Rat der
Europäischen Union

Brüssel, den 22. Mai 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Betr.:	Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU

Die Delegationen erhalten anbei die Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU, die der Rat auf seiner Tagung vom 22. Mai 2023 gebilligt hat.

Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU

1. Aufbauend auf dem Politikrahmen für die Cyberabwehr von 2014 und seiner Aktualisierung von 2018 begrüßt der Rat die ehrgeizige Gemeinsame Mitteilung über die EU-Cyberabwehrpolitik, nach der weiter in unsere modernen und interoperablen Streitkräfte, Spitzentechnologien und modernste Cyberabwehrfähigkeiten investiert und Partnerschaften zur Bewältigung gemeinsamer Herausforderungen ausgebaut werden sollen. In diesen Zeiten der zunehmenden Abhängigkeit von digitalen Technologien ist der Cyberraum zum Schauplatz eines strategischen Wettbewerbs geworden. Es gilt daher unbedingt, einen offenen, freien, stabilen und sicheren Cyberraum aufrechtzuerhalten. Der Einsatz von Cyberoperationen, die den grundlosen und ungerechtfertigten Angriffskrieg Russlands gegen die Ukraine ermöglichen und damit einhergehen, beeinträchtigt die globale Stabilität und Sicherheit, stellt ein erhebliches Eskalationsrisiko dar und erhöht den bereits in den letzten Jahren verzeichneten deutlichen Anstieg böswilliger Cyberaktivitäten außerhalb des bewaffneten Konflikts.

2. Der Krieg in der Ukraine hat einen neuen strategischen Kontext geschaffen und deutlich gemacht, dass die EU, ihre Mitgliedstaaten und ihre Partner die Resilienz der EU gegenüber Cyberbedrohungen weiter stärken und ihre gemeinsame Cybersicherheit und Cyberabwehr gegen böswillige Handlungen und Angriffshandlungen im Cyberraum ausweiten müssen. In der Gemeinsamen Mitteilung über die EU-Cyberabwehrpolitik wird unsere Entschlossenheit zum Ausdruck gebracht, unverzügliche und langfristige Maßnahmen zu ergreifen, um sicherzustellen, dass die Handlungsfreiheit im Cyberraum gegeben ist und dass den Bedrohungsakteuren, die unter anderem beabsichtigen, in die Netz- und Informationssysteme der EU und ihrer Partner einzudringen, diese zu stören oder zu zerstören, begegnet wird. Diese Gemeinsame Mitteilung, die die Cybersicherheitsstrategie der EU ergänzt und im Einklang mit dem Strategischen Kompass steht, stellt einen wichtigen Schritt auf dem Weg zum umfassenden Ansatz der EU für Resilienz, Reaktion, Konfliktverhütung, Zusammenarbeit und Stabilität im Cyberraum dar. In diesem Zusammenhang unterstreicht der Rat, dass angemessene und kohärente Reaktionen der EU, ihrer Mitgliedstaaten und ihrer Partner erforderlich sind, und sieht auch der Überarbeitung der Durchführungsleitlinien des EU-Instrumentariums für die Cyberdiplomatie als weiteren wichtigen Schritt bei der Entwicklung der Cyberabwehr der EU entgegen.

3. Der Rat betont, dass die jüngsten Cyberangriffe auf kritische europäische Infrastruktur, die sich rasch verändernde Cyberbedrohungslandschaft und die Geschwindigkeit der technologischen Entwicklung auch zeigen, dass die zivil-militärische Koordinierung und Zusammenarbeit verstärkt werden muss, wobei er unterstreicht, dass zwischen den zivilen und militärischen Gemeinschaften keine Hierarchie besteht.
Die EU-Cyberabwehrpolitik ermöglicht es der EU und ihren Mitgliedstaaten, ihre Fähigkeit, für Schutz, Erkennung, Abwehr und Abschreckung zu sorgen, zu stärken, indem sie die gesamte Bandbreite an Verteidigungsoptionen, die den zivilen und militärischen Gemeinschaften mit Blick auf die weiter gefasste Sicherheit und Verteidigung der EU zur Verfügung stehen, im Einklang mit dem Völkerrecht, einschließlich der Menschenrechtsnormen und des humanitären Völkerrechts, angemessen nutzen.

4. Während die nationale Sicherheit, auch im Cyberraum, gemäß Artikel 4 Absatz 2 EUV weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, betont der Rat, dass einzeln und gemeinsam erhebliche Investitionen in die Stärkung der Resilienz, den Einsatz umfassender Cyberabwehrfähigkeiten und die Mobilisierung von Kooperationsrahmen der EU und finanziellen Anreizen getätigt werden müssen. Der Rat hebt hervor, dass die Maßnahmen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU weiter verstärkt werden müssen, um die Union, ihre Bürgerinnen und Bürger, die Organe, Einrichtungen und sonstigen Stellen der EU sowie die GSVP-Missionen und -Operationen im Cyberraum zu schützen. Darüber hinaus betont er, wie wichtig die Resilienz der EU im Cyberraum ist, indem Cyberabwehrfähigkeiten entwickelt werden und die Zusammenarbeit mit einem vertrauenswürdigen privaten Ökosystem verstärkt wird.

