Rat der
Europäischen Union

Brüssel, den 23. März 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	22. März 2021
Empfänger:	Delegationen
Betr.:	Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade – Vom Rat auf seiner Tagung vom 22. März 2021 gebilligte Schlussfolgerungen des Rates

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade, die der Rat auf seiner Tagung am 22. März 2021 gebilligt hat.

ANLAGE

Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS auf seine Schlussfolgerungen

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

– zur Internet-Governance[2],

– 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“[3],

– über Cybersicherheitskapazitäten und deren Aufbau in der EU[4],

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

– zur Zukunft eines hoch digitalisierten Europas nach 2020: „Förderung der digitalen und wirtschaftlichen Wettbewerbsfähigkeit in der gesamten Union und des digitalen Zusammenhalts“[6],

– zu zusätzlichen Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen[7],

– zur Gestaltung der digitalen Zukunft Europas[8],

---

1 Dok. 12109/13.
2 Dok. 16200/14.
3 Dok. 14435/17 + COR 1.
4 Dok. 7737/19.
5 Dok. 14517/19.
6 Dok. 9596/19.
7 Dok. 14972/19.
8 Dok. 8711/20.

– zur digitalen Diplomatie[9],

– zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen, einschließlich der Desinformation, im Zusammenhang mit der COVID-19-Pandemie[10],

– zur Cyberdiplomatie[11],

– zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen[12],

– zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (Instrumentarium für die Cyberdiplomatie/„Cyber Diplomacy Toolbox“)[13],

– zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten[14],

– zum Thema „Ein Aufschwung, der den Übergang zu einer dynamischeren, widerstandsfähigeren und wettbewerbsfähigeren europäischen Industrie voranbringt“[15],

– zur Cybersicherheit vernetzter Geräte[16],

– zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche[17],

sowie auf die Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung[18]

---

9 Dok. 12804/20.
10 Dok. 14064/20.
11 Dok. 6122/15 + COR 1.
12 Dok. 10086/18.
13 Dok. 10474/17.
14 Dok. 10496/18.
15 Dok. 13004/20.
16 Dok. 13629/20.
17 Dok. 14540/16.
18 Dok. 13084/1/20 REV 1.

und auf die Erklärung der Mitgliedstaaten vom 15. Oktober 2020 zum Aufbau der Cloud der nächsten Generation für Unternehmen und den öffentlichen Sektor in der EU;

UNTER HINWEIS auf die Schlussfolgerungen des Europäischen Rates zu COVID-19, zum Binnenmarkt, zur Industriepolitik und zur Digitalisierung sowie zu den Außenbeziehungen vom 1./2. Oktober 2020[19] und denjenigen zu Desinformation und hybriden Bedrohungen und zu einer neuen Strategischen Agenda 2019-2024 vom 20. Juni 2019[20];

UNTER HINWEIS auf die Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union – Gemeinsame Vision, gemeinsames Handeln: ein stärkeres Europa – vom 28. Juni 2016;

UNTER HINWEIS auf die Mitteilungen der Europäischen Kommission zur Gestaltung der digitalen Zukunft Europas vom 19. Dezember 2020[21] und zu der EU-Strategie für eine Sicherheitsunion vom 24. Juli 2020[22];

UNTER HINWEIS auf die Gemeinsame Mitteilung der Europäischen Kommission und des Hohen Vertreters über eine neue EU-US-Agenda für den globalen Wandel vom 2. Dezember 2020[23] —

1. HEBT HERVOR, dass die Cybersicherheit für den Aufbau eines widerstandsfähigen, grünen und digitalen Europas von wesentlicher Bedeutung ist, und BEGRÜßT die Gemeinsame Mitteilung an das Europäische Parlament und den Rat mit dem Titel „Die Cybersicherheitsstrategie der EU für die digitale Dekade“, in der der neue Rahmen für die Maßnahmen der EU im Bereich „Resilienz, technologische Souveränität und Führungsrolle“ umrissen und dargelegt wird, wie die Menschen, Unternehmen und Organe und Einrichtungen vor Cybervorfällen und -bedrohungen geschützt werden und gleichzeitig das Vertrauen von Personen und Organisationen in die Fähigkeit der EU zur Förderung sicherer und zuverlässiger Netz- und Informationssysteme, Infrastrukturen und Netzanbindungen gestärkt und ein globaler, offener, freier, stabiler und sicherer Cyberraum gefördert und geschützt wird, der auf Menschenrechte, Grundfreiheiten, Demokratie und Rechtsstaatlichkeit gegründet ist;

---

19 Dok. EUCO 13/20.
20 Dok. EUCO 9/19.
21 19.2.2020, Dok. COM(2020) 67 final.
22 24.7.2020, Dok. COM(2020) 605 final.
23 2.12.2020, Dok. JOIN(2020) 22 final.

