Rat der
Europäischen Union

Brüssel, den 17. Oktober 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	17. Oktober 2022
Empfänger:	Delegationen
Nr. Vordok.:	12930/22
Betr.:	Schlussfolgerungen des Rates zur Sicherheit der IKT-Lieferketten – Schlussfolgerungen des Rates, gebilligt auf seiner Tagung vom 17. Oktober 2022

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Sicherheit der IKT-Lieferketten, die der Rat auf seiner Tagung am 17. Oktober 2022 gebilligt hat.

ANLAGE

Schlussfolgerungen des Rates zur Sicherheit der IKT-Lieferketten

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS auf 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“,

– über Cybersicherheitskapazitäten und deren Aufbau in der EU,

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

– zur Gestaltung der digitalen Zukunft Europas,

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

– zur Cybersicherheit vernetzter Geräte,

– zur Cybersicherheitsstrategie der EU für die digitale Dekade,

– zur Entwicklung der Cyberabwehr der Europäischen Union,

– zum Sonderbericht Nr. 03/2022 des Europäischen Rechnungshofs mit dem Titel „5G-Einführung in der EU: Verzögerungen beim Auf- und Ausbau der Netze und ungelöste Sicherheitsprobleme“;

UNTER HINWEIS auf die Schlussfolgerungen des Europäischen Rates

– vom 1./2. Oktober 2020 zu den Themen COVID-19, Binnenmarkt, Industriepolitik und Digitalisierung sowie Außenbeziehungen,

– vom 24./25. März 2022 zu den Themen militärische Aggression Russlands gegen die Ukraine, Sicherheit und Verteidigung, Energie, wirtschaftliche Aspekte, COVID-19 sowie Außenbeziehungen,

– vom 30./31. Mai 2022 zu den Themen Ukraine, Ernährungssicherheit, Sicherheit und Verteidigung sowie Energie —

1. BEKRÄFTIGT angesichts der zunehmenden Bedeutung der Geopolitik für die Cybersicherheit, dass die Europäische Union und ihre Mitgliedstaaten einen umfassenden und strategischen Ansatz in Bezug auf die Cybersicherheit verfolgen müssen. Russlands militärische Aggression gegen die Ukraine hat zu einer umfassenden Verschiebung im strategischen und sicherheitspolitischen Umfeld der Europäischen Union geführt und gezeigt, dass es im Bereich Sicherheit und Verteidigung einer stärkeren und fähigeren Europäischen Union bedarf. Dadurch wurde deutlich, dass es von größter Bedeutung ist, das geopolitische Umfeld nicht nur bei der Reaktion auf böswillige Cyberaktivitäten angemessen zu berücksichtigen, sondern auch beim Aufbau und der Aufrechterhaltung der Resilienz von Informations- und Kommunikationstechnologien (IKT). Dies ist besonders relevant für die Lieferketten von IKT-Produkten und -Diensten (im Folgenden „IKT-Lieferketten“), die sowohl auf der Grundlage geopolitischer Rivalitäten gefährdet sein könnten, wie durch den SolarWinds-Angriff veranschaulicht wurde, als auch durch geopolitische Spannungen und Instabilität beeinträchtigt werden könnten, wie durch die Gefahr im Zusammenhang mit der Abhängigkeit von russischen IKT-Anbietern angesichts der militärischen Aggression Russlands gegen die Ukraine deutlich wurde;

2. WEIST DARAUF HIN, dass die Risiken im Zusammenhang mit IKT-Lieferketten, die sich aus einer eng verzahnten Reihe von Ressourcen und Prozessen zwischen Wirtschaftsakteuren (im Sinne der Verordnung (EU) 2019/1020) zusammensetzen, die mit der Beschaffung von Rohstoffen beginnt und über die Herstellung, Verarbeitung und Handhabung bis zur Lieferung von IKT-Produkten und -Diensten, einschließlich Erbringung von Unterstützungsleistungen während des Lebenszyklus der IKT-Produkte und -Dienste, reicht, aufgrund ihres Wesens einzigartige Herausforderungen und potenziell weitreichende Folgen mit sich bringen. Neben den Risiken im Zusammenhang mit der Nichtverfügbarkeit von IKT-Produkten, z. B. aufgrund von Engpässen bei kritischen Rohstoffen und Halbleitern, die für ihre Herstellung benötigt werden, sind die Lieferketten von IKT-Produkten und -Diensten auch anderen Gefahren ausgesetzt. Insbesondere können sie von böswilligen Akteuren durch ausgefeilte, oft verborgene Methoden ins Visier genommen oder missbraucht werden, die die Vertraulichkeit, Integrität und Verfügbarkeit von übertragenen und gespeicherten sensiblen Daten beeinträchtigen;

