Rat der
Europäischen Union

Brüssel, den 23. Mai 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	23. Mai 2022
Empfänger:	Delegationen
Betr.:	Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union – Schlussfolgerungen des Rates, gebilligt auf seiner Tagung vom 23. Mai 2022

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union, die der Rat auf seiner Tagung vom 23. Mai 2022 gebilligt hat.

ANLAGE

Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS auf

– seine Schlussfolgerungen zur gemeinsamen Mitteilung vom 25. Juni 2013 an das Europäische Parlament und den Rat „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“[1],

– seine Schlussfolgerungen zum EU-Politikrahmen für die Cyberabwehr[2],

– seine Schlussfolgerungen zur Internet-Governance[3],

– seine Schlussfolgerungen zur Cyberdiplomatie[4],

– seine Schlussfolgerungen zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche[5],

– seine Schlussfolgerungen zur Gemeinsamen Mitteilung vom 20. November 2017 an das Europäische Parlament und den Rat: „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“[6],

– seine Schlussfolgerungen zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“)[7],

– seine Schlussfolgerungen zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen[8],

– seine Schlussfolgerungen zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten[9],

– den Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die Integrierte EU-Regelung für die politische Reaktion auf Krisen[10],

---

1 Dok. 12109/13.
2 Dok. 15585/14.
3 Dok. 16200/14.
4 Dok. 6122/15 + COR 1.
5 Dok. 14540/16.
6 Dok. 14435/17 + COR 1.
7 Dok. 10474/17.
8 Dok. 10086/18.
9 Dok. 10496/18.

– seine Schlussfolgerungen über Cybersicherheitskapazitäten und deren Aufbau in der EU[11],

– seine Schlussfolgerungen zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G[12],

– seine Schlussfolgerungen zur Zukunft eines hoch digitalisierten Europas nach 2020: „Förderung der digitalen und wirtschaftlichen Wettbewerbsfähigkeit in der gesamten Union und des digitalen Zusammenhalts“[13],

– seine Schlussfolgerungen zum Thema „Zusätzliche Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen“[14],

– seine Schlussfolgerungen zur Gestaltung der digitalen Zukunft Europas[15],

– seine Schlussfolgerungen zur Cybersicherheit vernetzter Geräte[16],

– seine Schlussfolgerungen zur Cybersicherheitsstrategie der EU für die digitale Dekade[17],

– seine Schlussfolgerungen zu Sicherheit und Verteidigung[18],

– seine Schlussfolgerungen zur Prüfung des Potenzials der Initiative für eine Gemeinsame Cyber-Einheit als Ergänzung zur koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen[19],

– den Strategischen Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt[20],

---

10 ABl. L 320 vom 17.12.2018, S. 28-34.
11 Dok. 7737/19.
12 Dok. 14517/19.
13 Dok. 9596/19.
14 Dok. 14972/19.
15 Dok. 8711/20.
16 Dok. 13629/20.
17 Dok. 7290/21.
18 Dok. 8396/21.
19 Dok. 13048/21.
20 Dok. 7371/22.

1. HEBT HERVOR, dass böswillige Handlungen im Cyberraum, die sowohl von staatlichen als auch von nichtstaatlichen Akteuren begangen werden, in den letzten Jahren zugenommen haben, einschließlich einer drastischen und kontinuierlichen Zunahme an böswilligen Aktivitäten gegen kritische Infrastrukturen, Lieferketten und geistiges Eigentum der EU und ihrer Mitgliedstaaten, des erhöhten Risikos von Spillover-Effekten sowie einer Zunahme an Ransomware-Angriffen auf unsere Unternehmen, Organisationen und Bürgerinnen und Bürger; STELLT FEST, dass mit der Rückkehr zur Machtpolitik einige Länder zunehmend versuchen, die regelbasierte internationale Ordnung im Cyberraum in Frage zu stellen und zu untergraben, indem sie den Cyberbereich zusammen mit der Hohen See, dem Luftraum und dem Weltraum zu einem zunehmend umkämpften Bereich machen; ERKENNT AN, dass groß angelegte, systemgefährdende Cyberangriffe oder Versuche, in Netz- und Informationssysteme einzudringen, diese zu stören oder zu zerstören, zugenommen haben, unsere wirtschaftliche Sicherheit untergraben und unsere demokratischen Institutionen und Prozesse beeinträchtigen könnten und zeigen, dass einige Akteure bereit sind, die internationale Sicherheit und Stabilität zu gefährden; UNTERSTREICHT, dass die militärische Aggression Russlands gegen die Ukraine gezeigt hat, dass offensive Cyberaktivitäten als integraler Bestandteil hybrider Strategien durchgeführt werden können, bei denen Einschüchterung, Destabilisierung und wirtschaftliche Störungen kombiniert werden;

2. BEKRÄFTIGT, dass die Stärke unserer Union angesichts der derzeitigen geopolitischen Verschiebungen in Einheit, Solidarität und Entschlossenheit liegt und dass die Umsetzung des Strategischen Kompasses die strategische Autonomie der EU und ihre Fähigkeit stärken wird, mit Partnern zusammenzuarbeiten, um ihre Werte und Interessen, auch im Cyberbereich zu wahren; UNTERSTREICHT, dass eine stärkere und fähigere EU im Bereich Sicherheit und Verteidigung einen konstruktiven Beitrag zur globalen und transatlantischen Sicherheit leisten wird und eine Ergänzung zur NATO bildet, die das Fundament der kollektiven Verteidigung ihrer Mitglieder bleibt; BEKRÄFTIGT die Absicht der EU, die regelbasierte internationale Ordnung mit den Vereinten Nationen als Mittelpunkt stärker zu unterstützen;