2. IST SICH BEWUSST, dass die COVID-19-Pandemie das wachsende Bedürfnis nach Vertrauen in die Instrumente und Systeme der Informations- und Kommunikationstechnologie (IKT) und deren Sicherheit in den Mittelpunkt unseres täglichen Lebens gerückt hat; BETONT, dass Cybersicherheit und das globale und offene Internet für das Funktionieren der öffentlichen Verwaltung und der öffentlichen Institutionen sowohl auf nationaler als auch auf EU-Ebene sowie für unsere Gesellschaft und die Wirtschaft insgesamt von entscheidender Bedeutung sind;

3. BETONT die Notwendigkeit, das Bewusstsein für Cyberfragen auf den politischen und strategischen Entscheidungsebenen zu erhöhen, indem den Entscheidungsträgern relevante Kenntnisse und Informationen zur Verfügung gestellt werden, und UNTERSTREICHT die Notwendigkeit, die Sensibilisierung der breiten Öffentlichkeit zu verbessern und die Cyberhygiene zu fördern;

4. RUFT AUF zur Förderung und zum Schutz der zentralen Werte der EU – Demokratie, Rechtsstaatlichkeit sowie Menschenrechte und Grundfreiheiten, einschließlich des Rechts auf Meinungs- und Informationsfreiheit, des Rechts auf Versammlungs- und Vereinigungsfreiheit und des Rechts auf Privatsphäre im Cyberraum; BEGRÜßT in diesem Zusammenhang weitere anhaltende Anstrengungen zum Schutz von Menschenrechtsverteidigern, der Zivilgesellschaft und von Wissenschaftskreisen, die sich mit Fragen wie Cybersicherheit, Datenschutz, Überwachung und Zensur im Internet befassen, indem weitere praktische Leitlinien erstellt, bewährte Verfahren gefördert und die Bemühungen der EU zur Verhinderung von Menschenrechtsverletzungen und -verstößen sowie des Missbrauchs neu aufkommender Technologien verstärkt werden, indem insbesondere bei Bedarf diplomatische Maßnahmen ergriffen werden und die Ausfuhr solcher Technologien kontrolliert wird; BETONT in diesem Zusammenhang die Bedeutung des Aktionsplans der EU für Menschenrechte und Demokratie 2020-2024 und der darin enthaltenen Menschenrechtsleitlinien für die Meinungsfreiheit sowohl online als auch offline;

5. HEBT HERVOR, dass ein zentrales Ziel der Union darin besteht, strategische Autonomie zu erreichen und zugleich eine offene Wirtschaft zu bewahren, damit sie ihren wirtschaftlichen Weg und ihre Wirtschaftsinteressen selbst bestimmen kann. Dazu gehört auch die Stärkung der Fähigkeit zu autonomen Entscheidungen im Bereich der Cybersicherheit, um die digitale Führungsrolle der EU und ihre strategischen Kapazitäten zu stärken; WEIST DARAUF HIN, dass dazu auch die Ermittlung und Verringerung strategischer Abhängigkeiten und die Stärkung der Resilienz in den sensibelsten industriellen Ökosystemen und spezifischen Gebieten gehören; UNTERSTREICHT, dass dies die Diversifizierung der Produktions- und Lieferketten, die Förderung von Produktion und Investitionen in Europa und die Schaffung von Anreizen hierfür, die Erkundung von alternativen Lösungen und Kreislaufmodellen sowie die Förderung einer breit angelegten industriellen Zusammenarbeit zwischen den Mitgliedstaaten umfassen kann;

6. BETONT, in Anbetracht mangelnder digitaler und Cybersicherheitskompetenzen der Arbeitskräfte, die Bedeutung der Deckung der Nachfrage nach geschulten Arbeitskräften im Bereich der Digitalisierung und Cybersicherheit, indem insbesondere die besten Talente gefördert, gebunden und angezogen werden – beispielsweise durch allgemeine und berufliche Bildung –, um unsere Gesellschaft auf cybersichere Art und Weise digitalisieren zu können; ERMUTIGT zur stärkeren Teilhabe von Frauen und Mädchen an der Ausbildung in den Bereichen Mathematik, Informatik, Naturwissenschaften und Technik (MINT-Fächer) und an der beruflichen Aus- und Weiterbildung sowie Umschulung im IKT-Bereich in Bezug auf digitale Kompetenzen als ein Mittel zur Beseitigung der digitalen Kluft zwischen den Geschlechtern;

7. 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; BESTÄTIGT in diesem Zusammenhang ERNEUT sein Engagement für die friedliche Beilegung internationaler Streitigkeiten in Bezug auf den Cyberraum und dass alle diplomatischen Bemühungen der EU vorrangig darauf abzielen sollten, die Sicherheit und Stabilität im Cyberraum durch verstärkte internationale Zusammenarbeit zu fördern und das Risiko von Fehleinschätzungen, Eskalationen und Konflikten, die sich möglicherweise aus IKT-Vorfällen ergeben, zu verringern, und UNTERSTÜTZT die Weiterentwicklung und Umsetzung vertrauensbildender Maßnahmen auf regionaler und internationaler Ebene; BEKRÄFTIGT die seitens der Generalversammlung der Vereinten Nationen im Konsens vereinbarte Aufforderung, dass sich die EU-Mitgliedstaaten bei ihrer Nutzung von IKT an den Empfehlungen der Berichte der VN-Regierungssachverständigen (UNGGE) orientieren sollen, und BESTÄTIGT ERNEUT die Geltung des Völkerrechts – insbesondere der Charta der Vereinten Nationen in ihrer Gesamtheit – im Cyberraum;