3. WÜRDIGT – unter Anerkennung, dass ein gefahrenübergreifender Ansatz bei der Sicherung von IKT-Ressourcen vonnöten ist, – die Bedeutung des Vorschlags für eine Richtlinie über die Resilienz kritischer Einrichtungen für die Verbesserung der physischen Sicherheit kritischer Einrichtungen, und BEKRÄFTIGT, dass es neben der Verbesserung der Resilienz gegen Angriffe auf Lieferketten mittels Cybermethoden gleichermaßen wichtig ist, die Resilienz und Sicherheit von IKT-Lieferketten insgesamt gegen die gesamte Vielfalt von Risikofaktoren, wie Naturereignisse, Systemausfälle, Insider-Bedrohungen oder menschliches Versagen, zu stärken; ERKENNT in dieser Hinsicht AN, dass die Sicherheit der IKT-Lieferketten die Gewährleistung des Schutzes der in IKT-Lieferketten hergestellten, gelieferten, erbrachten und verwendeten IKT-Produkte und -Dienste umfasst, auch durch den Schutz einzelner Bestandteile und übertragener Daten;

4. ERMUTIGT die Mitgliedstaaten – gestützt auf die Lehren aus den Folgen der strategischen Abhängigkeiten der Europäischen Union von fossilen Brennstoffen aus Russland und aus den Auswirkungen der Unterbrechungen der Lieferketten während der COVID-19-Pandemie, insbesondere in Bezug auf Arzneimittel und Halbleiter, bei denen die strategischen Abhängigkeiten der EU aufgezeigt wurden, – darauf hinzuarbeiten, ähnliche Situationen ungewollter strategischer externer Abhängigkeiten in Bezug auf IKT-Produkte und -Dienste zu vermeiden. Aufgrund der steigenden Digitalisierung der Gesellschaft und der stetig zunehmenden Nutzung von IKT in kritischen Infrastrukturen sollten strategische externe Abhängigkeiten im Zusammenhang mit IKT-Produkten und -Diensten und deren Lieferketten kontinuierlich bewertet und – sofern erforderlich – angegangen werden;

5. WEIST DARAUF HIN, dass die Herbeiführung von strategischer Autonomie bei gleichzeitiger Aufrechterhaltung einer offenen Wirtschaft ein zentrales Ziel der Union ist, zu dem auch die Ermittlung und Verringerung strategischer Abhängigkeiten und die Steigerung der Resilienz in den sensibelsten industriellen Ökosystemen und spezifischen Bereichen, einschließlich des digitalen Bereichs, gehört. Dies umfasst die Entwicklung und den Einsatz strategischer digitaler Kapazitäten und Infrastrukturen sowie die Stärkung der Fähigkeit, autonome technische Entscheidungen zu treffen, und – als eine der wichtigsten Säulen – die Gewährleistung resilienter und sicherer Infrastrukturen, Produkte und Dienste im Hinblick auf den Aufbau von Vertrauen in den digitalen Binnenmarkt und innerhalb der europäischen Gesellschaft, bei gleichzeitiger Erhaltung von Offenheit, globaler Zusammenarbeit mit gleichgesinnten Partnern und Wettbewerbsfähigkeit und der Nutzung der potenziellen Vorteile daraus. Die Grundwerte der Europäischen Union umfassen insbesondere die Privatsphäre, Sicherheit, Gleichberechtigung, die Menschenwürde, Rechtsstaatlichkeit sowie das offene Internet als Voraussetzungen für eine von digitalen Technologien geleitete und auf den Menschen ausgerichtete Gesellschaft, Wirtschaft und Industrie;

6. STELLT FEST, dass aufgrund von Entwicklungen der Bedrohungslage im Cyberbereich, wie durch die aufkommende Tendenz zu auswirkungsintensiven und ausgefeilten Angriffen auf Lieferketten in den vergangenen Jahren, etwa durch SolarWinds, Mimecast oder Kaseya, verdeutlicht wird, verbunden mit der Auslagerung wesentlicher IKT-Dienste und verstärkt durch die breite Abhängigkeit von IKT-Produkten und -Diensten, die von Dritten hergestellt, erbracht oder gepflegt werden, ein künftiges verstärktes Auftreten von Angriffen auf Lieferketten mit erheblichem Schaden für die Wirtschaft und die Gesellschaft sehr wahrscheinlich ist; BEKRÄFTIGT vor diesem Hintergrund, wie wichtig die Verbesserung der Sicherheit und Resilienz der IKT-Lieferketten für das Funktionieren des Binnenmarkts ist, zusammen mit der Notwendigkeit, die Verfügbarkeit, Sicherheit und Vielfalt von IKT-Produkten und -Diensten im Binnenmarkt zu gewährleisten; IST SICH daher BEWUSST, dass die Nutzung bestehender Instrumente und Konzepte der EU zur Verwirklichung dieser Ziele maximiert und gestrafft werden muss und dass eine kontinuierliche Anpassung an die sich verändernde Bedrohungslage im Cyberbereich erfolgen muss, indem zusätzliche geeignete Maßnahmen und Mechanismen eingeführt werden, auch im Zusammenhang mit etwaigen Sicherheitsrisiken neuer disruptiver Technologien; ERMUTIGT die Mitgliedstaaten, diesbezüglich einen risikobasierten Ansatz im Hinblick auf neue technologische Entwicklungen zu verfolgen;