3. BEKRÄFTIGT im Einklang mit den Schlussfolgerungen des Rates zur EU-Cybersicherheitsstrategie und dem Strategischen Kompass, dass die Cyberabwehr der Union weiterentwickelt werden muss, indem wir unsere Fähigkeit zur Verhinderung von Cyberangriffen durch Kapazitätsaufbau, Fähigkeitenentwicklung, Aus- und Weiterbildung, Übungen und eine stärkere Resilienz verbessern und unter Einsatz aller verfügbaren EU-Instrumente entschlossen auf Cyberangriffe gegen die EU und ihre Mitgliedstaaten reagieren. Dazu gehört auch, dass die EU weiterhin ihre Entschlossenheit unter Beweis stellt, den Bedrohungsakteuren, die der EU und ihren Partnern einen sicheren und offenen Zugang zum Cyberraum verweigern und unsere strategischen Interessen, einschließlich der Sicherheit unserer Partner, beeinträchtigen wollen, unverzüglich und langfristig zu begegnen; BETONT in diesem Zusammenhang, dass es bei der Cyberabwehr darum geht, die verschiedenen Initiativen im Rahmen von EU-Maßnahmen mit dem Ziel zu bündeln, Frieden und Stabilität im Cyberraum zu fördern und einen offenen, freien, globalen, stabilen und sicheren Cyberraum zu begünstigen und gleichzeitig kurz-, mittel- und langfristige Maßnahmen zur Verhinderung von Cyberbedrohungen und -angriffen, zur Abschreckung vor ihnen und zur Reaktion auf sie besser zu koordinieren und Cyberkapazitäten zu mobilisieren; HEBT HERVOR, dass diese Elemente in die Cyberabwehr der EU aufgenommen und auf fünf Aufgaben der EU im Cyberbereich ausgerichtet werden sollten: Stärkung unserer Cyberresilienz und unserer Schutzkapazitäten; Stärkung der solidarischen und umfassenden Krisenbewältigung; Förderung unserer Vision des Cyberraums; Verstärkung der Zusammenarbeit mit Partnerländern und internationalen Organisationen; Verhinderung, Abwehr und Bewältigung von Cyberangriffen.

I. STÄRKUNG UNSERER CYBERRESILIENZ UND UNSERER SCHUTZKAPAZITÄTEN

4. BEKRÄFTIGT, dass das allgemeine Niveau an Cybersicherheit der EU erhöht werden muss, SIEHT der raschen Annahme des Entwurfs einer Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-Richtlinie), des Entwurfs einer Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) sowie des Entwurfs einer Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) ERWARTUNGSVOLL ENTGEGEN und NIMMT KENNTNIS von dem Vorschlag zur Festlegung von Maßnahmen für ein hohes Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union, mit dem eine Europäische Union gefördert werden soll, die ihre Bürgerinnen und Bürger, öffentlichen Dienste und Unternehmen im Cyberraum schützt; ERMUTIGT die Kommission, die Annahme wichtiger Vorschläge abzuschließen, um sicherzustellen, dass digitale Infrastrukturen, Technologien, Produkte und Dienstleistungen gesichert sind und somit ein klares Signal für die Ambitionen der EU in diesen Bereichen gesendet wird und Unternehmen darin unterstützt werden können, sich der Herausforderung zu stellen; FORDERT die Kommission AUF, gemeinsame Anforderungen der EU an die Cybersicherheit vernetzter Geräte und damit verbundener Prozesse und Dienste im Rahmen des Rechtsakts zur Cyberresilienz, der von der Kommission bis Ende 2022 vorgelegt werden sollte, vorzuschlagen, wobei der Notwendigkeit eines horizontalen und ganzheitlichen Ansatzes, der den gesamten Lebenszyklus digitaler Produkte abdeckt, sowie bestehenden Rechtsvorschriften, insbesondere im Bereich der Cybersicherheit, Rechnung zu tragen ist;

5. ERSUCHT die zuständigen Behörden wie das Gremium europäischer Regulierungsstellen für elektronische Kommunikation (GEREK), die Agentur der Europäischen Union für Cybersicherheit (ENISA) und die Kooperationsgruppe für Netz- und Informationssysteme sowie die Europäische Kommission, auf der Grundlage einer Risikobewertung Empfehlungen an die Mitgliedstaaten und die Europäische Kommission zu richten, um die Resilienz der Kommunikationsnetze und Infrastrukturen in der Europäischen Union zu stärken, einschließlich der weiteren Umsetzung des 5G-Instrumentariums der EU;

6. FORDERT die EU und ihre Mitgliedstaaten AUF, ihre Bemühungen um die Erhöhung des allgemeinen Cybersicherheitsniveaus zu verstärken, indem beispielsweise vertrauenswürdige Anbieter von Cybersicherheitsdiensten gefördert werden, und BETONT, dass es eine Priorität der Industriepolitik der EU im Bereich Cybersicherheit sein sollte, die Etablierung solcher Anbieter zu fördern; ERSUCHT die Kommission, Optionen vorzuschlagen, um die Herausbildung einer Industrie für vertrauenswürdige Cybersicherheitsdienste zu fördern, die Cybersicherheit der IKT-bezogenen Lieferketten zu stärken, die möglichen Auswirkungen von Software-Schwachstellen auf die EU und ihre Mitgliedstaaten – auch im Hinblick auf den künftigen Rechtsakt zur Cyberresilienz – anzugehen und die Ermittlung von Cyberbedrohungen und die gemeinsame Nutzung von Fähigkeiten in und zwischen den Mitgliedstaaten zu verbessern, damit Cyberangriffe mit potenziell systemischen Auswirkungen besser abgewehrt und ihnen besser entgegengetreten werden kann und Lehren aus der Bewältigung der Schwachstellen von SolarWinds, Microsoft Exchange und Apache Log4J gezogen werden können;