I. **Gemeinsames Handeln für eine stärkere Cyberabwehr**

5. Der Rat bekräftigt, dass ein schrittweiser, transparenter und inklusiver Prozess von wesentlicher Bedeutung für die Stärkung des Vertrauens ist, das für die Weiterentwicklung eines Rahmens der EU für das Krisenmanagement im Bereich der Cybersicherheit entscheidend ist, wobei der vom Rat entwickelte Fahrplan für das Cyberkrisenmanagement berücksichtigt werden muss. Der Rat bekräftigt, dass unsere Fähigkeit, bei Cyberangriffen für Schutz, Erkennung, Abwehr und Abschreckung sorgen zu können, weiter ausgebaut werden muss, indem Lagebewusstsein, Kapazitätsaufbau, Fähigkeitenentwicklung, Aus- und Weiterbildungsmaßnahmen und Übungen verbessert werden, die Resilienz gestärkt wird sowie unter Verwendung aller angemessenen Mittel entschlossen auf Cyberangriffe gegen die EU, ihre Mitgliedstaaten, die Organe, Einrichtungen und sonstigen Stellen der EU sowie die GSVP-Missionen und -Operationen reagiert wird. Dabei fordert der Rat den Hohen Vertreter und die Kommission auf, die Komplexität im Cyberbereich zu verringern, unnötige Überschneidungen zu vermeiden und für Zusammenarbeit und Synergien mit bestehenden Initiativen zu sorgen. Die Zusammenarbeit und die Koordinierung zwischen den im Bereich Cyberabwehr tätigen Akteuren der EU und der Mitgliedstaaten sowie innerhalb der EU und der Mitgliedstaaten, zwischen den militärischen und zivilen Cyber-Gemeinschaften und zwischen dem öffentlichen und einem vertrauenswürdigen privaten Ökosystem müssen verstärkt werden. In diesem Zusammenhang werden die Mitgliedstaaten aufgefordert, die nationalen zivil-militärischen Koordinierungsmechanismen weiter zu sondieren und zu stärken, den gemeinsamen freiwilligen Informationsaustausch zu erleichtern, gewonnene Erkenntnisse auszutauschen, zur Entwicklung interoperabler Normen beizutragen, Risikobewertungen durchzuführen, Risikoszenarien zu erstellen und gemeinsame Übungen insbesondere auf europäischer Ebene durchzuführen, wobei die Bestimmungen der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) uneingeschränkt einzuhalten sind.

6. In Anerkennung der Bemühungen um eine weitere Stärkung der Resilienz der Union im Rahmen der NIS-2-Richtlinie und der Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) bekräftigt der Rat seine Empfehlung für einen EU-weiten koordinierten Ansatz zur Stärkung der Resilienz kritischer Infrastruktur[1]. Er fordert Maßnahmen zur weiteren Stärkung der Resilienz von kritischen Einrichtungen, kritischer Infrastruktur sowie digitalen Produkten und Dienstleistungen und stellt fest, dass die Umsetzung der NIS-2-Richtlinie nach wie vor der wichtigste Schritt ist. Dies ist zwar überwiegend eine zivile Verantwortung, trägt aber auch zu einer stärkeren Cyberabwehr bei. In diesem Zusammenhang werden die Organe, Einrichtungen und sonstigen Stellen der EU und die Mitgliedstaaten aufgefordert, die Weiterentwicklung und den Einsatz von neuen und bestehenden EU-Koordinierungsmechanismen, Risikobewertungen, -evaluierungen und -szenarien, den gemeinsamen freiwilligen Informationsaustausch und Übungen in einer Weise zu unterstützen, dass ein Mehrwert geschaffen wird und unnötige Überschneidungen mit bestehenden Initiativen vermieden werden.

7. Um das Vertrauen weiter zu stärken, die Zusammenarbeit zu konsolidieren und den zeitnahen Austausch von Informationen über erhebliche und große Cybersicherheitsvorfälle, die sich auf Verteidigungssysteme auswirken, zu erleichtern, begrüßt der Rat die Initiative zur Weiterentwicklung der EU-Konferenz der Cyberkommandeure, die von jedem Vorsitz des Rates der EU mit Unterstützung der Europäischen Verteidigungsagentur (EDA) und unter Beteiligung des Europäischen Auswärtigen Dienstes (EAD) auszurichten ist. Der Rat ermutigt alle Mitgliedstaaten zur Teilnahme an diesen Treffen. Um die Resilienz der EU gegenüber großen Cybersicherheitsvorfällen zu stärken, ersucht der Rat das EU-Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) und die EU-Konferenz der Cyberkommandeure, festzustellen, wie sie zusammenarbeiten und von einer gemeinsamen militärischen und zivilen Perspektive profitieren können.