8. BEKRÄFTIGT, dass die Weiterentwicklung von Normen und Standards innerhalb der Union – im Hinblick auf die wesentliche Gestaltung internationaler Normen und Standards in den Bereichen neu entstehender Technologien und der technischen und logischen Infrastruktur, die für die allgemeine Verfügbarkeit und Integrität des öffentlichen Kerns des Internets wesentlich sind, sodass sie mit den universellen Werten und den Werten der EU im Einklang stehen, und durch einen Multi-Stakeholder-Ansatz – von wesentlicher Bedeutung ist. Dadurch wird sichergestellt, dass das Internet global, offen, frei, stabil und sicher bleibt und dass bei der Nutzung und Entwicklung digitaler Technologien die Menschenrechte respektiert werden, und diese Nutzung auf rechtmäßige, sichere und ethische Weise erfolgt NIMMT KENNTNIS von der bevorstehenden Normungsstrategie und VERPFLICHTET SICH zur Ergreifung proaktiver und koordinierter Outreach-Maßnahmen, um die EU-Führungsrolle und die Ziele der EU auf internationaler Ebene, auch in verschiedenen internationalen Normungsgremien und durch Zusammenarbeit mit gleichgesinnten Partnern, der Zivilgesellschaft, der Wissenschaft und dem Privatsektor, zu fördern;

9. UNTERSTÜTZT MIT NACHDRUCK das Multi-Stakeholder-Modell für Internet-Governance und Cybersicherheit und verpflichtet sich, einen regelmäßigen und strukturierten Austausch mit den Interessenträgern – einschließlich Privatsektor, Wissenschaft und Zivilgesellschaft – in internationalen Foren, auch im Rahmen des Pariser Aufrufs zu Vertrauen und Sicherheit im Cyberraum, zu verstärken; FÖRDERT einen universellen, erschwinglichen und gleichberechtigten Zugang zum Internet zur Beseitigung der digitalen Kluft sowie insbesondere die Teilhabe von Frauen und Mädchen und Menschen, die sich in einer Situation der Gefährdung oder Ausgrenzung befinden, sowohl bei der Entwicklung von Strategien als auch bei der Nutzung des Internets;

10. BETONT die Notwendigkeit, Cybersicherheit in digitale Investitionen und Initiativen der kommenden Jahre einzubeziehen, und die Notwendigkeit, schrittweise zu fairen Wettbewerbsbedingungen im Bereich Cybersicherheit beizutragen, und NIMMT KENNTNIS von dem Plan der Kommission, die öffentlichen Ausgaben zu erhöhen und private Investitionen im Bereich der Cybersicherheit zu mobilisieren; HEBT die Bedeutung der kleinen und mittleren Unternehmen (KMU) im Cybersicherheits-Ökosystem HERVOR und WÜRDIGT die einschlägigen Finanzierungsinstrumente, die zur Unterstützung einer starken Konzentration auf die Cybersicherheit innerhalb des digitalen Wandels im Mehrjährigen Finanzrahmen (MFR) 2021-2027 sowie in der Aufbau- und Resilienzfazilität zur Verfügung stehen;

11. SIEHT der zügigen Umsetzung der Verordnung über das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und das Netz nationaler Koordinierungszentren (CCCN), einschließlich der raschen Einrichtung und Inbetriebnahme des Europäischen Kompetenzzentrums für Cybersicherheit in Bukarest, ERWARTUNGSVOLL ENTGEGEN. Eine unverzügliche Annahme ihrer Agenda wird dazu beitragen, die Wirkung der Investitionen zur Stärkung der Führungsrolle und strategischen Autonomie der Union im Bereich der Cybersicherheit zu maximieren und technologische Kapazitäten und Kompetenzen zu unterstützen und die globale Wettbewerbsfähigkeit der Union durch Beiträge von Industrie und Wissenschaft im Bereich Cybersicherheit – einschließlich KMU und Forschungszentren, die von einer systematischeren, integrativeren und strategischeren Zusammenarbeit im Hinblick auf den Zusammenhalt der Union und all ihrer Mitgliedstaaten profitieren werden – zu steigern;

12. BEGRÜßT die laufenden Arbeiten, die unter Führung der ENISA zusammen mit den Mitgliedstaaten und Interessenträgern durchgeführt werden, um der EU Zertifizierungssysteme für IKT-Produkte, -Dienste und -Prozesse zur Verfügung zu stellen, die dazu beitragen sollen, das allgemeine Niveau an Cybersicherheit im digitalen Binnenmarkt zu erhöhen; SIEHT in diesem Zusammenhang dem fortlaufenden Arbeitsprogramm der Union (URWP) im Hinblick auf die Entwicklung von Programmen für die Cybersicherheitszertifizierung der EU im Rahmen des Rechtsakts zur Cybersicherheit (CSA) ERWARTUNGSVOLL ENTGEGEN; WÜRDIGT in diesem Zusammenhang die zentrale Rolle der EU bei der Entwicklung von Standards, die die Cybersicherheitslandschaft prägen können und zur Gewährleistung eines fairen Wettbewerbs innerhalb der EU und auf globaler Ebene und zur Förderung des Marktzugangs sowie zur Bewältigung von Sicherheitsrisiken beitragen, während gleichzeitig die Anwendbarkeit des EU-Rechtsrahmens sichergestellt wird;