7. BEKRÄFTIGT, dass Investitionen in Innovation und eine bessere Nutzung ziviler Technologien von entscheidender Bedeutung sind, um unsere technische Souveränität, auch im Cyberbereich zu stärken, FORDERT die Kommission AUF, das Europäische Kompetenzzentrum für Cybersicherheitsforschung rasch in Betrieb zu nehmen, um ein starkes europäisches Forschungs-, Industrie- und Technologieökosystem für den Cyberbereich zu entwickeln, und UNTERSTREICHT, dass Forschung und Innovation gefördert werden müssen, zur Stärkung der verteidigungspolitischen, technologischen und industriellen Basis der EU mehr in zivile und verteidigungspolitische Bereiche investiert werden muss und die Cyberkapazitäten der EU und ihrer Mitgliedstaaten, einschließlich strategischer Unterstützungskapazitäten, entwickelt werden müssen; BETONT, wie wichtig es ist, neue Technologien, insbesondere Quanteninformatik, künstliche Intelligenz und Big Data, weiterzuentwickeln und intensiv zu nutzen, um komparative Vorteile zu erzielen, auch in Bezug auf Operationen zur Reaktion auf Cybervorfälle;

8. BETONT – IN ANERKENNUNG DESSEN, dass die Stärkung unserer Cybersicherheit eine Möglichkeit zur Verbesserung der Wirksamkeit und Sicherheit unserer Bemühungen an Land, in der Luft, auf Hoher See und im Weltraum darstellt –, wie wichtig es ist, Cybersicherheitsaspekte in allen öffentlichen Politikbereichen der EU, einschließlich sektorspezifischer Rechtsvorschriften zur Ergänzung der NIS-2-Richtlinie, durchgängig zu berücksichtigen, und ERSUCHT die Kommission, Optionen zur Verbesserung der Cybersicherheit in der gesamten Lieferkette der verteidigungspolitischen, technologischen und industriellen Basis der EU zu sondieren;

9. ERKENNT AN, dass die Gewährleistung angemessener finanzieller und personeller Ressourcen für die Cybersicherheit und Maßnahmen zur Schaffung eines günstigen Umfelds für einen wettbewerbsfähigen Privatsektor für die Entwicklung der Cyberabwehr der EU von entscheidender Bedeutung sind und dass die Frage einer stabilen und langfristigen Finanzierung der Cybersicherheit auch auf EU-Ebene, einschließlich der Kosten für hochqualifizierte Arbeitskräfte, angegangen werden sollte, indem ein horizontaler Mechanismus konzipiert und umgesetzt wird, der mehrere Finanzierungsquellen kombiniert; FORDERT die Kommission daher AUF, bis Ende 2022 Optionen für einen solchen Mechanismus zu sondieren, die in den einschlägigen Ratsgremien zu erörtern sind;

10. HEBT HERVOR, dass unsere Anstrengungen und die Zusammenarbeit bei der Bekämpfung der internationalen Cyberkriminalität, insbesondere Ransomware, durch EMPACT (Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen), durch den Austausch zwischen den Bereichen Cybersicherheit, Strafverfolgung und Diplomatie sowie durch den Ausbau der Strafverfolgungskapazitäten für die Ermittlung und Verfolgung von Cyberkriminalität verstärkt werden müssen; BEKRÄFTIGT seine Zusage, die Öffentlichkeit über Cyberbedrohungen und die auf nationaler und EU-Ebene ergriffenen Gegenmaßnahmen unter Einbeziehung der Zivilgesellschaft, des Privatsektors und der Wissenschaft zu informieren, um das Bewusstsein für diese Bedrohungen zu schärfen und ein angemessenes Maß an Cyberschutz und Cyberhygiene zu fördern; BETONT, dass der Schwerpunkt auf den Kompetenzen und Fähigkeiten der Bürgerinnen und Bürger im Bereich der Cybersicherheit auf Ebene der EU und der Mitgliedstaaten liegen muss und dass die Nutzer aktiv in ihren eigenen Schutz einbezogen werden müssen;

II. **STÄRKUNG DER SOLIDARISCHEN UND UMFASSENDEN KRISENBEWÄLTIGUNG**

11. BETONT auf der Grundlage der jährlichen Cyberübungen, anderer Übungen mit Cyberdimension sowie der Cyberübungen 2022 (EU CyCLES), wie wichtig es ist, ein Programm mit regelmäßigen gemeinschaftsübergreifenden und mehrstufigen Cyberübungen aufzustellen, um die interne und externe Reaktion der EU auf große Cybersicherheitsvorfälle mit Beteiligung des Rates, des EAD, der Kommission und einschlägiger Interessenträger wie der ENISA und des Privatsektors zu testen und weiterzuentwickeln, wobei dieses Programm mit der allgemeinen Übungspolitik der EU verknüpft und einen Beitrag dazu leisten wird; BETONT, wie wichtig es ist, die Übungen im Rahmen von Cyber-Europe und Blue OLEx weiterzuentwickeln, bei denen die Reaktionen über verschiedene Ebenen kombiniert werden; ERKENNT AN, dass die bestehenden Übungen bewertet und konsolidiert und Möglichkeiten für weitere Übungen zu bestimmten Segmenten des Cyberbereichs geprüft werden müssen, insbesondere eine militärische Übung des CERT und eine Übung mit Schwerpunkt auf der Zusammenarbeit zwischen den Organen, Einrichtungen und sonstigen Stellen der EU in Krisensituationen; ERKENNT AN, dass die Cyberabwehr der Union unsere Fähigkeit zur Verhinderung von Cyberangriffen durch verschiedene Maßnahmen, einschließlich Schulungen, stärken wird, und ERSUCHT daher die Mitgliedstaaten, die zivil-militärische Zusammenarbeit bei Schulungen und gemeinsamen Übungen im Cyberbereich zu verstärken;

