Rådet for
Den Europæiske Union

Bruxelles, 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

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	17. oktober 2022
til:	delegationerne
Tidl. dok. nr.:	12930/22
Vedr.:	Rådets konklusioner om sikkerhed i IKT-forsyningskæden – Rådets konklusioner godkendt af Rådet på samlingen den 17. oktober 2022

Vedlagt følger til delegationerne Rådets konklusioner om sikkerhed i IKT-forsyningskæden, der blev godkendt af Rådet på samlingen den 17. oktober 2022.

BILAG

Rådets konklusioner om sikkerhed i IKT-forsyningskæden

RÅDET FOR DEN EUROPÆISKE UNION,

SOM MINDER OM sine konklusioner om

– den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU (konklusioner af 20. november 2017)

– opbygning af cybersikkerhedskapacitet i EU

– betydningen af 5G for den europæiske økonomi og behovet for at afbøde de sikkerhedsrisici, der er forbundet med 5G

– Europas digitale fremtid i støbeskeen

– en genopretning, der fremmer omstillingen til en mere dynamisk, modstandsdygtig og konkurrencedygtig europæisk industri

– cybersikkerheden ved forbundet udstyr

– EU's strategi for cybersikkerhed for det digitale årti

– udviklingen af Den Europæiske Unions cyberposition

– Den Europæiske Revisionsrets særberetning nr. 03/2022 med titlen "5G-udrulningen i EU: Udrulningen af net er forsinket, og der er stadig uafklarede sikkerhedsspørgsmål",

SOM MINDER OM Det Europæiske Råds konklusioner om

– covid-19, det indre marked, industripolitik, det digitale og eksterne forbindelser (konklusioner af 1.-2. oktober 2020)

– Ruslands militære aggression mod Ukraine, sikkerhed og forsvar, energi, økonomiske spørgsmål, covid-19 og eksterne forbindelser (konklusioner af 24.-25. marts 2022)

– Ukraine, fødevaresikkerhed, sikkerhed og forsvar samt energi (konklusioner af 30.-31. maj 2022),

1. UNDERSTREGER i betragtning af geopolitikkens stigende betydning for cybersikkerhed, at Den Europæiske Union og dens medlemsstater skal have en omfattende og strategisk tilgang til cybersikkerhed. Ruslands militære aggression mod Ukraine har medført en stor forandring i Den Europæiske Unions strategiske og sikkerhedsmæssige miljø og har vist, at der er behov for en stærkere og mere kompetent Europæisk Union på sikkerheds- og forsvarsområdet. Den har understreget, at det er yderst vigtigt at tage behørigt hensyn til det geopolitiske miljø, ikke kun når der reageres på ondsindede cyberaktiviteter, men også når informations- og kommunikationsteknologiernes (IKT) modstandsdygtighed opbygges og opretholdes. Dette har særlig betydning for forsyningskæder for IKT-produkter og -tjenester (IKT-forsyningskæder), som både kan komme i fare på grund af geopolitisk rivalisering, hvilket angrebet på SolarWinds viste, og påvirkes af geopolitiske spændinger og ustabilitet, hvilket kom til udtryk med truslen vedrørende russiske IKT-leverandørers afhængighed på tidspunktet for Ruslands militære aggression mod Ukraine,

2. BEMÆRKER, at karakteren af de risici, der er forbundet med IKT-forsyningskæden, som består af en række indbyrdes forbundne ressourcer og processer mellem erhvervsdrivende (som defineret i forordning (EU) 2019/1020), og som begynder med tilvejebringelse af råvarer og strækker sig over fremstilling, forarbejdning, håndtering og levering af IKT-produkter og -tjenester, herunder levering af støtte i løbet af IKT-produkters og -tjenesters livscyklus, medfører unikke udfordringer og konsekvenser, der kan være vidtrækkende. Ud over de risici, der er forbundet med manglende adgang til IKT-produkter, f.eks. på grund af mangel på kritiske råstoffer og halvledere, der er nødvendige for produktionen heraf, er forsyningskæderne for IKT-produkter og -tjenester udsat for andre trusler. De kan navnlig være mål for eller misbruges af ondsindede aktører på sofistikerede og ofte skjulte måder, der har indvirkning på fortroligheden, integriteten og tilgængeligheden af overførte og lagrede følsomme data,