7. IST SICH BEWUSST, dass das Verständnis der sich ständig entwickelnden Bedrohungslage im Cyberbereich sowie der Komplexität von Angriffen auf Lieferketten von entscheidender Bedeutung für eine wirksame Minderung der Risiken im Zusammenhang mit den IKT-Lieferketten ist; BETONT in diesem Zusammenhang, dass die Anpassung an neue Bedrohungen durch aktive und kontinuierliche Beobachtung, Analyse und Bewertung der Bedrohungslage für Lieferketten, die Sensibilisierung und der Wissensaufbau in Bezug auf Bedrohungen und Schwachstellen sowie die proaktive und gezielte Warnung der einschlägigen Einrichtungen unerlässlich sind; BEGRÜßT die Arbeit der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Zusammenhang mit der Sicherheit der IKT-Lieferketten, insbesondere ihren Bericht über die Bedrohungslage hinsichtlich Angriffen auf Lieferketten;

SEKTORÜBERGREIFENDE INSTRUMENTE UND ANSÄTZE

8. BEKRÄFTIGT, wie wichtig es ist, dass die Mitgliedstaaten die Notwendigkeit einer Diversifizierung der Anbieter kritischer IKT prüfen, um die Entstehung wesentlicher Abhängigkeiten von einzelnen Anbietern, und insbesondere Hochrisikoanbietern, zu vermeiden oder zu begrenzen, da dies die Anfälligkeit für die Folgen potenzieller Störungen erhöht; ERKENNT AN, dass die Vermeidung von Anbieterabhängigkeit und die Diversifizierung von IKT-Anbietern zu den wichtigsten Komponenten für die Gewährleistung von Stabilität und Sicherheit des Binnenmarkts gehören; HEBT HERVOR, dass angemessene Strategien zur Erleichterung der Diversifizierung von Anbietern und Verbesserung der Wettbewerbsfähigkeit technologieneutral gefördert und umgesetzt werden müssen; ERMUTIGT darüber hinaus dazu, Aspekte im Zusammenhang mit der Vermeidung von Anbieterabhängigkeit in die EU-Rechtsvorschriften aufzunehmen; WÜRDIGT diesbezüglich den Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), mit dem darauf abgezielt wird, die Interoperabilität von Datenverarbeitungsdiensten zu erhöhen und Hindernisse für den Wechsel zwischen Anbietern von Datenverarbeitungsdiensten zu beseitigen;

9. IST SICH BEWUSST, dass eine Verbindung zwischen der Sicherheit der IKT-Lieferketten und der Vergabe öffentlicher Aufträge besteht; BEKRÄFTIGT, dass der Bedeutung der Sicherheit der IKT-Lieferketten bei den Verfahren zur Vergabe öffentlicher Aufträge angemessen Rechnung getragen werden muss, indem gegebenenfalls objektive und risikobasierte Auswahlkriterien im Zusammenhang mit der Fähigkeit der Bieter, ein hohes Maß an Sicherheit der erbrachten Dienste zu gewährleisten, festgelegt werden; FORDERT, dass ein angemessenes Gleichgewicht zwischen dem öffentlichen Interesse an einer möglichst effizienten und fairen Nutzung öffentlicher Mittel einerseits und dem öffentlichen Interesse an der Sicherung von Informationssystemen und der Gewährleistung eines reibungslosen Funktionierens des Binnenmarkts andererseits gefunden wird; ERSUCHT die Kommission, zur Erleichterung der Umsetzung der einschlägigen Vorschriften für die Vergabe öffentlicher Aufträge im Hinblick auf die Steigerung der Cybersicherheit, bis zum dritten Quartal 2023 methodische Leitlinien auszuarbeiten, um die öffentlichen Auftraggeber dazu zu ermutigen, ein angemessenes Augenmerk auf die Cybersicherheitsverfahren von Bietern und ihren Unterauftragnehmern zu legen, sowie die einschlägigen Rechtsvorschriften für die Vergabe öffentlicher Aufträge zu prüfen und erforderlichenfalls Vorschläge für deren Überarbeitung oder Ergänzung vorzulegen;