12. UNTERSTREICHT, dass die operative Zusammenarbeit und die gemeinsame Lageerfassung der Mitgliedstaaten weiter getestet und verstärkt werden müssen, unter anderem durch bestehende Netze wie das Netzwerk von Computer-Notfallteams (CSIRTs network) und das Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU CyCLONe), um die Abwehrbereitschaft der EU gegen große Cybersicherheitsvorfälle zu verbessern; UNTERSTREICHT, wie wichtig es ist, die Entwicklung einer gemeinsamen Sprache unter den Mitgliedstaaten und mit den Organen, Einrichtungen und sonstigen Stellen der EU voranzutreiben, die auf Beratungen auf politischer Ebene zugeschnitten ist, um die Erstellung einer konsolidierten Bewertung der Schwere und der Auswirkungen relevanter Cybervorfälle sowie möglicher Entwicklungsszenarien und des sich daraus ergebenden Bedarfs gegebenenfalls zu unterstützen; UNTERSTREICHT in diesem Zusammenhang, dass die Komplementarität der Berichte über die Lagebeurteilung, einschließlich der Berichte des EU CyCLONE über die Auswirkungen und Schwere großer Cybersicherheitsvorfälle in den EU-Mitgliedstaaten und der vom EU INTCEN im Rahmen des EU-Instrumentariums für die Cyberdiplomatie bereitgestellten Bewertungen der Bedrohungslage, verbessert werden muss; ERSUCHT die Kommission, den Hohen Vertreter und die NIS-Kooperationsgruppe, in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen und Agenturen sowie bestehenden Netzwerken wie dem EU CyCLONe bis Ende 2022 eine Risikobewertung durchzuführen und Risikoszenarien aus der Perspektive der Cybersicherheit in einer Bedrohungssituation oder einer möglichen Angriff gegen Mitgliedstaaten oder Partnerländer zu erstellen und sie den zuständigen Ratsgremien vorzulegen; BETONT, dass eine angemessene und koordinierte öffentliche Kommunikation über die Reaktion der EU auf große Cybersicherheitsvorfälle erforderlich ist;

13. BETONT, dass im Falle eines großen Cybersicherheitsvorfalls die Koordinierung und – gegebenenfalls auf der Grundlage der erzielten Fortschritte und der durch das SSZ-Team für die rasche Reaktion auf Cybervorfälle geleistete Arbeit und unter Berücksichtigung der Arbeit des Netzwerkes von Computer-Notfallteams und des EU CyCLONe – die freiwillige Bündelung unserer Reaktionskapazitäten unter den Mitgliedstaaten verstärkt werden müssen; IST SICH BEWUSST, dass der Ausbau der Beziehungen zur Privatwirtschaft eine Verstärkung der öffentlichen Kapazitäten darstellen könnte, insbesondere angesichts des EU-weiten Fachkräftemangels, und dass die Ermittlung und Koordinierung dieser privaten Partner bei großen Cybersicherheitsvorfällen viel bewirken könnte; ERSUCHT die Kommission, zur vollständigen Vorbereitung der Abwehr von großen Cybersicherheitsvorfällen bis Ende des dritten Quartals 2022 einen Vorschlag für einen neuen Cybersicherheits-Notfallfonds vorzulegen;

14. BEKRÄFTIGT im Einklang mit dem Strategischen Kompass, dass in unsere gegenseitige Unterstützung nach Artikel 42 Absatz 7 des Vertrags über die Europäische Union sowie in die Solidarität nach Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union investiert werden muss, insbesondere durch häufige Übungen; BETONT in diesem Zusammenhang, dass weiter an der Bereitstellung und Koordinierung bilateraler zivil-militärischer Unterstützung gearbeitet werden muss, unter anderem durch Prüfung der Frage, ob die EU auf ausdrückliches Ersuchen der Mitgliedstaaten eine Unterstützung bereitstellen kann, und an der Ermittlung geeigneter Reaktionsmaßnahmen, auch durch die Entwicklung einer koordinierten Kommunikationsstrategie im Zusammenhang mit der Umsetzung von Artikel 42 Absatz 7; STELLT FEST, dass dies auch eine Prüfung der Verbindungen zu bestehenden EU-Mechanismen für die Krisenbewältigung und dem Katastrophenschutzverfahren der Union umfassen sollte;

15. UNTERSTREICHT, dass eine verstärkte EU-Cyberabwehr eine verbesserte sichere Kommunikation erfordern wird; BEKRÄFTIGT in diesem Zusammenhang die diesbezüglichen Leitlinien des Strategischen Kompasses und ERSUCHT die Kommission und andere einschlägige Organe, Einrichtungen und Agenturen, bis Ende 2022 eine Bestandsaufnahme der bestehenden Instrumente für eine sichere Kommunikation im Cyberbereich vorzunehmen, die in den einschlägigen Ratsgremien und mit den einschlägigen Kooperationsgruppen wie dem CSIRTs network und EU CyCLONe erörtert werden soll;