3. ANERKENDER betydningen af forslaget til direktiv om kritiske enheders modstandsdygtighed for at forbedre kritiske enheders fysiske sikkerhed, idet det anerkender, at der er behov for en tilgang, der omfatter alle farer, for at sikre IKT-aktiver, og UNDERSTREGER, at det ud over at øge modstandsdygtigheden over for angreb i forsyningskæden, der udføres ved hjælp af cybermidler, er lige så vigtigt at styrke IKT-forsyningskædernes overordnede modstandsdygtighed og sikkerhed over for alle de forskellige trusselsfaktorer såsom naturkatastrofer, systemsvigt, insidertrusler eller menneskelige fejl, ANERKENDER i den forbindelse, at sikkerhed i IKT-forsyningskæden omfatter sikring af beskyttelsen af IKT-produkter og -tjenester, der produceres, leveres, indkøbes og anvendes i IKT-forsyningskæder, herunder ved at beskytte individuelle komponenter og overførte data,

4. TILSKYNDER på grundlag af erfaringerne fra konsekvenserne af Den Europæiske Unions strategiske afhængighed af russiske fossile brændstoffer samt fra virkningerne af forstyrrelserne i forsyningskæderne under covid-19-pandemierne, navnlig i forbindelse med lægemidler og halvledere, hvor EU's strategiske afhængighed blev eksponeret, medlemsstaterne TIL at arbejde hen imod at undgå lignende situationer med uønskede strategiske eksterne afhængighedsforhold i forbindelse med IKT-produkter og -tjenester. Som følge af den voksende digitalisering af samfundet og den stadig stigende brug af IKT i kritisk infrastruktur bør strategisk ekstern afhængighed i forbindelse med IKT-produkter og -tjenester og deres forsyningskæder løbende vurderes og, hvor det er relevant, adresseres,

5. MINDER OM, at det er et centralt mål for Unionen at opnå strategisk autonomi og samtidig bevare en åben økonomi, og at det omfatter identifikation og reduktion af strategisk afhængighed og øget modstandsdygtighed i de mest følsomme industrielle økosystemer og på specifikke områder, herunder på det digitale område. Dette omfatter udvikling og udbredelse af strategisk digital kapacitet og infrastruktur samt styrkelse af evnen til at træffe selvstændige teknologiske valg og som en af de vigtigste søjler at garantere modstandsdygtige og sikre infrastrukturer, produkter og tjenester med henblik på at opbygge tillid til det digitale indre marked og i det europæiske samfund, samtidig med at åbenheden, det globale samarbejde med ligesindede partnere og konkurrenceevnen opretholdes, og at de potentielle fordele herved udnyttes. Den Europæiske Unions kerneværdier værner om navnlig privatlivets fred, sikkerheden, ligheden, den menneskelige værdighed, retsstatsprincippet og et åbent internet som forudsætninger for at opnå et samfund, en økonomi og en industri, der er digitalt drevet og sætter mennesket i centrum,