13. BEKRÄFTIGT die Bedeutung einer Bewertung in der Frage, ob langfristig horizontale Rechtsvorschriften, in denen auch die Bedingungen für das Inverkehrbringen festgelegt werden, notwendig sind, um alle einschlägigen Aspekte der Cybersicherheit vernetzter Geräte, wie Verfügbarkeit, Integrität und Vertraulichkeit, anzugehen; BEGRÜßT in diesem Zusammenhang eine Diskussion zur Auslotung der Tragweite solcher Rechtsvorschriften und ihrer Verbindungen zum Rahmen für die Cybersicherheitszertifizierung, wie sie im CSA festgelegt ist, mit dem Ziel, das Sicherheitsniveau im digitalen Binnenmarkt zu erhöhen; BETONT, dass Anforderungen an die Cybersicherheit im Einklang mit den einschlägigen Unionsvorschriften, einschließlich des CSA, des Neuen Rechtsrahmens (NLF), der Verordnung über die europäische Normung und eines möglichen künftigen horizontalen Rechtsakts, festgelegt werden sollten, um Zweideutigkeit und Fragmentierung innerhalb der Vorschriften zu vermeiden;

14. ERKENNT die Bedeutung eines umfassenden und horizontalen Ansatzes für die Cybersicherheit in der Union AN, wobei die Zuständigkeiten und Bedürfnisse der Mitgliedstaaten sowie die Bedeutung der kontinuierlichen Unterstützung der technischen Hilfe und Zusammenarbeit beim Aufbau der Kapazitäten der Mitgliedstaaten uneingeschränkt respektiert werden; NIMMT unter Berücksichtigung der Entwicklung der Bedrohungslandschaft KENNTNIS von dem neuen Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, der auf der NIS-Richtlinie aufbaut, und bekräftigt seine Unterstützung für die Stärkung und Harmonisierung der nationalen Cybersicherheitsrahmen und die nachhaltige Zusammenarbeit zwischen den Mitgliedstaaten; BETONT ferner die Notwendigkeit einer Angleichung und Verknüpfung der sektorspezifischen Rechtsvorschriften in diesem Bereich;

15. NIMMT KENNTNIS von dem Vorschlag der Kommission, die Mitgliedstaaten bei der Einrichtung und Stärkung von Sicherheitseinsatzzentren (SOC) zu unterstützen, um ein Netz von SOC in der gesamten EU aufzubauen, damit Anzeichen für Angriffe auf Netze weiter überwacht und antizipiert werden; ERWARTET in diesem Zusammenhang die detaillierten Pläne der Kommission in Bezug auf das Netz der SOC unter Wahrung der Zuständigkeiten der Mitgliedstaaten; WEIST auf die Bemühungen der Mitgliedstaaten HIN, mit Unterstützung der EU sektorale, nationale und regionale CSIRT und nationale oder europäische Informationsaustausch- und -analysezentren (ISAC) als Teil eines wirksamen Netzes von Cybersicherheitspartnerschaften in der Union zu errichten; SIEHT der Erkundung des Potenzials dieses Netzes zur Stärkung der SOC sowie ihrer Komplementarität und Koordinierung mit bestehenden Netzen und Akteuren (insbesondere dem CSIRT-Netz), womit eine effiziente, sichere und zuverlässige Kultur des Informationsaustauschs gefördert werden soll, ERWARTUNGSVOLL ENTGEGEN; BETONT, dass dieser Prozess auf der Arbeit aufbaut, die im Rahmen der Initiativen zu künstlicher Intelligenz und Hochleistungsrechnen und von den europäischen digitalen Innovationszentren geleistet wurde;

16. NIMMT KENNTNIS von der möglichen Entwicklung eines sicheren Konnektivitätssystems, das auf der europäischen Quantenkommunikationsinfrastruktur (EuroQCI) und der staatlichen Satellitenkommunikation in der Europäischen Union (GOVSATCOM) aufbaut, und ERKENNT AN, dass jede mögliche künftige Entwicklung auf einem soliden Cybersicherheitsrahmen basieren und die gesamte elektronische Kommunikationsinfrastruktur wie Weltraum-, Land- und Unterseenetze berücksichtigen sollte;

17. SIEHT den Gesprächen mit der Kommission, der ENISA, den Betreibern der beiden DNS-Root-Server in der EU sowie der Multi-Stakeholder-Gemeinschaft, bei denen die Rolle der beiden DNS-Root-Serverbetreiber in der EU bei der Sicherstellung eines weiterhin global zugänglichen und nicht fragmentierten Internets bewertet werden soll, ERWARTUNGSVOLL ENTGEGEN; BEGRÜßT die weitere Diskussion über die Absicht der Kommission, einen alternativen europäischen Dienst für den Zugang zum globalen Internet („DNS4EU“-Initiative) aufzubauen, der auf einem transparenten Modell basiert, das neuesten Sicherheits- und Datenschutznormen sowie den Grundsätzen des konzeptionsbedingten Datenschutzes und der datenschutzfreundlichen Voreinstellungen entspricht, um zu einer erhöhten Abwehrfähigkeit beizutragen und gleichzeitig die internationale Konnektivität für alle Mitgliedstaaten aufrechtzuerhalten und zu verbessern;