III. FÖRDERUNG UNSERER VISION DES CYBERRAUMS

16. WEIST DARAUF HIN, dass das gemeinsame und umfassende Konzept der EU für die Cyberdiplomatie darauf abzielt, zur Konfliktverhütung, zur Eindämmung von Cyberbedrohungen und zu größerer Stabilität in den internationalen Beziehungen beizutragen; BEKRÄFTIGT in diesem Zusammenhang das Engagement der EU für die friedliche Beilegung internationaler Streitigkeiten im Cyberraum und die Anwendung des Völkerrechts, einschließlich der internationalen Menschenrechtsnormen und des humanitären Völkerrechts, auf Maßnahmen von Staaten im Cyberraum; UNTERSTREICHT die Zusage der EU und ihrer Mitgliedstaaten, im Einklang mit den freiwilligen, unverbindlichen Normen für ein verantwortungsvolles staatliches Handeln im Cyberraum zu handeln, die von allen VN-Mitgliedstaaten vereinbart wurden; BETONT, wie wichtig ein offener, freier, globaler, stabiler und sicherer Cyberraum ist, in dem zur Unterstützung des sozialen Wohlergehens, des Wirtschaftswachstums, des Wohlstands und der Integrität unserer freien und demokratischen Gesellschaften die Menschenrechte, die Grundfreiheiten und die Rechtsstaatlichkeit uneingeschränkt gelten, und BEKRÄFTIGT die Zusage der EU und ihrer Mitgliedstaaten, diese Werte und Grundsätze weiterhin zu fördern; BETONT im Hinblick auf die Entwicklung von Kanälen für einen konstruktiven, ehrlichen und offenen Dialog mit den wichtigsten Akteuren des Cyberraums, wie wichtig es ist, Fragen der Cybersicherheit, einschließlich des EU-Instrumentariums für die Cyberdiplomatie, zu einem integralen Bestandteil der EU-Beitrittsverhandlungen und der strategischen und politischen Dialoge der EU mit internationalen Partnern und Wettbewerbern zu machen, und FORDERT gleichzeitig den Hohen Vertreter AUF, die bestehenden bilateralen Cyberdialoge zu überprüfen und gegebenenfalls vorzuschlagen, eine ähnliche Zusammenarbeit mit weiteren Ländern oder einschlägigen internationalen Organisationen aufzunehmen;

17. WEIST DARAUF HIN, wie wichtig die Zusammenarbeit mit verschiedenen Interessenträgern ist, da auch andere Interessenträger Verantwortung für die Cybersicherheit tragen, insbesondere wenn es um die Umsetzung der Empfehlungen und Beschlüsse geht, die in internationalen und regionalen Foren getroffen wurden; RUFT die EU und ihre Mitgliedstaaten AUF, unser Modell von Cyberraum und Internet, das auf dem Multi-Stakeholder-Ansatz und auf Initiativen wie dem Pariser Aufruf zu Vertrauen und Sicherheit im Cyberraum und der Erklärung über die Zukunft des Internets beruhen, weiter zu fördern, wobei der Nutzen eines stabilen Cyberraums für die Allgemeinheit hervorzuheben und auf die Gefahren einer auf den Staat ausgerichteten und autoritären Vision des Internets aufmerksam zu machen ist, und RUFT die EU und ihre Mitgliedstaaten DAZU AUF, die Zusammenarbeit mit der Gemeinschaft der verschiedenen Interessenträger auch durch Nutzung einschlägiger Projekte, wie die EU-Initiative für Cyberdiplomatie im Rahmen der außenpolitischen Instrumente der EU, weiter auszubauen;

18. VERPFLICHTET SICH, kontinuierlich an den Arbeiten in einschlägigen internationalen Organisationen mitzuwirken, insbesondere an den Verfahren im Ersten und Dritten Ausschuss der Vereinten Nationen, wobei zu betonen ist, dass geltendes Völkerrecht im Cyberraum und in Bezug auf diesen uneingeschränkt Anwendung findet; UNTERSTREICHT die Notwendigkeit kontinuierlicher Anstrengungen, um den Rahmen der Vereinten Nationen für verantwortungsvolles staatliches Handeln aufrechtzuerhalten und zu fördern, und BETONT, dass die EU und ihre Mitgliedstaaten aktiv darauf hinarbeiten werden, dessen Umsetzung zu verbessern, unter anderem durch die Aufstellung des Aktionsprogramms zur Förderung eines verantwortungsvollen staatlichen Handelns im Cyberraum; BETONT, dass sich die EU und ihre Mitgliedstaaten aktiv an den Verhandlungen über ein künftiges VN-Übereinkommen beteiligen werden, das als wirksames Instrument für die Strafverfolgungs- und Justizbehörden bei der weltweiten Bekämpfung der Cyberkriminalität dienen soll, und dabei den bestehenden Rahmen internationaler und regionaler Instrumente in diesem Bereich, insbesondere das Budapester Übereinkommen über Computerkriminalität, in vollem Umfang berücksichtigen werden; BETONT, wie wichtig es ist, die Entwicklung und Umsetzung vertrauensbildender Maßnahmen auf regionaler und internationaler Ebene weiter zu unterstützen und die Nutzung vorhandener vertrauensbildender Maßnahmen im Bereich der Cybersicherheit bei der OSZE, auch in Zeiten internationaler Spannungen, weiter zu fördern;

19. BEKRÄFTIGT, dass ein menschenrechtsbasierter Ansatz für die Gewährleistung internationaler Standards in den Bereichen neu entstehender Technologien und der Kernarchitektur des Internets im Einklang mit demokratischen Werten und Grundsätzen von entscheidender Bedeutung ist, um sicherzustellen, dass das Internet global, unfragmentiert und offen bleibt, und UNTERSTÜTZT den Grundsatz, dass bei der Nutzung und Entwicklung von Technologien die Menschenrechte geachtet werden und der Schutz der Privatsphäre im Mittelpunkt steht und dass diese Technologien auf rechtmäßige, sichere und ethische Weise genutzt werden; ERMUTIGT den Hohen Vertreter und die Kommission, eine strategische Vision für technische Fragen im digitalen Bereich zu entwickeln, die außenpolitische Auswirkungen haben und sich auf die Stabilität des Cyberraums und insbesondere des Internets auswirken könnten, auch in den einschlägigen internationalen Fachorganisationen (Internationale Fernmeldeunion usw.);