6. BEMÆRKER, at det på grund af udviklingen i cybertrusselsbilledet, som ses af tendensen til yderst virkningsfulde og sofistikerede angreb i forsyningskæden i de seneste år såsom angrebet på SolarWinds, Mimecast eller Kaseya, der er opstået sammen med outsourcing af væsentlige IKT-tjenester og er intensiveret af den generelle afhængighed af IKT-produkter og -tjenester, der fremstilles, leveres eller betjenes af tredjeparter, er meget sandsynligt, at der i fremtiden forekommer flere angreb på forsyningskæden med betydelig skade på økonomien og for samfundet, UNDERSTREGER i lyset heraf betydningen af at øge sikkerheden og modstandsdygtigheden i IKT-forsyningskæderne for at sikre et velfungerende indre marked sammen med behovet for at sikre tilgængeligheden, sikkerheden og mangfoldigheden af IKT-produkter og -tjenester i det indre marked, ANERKENDER derfor behovet for at maksimere og strømline anvendelsen af eksisterende EU-instrumenter og -tilgange for at nå disse mål samt behovet for løbende at tilpasse sig det skiftende cybertrusselsbillede ved at indføre yderligere passende foranstaltninger og mekanismer, herunder i forbindelse med eventuelle sikkerhedsrisici ved nye og disruptive teknologier, TILSKYNDER i denne forbindelse medlemsstaterne TIL at følge den risikobaserede tilgang til håndtering af ny teknologisk udvikling,

7. ANERKENDER, at forståelse af det konstant skiftende cybertrusselsbillede samt kompleksiteten af angreb i forsyningskæden er afgørende for en effektiv afgrænsning af de risici, der er forbundet med IKT-forsyningskæder, UNDERSTREGER i den forbindelse, at det er nødvendigt at tilpasse sig nye trusler ved aktivt og løbende at overvåge, analysere og vurdere trusselsbilledet i forsyningskæden, øge bevidstheden og opbygge viden om trusler og sårbarheder og proaktivt advare relevante enheder på en skræddersyet måde, UDTRYKKER TILFREDSHED MED arbejdet i Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) vedrørende sikkerhed i IKT-forsyningskæden, navnlig dets rapport om trusselsbilledet for angreb i forsyningskæden,

TVÆRSEKTORIELLE INSTRUMENTER OG TILGANGE

8. BEKRÆFTER PÅ NY, at det er vigtigt, at medlemsstaterne overvejer behovet for at diversificere leverandører af kritisk IKT for at undgå eller begrænse stor afhængighed af enkelte leverandører, navnlig højrisikoleverandører, da det øger eksponeringen for konsekvenserne af mulige forstyrrelser, ANERKENDER, at undgåelse af leverandørbinding og diversificering af IKT-leverandører er et af de vigtige elementer til at sikre stabilitet og sikkerhed på det indre marked, FREMHÆVER behovet for at fremme og gennemføre passende strategier, der letter leverandørdiversificering og konkurrenceevne på en teknologineutral måde, TILSKYNDER desuden TIL, at aspekter vedrørende forebyggelse af leverandørbinding integreres i EU-lovgivningen, ANERKENDER i den forbindelse forslaget til forordning om harmoniserede regler om fair adgang til og anvendelse af data (dataforordningen), der har til formål at øge databehandlingstjenesternes interoperabilitet og fjerne hindringer for skift mellem udbydere af databehandlingstjenester,

9. ANERKENDER forbindelsen mellem sikkerhed i IKT-forsyningskæden og offentlige indkøb, UNDERSTREGER behovet for, at procedurerne for offentlige indkøb tager behørigt hensyn til betydningen af sikkerhed i IKT-forsyningskæden ved, hvor det er relevant, at indføre objektive og risikobaserede udvælgelseskriterier vedrørende tilbudsgivernes evne til at sikre et højt sikkerhedsniveau for de leverede tjenester, OPFORDRER TIL på den ene side at finde den rette balance mellem offentlighedens interesse i den mest effektive og retfærdige anvendelse af offentlige midler og på den anden side offentlighedens interesse i at sikre informationssystemer og sikre et velfungerende indre marked, OPFORDRER for at lette gennemførelsen af relevante regler for offentlige indkøb i lyset af den stigende cybersikkerhed Kommissionen TIL at udarbejde metodologiske retningslinjer senest i tredje kvartal af 2023 med henblik på at tilskynde de ordregivende myndigheder til at sætte passende fokus på tilbudsgiveres og deres underentreprenørers cybersikkerhedspraksis og TIL at vurdere og om nødvendigt fremsætte forslag til revision eller supplering af relevant lovgivning om offentlige indkøb,