---

[1] Vorschlag für eine Empfehlung des Rates für eine koordinierte Vorgehensweise der Union zur Stärkung der Resilienz kritischer Infrastruktur (COM(2022) 551).

8. Um eine robustere und besser koordinierte Reaktion auf EU-Ebene zu fördern, begrüßt der Rat die Einrichtung des operativen Netzes für die militärischen IT-Notfallteams (MICNET) und sieht seiner ersten Einsatzfähigkeit bis Mitte 2024 entgegen, um den Austausch technischer Informationen über Cybersicherheitsvorfälle, die sich auf Verteidigungssysteme auswirken, zwischen den teilnehmenden Mitgliedstaaten zu verbessern. Der Rat fordert alle Mitgliedstaaten auf, sich am MICNET zu beteiligen, um die Wirksamkeit des Netzes zu gewährleisten. Darüber hinaus ersucht der Rat die Mitgliedstaaten, auf den Erfahrungen des Netzwerks von Computer-Notfallteams (CSIRT) aufzubauen, und ruft nachdrücklich dazu auf, zu gegebener Zeit einen wirksamen Mechanismus für die Zusammenarbeit und Koordinierung zwischen den beiden Netzen zu schaffen, wobei die Governance-Mechanismen und die Nutzer beider Einrichtungen uneingeschränkt zu achten sind.

9. Angesichts der Zunahme böswilliger Cyberaktivitäten staatlicher und nichtstaatlicher Akteure im Zusammenhang mit GSVP-Missionen und -Operationen der EU ersucht der Rat die EU und ihre Mitgliedstaaten, ihre Kapazitäten zur Verteidigung und Sicherung der GSVP-Missionen und -Operationen zu stärken. In dieser Hinsicht begrüßt der Rat das Ziel, den Schutz der militärischen Netze und Strukturen der EU weiter voranzubringen, was unter anderem mit der militärischen Vision und Strategie der EU für den Cyberraum als Einsatzbereich[2] im Einklang steht.

[2] EEAS(2021) 706 REV 4.

10. Der Rat bekräftigt die Schlussfolgerungen des Rates vom Mai 2022[3] und das Erfordernis, in unsere gegenseitige Unterstützung nach Artikel 42 Absatz 7 EUV sowie in die Solidaritätsklausel nach Artikel 222 AEUV zu investieren. Der Rat betont, wie wichtig es ist, das gemeinsame Verständnis der EU und ihrer Mitgliedstaaten in Bezug auf die Umsetzung von Artikel 42 Absatz 7 EUV, auch in komplexen Szenarien mit Cyberangriffen und im Einklang mit den einschlägigen Grundsätzen des Völkerrechts, weiter zu vertiefen. Er begrüßt die Möglichkeit, dass die EU im Fall eines Cyberangriffs auf ausdrückliches Ersuchen des betreffenden Mitgliedstaats bzw. der betreffenden Mitgliedstaaten Unterstützung bereitstellen kann, und zwar unbeschadet des besonderen Charakters der Sicherheits- und Verteidigungspolitik bestimmter Mitgliedstaaten.

11. Der Rat hebt die Fortschritte hervor, die im Rahmen des SSZ-Projekts „Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit“ erzielt wurden, und betont seine Bereitschaft, auf Ersuchen als Fähigkeit zur Deckung des Bedarfs der Mitgliedstaaten und der EU – und zur Unterstützung von GSVP-Missionen und -Operationen – tätig zu werden und die EU-Partner zu unterstützen. Der Rat begrüßt die Weiterentwicklung der Fähigkeiten des SSZ-Teams für die rasche Reaktion auf Cybervorfälle, der nationalen Teams für die Reaktion auf Cybervorfälle und gegebenenfalls zusätzlicher Reaktionsfähigkeiten, etwa des künftigen, im Strategischen Kompass vorgesehenen Teams für die rasche Reaktion auf hybride Bedrohungen, auch indem ihre Koordinierung und Zusammenarbeit auf EU-Ebene gefördert wird.

[3] Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union vom 23. Mai 2022 (Dok. 9364/22).

12. Der Rat begrüßt die Arbeit im Rahmen des SSZ-Projekts „Koordinierungszentrum für den Cyber- und Informationsraum“ (CIDCC), das auf die Bereitstellung einer militärischen Fähigkeit zur Sammlung und Analyse von Informationen abzielt, die für ein gemeinsames operatives Lagebild des Cyberraums relevant sind. Darüber hinaus begrüßt der Rat den Vorschlag, den Konzeptnachweis ab 2025 – wenn er sich in Bezug auf das Informationskoordinierungszentrum als erfolgreich erwiesen hat – in ein EU-Koordinierungszentrum für die Cyberabwehr (EUCDCC) zu integrieren, womit die Koordinierung und das Lagebewusstsein insbesondere der Befehlshaber der GSVP-Missionen und -Operationen der EU verbessert wird und die umfassenderen Führungs- und Kontrollstrukturen der EU gestärkt werden. Der Rat fordert den Hohen Vertreter auf, ein Konzept und einen Fahrplan für die Einrichtung des EUCDCC vorzulegen und dabei auf den Lehren aus ähnlichen internationalen Einrichtungen aufzubauen, die erforderlichen Ressourcen zu ermitteln, unnötige Überschneidungen zu vermeiden und Komplementarität mit dem umfassenderen EU-Rahmen für Cybersicherheit anzustreben.