IV. VERSTÄRKTE ZUSAMMENARBEIT MIT PARTNERLÄNDERN UND INTERNATIONALEN ORGANISATIONEN

20. BETONT, dass die Strategie der EU für den Cyberkapazitätsaufbau besser mit den VN-Normen für ein verantwortungsvolles staatliches Handeln im Cyberraum verknüpft werden muss, unter anderem durch die Entwicklung maßgeschneiderter Kooperations- und Kapazitätsaufbauprogramme, um Drittstaaten bei ihren Umsetzungsbemühungen zu unterstützen, und dass wir dabei unsere Anstrengungen zur Unterstützung des Aktionsprogramms der Vereinten Nationen zur Förderung von verantwortungsvollem staatlichen Handeln im Cyberraum fortsetzen und ausbauen müssen; BETONT, wie wichtig es ist, den Aufbau von Cyberkapazitäten als Teil des Angebots der EU als Bereitsteller von Sicherheit umfassend zu integrieren und die Anstrengungen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU angemessen zu koordinieren, und BEGRÜSST insbesondere die Zusammenarbeit der Mitgliedstaaten untereinander und mit Partnern des öffentlichen und des privaten Sektors, insbesondere über das EU-CyberNet (EU-Netz für den Cyberkapazitätsaufbau) und das globale Forum für Cyber-Fachwissen (GFCE), damit Koordinierung gewährleistet und Doppelarbeit vermieden wird;

FORDERT den Hohen Vertreter und die Kommission AUF, bis zum dritten Quartal 2022 einen *Ausschuss für den Aufbau von Cyberkapazitäten* einzurichten und einen regelmäßigen Austausch in der Horizontalen Gruppe „Fragen des Cyberraums“ zu führen; FORDERT die Kommission und den Hohen Vertreter auf, das Instrument für Nachbarschaft, Entwicklungszusammenarbeit und internationale Zusammenarbeit (NDICI), das Instrument für Heranführungshilfe (IPA III) und andere Finanzinstrumente wie die Europäische Friedensfazilität (EFF) und die „Global Gateway“-Initiative weiter zu mobilisieren, um die Stärkung der Resilienz unserer Partner und ihrer Kapazität zur Erkennung und Bewältigung

von Cyberbedrohungen und zur Untersuchung und strafrechtlichen Verfolgung von Cyberkriminalität sowie die Entwicklung von Kooperationsprojekten zu unterstützen, auch im Kontext von Krisen, und ERMUTIGT insbesondere zur Zusammenarbeit mit Partnern im westlichen Balkan sowie in der östlichen und südlichen Nachbarschaft der EU und zur Entsendung von Sachverständigen der EU und der Mitgliedstaaten, um unter Berücksichtigung bestehender rechtlicher Mandate Unterstützung in Cyberkrisen anzubieten;

21. BETONT, dass die Bemühungen um die Entwicklung eines strukturierten und offenen Ansatzes der EU zur Förderung eines weltweiten gemeinsamen Verständnisses hinsichtlich der Anwendung des Völkerrechts im Cyberraum, des VN-Rahmens für verantwortungsvolles Verhalten der Staaten im Cyberraum, einschließlich der Initiative für ein Aktionsprogramm zur Förderung des verantwortungsvollen staatlichen Handelns im Cyberraum, sowie des Standpunkts der EU und ihrer Mitgliedstaaten bei den laufenden Verhandlungen über ein VN-Übereinkommen gegen Cyberkriminalität verstärkt werden müssen und ERSUCHT den Hohen Vertreter, als Teil dieser Bemühungen dem Rat bis Ende 2022 einen Outreach-Plan vorzulegen; ERMUTIGT den Hohen Vertreter und die Kommissionsdienststellen, die 145 Delegationen in vollem Umfang und systematisch zu nutzen und eine regelmäßige und erfolgreiche Zusammenarbeit zwischen ihnen und den Botschaften der Mitgliedstaaten in Drittländern unter der Schirmherrschaft des geplanten EU-Netzes für Cyberdiplomatie aufzubauen; FORDERT den Hohen Vertreter AUF, bis zum dritten Quartal 2022 das EU-Netz für Cyberdiplomatie einzurichten, das zum Informationsaustausch, zu gemeinsamen Schulungsmaßnahmen für das Personal der EU und der Mitgliedstaaten, zum kohärenten Aufbau von Kapazitäten und zur Stärkung der Umsetzung des VN-Rahmens für verantwortungsvolles Verhalten der Staaten sowie zu vertrauensbildenden Maßnahmen zwischen Staaten beiträgt;