10. IST SICH BEWUSST, dass ausländische Direktinvestitionen im Zusammenhang mit IKT-Produkten und -Diensten zwar einen wirtschaftlichen und gesellschaftlichen Nutzen für Mitgliedstaaten, Unternehmen sowie Bürgerinnen und Bürger bieten, aber auch Risiken für die Sicherheit und die öffentliche Ordnung bergen könnten, und WEIST DARAUF HIN, dass der Überprüfungsmechanismus der EU für ausländische Direktinvestitionen zusammen mit den jeweiligen nationalen Überprüfungssystemen, die Mittel zur Bekämpfung dieser Risiken bieten, auch als nützliches Instrument zur Wahrung der Sicherheit und Resilienz der IKT-Lieferketten eingesetzt werden könnte, da damit zur Verhinderung risikoreicher Investitionen beigetragen würde, die diese Sicherheit und Resilienz beeinträchtigen können; ERKENNT AN, dass der Austausch und die gemeinsame Nutzung von Informationen über diesen Mechanismus den Mitgliedstaaten dabei helfen könnten, die möglichen Bedrohungen für die Sicherheit der IKT-Lieferketten besser einzuschätzen und die jeweils erforderlichen Schritte zu ergreifen; RUFT die einschlägigen nationalen Akteure AUF, erforderlichenfalls auch diese Dimension des Überprüfungsmechanismus zu berücksichtigen;

11. BEKRÄFTIGT in Bezug auf den Bereich Verteidigung seine Aufforderung an die Kommission, im Jahr 2023 zusammen mit den Mitgliedstaaten eine Bewertung der Risiken für die Lieferketten kritischer Infrastrukturen in verschiedenen Bereichen, einschließlich des digitalen Bereichs, im Zusammenhang mit den sicherheits- und verteidigungspolitischen Interessen der EU vorzunehmen und die Optionen zur Steigerung der Cybersicherheit entlang der gesamten Lieferkette der technologischen und industriellen Basis der europäischen Verteidigung zu erforschen; ERSUCHT die Mitgliedstaaten und die Kommission darüber hinaus, Überlegungen über die Sicherheit der IKT-Lieferketten bei der Umsetzung der Verpflichtungen und Maßnahmen im Rahmen des Strategischen Kompasses anzustellen;

12. ERMUTIGT – unter Würdigung der Bedeutung kritischer Rohstoffe sowie aller Arten von Halbleitern als grundlegende Bausteine für IKT-Produkte – zu konstruktiven Verhandlungen über den Vorschlag für eine Verordnung zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Halbleiter-Ökosystems (Chip-Gesetz) und den Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung (EU) 2021/2085 zur Gründung der gemeinsamen Unternehmen im Rahmen von „Horizont Europa“ hinsichtlich des Gemeinsamen Unternehmens für Chips;

CYBERSPEZIFISCHE INSTRUMENTE

13. WÜRDIGT – insbesondere in Bezug auf die Telekommunikationsinfrastruktur – die Erfolge auf Unionsebene zur Verbesserung der Sicherheit der Lieferketten für 5G-Netze, besonders durch das EU-Instrumentarium für die 5G-Cybersicherheit (5G-Toolbox); FORDERT die Mitgliedstaaten AUF, weiter Informationen über bewährte Verfahren und Methoden für die Umsetzung der im Rahmen der 5G-Toolbox empfohlenen Maßnahmen auszutauschen und insbesondere bei wichtigen Anlagen und Einrichtungen, die in der von der EU koordinierten Risikobewertung als kritisch und sensibel eingestuft werden, die einschlägigen Beschränkungen für Hochrisikoanbieter anzuwenden; HEBT HERVOR, dass die 5G-Toolbox ein flexibles risikobasiertes Instrument zur Bewältigung der ermittelten Sicherheitsherausforderungen darstellt, das es ermöglicht, Aspekte der 5G-Cybersicherheit unter Achtung der Zuständigkeiten der Mitgliedstaaten zeitnah und effizient anzugehen, und WÜRDIGT sie als wertvolles Instrument für die weitere Verbesserung – bei voller Transparenz – der Sicherheit der Lieferketten von Telekommunikationsnetzen in koordinierter Weise, das als Modell für Risikobewertungs- und -minderungsinstrumente im Zusammenhang mit anderen wichtigen Sektoren dienen könnte; WEIST DARAUF HIN, dass die einschlägigen Behörden ersucht wurden, Empfehlungen auf der Grundlage von Risikobewertungen an die Mitgliedstaaten und die Kommission zu richten, um die Resilienz von Kommunikationsnetzen und -infrastrukturen in der Europäischen Union zu stärken, was auch die weitere Umsetzung der 5G-Toolbox betrifft;