18. ANERKENNT die Notwendigkeit einer gemeinsamen Anstrengung der Kommission und der Mitgliedstaaten, um die Verbreitung wichtiger Internetstandards, einschließlich IPv6, und etablierter Internetsicherheitsstandards zu beschleunigen, da sie entscheidend dafür sind, das allgemeine Maß an Sicherheit, Abwehrfähigkeit, Offenheit und Interoperabilität des globalen Internets zu erhöhen und gleichzeitig die Wettbewerbsfähigkeit der europäischen Industrie und insbesondere der Internetinfrastrukturbetreiber zu steigern;

19. BETONT die Bedeutung eines koordinierten Ansatzes sowie die Entwicklung und Umsetzung wirksamer Maßnahmen auf nationaler Ebene zur Stärkung der Cybersicherheit von 5G-Netzen; UNTERSTÜTZT die nächsten Schritte zur Cybersicherheit von 5G-Netzen, wie sie in der Anlage zur Cybersicherheitsstrategie der EU dargelegt werden und auf den Ergebnissen des Berichts über die Auswirkungen der Empfehlung der Kommission über die Sicherheit von 5G-Netzen beruhen, beispielsweise im Hinblick auf die Festlegung eines langfristigen und umfassenden Ansatzes, der die gesamte 5G-Wertschöpfungskette und das gesamte 5G-Ökosystem berücksichtigt; FORDERT die Mitgliedstaaten, die EU-Organe und andere einschlägige Interessenträger NACHDRÜCKLICH AUF, im Hinblick auf eine weitere Stärkung des koordinierten Ansatzes für die Sicherheit von 5G-Netzen ihre regelmäßige Bestandsaufnahme zusammen mit dem Austausch von Informationen und bewährten Verfahren im Rahmen der Arbeit der eigens eingerichteten NIS-Kooperationsgruppe zur 5G-Cybersicherheit fortzusetzen und dem Rat regelmäßig über die erzielten Fortschritte Bericht zu erstatten; HEBT unter Betonung der Verantwortung der Mitgliedstaaten für den Schutz der nationalen Sicherheit sein Engagement dafür HERVOR, die Umsetzung der Maßnahmen des 5G-Instrumentariums der EU durchzuführen und zügig abzuschließen und sich weiterhin für die Sicherstellung der Sicherheit der 5G-Netze und die Entwicklung künftiger Netzgenerationen einzusetzen. Die enge Zusammenarbeit zwischen den Mitgliedstaaten, der Kommission und der ENISA bei der Sicherheit von 5G-Netzen könnte als Beispiel für andere Fragen im Bereich der Cybersicherheit dienen, wobei die Zuständigkeiten der Mitgliedstaaten und die Grundsätze der Subsidiarität und der Verhältnismäßigkeit zu wahren sind;

20. IST SICH der Relevanz der weiteren Integration der Cybersicherheit in die Krisenreaktionsmechanismen der EU und deren Erprobung bei einschlägigen Übungen BEWUSST und HEBT die Bedeutung der Verbesserung der Zusammenarbeit und des Informationsaustauschs zwischen den verschiedenen Cybergemeinschaften innerhalb der EU und der Verknüpfung bestehender Initiativen, Strukturen und Verfahren (wie die IPCR, das CSIRT-Netz, die NIS-Kooperationsgruppe, das CyCLONe, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität, das EU-INTCEN und andere einschlägige EU-Einrichtungen) im Falle groß angelegter grenzüberschreitender Cybervorfälle oder -krisen HERVOR; ERWARTET ANGESICHTS der in diesem Bereich bereits erzielten Fortschritte den Vorschlag der Kommission zu dem Verfahren, den Etappenziele und dem Zeitplan für die Festlegung der gemeinsamen Cyberstelle (JCU), um einen Mehrwert und klaren Schwerpunkt zu schaffen und den europäischen Rahmen für das Krisenmanagement im Bereich der Cybersicherheit zu straffen, unter anderem durch – transparent und stufenweise verwirklichte – Bereitschaft, gemeinsame Lageerfassung, Stärkung der koordinierten Reaktion und Übungen bei gleichzeitiger Vermeidung von Doppelarbeit und Überschneidungen und unter Wahrung der Zuständigkeiten der Mitgliedstaaten;