13. Der Rat betont, wie wichtig die strategische nachrichtendienstliche Zusammenarbeit im Bereich Cyberbedrohungen und -aktivitäten ist, und ersucht die Mitgliedstaaten, über ihre zuständigen Behörden weiterhin zur Arbeit des EU INTCEN, der Abteilung „Aufklärung“ des Militärstabs der Europäischen Union (EUMS) und der Mitgliedstaaten im Rahmen des Einheitlichen Analyseverfahrens (SIAC) beizutragen. Ferner betont der Rat, wie wichtig es ist, unsere Kapazitäten im Bereich Cyberaufklärung auszubauen, um unsere Cyberresilienz und Reaktionen zu verbessern sowie unsere zivilen und militärischen GSVP-Missionen und -Operationen, unsere Streitkräfte und die Kapazität des SIAC im Cyberbereich wirksam zu unterstützen, wobei auf freiwilligen nachrichtendienstlichen Beiträgen seitens der Mitgliedstaaten und unbeschadet ihrer Zuständigkeiten aufgebaut wird.

14. Der Rat nimmt Kenntnis von dem Cyber-Lage- und Analysezentrum der Europäischen Kommission, mit dem das Lagebewusstsein der Kommission verbessert werden soll. Der Rat betont, wie wichtig es ist, eine für beide Seiten vorteilhafte Zusammenarbeit zwischen diesem Zentrum und anderen Organen, Einrichtungen und sonstigen Stellen der EU, insbesondere der ENISA und dem CERT-EU, aufzubauen. Der Rat unterstreicht, wie wichtig es ist, bei der Entwicklung des Lagebewusstseins für eine enge Zusammenarbeit mit den Kooperationsnetzen der EU zu sorgen und die Vertraulichkeit zu wahren. Der Rat stellt fest, dass die gemeinsame Lageerfassung auf EU-Ebene gestärkt und der Rahmen der EU für das Krisenmanagement im Bereich der Cybersicherheit weiterentwickelt werden muss, wobei unnötige Doppelarbeit zu vermeiden ist.

15. Der Rat weist darauf hin, dass die Aus- und Weiterbildung, Schulungen und Übungen im Cyberbereich von wesentlicher Bedeutung sind, um die Vorsorge und Wirksamkeit zu gewährleisten, und begrüßt die nationalen Maßnahmen sowie die Maßnahmen, die von der EU über das Europäische Sicherheits- und Verteidigungskolleg (ESVK), die EDA, die ENISA und laufende SSZ-Projekte, wie die Cyber-Range-Verbände und dem Projekt „EU Cyber-Akademie und Innovation Hub“ (CAIH), durchgeführt werden. Im Hinblick auf eine weitere Verstärkung dieser Bemühungen sieht der Rat der Einrichtung des EDA-Rahmenprojekts CyDef-X zur Synchronisierung und Unterstützung von Cyberabwehrübungen erwartungsvoll entgegen. Der Rat fordert die EDA auf, in enger Zusammenarbeit mit den Mitgliedstaaten und dem EAD zu prüfen, wie mit CyDef-X Übungen wie CYBER PHALANX weiter unterstützt werden können, auch in Bezug auf die gegenseitige Unterstützung nach Artikel 42 Absatz 7 EUV und die Solidaritätsklausel nach Artikel 222 AEUV, und mit der Kommission und der ENISA zivile Übungen zu erörtern. Darüber hinaus ruft der Rat dazu auf, innerhalb von CyDef-X bestehende Test- und Übungsumgebungen für die Cyberabwehr, wie die Cyber-Range-Verbände, zu nutzen und weiterzuentwickeln. Um einen flexiblen und effizienten Entscheidungsprozess im Fall einer Cyberkrise zu gewährleisten, unterstreicht der Rat, wie wichtig es ist, dass regelmäßige Tischübungen für die Entscheidungsebene der Mitgliedstaaten durchgeführt werden.

16. Der Rat nimmt Kenntnis von dem Vorschlag für einen Rechtsakt zur Cybersolidarität und der Absicht, die Fähigkeiten zur Erkennung von cybersicherheitsbezogenen Risiken und Vorfällen in der EU und die Reaktion darauf zu verbessern. Der Rat unterstreicht, dass Vorschläge in diesem Bereich nur wirksam sein können, wenn sie auf die Krisenmanagementrahmen und -bedürfnisse der Mitgliedstaaten abgestimmt sind. Der Rat betont, wie wichtig es ist, kritische Infrastruktur im Rahmen der nationalen Zuständigkeit auf potenzielle Schwachstellen zu testen, sofern dies als nützlich eingestuft wird und die verfügbaren EU-Risikobewertungen berücksichtigt werden.