14. NIMMT ZUR KENNTNIS, wie wichtig interoperable Ansätze sind, die Anbieterabhängigkeit angehen und das Konzentrationsrisiko mindern können und gleichzeitig die Sicherheit der Lieferketten über das gesamte Spektrum von IKT-Infrastrukturen und -Diensten verbessern; WÜRDIGT insbesondere im Zusammenhang mit 5G-Netzen die potenziellen Vorteile des Konzepts Open RAN in dieser Hinsicht, WEIST jedoch gleichzeitig auf den Bericht über die Cybersicherheit von Open RAN HIN, der von der NIS-Kooperationsgruppe veröffentlicht wurde und in dem festgestellt wird, dass dieses Konzept sich noch in der Entwicklungsphase befindet und seine Sicherheit, Transparenz und Standardisierung noch nicht ausgereift sind, und BEKRÄFTIGT, wie wichtig es ist, im Vorfeld des Übergangs zu neuen Standards oder Architekturen eine Risikobewertung vorzunehmen;

15. HEBT die Bedeutung bestehender und geplanter horizontaler Rechtsinstrumente im Bereich der Cybersicherheit für die Stärkung der Sicherheit der IKT-Lieferketten HERVOR, insbesondere der Verordnungen über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit), der bevorstehenden Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2), des Vorschlags für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union sowie des Vorschlags für eine Verordnung über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen (Rechtsakt zur Cyberresilienz); WEIST darüber hinaus AUF wichtige Entwicklungen in sektorspezifischen Verordnungen über Cybersicherheit HIN, insbesondere der künftigen Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA), die einen Aufsichtsrahmen für IKT-Drittanbieter, die für Finanzunternehmen von entscheidender Bedeutung sind, beinhaltet. Mit diesen Verordnungen werden allgemeine Verpflichtungen im Zusammenhang mit der Sicherheit der Lieferketten sowie detaillierte und spezifische Anforderungen, die für den betreffenden Sektor von Belang sind, eingeführt; BETONT gleichzeitig, dass die Anbieter ihre Produkte und Dienste oft in verschiedenen Sektoren anbieten, und nicht nur in einem einzigen Wirtschaftszweig. Daher muss unbedingt dafür gesorgt werden, dass die Anforderungen an die Sicherheit der Lieferketten so weit wie möglich für alle betreffenden Sektoren gleich sind, insbesondere jene, die durch die künftige NIS-2-Richtlinie abgedeckt werden, damit Abweichungen zwischen den für die Anbieter geltenden Verpflichtungen vermieden werden und der Aufwand für die Betreiber in kritischen Sektoren in Bezug auf die Bewertung der Einhaltung der Verpflichtungen durch die Anbieter verringert wird, wobei den jeweiligen Besonderheiten der Sektoren Rechnung zu tragen ist;

16. BEGRÜßT den Vorschlag für den Rechtsakt zur Cyberresilienz als wichtiges Rechtsinstrument, um die sichere Entwicklung von Produkten mit digitalen Elementen voranzubringen und dafür zu sorgen, dass die Cybersicherheit im gesamten Lebenszyklus von Produkten mit digitalen Elementen berücksichtigt wird; WEIST DARAUF HIN, dass der Rechtsakt zur Cyberresilienz das Potenzial hat, einen wesentlichen Beitrag zur Stärkung der Sicherheit der IKT-Lieferketten zu leisten; ERMUTIGT zu konstruktiven Verhandlungen über diesen Rechtsakt und zu seiner raschen Annahme;

17. WÜRDIGT in diesem Zusammenhang die laufenden Arbeiten, die unter Führung der ENISA zusammen mit den Mitgliedstaaten und anderen Interessenträgern durchgeführt werden, um der EU Zertifizierungssysteme für IKT-Produkte, -Dienste und -Prozesse im Einklang mit dem Rechtsakt zur Cyberresilienz zur Verfügung zu stellen, die dazu beitragen sollen, das allgemeine Niveau an Cybersicherheit im digitalen Binnenmarkt zu erhöhen; ERMUTIGT alle Interessenträger zur Teilnahme an den Vorbereitungsarbeiten für die einzelnen europäischen Zertifizierungssysteme, um Vertrauen in sichere IKT-Produkte, -Prozesse und -Dienste aufzubauen und deren Resilienz zu stärken, und FORDERT die Kommission AUF, nach Abschluss der Vorbereitungsarbeiten rasch Durchführungsrechtsakte für die europäischen Zertifizierungssysteme, insbesondere das auf gemeinsamen Kriterien beruhende europäische Schema für die Cybersicherheitszertifizierung, auszuarbeiten; WEIST DARAUF HIN, dass die europäischen Zertifizierungssysteme erforderlichenfalls Anforderungen an die Sicherheit der Lieferketten, einschließlich der Beziehungen zu Anbietern, enthalten sollten;