21. BETONT sowohl die Bedeutung der Förderung der Zusammenarbeit und des Informationsaustauschs zwischen den einschlägigen Akteuren im Bereich der Cybersicherheit und den zuständigen Behörden im Bereich Sicherheit und Strafjustiz, z. B. Strafverfolgungs- und Justizbehörden, als auch die Notwendigkeit der Erweiterung und Verbesserung der Kapazitäten dieser Behörden zur Ermittlung und Verfolgung von Cyberkriminalität und der Förderung internationaler Verhandlungen und EU-Vorschriften über den grenzüberschreitenden Zugriff auf elektronische Beweismittel. Unabhängig vom derzeitigen technologischen Umfeld ist es unerlässlich, die Befugnisse der zuständigen Behörden im Bereich Sicherheit und Strafjustiz durch rechtmäßigen Zugriff zu wahren, damit sie ihre Aufgaben wie gesetzlich vorgeschrieben und zulässig wahrnehmen können. Solche Gesetze, in denen die Durchsetzungsbefugnisse vorgesehen sind, müssen stets im vollen Einklang mit einem ordnungsgemäßen Verfahren und anderen Garantien sowie den Grundrechten stehen, insbesondere dem Recht auf Achtung des Privatlebens und der privaten Kommunikation und dem Recht auf den Schutz personenbezogener Daten;

22. BESTÄTIGT ERNEUT seine Unterstützung für die Entwicklung, Umsetzung und Nutzung einer starken Verschlüsselung als notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Einzelpersonen, Regierungen, Industrie und Gesellschaft und ERKENNT gleichzeitig die Notwendigkeit der Sicherstellung der Fähigkeit der zuständigen Behörden im Bereich Sicherheit und Strafjustiz, z. B. Strafverfolgungs- und Justizbehörden, ihre rechtmäßigen Befugnisse sowohl online als auch offline ausüben können, um unsere Gesellschaften und Bürgerinnen und Bürger zu schützen, AN. Die zuständigen Behörden müssen unter uneingeschränkter Achtung der Grundrechte und der einschlägigen Datenschutzgesetze rechtmäßig und gezielt auf Daten zugreifen können und gleichzeitig die Cybersicherheit wahren; BETONT, dass bei allen Maßnahmen diese Interessen sorgfältig gegen die Grundsätze der Notwendigkeit, Verhältnismäßigkeit und Subsidiarität abgewogen werden müssen;

23. UNTERSTÜTZT und FÖRDERT das Budapester Übereinkommen über Computerkriminalität und die laufenden Arbeiten am zweiten Zusatzprotokoll zu diesem Übereinkommen; BETEILIGT SICH darüber hinaus weiterhin an einem multilateralen Austausch über Cyberkriminalität, u. a. auch im Rahmen von Prozessen im Zusammenhang mit dem Europarat, dem Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) und der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ), um eine verstärkte internationale Zusammenarbeit bei der Bekämpfung der Cyberkriminalität, einschließlich des Austauschs bewährter Verfahren und technischer Kenntnisse und der Unterstützung beim Aufbau von Kapazitäten, zu gewährleisten, wobei die Menschenrechte und Grundfreiheiten respektiert, gefördert und geschützt werden;

24. WÜRDIGT – während die nationale Sicherheit in der alleinigen Verantwortung jedes Mitgliedstaats liegt – die Bedeutung der strategischen nachrichtendienstlichen Zusammenarbeit gegen Cyberbedrohungen und -aktivitäten und ERSUCHT die Mitgliedstaaten, über ihre zuständigen Behörden weiterhin einen Beitrag zur Arbeit des EU-INTCEN als Plattform für Lageerfassung und Bewertungen von Bedrohungen in Cyberfragen für die EU zu leisten und den Vorschlag für die etwaige Einrichtung einer Arbeitsgruppe der Mitgliedstaaten für EU-Cybernachrichtendienste zu prüfen, um die eigene Kapazität des INTCEN in diesem Bereich auf Grundlage freiwilliger nachrichtendienstlicher Beiträge seitens der Mitgliedstaaten und unbeschadet ihrer Zuständigkeiten zu stärken;

25. HEBT HERVOR, wie wichtig ein robuster und kohärenter Sicherheitsrahmens ist, um alle Mitarbeiter, Daten, Kommunikationsnetze und Informationssysteme der EU sowie Entscheidungsprozesse auf Grundlage umfassender, kohärenter und einheitlicher Regeln zu schützen. Dies sollte insbesondere durch die Stärkung der Abwehrfähigkeit und die Verbesserung der Sicherheitskultur der EU gegenüber Cyberbedrohungen sowie durch die Stärkung der Sicherheit von vertraulichen und nicht vertraulichen EU-Netzen erfolgen, während eine angemessene Governance und die Bereitstellung ausreichender Ressourcen und Fähigkeiten, auch im Zusammenhang mit der Stärkung des Mandats des CERT-EU, sichergestellt wird; BEGRÜßT in diesem Zusammenhang die laufenden Beratungen über die Festlegung gemeinsamer Vorschriften für die Informationssicherheit unter gebührender Berücksichtigung der Sicherheitsvorschriften des Rates für den Schutz von EU-Verschlusssachen sowie über die Festlegung gemeinsamer verbindlicher Cybersicherheitsvorschriften für alle Organe, Einrichtungen und Agenturen der EU;