17. Der Rat nimmt Kenntnis von dem Vorschlag der Kommission zur Einrichtung eines Cyber-Notfallmechanismus, mit dem die Verfügbarkeit von Cybersicherheitsdienstleistungen vertrauenswürdiger privater Anbieter gefördert werden könnte, um die Mitgliedstaaten im Fall großer Cybersicherheitsvorfälle auf Ersuchen zu unterstützen; gleichzeitig betont er, dass die europäische Cybersicherheitsbranche mit Unterstützung des Europäischen Kompetenzzentrums für Cybersicherheitsforschung (ECCC) als wesentliche Säule für die Funktionsfähigkeit dieses Mechanismus ausgebaut werden muss. Der Rat unterstreicht die Schlüsselrolle der einzelnen Mitgliedstaaten bei der Überwachung und Bewertung ihrer nationalen Bedürfnisse.

II. **Sicherung des Verteidigungsökosystems der EU**

18. Der Rat erinnert an seine Forderung an die Mitgliedstaaten, ihre eigenen Fähigkeiten zur Durchführung von Cyberabwehroperationen weiterzuentwickeln, gegebenenfalls einschließlich proaktiver Maßnahmen zum Schutz, zur Erkennung, zur Abwehr und zur Abschreckung in Bezug auf Cyberangriffe. Da die NIS-2-Richtlinie nicht für Einrichtungen der öffentlichen Verwaltung gilt, die im Verteidigungsbereich tätig sind, ersucht der Rat die EDA, die Mitgliedstaaten gegebenenfalls mit Unterstützung der Kommission und des EAD bei der Ausarbeitung nicht rechtsverbindlicher freiwilliger Empfehlungen auf der Grundlage der NIS-2-Richtlinie zu unterstützen, um die Cybersicherheit in der Verteidigungsgemeinschaft zu erhöhen; ferner ersucht er alle Mitgliedstaaten, sich aktiv an diesen Bemühungen zu beteiligen. Bei diesen Empfehlungen sollten ähnliche Anstrengungen, die in anderen Rahmen unternommen werden, berücksichtigt werden.

19. Wie im Strategischen Kompass anerkannt, hängt die Handlungsfähigkeit der EU davon ab, ob sie in der Lage ist, strategische Abhängigkeiten bei ihren Cyberabwehrfähigkeiten und Lieferketten zu verringern und modernste Technologien für die Cyberabwehr zu entwickeln und zu beherrschen. Dies umfasst die Stärkung der technologischen und industriellen Basis der europäischen Verteidigung (EDTIB) in der gesamten EU und ihrer Fähigkeit, mit gleichgesinnten Partnern weltweit auf der Grundlage der Gegenseitigkeit zusammenzuarbeiten, um gegenseitigen Nutzen sicherzustellen. Daher fordert der Rat die Cybersicherheits- und die Cyberabwehrbranche auf, eng zusammenzuarbeiten, um Synergien mit dem Ziel zu schaffen, umfassende Cyberabwehrfähigkeiten zu entwickeln und bereitzustellen. Der Rat ersucht die Kommission, gegebenenfalls in enger Zusammenarbeit mit dem ECCC die Entwicklung einer starken, agilen, weltweit wettbewerbsfähigen und innovativen industriellen und technologischen Basis der europäischen Cyberabwehr, einschließlich kleiner und mittlerer Unternehmen (KMU), im Rahmen von Investitionen und politischen Maßnahmen weiter zu unterstützen.

20. Angesichts der Bedeutung der Interoperabilität und der Einheitlichkeit der Cyberabwehrfähigkeiten, auch im Hinblick auf die gemeinsame Entwicklung von Cyberabwehrfähigkeiten der nächsten Generation, ersucht der Rat die EDA und den Militärstab der EU, eine Reihe von Interoperabilitätsanforderungen der EU im Bereich der Cyberabwehr auszuarbeiten, die auf bestehenden Grundsätzen, Verfahren und Normen, die insbesondere im Rahmen der Nordatlantikvertrags-Organisation (NATO) festgelegt wurden, aufbauen und mit ihnen kompatibel sind. Darüber hinaus ersucht der Rat die Mitgliedstaaten, im Rahmen des Europäischen Komitees für die Normung im Verteidigungsbereich zu prüfen, ob bestimmte freiwillige Normen für Verteidigungssysteme erforderlich sein könnten, und dabei eng mit allen einschlägigen Interessenträgern, gegebenenfalls einschließlich europäischer Normungsorganisationen und der NATO, zusammenzuarbeiten.