18. HEBT HERVOR, dass alle künftigen NIS-2-Bestimmungen im Zusammenhang mit der Sicherheit der IKT-Lieferketten umfassend umgesetzt werden müssen; UNTERSTREICHT in diesem Zusammenhang die Bedeutung von auf EU-Ebene koordinierten Risikobewertungen kritischer Lieferketten (koordinierte Lieferketten-Risikobewertungen), nationalen Strategien für die Sicherheit der Lieferketten und Maßnahmen im Zusammenhang mit der Sicherheit von Lieferketten; WEIST DARAUF HIN, dass nicht nur den Hauptanbietern Aufmerksamkeit geschenkt werden sollte, sondern auch den einschlägigen Unterauftragnehmern in Bezug auf Risiken für die Sicherheit der Hauptanbieter oder der Endkunden; ERMUTIGT die ENISA dazu, im Hinblick auf die Erleichterung der Umsetzung von Risikomanagementmaßnahmen für Lieferketten, mit Unterstützung der NIS-Kooperationsgruppe eine Bestandsaufnahme der verfügbaren bewährten Verfahren für das Lieferketten-Risikomanagement vorzunehmen und sie zu methodischen Leitlinien zusammenzustellen; ERMUTIGT die ENISA ferner dazu, Investitionen in die Sicherheit der IKT-Lieferketten durch die der bevorstehenden NIS-2-Richtlinie unterliegenden Einrichtungen zu überwachen;

19. HEBT auch die Vorteile und Risiken HERVOR, die mit dem Einsatz von Anbietern von verwalteten Diensten (Managed Service Provider – MSP) und Anbietern von verwalteten Sicherheitsdiensten (Managed Security Service Provider – MSSP) im Kontext der Sicherheit der Lieferketten verbunden sind. Während der Einsatz dieser Anbieter die Sicherheit innerhalb von Organisationen erheblich verbessern und zu einem höheren Maß an Cybersicherheit führen kann, kann die Fernverwaltung von IKT-Systemen und -Diensten, zusammen mit dem bevorrechtigten Zugang zu den IKT-Umgebungen der Kunden, den die MSP und MSSP möglicherweise benötigen, im Falle kompromittierter MSP oder MSSP zu wirkungsintensiven Kaskadeneffekten für eine große Zahl von Kunden führen. Daher ist es von größter Bedeutung, dass die MSP und MSSP ein hohes Maß an eigener interner Sicherheit und die Sicherheit der von ihnen erbrachten Dienste aufrechterhalten und gegenüber ihren Kunden einen transparenten Ansatz in Bezug auf die Sicherheit der von ihnen erbrachten Dienste befolgen; BEGRÜßT in diesem Zusammenhang ihre künftige Aufnahme in den Geltungsbereich der bevorstehenden NIS-2-Richtlinie;

20. WEIST in Bezug auf die Umsetzung des Mechanismus für koordinierte Lieferketten-Risikobewertungen gemäß der bevorstehenden NIS-2-Richtlinie AUF die Bedeutung nichttechnischer Risikofaktoren in diesem Kontext, wie der ungebührlichen Einflussnahme durch einen Drittstaat auf Anbieter und Diensteanbieter, HIN und IST SICH in diesem Zusammenhang der Faktoren BEWUSST, die herangezogen werden können, um das Risikoprofil im Sinne der von der EU koordinierten Risikobewertung der Cybersicherheit von 5G-Netzen zu bewerten; ERSUCHT die Kommission, bis zum zweiten Quartal 2023 nach Konsultation der NIS-Kooperationsgruppe und der ENISA die spezifischen IKT-Dienste, -Systeme oder -Produkte zu ermitteln, die vorrangig einer koordinierten Lieferketten-Risikobewertung unterzogen werden könnten;