26. VERPFLICHTET SICH, AUFBAUEND auf die Bemühungen der EU im Bereich Cyberdiplomatie, die Wirksamkeit und Effizienz des Instrumentariums für die Cyberdiplomatie zu erhöhen und SIEHT einer Vertiefung der Beratungen über dessen Anwendungsbereich und Nutzung aufbauend auf den bisherigen Erfahrungen bei der Anwendung dieses Instrumentariums ERWARTUNGSVOLL ENTGEGEN. Diese Beratungen sollten zur Förderung der Sicherheit auf internationaler Ebene beitragen, indem sie den Dialog sowie eine gemeinsame Vision in Fragen der Cybersicherheit fördern, Prävention, Stabilität und Zusammenarbeit stärken und Vertrauen fördern und Kapazitäten aufbauen und erforderlichenfalls die Anwendung restriktiver Maßnahmen beinhalten, um böswilligen Cyberaktivitäten, die auf die Integrität und Sicherheit der EU und ihrer Mitgliedstaaten abzielen, vorzubeugen, sie zu verhindern, von ihnen abzuschrecken und auf sie zu reagieren, wodurch unter uneingeschränkter Achtung der nationalen Zuständigkeiten und Vorrechte ein Beitrag zur internationalen Sicherheit und Stabilität und zur Konsolidierung der Cyberabwehr der EU geleistet wird. Besondere Aufmerksamkeit sollte insbesondere der Prävention und Bekämpfung von Cyberangriffen mit systemischen Auswirkungen gelten, die unsere Lieferketten, kritischen Infrastrukturen und grundlegenden Dienste, demokratischen Institutionen und Prozesse beeinträchtigen und unsere wirtschaftliche Sicherheit, auch durch mit dem Cyberraum ermöglichten Diebstahl geistigen Eigentums, untergraben können. Die Mitgliedstaaten und die Organe der EU sollten auch weitere Überlegungen über die Verknüpfung zwischen dem europäischen Rahmen für das Krisenmanagement im Bereich der Cybersicherheit, dem Instrumentarium für die Cyberdiplomatie und den Bestimmungen des Artikels 42 Absatz 7 EUV und des Artikels 222 AEUV anstellen, insbesondere durch szenariobasierte Arbeit, um ein gemeinsames Verständnis der praktischen Modalitäten für die Umsetzung des Artikels 42 Absatz 7 EUV zu schaffen;

27. WÜRDIGT die Bedeutung der Stärkung der Zusammenarbeit mit internationalen Organisationen und Partnerländern, um das gemeinsame Verständnis der Cyberbedrohungslandschaft voranzubringen, Dialoge und Kooperationsmechanismen zu entwickeln, gegebenenfalls kooperative diplomatische Reaktionen zu identifizieren sowie den Informationsaustausch zu verbessern, unter anderem durch Ausbildung, Schulung und Übungen; HEBT insbesondere HERVOR, dass eine starke transatlantische Partnerschaft im Bereich der Cybersicherheit zu unserer gemeinsamen Sicherheit, Stabilität und unserem Wohlstand beiträgt, und NIMMT KENNTNIS von den Bestimmungen über die Zusammenarbeit im Bereich der Cybersicherheit im Rahmen des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich; BEKRÄFTIGT UNTER HINWEIS auf die entscheidenden Errungenschaften der Zusammenarbeit zwischen EU und NATO im Bereich der Cybersicherheit im Rahmen der Umsetzung der Gemeinsamen Erklärungen von Warschau von 2016 und von Brüssel von 2018 die Bedeutung einer engeren, sich gegenseitig verstärkenden und für beide Seiten vorteilhaften Zusammenarbeit durch Ausbildung, Schulung und Übungen und einer koordinierten Reaktion auf böswillige Cyberaktivitäten unter uneingeschränkter Achtung der Beschlussfassungsautonomie und der Verfahren beider Organisationen auf Grundlage der Grundsätze der Transparenz, der Gegenseitigkeit und der Inklusivität;

28. VERPFLICHTET SICH – um zu einem globalen, offenen, freien, stabilen und sicheren Cyberraum beizutragen, der für den anhaltenden Wohlstand, das Wachstum, die Sicherheit, das Wohlergehen, die Konnektivität und die Integrität unserer Gesellschaften von immer größerer Bedeutung wird –, sich kontinuierlich an Normierungsverfahren in internationalen Organisationen zu beteiligen, insbesondere im Rahmen von mit dem ersten Ausschuss der Vereinten Nationen zusammenhängenden Verfahren, um die Anerkennung der Anwendung des Völkerrechts im Cyberraum und die Einhaltung der Normen, Regeln und Grundsätze für verantwortungsvolles staatliches Handeln im Cyberraum – unter anderem durch die Förderung der raschen Einrichtung eines Aktionsprogramms (PoA) zur Förderung verantwortungsvollen staatlichen Handelns im Cyberraum als konstruktive, integrative und einvernehmliche Weiterverfolgung der beiden aktuellen Prozesse der Gruppe von Regierungssachverständigen (UN GGE) und der offenen Arbeitsgruppe (OEWG) – zu fördern und dazu beizutragen;