22. BETONT, dass er entschlossen ist, weiter mit internationalen Organisationen und Partnerländern zusammenzuarbeiten, um das gemeinsame Verständnis der Cyberbedrohungslandschaft voranzubringen, Dialoge und Kooperationsmechanismen zu entwickeln und kooperative diplomatische Reaktionen auf proaktive Weise zu identifizieren; WEIST auf die wichtigsten Erfolge der Zusammenarbeit zwischen der EU und der NATO im Bereich der Cybersicherheit im Rahmen der Umsetzung der Gemeinsamen Erklärung von Warschau von 2016 und der Gemeinsamen Erklärung von Brüssel von 2018 HIN und BETONT unter uneingeschränkter Achtung der Beschlussfassungsautonomie und der Verfahren beider Organisationen und auf der Grundlage der Grundsätze der Transparenz, Gegenseitigkeit und Inklusivität, dass die Zusammenarbeit mit der NATO im Cyberbereich durch Übungen, Informationsaustausch und Austausch zwischen Sachverständigen verstärkt werden muss, einschließlich in Bezug auf Fähigkeitenentwicklung, Aufbau von Kapazitäten für Partner, Missionen und Operationen sowie die Anwendbarkeit des Völkerrechts und der VN-Normen für ein verantwortungsvolles staatliches Handeln im Cyberraum und mögliche koordinierte Reaktionen auf böswillige Cyberaktivitäten;

V. VERHINDERUNG, ABWEHR UND BEWÄLTIGUNG VON CYBERANGRIFFEN

23. STELLT FEST, dass der Cyberraum zu einem Bereich des geopolitischen Wettbewerbs geworden ist, und BEKRÄFTIGT daher, dass die EU in der Lage sein muss, zügig und energisch auf Cyberangriffe wie staatlich geförderte böswillige Cyberaktivitäten gegen die EU und ihre Mitgliedstaaten zu reagieren, und daher das EU-Instrumentarium für die Cyberdiplomatie stärken und alle ihre Instrumente uneingeschränkt nutzen muss, einschließlich der verfügbaren politischen, wirtschaftlichen, diplomatischen, rechtlichen und strategischen Kommunikationsinstrumente, die eingesetzt werden, um böswillige Cyberaktivitäten zu verhindern, davon abzuschrecken und darauf zu reagieren; UNTERSTREICHT, dass feindseligen Akteuren bewusst sein muss, dass Cyberangriffe gegen Mitgliedstaaten und EU-Organe frühzeitig entdeckt, rasch erkannt und mit allen erforderlichen Instrumenten und Strategien bewältigt werden; ERSUCHT die Mitgliedstaaten und den Hohen Vertreter, mit Unterstützung der Kommission auf eine Überarbeitung der Durchführungsleitlinien des EU-Instrumentariums für die Cyberdiplomatie bis zum Ende des ersten Quartals 2023 hinzuarbeiten, sich dabei insbesondere auf die Elemente der Cyberabwehr und die Lehren, die aus der Umsetzung des Instrumentariums für die Cyberdiplomatie seit seiner Einführung und der Cyberübung der EU CyCLES gezogen wurden, zu stützen und vor allem zusätzliche Reaktionsmaßnahmen zu sondieren;

24. UNTERSTREICHT die Notwendigkeit, in den einschlägigen Gremien und Ausschüssen des Rates einen regelmäßigen Austausch über die Cyberbedrohungslandschaft zu führen – auch in regelmäßiger Zusammenarbeit mit dem Privatsektor – und sich dabei auf die Bewertung der Auswirkungen und Schwere der jüngsten Vorfälle zu stützen, das allgemeine Bewusstsein und die Bereitschaft für weitere Anwendungen des EU-Instrumentariums für die Cyberdiplomatie zu schärfen und weitere Instrumente zur Unterstützung seiner Umsetzung zu entwickeln; STELLT FEST, dass der Austausch von nachrichtendienstlichen Erkenntnissen und Informationen und die Zusammenarbeit zwischen den Mitgliedstaaten sowie mit dem EU INTCEN gestärkt werden müssen, damit zu Beginn des Entscheidungsprozesses Erkenntnisse, auch in Bezug auf die Frage der Attribution, ausgetauscht werden können und somit eine rasche, wirksame und fundierte Reaktion auf böswillige Cyberaktivitäten, die sich gegen die EU und ihre Partner richten, ermöglicht wird, wobei die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt; BEKRÄFTIGT, wie wichtig es ist, die Kapazitäten des EU INTCEN im Cyberbereich auf der Grundlage freiwilliger nachrichtendienstlicher Beiträge seitens Mitgliedstaaten und unbeschadet ihrer Zuständigkeiten zu stärken und den Vorschlag für die etwaige Einrichtung einer Arbeitsgruppe der Mitgliedstaaten für EU-Cybernachrichtendienste zu prüfen;

25. ERKENNT AN, dass die Erklärungen und restriktiven Maßnahmen der EU im Rahmen des EU-Instrumentariums für die Cyberdiplomatie sehr deutliche gemacht haben, dass böswillige Cyberaktivitäten, die eine externe Bedrohung für die EU, ihre Mitgliedstaaten und ihre Partner darstellen, nicht hingenommen werden, und somit dazu beitragen, böswillige Cyberaktivitäten zu verhindern, davon abzuschrecken und darauf zu reagieren, und BEKRÄFTIGT seine Entschlossenheit, diese Maßnahmen im Hinblick auf die Weiterentwicklung und Förderung eines gemeinsamen Standpunkts der EU zur Anwendung des Völkerrechts im Cyberraum zu nutzen, um auf die völkerrechtlichen Verpflichtungen in Bezug auf den Cyberraum hinzuweisen, einschließlich der Charta der Vereinten Nationen in ihrer Gesamtheit, und um den VN-Rahmen für verantwortungsvolles Verhalten der Staaten zu fördern, einschließlich der Verpflichtung aller Staaten zur Erfüllung der Sorgfaltspflicht, nicht wissentlich zuzulassen, dass auf ihrem Hoheitsgebiet mit Hilfe von IKT völkerrechtswidrige Handlungen begangen werden; ERSUCHT den Hohen Vertreter unter Hinweis darauf, dass angemessene und rasche Nachrichten die Risiken einer Eskalation mindern und Angreifer, die auf europäische Interessen abzielen, abschrecken können, eine umfassende Kommunikationsstrategie für die Nutzung des EU-Instrumentariums für die Cyberdiplomatie auszuarbeiten und den Mitgliedstaaten vorzulegen;