21. Der Rat begrüßt die Bemühungen der Kommission, einen Plan zur Förderung der Nutzung bestehender Normen für zivile Anwendungen in den Bereichen Cybersicherheit und Cyberabwehr sowie der Entwicklung neuer freiwilliger Normen vorzulegen. Der Rat betont, dass die Normen in den Bereichen Cybersicherheit und Cyberabwehr gegebenenfalls aufeinander abgestimmt werden müssen. Der Rat erkennt an, dass derartige freiwillige Normen für die Cybersicherheits- und die Cyberabwehrbranche der EU nützlich sein könnten, und fordert nachdrücklich zur engeren Zusammenarbeit zwischen zivilen und verteidigungspolitischen Normungsgremien auf.

22. Der Rat fordert, dass rasch Empfehlungen auf der Grundlage der von der Kommission und den einschlägigen Organen durchgeführten Bestandsaufnahme der bestehenden Instrumente für eine sichere Kommunikation im Cyberbereich ausgearbeitet werden. Die Empfehlungen sollten gegebenenfalls auf bestehende Initiativen zum Informationsaustausch abgestimmt werden und auch die Risiken berücksichtigen, die von neu aufkommenden und disruptiven Technologien für die derzeitigen Verschlüsselungsmethoden ausgehen.

23. Darüber hinaus begrüßt der Rat, dass die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe auf Ersuchen des Rates erste Arbeiten – zunächst – im Zusammenhang mit den Sektoren Energie und Telekommunikation in Bezug auf Risikoevaluierungen und -szenarien unternommen und diese entwickelt haben. Der Rat würdigt, dass auch gezielte Risikobewertungen im Hinblick auf die Cybersicherheit für Kommunikationsinfrastrukturen und -netze in der EU ausgearbeitet werden. Der Rat bekräftigt, dass es von größter Bedeutung ist, dass die Mitgliedstaaten, aber auch die Organe, Einrichtungen und sonstigen Stellen der EU über ein gemeinsames Verständnis der möglichen Auswirkungen von Cybervorfällen verfügen. Daher ersucht der Rat die oben genannten Akteure, dafür zu sorgen, dass Risikoevaluierungen, Risikoszenarien und nachfolgende Empfehlungen bei der Festlegung und Priorisierung von Maßnahmen und Unterstützungsleistungen auf EU-Ebene und gegebenenfalls auf nationaler Ebene berücksichtigt werden. Ferner fordert der Rat, dass die Risikoszenarien von allen einschlägigen Akteuren bei Risikobewertungsprozessen sowie bei der Entwicklung von Cyberübungen berücksichtigt werden.

III. **Investitionen in Cyberabwehrfähigkeiten**

24. Der Rat fordert die Mitgliedstaaten auf, ihre Investitionen für den Aufbau, die Erhaltung und die Weiterentwicklung interoperabler Cyberabwehrfähigkeiten aufzustocken. Der Rat unterstützt die Ausarbeitung einer Reihe freiwilliger Verpflichtungen für die Weiterentwicklung der nationalen Cyberabwehrfähigkeiten unter Berücksichtigung ähnlicher Anstrengungen, die in anderen Rahmen unternommen werden.

25. Der Rat fordert die Mitgliedstaaten und die EDA auf, die Überarbeitung des Fähigkeitenentwicklungsplans dazu zu nutzen, ehrgeizige Ziele für die Entwicklung einer kooperativen Cyberabwehr auf EU-Ebene festzulegen. Der Rat fordert die Mitgliedstaaten ferner auf, auf den aktualisierten Prioritäten und ihren Verpflichtungen im Rahmen der SSZ aufzubauen, um ihr Engagement in kooperativen EU-Projekten zur Entwicklung der Cyberabwehrfähigkeiten zu erhöhen, und erkennt den direkten Nutzen kooperativer Projekte auf EU-Ebene für die Entwicklung nationaler Cyberabwehrfähigkeiten an.

26. Der Rat begrüßt die gemeinsamen Forschungsanstrengungen auf EU-Ebene, um mögliche Anwendungen neu aufkommender und disruptiver Technologien in verteidigungsbezogenen Systemen auszuloten, und stellt ferner fest, dass sichergestellt werden muss, dass diese technologischen Entwicklungen rasch in bestehende und künftige Fähigkeiten integriert werden. Der Rat fordert die Mitgliedstaaten und die EU-Industrie auf, die gemeinsamen Forschungsmöglichkeiten auf EU-Ebene bestmöglich zu nutzen, beispielsweise solche im Rahmen der EDA, laufende SSZ-Projekte wie das Projekt CAIH, den Europäischen Verteidigungsfonds und gegebenenfalls Horizont Europa und die Projekte mit doppeltem Verwendungszweck im Rahmen des Programms „Digitales Europa“. Darüber hinaus begrüßt der Rat, die Mobilisierung der speziellen Rahmen zur Förderung von Innovationen im Verteidigungsbereich durch die Nutzung von Spin-ins aus dem zivilen Bereich, insbesondere des EU-Innovationsprogramms im Verteidigungsbereich und des Innovationszentrums für den Verteidigungsbereich. Der Rat fordert das ECCC und die EDA ferner auf, Arbeitsvereinbarungen auszuarbeiten, um den Informationsaustausch zwischen den jeweiligen Mitarbeitern über die Prioritäten in den Bereichen zivile Technologie, Technologie mit doppeltem Verwendungszweck und Verteidigungstechnologie zu erleichtern, damit Synergien geschaffen und Überschneidungen vermieden werden können.