29. WEIST auf sein starkes Engagement für einen wirksamen Multilateralismus und eine auf Regeln basierende internationale Ordnung mit den Vereinten Nationen als Mittelpunkt und seine Entschlossenheit HIN, die Zusammenarbeit und Koordinierung mit internationalen und regionalen Organisationen – insbesondere mit dem VN-System, der NATO, dem Europarat, der OSZE, der OECD, der AU, der OAS, dem ASEAN, dem ARF, dem Golf-Kooperationsrat und der LAS – in Bezug auf Beratungen zu Cyberfragen sowie die Fortsetzung und Ausweitung strukturierter EU-Cyberdialoge und -konsultationen mit Drittländern zu stärken; BETONT seine aktive Unterstützung der Vereinten Nationen, insbesondere in Bezug auf ihre Agenda 2030, einschließlich der Ziele für nachhaltige Entwicklung, und BEGRÜßT den Fahrplan des Generalsekretärs der Vereinten Nationen für die digitale Zusammenarbeit und die Abrüstungsagenda des Generalsekretärs der Vereinten Nationen, mit denen die Rechenschaftspflicht und Einhaltung von Normen im Cyberraum gefördert werden und die zur Prävention und gütlichen Beilegung von Konflikten aufgrund böswilliger Aktivitäten im Cyberraum beitragen; BEGRÜßT den Vorschlag des Hohen Vertreters der Union für Außen- und Sicherheitspolitik, ein informelles EU-Netz für Cyberdiplomatie einzurichten, um das Engagement und das Fachwissen sowohl der EU als auch der Mitgliedstaaten in internationalen Cyberfragen weiterzuentwickeln, um koordinierte Outreach-Maßnahmen zu stärken;

30. SIEHT dem bevorstehenden Vorschlag für eine Überprüfung des Rahmens für die Cyberabwehr (CDPF) ERWARTUNGSVOLL ENTGEGEN und VERPFLICHTET SICH, die Anstrengungen zur Stärkung der Dimensionen Cybersicherheit und Cyberabwehr fortzusetzen, um sicherzustellen, dass diese vollständig in den breiteren Bereich Sicherheit und Verteidigung integriert werden, insbesondere im Rahmen der Arbeit am Strategischen Kompass; IST DER AUFFASSUNG, dass die künftige „militärische Vision und Strategie für den Cyberraum als Einsatzbereich“ zur Förderung dieser Beratungen beitragen wird; BEGRÜßT die Initiative der Europäischen Verteidigungsagentur (EDA), die Zusammenarbeit zwischen militärischen CERT zu fördern, und UNTERSTÜTZT die Bemühungen zur Verbesserung der zivil-militärischen Synergien und der Koordinierung in den Bereichen Cyberabwehr und Cybersicherheit, auch hinsichtlich weltraumbezogener Aspekte, unter anderem durch die speziellen Projekte des SSZ;

31. BEGRÜßT den Vorschlag zur Entwicklung einer EU-Agenda für den Aufbau externer Cyberkapazitäten, den Vorschlag zur Einrichtung eines EU-Gremiums für den Cyberkapazitätsaufbau und die Einrichtung und Umsetzung des EU-Netzes für den Cyberkapazitätsaufbau (EU CyberNet), um die Cyberresilienz und -kapazitäten weltweit zu erhöhen. BEGRÜßT in diesem Zusammenhang die Zusammenarbeit mit den Mitgliedstaaten sowie mit Partnern aus dem öffentlichen und dem privaten Sektor, insbesondere dem Globalen Forum für Cyber-Fachwissen (GFCE) und anderen einschlägigen internationalen Gremien, um die Koordinierung zu gewährleisten und Doppelarbeit zu vermeiden; ERMUTIGT insbesondere zur Zusammenarbeit mit den Partnern im westlichen Balkan sowie in der östlichen und südlichen Nachbarschaft der EU;

32. VERPFLICHTET SICH – um sicherzustellen, dass alle Länder in der Lage sind, von den sozialen, wirtschaftlichen und politischen Vorteilen des Internets und der Nutzung von Technologien zu profitieren –, die Partnerländer bei der Bewältigung der wachsenden Herausforderungen durch böswillige Cyberaktivitäten, die der Entwicklung ihrer Volkswirtschaften und Gesellschaften und der Integrität und Sicherheit demokratischer Systeme schaden, zu unterstützen, auch im Einklang mit den Bemühungen im Rahmen des Europäischen Aktionsplans für Demokratie;

33. ERMUTIGT die Kommission und den Hohen Vertreter der Union für Außen- und Sicherheitspolitik, einen detaillierten Umsetzungsplan mit den Prioritäten und dem Zeitplan für die geplanten Maßnahmen aufzustellen, um die Entwicklung, Umsetzung und Überwachung der im Rahmen der Cybersicherheitsstrategie der EU vorgelegten Vorschläge sicherzustellen und dabei dem Mehrjahrescharakter einiger der Initiativen Rechnung zu tragen; WIRD die Fortschritte bei der Umsetzung dieser Schlussfolgerungen mittels eines Aktionsplans ÜBERWACHEN, der vom Rat in enger Zusammenarbeit mit der Europäischen Kommission und dem Hohen Vertreter regelmäßig überprüft und aktualisiert wird.