10. ANERKENDER, at udenlandske direkte investeringer i forbindelse med IKT-produkter og -tjenester ganske vist giver medlemsstaterne, virksomhederne og borgerne økonomiske og sociale fordele, men kan medføre risici for sikkerheden og den offentlige orden, og NOTERER SIG, at EU's mekanisme til screening af udenlandske direkte investeringer sammen med de respektive nationale screeningsystemer, der giver mulighed for at imødegå sådanne risici, også kan anvendes som et nyttigt redskab til at beskytte sikkerheden og modstandsdygtigheden i IKT-forsyningskæden ved at bidrage til at eliminere højrisikoinvesteringer, der kan påvirke en sådan sikkerhed og modstandsdygtighed., ANERKENDER, at oplysninger, der udveksles og deles gennem denne mekanisme, kan hjælpe medlemsstaterne med bedre at vurdere de mulige trusler mod sikkerheden i IKT-forsyningskæderne og træffe de nødvendige foranstaltninger i overensstemmelse hermed, OPFORDRER de relevante nationale aktører TIL også at tage højde for denne dimension af screeningmekanismen, hvor det er relevant,

11. BEKRÆFTER med hensyn til forsvar PÅ NY sin opfordring til Kommissionen om i 2023 sammen med medlemsstaterne at vurdere risiciene for forsyningskæderne for kritisk infrastruktur på forskellige områder, herunder det digitale område, i forbindelse med EU's sikkerheds- og forsvarsinteresser samt at undersøge mulighederne for at øge cybersikkerheden i hele forsyningskæden i EU's forsvarsteknologiske og -industrielle base, OPFORDRER endvidere medlemsstaterne og Kommissionen TIL at overveje sikkerhed i IKT-forsyningskæden i forbindelse med gennemførelsen af forpligtelserne og tiltagene i det strategiske kompas,

12. TILSKYNDER, idet det anerkender betydningen af kritiske råstoffer og alle former for halvledere som de grundlæggende byggesten til IKT-produkter, TIL konstruktive forhandlinger om forslaget til forordning om en ramme for foranstaltninger til styrkelse af det europæiske økosystem for halvledere (mikrochipforordningen) og forslaget til Rådets forordning om ændring af forordning (EU) 2021/2085 om oprettelse af fællesforetagenderne under Horisont Europa for så vidt angår fællesforetagendet for mikrochips,

CYBERSPECIFIKKE INSTRUMENTER

13. ANERKENDER specifikt med hensyn til telekommunikationsinfrastruktur de resultater, der er opnået på EU-plan med hensyn til at forbedre sikkerheden i forsyningskæden for 5G-net, navnlig gennem EU-værktøjskassen til 5G-sikkerhed (EU's 5G-værktøjskasse), OPFORDRER medlemsstaterne TIL yderligere at udveksle oplysninger om bedste praksis og metoder vedrørende gennemførelsen af de foranstaltninger, der anbefales i EU's 5G-værktøjskasse, og navnlig TIL at anvende de relevante restriktioner over for højrisikoleverandører af centrale aktiver, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering, FREMHÆVER, at EU's 5G-værktøjskasse udgør et smidigt risikobaseret instrument til håndtering af identificerede sikkerhedsudfordringer, som gør det muligt at håndtere 5G-cybersikkerhedsaspekter på en rettidig og effektiv måde, samtidig med at medlemsstaternes kompetencer respekteres, og ANERKENDER, at den er et værdifuldt instrument til i fuld gennemsigtighed yderligere at forbedre sikkerheden i telekommunikationsnets forsyningskæde på en koordineret måde, der kan tjene som inspiration for risikovurderings- og risikobegrænsningsværktøjer i forbindelse med andre vigtige sektorer, MINDER OM de relevante myndigheders opfordring til at fremsætte henstillinger på grundlag af risikovurderinger til medlemsstaterne og Kommissionen med henblik på at styrke modstandsdygtigheden af kommunikationsnet og -infrastrukturer i Den Europæiske Union, herunder den fortsatte gennemførelse af EU's 5G-værktøjskasse,