21. STELLT FEST, dass Abhängigkeiten von Hochrisikoanbietern von IKT-Produkten und -Diensten, die für den Betrieb kritischer Netze und Systeme verwendet werden, eine strategische Bedrohung darstellen, die es durch angemessene politische Maßnahmen sowohl auf nationaler als auch auf europäischer Ebene und durch die Zusammenarbeit der Mitgliedstaaten untereinander und mit gleichgesinnten internationalen Partnern zu mindern gilt; ERSUCHT die NIS-Kooperationsgruppe im Hinblick auf die Erleichterung der Minderung dieses strategischen Risikos und auf die Unterstützung der koordinierten Lieferketten-Risikobewertungen, in Zusammenarbeit mit der Kommission und der ENISA ein Instrumentarium zur Verringerung der Risiken für kritische IKT-Lieferketten (IKT-Lieferketten-Toolbox) zu entwickeln. Die IKT-Lieferketten-Toolbox sollte auf den für die IKT-Lieferketten ermittelten strategischen Bedrohungsszenarien aufbauen und Maßnahmen zur Reaktion auf diese Szenarien bieten, wobei die mit der 5G-Toolbox und die auf nationaler Ebene gewonnenen Erfahrungen genutzt werden sollten. Sie sollte in transparenter Weise die koordinierten Lieferketten-Risikobewertungen für spezifische IKT-Dienste, -Systeme oder -Produkte im Rahmen der bevorstehenden NIS-2-Richtlinie ergänzen, indem sie generische Maßnahmen zur Risikoverringerung bietet, die skalierbar sind und an spezifische IKT-Dienste, -Systeme oder -Produkte angepasst werden können, und zwar auf der Grundlage der in den einzelnen koordinierten Lieferketten-Risikobewertungen ermittelten Risiken;

22. BETONT die Bedeutung von Forschung, Innovation, Investitionen und unternehmerischen Tätigkeiten im digitalen Bereich und im Bereich der Cybersicherheit sowie der Finanzierung dieser Tätigkeiten im Hinblick auf die Vermeidung möglicher künftiger ungewollter strategischer Abhängigkeiten und die Stärkung der Resilienz der IKT-Lieferketten insgesamt; BETONT in diesem Zusammenhang die Rolle und Bedeutung sowohl der strategischen als auch der auf die Umsetzung ausgerichteten Aufgaben des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) und des Netzwerks nationaler Koordinierungszentren, wenn es darum geht, einen Beitrag zur Maximierung der Wirkung von Investitionen zur Stärkung der Führungsrolle der Union und der offenen strategischen Autonomie im Bereich der Cybersicherheit, zur Unterstützung der technologischen Kapazitäten und Kompetenzen der Union und zur Verbesserung der Wettbewerbsfähigkeit der Union insgesamt zu leisten; RUFT in diesem Zusammenhang dazu AUF, dass das ECCC rasch einsatzbereit sein sollte; ERSUCHT das ECCC, die Aspekte im Zusammenhang mit der Sicherheit der IKT-Lieferketten, einschließlich beispielsweise der Entwicklung von sicherer Software, in seiner Strategischen Agenda zu berücksichtigen und gleichzeitig für Kohärenz und Komplementarität zu sorgen und jede Doppelarbeit zu vermeiden; UNTERSTÜTZT die Stärkung der europäischen Wettbewerbsfähigkeit im Bereich der Cybersicherheit durch Finanzierungsprogramme wie das Programm „Horizont Europa“ für Forschung und Innovation sowie das Programm „Digitales Europa“ zur Stärkung, zum Aufbau und zum Erwerb unerlässlicher Kompetenzen für die digitale Wirtschaft, die Gesellschaft und die Demokratie in der EU;

UNTERSTÜTZUNGSMECHANISMEN

23. ERMUTIGT dazu, Anreize zur finanziellen Unterstützung im Zusammenhang mit Maßnahmen zur Stärkung der Sicherheit der IKT-Lieferketten zu fördern; FORDERT das ECCC, die Kommission und die einschlägigen Interessenträger – auch im Hinblick auf die Umsetzung der bevorstehenden NIS-2-Richtlinie – vorrangig AUF, Optionen für die Einbeziehung von Aspekten der Sicherheit der IKT-Lieferketten in die bevorstehenden Aufforderungen zur Einreichung von Vorschlägen im Rahmen der Cybersicherheits-Arbeitsprogramme des Programms „Digitales Europa“ und des Programms „Horizont Europa“ oder alle anderen einschlägigen Finanzierungsmöglichkeiten zu erforschen. Diese Finanzierungsmöglichkeiten sollten unter anderem darauf abzielen, es den Organisationen zu ermöglichen, die Erhaltung eines hohen Maßes an Cybersicherheit in Bezug auf die Beschaffung von IKT-Produkten und -Diensten entlang der gesamten Lieferkette zu unterstützen, insbesondere im Zusammenhang mit der Ersetzung spezifischer kritischer IKT-Dienste, -Systeme oder -Produkte, die im Einklang mit den künftigen koordinierten Lieferketten-Risikobewertungen als mit hohem Risiko eingestuft werden;