27. Der Rat begrüßt die Absicht der Kommission, in Zusammenarbeit mit der EDA und dem ECCC im Einklang mit ihren jeweiligen Mandaten, mit den Mitgliedstaaten und in Abstimmung mit den einschlägigen Interessenträgern wie der Industrie einen Technologiefahrplan für kritische Cybertechnologien auszuarbeiten, der durch die Ermittlung kritischer Cybertechnologien und die Bestandsaufnahme technologischer Entwicklungen und strategischer Abhängigkeiten Wege aufzeigt, diese Abhängigkeiten zu verringern und so die strategische Autonomie und technologische Souveränität der EU zu unterstützen und gleichzeitig eine offene Wirtschaft zu wahren. Der Rat stellt fest, dass der Technologiefahrplan für kritische Cybertechnologien in die strategischen Prioritäten für die Finanzierungsinstrumente der EU einfließen kann, wobei sie mit den entsprechenden, für diese Instrumente geltenden Modalitäten im Einklang stehen. Der Rat erinnert daran, dass die EU eine ehrgeizige und entschlossene europäische Industriepolitik verfolgen sollte, um ein nachhaltiges, attraktives und wettbewerbsfähiges Geschäftsumfeld zu schaffen, das auch europäischen Einrichtungen im Cyberbereich eine Expansion ermöglicht.

28. Der Rat würdigt die Absicht, das erhebliche Kompetenzdefizit im Bereich der Cybersicherheit anzugehen, indem neue Fachkräfte, einschließlich Frauen, angezogen werden, Weiterbildungs- und Umschulungsmaßnahmen durchgeführt werden und Investitionen in Aus- und Weiterbildungsmaßnahmen und Übungen getätigt und diese organisiert werden, um eine vielfältige und inklusive Belegschaft aufzubauen. Der Rat erkennt die Herausforderungen an, mit denen die EU in Bezug auf das Humankapital in den Bereichen Cybersicherheit und Cyberabwehr konfrontiert ist, und begrüßt die Initiative der Akademie für Cybersicherheitskompetenzen, die auch für die Mitarbeiter in der Cyberabwehrbranche von Nutzen sein kann.

29. Der Rat ersucht die Mitgliedstaaten, Informationen über bewährte Verfahren zur Heranbildung qualifizierter Fachleute auf dem Gebiet der Cybersicherheit auszutauschen und dabei die Synergien zwischen militärischen, zivilen und Strafverfolgungsinitiativen auszunutzen, und fordert das ESVK auf, mit der Unterstützung und dem Fachwissen der EDA und der ENISA Optionen auszuloten, wie der Austausch bewährter Verfahren verstärkt, die Synergien zwischen den militärischen und zivilen Bereichen der Aus- und Weiterbildung besser genutzt und die Entwicklung spezifischer Kompetenzen im Bereich Cyberabwehr verbessert werden können.

30. Der Rat betont, wie wichtig ein gemeinsames Verständnis der Zusammensetzung des Personals im Bereich Cybersicherheit und der damit verbundenen Kompetenzen ist, um das Defizit auf dem Arbeitsmarkt für Cybersicherheit zu ermitteln und anzugehen; er betont ferner, dass alle Interessenträger, einschließlich der Mitgliedstaaten und der Industrie, einbezogen werden müssen. Der Rat erkennt an, dass die Festlegung von Indikatoren zur Überwachung des Arbeitsmarkts für Cybersicherheit dazu beitragen würde, den Bedarf an Cybersicherheitskompetenzen zu ermitteln und Mittel in angemessener Weise einzusetzen, wobei gleichzeitig ein Beitrag zur Erfüllung der politischen Verpflichtungen, insbesondere aus der NIS-2-Richtlinie, geleistet würde. Der Rat begrüßt den Vorschlag für einen Rahmen für die Zertifizierung von Kompetenzen im Bereich der Cyberabwehr und ersucht den Hohen Vertreter in seiner Eigenschaft als Leiter des ESVK, diese Rahmen gemeinsam mit dem EAD, der Kommission und den Mitgliedstaaten zu erarbeiten und dabei auf zivilen Initiativen aufzubauen.