26. BEFÜRWORTET die Entwicklung schrittweiser, zielgerichteter und kontinuierlicher Ansätze und Reaktionen auf böswillige Cyberaktivitäten, wobei das breite Spektrum von Instrumenten, die im Rahmen des EU-Instrumentariums für die Cyberdiplomatie zur Verfügung stehen, einschließlich des Cybersanktionssystem der EU, genutzt und zusätzliche Maßnahmen erwogen werden sollten; HEBT HERVOR, dass die Möglichkeit ausgeweitet werden muss, fallweise alle verfügbaren internen und externen Instrumente zu mobilisieren, um Cyberangriffen vorzubeugen, sie zu verhindern, von ihnen abzuschrecken und auf sie zu reagieren, und diese in einem raschen, wirksamen, schrittweisen, zielgerichteten und kontinuierlichen Ansatz umzusetzen, der auf einem langfristigen strategischen Engagement beruht; FORDERT den Hohen Vertreter auf, in Zusammenarbeit mit der Kommission die gesamte Bandbreite möglicher gemeinsamer Reaktionen der EU auf Cyberangriffe, darunter Sanktionsmöglichkeiten, zu ermitteln, um bereit zu sein, erforderlichenfalls rasche und wirksame Maßnahmen zu ergreifen, und diese dem Rat bis zum Ende des ersten Quartals 2023 vorzulegen;

27. ERMUTIGT die Mitgliedstaaten unter Hinweis auf die Tatsache, dass die Cyberabwehr in erster Linie in die nationale Zuständigkeit fällt, ihre eigenen Fähigkeiten zur Durchführung von Cyberabwehroperationen weiterzuentwickeln, einschließlich proaktiver Maßnahmen zum Schutz, zur Erkennung, zur Abwehr und zur Abschreckung in Bezug auf Cyberangriffe und möglicherweise zur Unterstützung anderer Mitgliedstaaten und der EU. Jeder Mitgliedstaat wird aufgefordert, erforderlichenfalls seine eigenen Fähigkeiten zur Bereitstellung und Inanspruchnahme von Hilfe und Unterstützung zu verbessern; BETONT, dass die Weiterentwicklung dieser Fähigkeiten eines der Hauptziele der künftigen Cyberabwehrpolitik der EU sein sollte; STELLT FEST, dass im Rahmen der Cyberabwehrpolitik der EU stärker berücksichtigt werden sollte, welche Rolle die einschlägigen Organe und Einrichtungen der EU spielen können, um – entsprechend ihren jeweiligen Mandaten – die Zusammenarbeit zwischen den im Bereich Cyberabwehr tätigen Akteuren der EU und der Mitgliedstaaten zu verstärken und ihre eigenen Kapazitäten zu entwickeln; ERSUCHT den Hohen Vertreter, gemeinsam mit der Kommission die Entwicklung einer Cyberabwehr der EU zu ergänzen, indem er 2022 einen ehrgeizigen Vorschlag für eine Cyberabwehrpolitik der EU vorlegt, der den Weg für die Weiterentwicklung der Cyberabwehr der EU durch den Rat ebnen wird;

28. HEBT HERVOR, dass die Interoperabilität und der Informationsaustausch durch die Zusammenarbeit zwischen militärischen IT-Notfallteams (military computer emergency response teams – milCERT) verbessert werden muss; ERSUCHT die Mitgliedstaaten, aufbauend auf der Arbeit der EDA, ein milCERT-Netz einzurichten, um die Zusammenarbeit auszubauen und den Informationstausch zu erleichtern, was auch zur Koordinierung mit anderen Cyber-Gemeinschaften beitragen würde, sowie ein Netz von für den Cyberbereich zuständigen militärischen Befehlshabern aufzubauen, um die strategische Zusammenarbeit zwischen den Cyberkommandostellen der EU-Mitgliedstaaten und anderen entsprechenden Behörden zu stärken. Die Einrichtung dieser Netze und die SSZ-Projekte im Cyberbereich würden zu einer verstärkten Cyberabwehr auf EU-Ebene beitragen; BETONT, wie wichtig die Zusammenarbeit zwischen dem vorgeschlagenen milCERT-Netz und dem bereits bestehenden zivilen Netz (CSIRT-Netz) für die Verbesserung des Informationsaustauschs und der Lageerfassung ist;

29. BEKRÄFTIGT auf der Grundlage der militärischen Vision und Strategie für den Cyberraum als Einsatzbereich und unter Berücksichtigung der laufenden Entwicklung des militärischen Konzepts für die Cyberabwehr bei EU-geführten militärischen Operationen und Missionen, dass die Cyberdimension in die Planung und Durchführung von GSVP-Missionen und -Operationen, einschließlich durch die Verbesserung ihrer Cyberkapazitäten, einfließen muss, und BETONT, dass dies zu einer besseren cyberbezogenen Lageerfassung auf EU-Ebene beitragen wird;

30. STELLT abschließend FEST, dass die Cyberabwehr ein Schritt hin zu einer EU-Doktrin für Maßnahmen im Cyberraum sein wird, die auf mehr Resilienz, Fähigkeiten und Reaktionsoptionen sowie einem gemeinsamen Standpunkt zur Anwendung des Völkerrechts im Cyberraum beruht. Der Rat wird 2023 eine BILANZ der Fortschritte bei der Umsetzung dieser Schlussfolgerungen ZIEHEN, um die Weiterentwicklung der Cyberabwehr der EU sicherzustellen.