufteilung der Aufgaben und Zuständigkeiten zwischen den beiden Gemeinschaften sowie zwischen der EU und der NATO, unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der gegenseitigen Offenheit und Transparenz sowie der Beschlussfassungsautonomie beider Organisationen; ERMUTIGT die ENISA, die Arbeitsvereinbarung mit der Kommunikations- und Informationsagentur der NATO fortzusetzen;

23. ERMUTIGT die EU, unsere gemeinsamen Werte und Anstrengungen in globalen Foren weiter zu fördern, um einen freien, globalen, offenen und sicheren Cyberraum zu wahren; BETONT, dass der grenzüberschreitende Charakter von Cyberbedrohungen und -vorfällen eine enge und wirksame Zusammenarbeit nicht nur auf EU-Ebene, sondern auch **mit internationalen Organisationen und Partnern** erfordert; STELLT FEST, dass das internationale Engagement der ENISA im Einklang mit der Gemeinsamen Außen- und Sicherheitspolitik der EU auf strategische Partner und EU-Bewerberländer ausgerichtet sein sollte; BETONT, dass die ENISA im Rahmen ihres internationalen Engagements im Einklang mit ihrem Mandat und den einschlägigen Bestimmungen der Cybersicherheitsverordnung handeln sollte; ERKENNT AN, dass das internationale Engagement der ENISA im Einklang mit den einschlägigen Verfahren geklärt werden muss, wobei insbesondere sicherzustellen ist, dass ihr Verwaltungsrat ordnungsgemäß und rechtzeitig über die damit verbundenen Tätigkeiten unterrichtet wird; ERMUTIGT die ENISA zur Beteiligung an einschlägigen internationalen Kooperationsrahmen im Bereich der Cybersicherheit, einschließlich Organisationen wie der NATO und der OSZE;

24. WEIST ERNEUT darauf HIN, dass die EU und ihre Mitgliedstaaten häufig Defizite bei den **Cybersicherheitskompetenzen** herausgestellt haben; WEIST darauf HIN, dass die Kommission und die ENISA einen umfassenden und übergreifenden Rahmen eingeführt haben, um allen Interessenträgern Leitlinien an die Hand zu geben, wie den Europäischen Kompetenzrahmen für Cybersicherheit, die Mitteilung über die Akademie für Cybersicherheitskompetenzen und die jährliche europäische Konferenz für Cyberkompetenzen, und ERMUTIGT die Kommission und die ENISA, auf diesen Initiativen – unter besonderer Berücksichtigung der laufenden Beratungen über das Konsortium für eine europäische Digitalinfrastruktur (EDIC) – aufzubauen; ERSUCHT zu diesem Zweck die Kommission, sich mit den Mitgliedstaaten in Verbindung zu setzen, die an der Einrichtung eines EDIC interessiert sind; ERKENNT AN, dass sowohl die ENISA als auch das ECCC den Auftrag haben, Kompetenzen in der gesamten Union zu fördern; ERSUCHT die ENISA, vorrangig die Bemühungen der Mitgliedstaaten um Kompetenzen und Ausbildung zu unterstützen, um die Öffentlichkeit stärker zu sensibilisieren, und gegebenenfalls mit dem ECCC zusammenzuarbeiten;

25. WÜRDIGT, dass die ENISA in den letzten Jahren eine **Zusammenarbeit mit dem Privatsektor** aufgebaut hat; WEIST darauf HIN, dass die von der Branche gesammelten Informationen dazu beitragen könnten, das gemeinsame Lagebewusstsein zu verbessern, da der Privatsektor die Cyberbedrohungslage kontinuierlich überwacht; ERMUTIGT daher die ENISA, in enger Abstimmung mit den Mitgliedstaaten und allen Einrichtungen der EU die Zusammenarbeit mit dem Privatsektor zu stärken;

26. FORDERT die Kommission und die ENISA AUF, zu prüfen, wie die Zusammenarbeit zwischen der ENISA und den europäischen **Normungsgremien** verbessert werden kann; BETONT, dass die ENISA ihr Fachwissen bezüglich der europäischen Normung im Bereich der Cybersicherheit ausbauen muss, indem sie unter anderem Normungstätigkeiten verfolgt und sich daran beteiligt;

27. FORDERT die Kommission und die ENISA NACHDRÜCKLICH AUF, unter Berücksichtigung der in diesen Schlussfolgerungen enthaltenen Empfehlungen und Vorschläge zu prüfen, wie die Funktionsweise des EU-Rahmens für Cybersicherheit weiter optimiert werden kann. Eine kontinuierliche Zusammenarbeit, die Priorisierung von Aufgaben und Ressourcen sowie die Vereinfachung der komplexen Cyberlandschaft werden Schlüsselelemente für die Bewältigung der derzeitigen und künftigen Herausforderungen sein.