IV. **Partner für die Bewältigung gemeinsamer Herausforderungen**

31. Der Rat fordert den Hohen Vertreter und die Kommission auf, ihre Zusammenarbeit zu stärken und voranzubringen und für beide Seiten vorteilhafte und maßgeschneiderte Partnerschaften im Bereich der Cyberabwehrpolitik zu sondieren, einschließlich des Kapazitätsaufbaus im Bereich Cyberabwehr im Rahmen der Europäischen Friedensfazilität. Zu diesem Zweck sollte die Cyberabwehr als Thema in die Dialoge und Konsultationen der EU über Cyberfragen und in die allgemeinen sicherheits- und verteidigungsbezogenen Konsultationen mit Partnern aufgenommen werden. Darüber hinaus sollten die Dialoge und die Zusammenarbeit mit dem Privatsektor verbessert werden. Der Rat unterstreicht, dass die internationale Zusammenarbeit in Bezug auf die Normen und Zertifizierungen im Bereich Cybersicherheit einen Mehrwert für die europäische Industrie darstellen würde. Daher begrüßt er die Zusage der Kommission, dies zu einem wesentlichen Bestandteil der EU-Cyberdialoge mit Drittländern und internationalen Organisationen zu machen.

32. Der Rat betont, wie wichtig es ist, durch die internationale Zusammenarbeit Konflikte im Cyberraum zu verhindern und das Risiko solcher Konflikte zu mindern, insbesondere durch die Weiterentwicklung und Umsetzung vertrauensbildender Maßnahmen (VBM) auf regionaler und internationaler Ebene – auch auf Ebene der VN –, und die Nutzung vorhandener VBM im Bereich der Cybersicherheit bei der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), auch in Zeiten internationaler Spannungen, weiter zu fördern.
Die EU und ihre Mitgliedstaaten heben hervor, dass das geltende Völkerrecht im Cyberraum Anwendung findet, und betonen, wie wichtig es ist, die Bemühungen zur Aufrechterhaltung und Förderung des VN-Rahmens für verantwortungsvolles staatliches Handeln fortzusetzen und auf dessen Umsetzung hinzuarbeiten, unter anderem durch die Aufstellung des Aktionsprogramms zur Förderung eines verantwortungsvollen staatlichen Handelns im Cyberraum.

33. Im Einklang mit den Gemeinsamen Erklärungen zur Zusammenarbeit zwischen der EU und der NATO ersucht der Rat den Hohen Vertreter, auch in seiner Eigenschaft als Leiter der EDA, und die Kommission, die Partnerschaft mit der NATO im Cyberbereich zu stärken, zu vertiefen und auszuweiten und dabei die Grundsätze Inklusivität, Gegenseitigkeit, Offenheit und Transparenz sowie die Beschlussfassungsautonomie beider Organisationen zu achten. Unter Berücksichtigung des Erfordernisses, ergänzende und koordinierte Anstrengungen unter möglichst umfassender Einbeziehung der Mitgliedstaaten, die nicht Teil der NATO sind, zu gewährleisten und unnötige Doppelarbeit zu vermeiden, fordert der Rat, dass zwischen der EU und der NATO auf den einschlägigen Ebenen Verbindungen in Bezug auf Aus- und Weiterbildung, Schulungen, Lagebewusstsein, Übungen und FuE-Plattformen hergestellt werden und potenzielle Synergien zwischen den jeweiligen freiwilligen Verpflichtungen für die Entwicklung nationaler Cyberabwehrfähigkeiten und den Krisenmanagementrahmen, den Schutz kritischer Infrastruktur und die Verbesserung des Austauschs über die Lageerfassung, koordinierte Reaktionen auf böswillige Cyberaktivitäten sowie Bemühungen zum Kapazitätsaufbau in Drittländern angestrebt werden. Dies umfasst die technische Vereinbarung zwischen der NATO-Einrichtung zur Bereitstellung von Reaktionsfähigkeit bei Computervorfällen (NCIRC) und dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) sowie einen verstärkten politischen Dialog über Fragen der Cyberabwehr auf allen Ebenen.

V. **Fazit**

34. Aufbauend auf den Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU fordert der Rat den Hohen Vertreter und die Kommission auf, bis zum zweiten Quartal 2023 einen Umsetzungsplan für die Cyberabwehrpolitik auszuarbeiten, der von den Mitgliedstaaten zu billigen ist. Der Rat ersucht die Mitgliedstaaten ferner, freiwillig ihre Absichten und Maßnahmen in Bezug auf die Cyberabwehr im Rahmen der Cyberabwehrpolitik der EU darzulegen und nicht rechtsverbindliche freiwillige Empfehlungen und Zusagen in vollem Umfang zu nutzen, um ihre nationalen und internationalen Bemühungen im Bereich Cyberabwehr mit Blick auf eine größtmögliche Wirkung auf EU-Ebene zu intensivieren.
Der Hohe Vertreter, die Kommission und die Mitgliedstaaten werden ersucht, ab dem zweiten Quartal 2024 jährlich über die Fortschritte bei der Umsetzung der Elemente der Gemeinsamen Mitteilung und ihres Umsetzungsplans Bericht zu erstatten und diese zu erörtern.