14. BEMÆRKER betydningen af interoperable tilgange, der kan håndtere leverandørbinding og udvande koncentrationsrisikoen, samtidig med at sikkerheden i forsyningskæden forbedres på tværs af hele spektret af IKT-infrastruktur og -tjenester, ANERKENDER navnlig i forbindelse med 5G-net de mulige fordele ved Open RAN-konceptet i denne henseende, men MINDER samtidig OM rapporten om cybersikkerheden af Open RAN, som NIS-samarbejdsgruppen har offentliggjort, idet det bemærker, at konceptet stadig er under udvikling, og at dets sikkerhed, gennemsigtighed og standardisering befinder sig på et tidligt stadie, og UNDERSTREGER, at det er vigtigt at vurdere risici forud for enhver overgang til nye standarder eller arkitekturer,

15. FREMHÆVER relevansen af eksisterende og kommende horisontale retsakter om cybersikkerhed, navnlig forordningen om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (forordningen om cybersikkerhed), det kommende direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2), forslaget til forordning om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer og forslaget til forordning om horisontale cybersikkerhedskrav for produkter med digitale elementer (forordningen om cyberrobusthed) med henblik på at øge sikkerheden i IKT-forsyningskæden, NOTERER SIG desuden den vigtige udvikling inden for sektorspecifikke cybersikkerhedsforordninger, navnlig den fremtidige forordning om digital operationel modstandsdygtighed i den finansielle sektor (DORA), som omfatter en tilsynsramme for tredjepartsudbydere af IKT-tjenester, der er kritiske for finansielle enheder. Disse forordninger indeholder generelle forpligtelser vedrørende sikkerhed i forsyningskæden samt detaljerede og specifikke krav, der er relevante for den pågældende sektor, UNDERSTREGER samtidig, at leverandører oftere leverer deres produkter og tjenester på tværs af forskellige sektorer end blot til en enkelt industri. Det er derfor yderst vigtigt at sikre, at kravene til sikkerhed i forsyningskæden så vidt muligt tilpasses i alle relevante sektorer, navnlig dem, der er omfattet af det fremtidige NIS 2-direktiv, for at undgå uoverensstemmelser mellem de forpligtelser, der pålægges leverandører, og for at lette byrden for operatører i kritiske sektorer ved at vurdere leverandørernes overholdelse af disse forpligtelser, samtidig med at der tages hensyn til de særlige forhold i den pågældende sektor,

16. UDTRYKKER TILFREDSMED MED forslaget til forordning om cyberrobusthed, da det er et vigtigt lovgivningsinstrument til at fremme en sikker udvikling af produkter med digitale elementer og til at sikre, at der tages højde for cybersikkerhed i hele livscyklussen for produkter med digitale elementer, BEMÆRKER, at forslaget til forordning om cyberrobusthed har potentiale til at bidrage væsentligt til at styrke sikkerheden i IKT-forsyningskæden, TILSKYNDER TIL konstruktive forhandlinger og rettidig vedtagelse af forordningen,