24. IST SICH BEWUSST, dass mit der Globalisierung und der Spezialisierung von IKT-Diensten und der zunehmenden Abhängigkeit von Produkten und Diensten Dritter die Notwendigkeit einer engen Zusammenarbeit innerhalb der EU und auf internationaler Ebene beim Austausch von Wissen und Fachkenntnissen zwischen den einschlägigen Interessenträgern einhergeht, und ERMUTIGT diese, eine starke und koordinierte Position einzunehmen, um die Sicherheit der IKT-Lieferketten umfassend zu gewährleisten; IST SICH ferner der Notwendigkeit BEWUSST, sowohl einschlägige, dem neuesten Stand entsprechende Ansätze und Techniken für eine angemessene grundlegende Cyberhygiene und langfristige Lösungen zur Verwirklichung sicherer und resilienter IKT-Lieferketten zu erforschen als auch die besten Wege für ihre Förderung und potenzielle Einbeziehung in politische oder andere Initiativen zu suchen; ERKENNT in dieser Hinsicht AN, dass ein besonderes Augenmerk auf die Erforschung der Vor- und Nachteile systematischer Lösungen wie Null-Vertrauen-Grundsätze, Software-Stücklisten und ähnlicher langfristiger Lösungen gelegt werden sollte; EMPFIEHLT, zu diesem Zweck auf die NIS-Kooperationsgruppe zurückzugreifen;

25. WEIST AUF die Vorteile HIN, die die Überwachung von Cybervorfällen und -bedrohungen und der wirksame Informationsaustausch darüber im Hinblick auf die Verhütung, Aufspürung und Minderung der Auswirkungen von Angriffen auf die Lieferketten mit sich bringen; BEKRÄFTIGT die Notwendigkeit des Vertrauensaufbaus zwischen den Mitgliedstaaten für den wirksamen Austausch dieser Informationen; WEIST in diesem Zusammenhang AUF den Vorschlag der Kommission HIN, 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; WEIST ERNEUT DARAUF HIN, dass für Komplementarität und Koordinierung zwischen den bestehenden Netzen und Mechanismen gesorgt werden muss, und UNTERSTREICHT in diesem Zusammenhang insbesondere die Rolle des Netzwerks von Computer-Notfallteams (CSIRT) und die Notwendigkeit, das Potenzial dieses Netzwerks für die Förderung einer Kultur des effizienten, sicheren und zuverlässigen Informationsaustauschs weiter zu erforschen; 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;

26. HEBT aufgrund der Verflechtungen und der weltweiten Dimension der Bedrohungen für die IKT-Lieferketten HERVOR, wie wichtig es ist, die Sicherheit der IKT-Lieferketten auf globaler Ebene anzugehen und zu verbessern; EMPFIEHLT daher die Verwendung von digitalen Partnerschaften, Cyberdialogen und anderen einschlägigen Initiativen der EU, einschließlich gegebenenfalls Freihandelsabkommen, für die Förderung risikobasierter Evaluierungen der Anbieter von IKT-Produkten und -Diensten, für den Einsatz vertrauenswürdiger Anbieter und für die Schaffung eines sicheren und innovativen digitalen Ökosystems auf der Grundlage offener, interoperabler und transparenter Standards; WEIST darüber hinaus ERNEUT auf die Vision der Global-Gateway-Partnerschaften sowie des EU-US-Handels- und Technologierates und die Tätigkeiten seiner Arbeitsgruppen HIN, bei denen es darum geht, den Einsatz vertrauenswürdiger Anbieter bzw. Nicht-Hochrisikoanbieter zu fördern und einen Finanzierungsmechanismus für Projekte zu entwickeln, die die Sicherheit, Resilienz und Vertrauenswürdigkeit von IKT-Infrastrukturen und -Diensten in Drittländern technologieunabhängig erhöhen, auch durch den Verzicht auf die Finanzierung von Ankäufen bei nicht vertrauenswürdigen Anbietern bzw. Hochrisikoanbietern;

27. BEKRÄFTIGT seine Zusage, zu einem offenen, freien, globalen, stabilen und sicheren Cyberraum beizutragen und sich an die im VN-Rahmen festgelegten Normen, Vorschriften und Grundsätze des verantwortungsvollen staatlichen Handelns im Cyberraum zu halten; WEIST insbesondere im Zusammenhang mit der Sicherheit der IKT-Lieferketten auf die von der VN-Gruppe von Regierungssachverständigen (UN GGE) und der offenen Arbeitsgruppe (OEWG) gebilligte Norm HIN, mit der die Mitgliedstaaten ermutigt werden, vernünftige Schritte zur Gewährleistung der Integrität der Lieferketten zu ergreifen, auch durch die Entwicklung objektiver Kooperationsmaßnahmen, damit die Endnutzer Vertrauen in die Sicherheit von IKT-Produkten haben können, und auf die Verhinderung der Verbreitung böswilliger IKT-Instrumente und -Techniken und der Nutzung schädlicher verborgener Funktionen hinzuarbeiten, und TRITT DAFÜR EIN, dass diese Norm auf breiter Basis angewandt wird.