17. ANERKENDER i denne forbindelse det igangværende arbejde ledet af ENISA sammen med medlemsstaterne og andre interessenter med henblik på at forsyne EU med certificeringsordninger for IKT-produkter, -tjenester og -processer i overensstemmelse med forordningen om cybersikkerhed, som bør bidrage til at øge det generelle cybersikkerhedsniveau på det digitale indre marked, TILSKYNDER alle interessenter TIL at deltage i det forberedende arbejde med individuelle europæiske certificeringsordninger med henblik på at opbygge tillid til sikre IKT-produkter, -processer og -tjenester og styrke deres modstandsdygtighed og OPFORDRER Kommissionen TIL hurtigt at udarbejde gennemførelsesretsakter om de europæiske certificeringsordninger efter afslutningen af det forberedende arbejde, navnlig den fælles kriteriebaserede europæiske cybersikkerhedscertificeringsordning, BEMÆRKER, at de europæiske certificeringsordninger om nødvendigt bør omfatte krav til sikkerhed i forsyningskæden, herunder forbindelser med leverandører,

18. FREMHÆVER behovet for en grundig gennemførelse af alle de kommende NIS 2-bestemmelser vedrørende sikkerhed i IKT-forsyningskæden, UNDERSTREGER i denne forbindelse relevansen af EU's koordinerede risikovurderinger af kritiske forsyningskæder (koordinerede risikovurderinger af forsyningskæden), nationale politikker for sikkerhed i forsyningskæden og sikkerhedsforanstaltninger forbundet med forsyningskæden, BEMÆRKER, at opmærksomheden ikke kun bør rettes mod de primære leverandører, men også mod de relevante underentreprenører for så vidt angår risici for den primære leverandørs eller slutkundens sikkerhed, TILSKYNDER med henblik på at lette gennemførelsen af risikostyringsforanstaltninger i forsyningskæden ENISA TIL med bistand fra NIS-samarbejdsgruppen at gøre status over bedste praksis for risikostyring i forsyningskæden og sammenfatte den i metodologiske retningslinjer, TILSKYNDER desuden ENISA TIL at overvåge investeringer i sikkerheden i IKT-forsyningskæden for de enheder, der reguleres i henhold til det kommende NIS 2-direktiv,

19. FREMHÆVER også fordelene og risiciene ved at anvende udbydere af administrerede tjenester (MSP'er) og udbydere af administrerede sikkerhedstjenester (MSSP'er) i forbindelse med sikkerhed i forsyningskæden. Selv om anvendelsen af disse udbydere kan forbedre sikkerheden inden for organisationer betydeligt og føre til højere cybersikkerhedsniveauer, kan fjernstyring af IKT-systemer og -tjenester kombineret med privilegeret adgang til kundernes IKT-miljø, som MSP'ere og MSSP'ere kan have behov for, i tilfælde af kompromitterede MSP'er eller MSSP'er føre til virkningsfulde kaskadevirkninger for et stort antal kunder. Det er derfor yderst vigtigt, at MSP'er og MSSP'er holder deres egen interne sikkerhed og sikkerheden i forbindelse med de tjenester, som de leverer, på et højt niveau og anlægger en gennemsigtig tilgang til deres kunder med hensyn til sikkerheden af de tjenester, som de leverer, SER i denne forbindelse MED TILFREDSHED PÅ deres fremtidige medtagelse i anvendelsesområdet for det kommende NIS 2-direktiv,

20. NOTERER SIG med hensyn til gennemførelsen af mekanismen for koordinerede risikovurderinger af forsyningskæden i henhold til det kommende NIS 2-direktiv, at ikketekniske risikofaktorer er relevante i denne forbindelse, såsom et tredjelands utilbørlige påvirkning af leverandører og tjenesteudbydere, og ANERKENDER i denne forbindelse de faktorer, der kan anvendes til at vurdere risikoprofilen som nævnt i EU's koordinerede risikovurdering af cybersikkerheden i 5G-net, OPFORDRER Kommissionen TIL senest i andet kvartal af 2023, efter høring af NIS-samarbejdsgruppen og ENISA, at udpege de specifikke IKT-tjenester, -systemer eller -produkter, der kan underkastes de koordinerede risikovurderinger af forsyningskæden som en prioritet,

21. BEMÆRKER, at afhængigheden af højrisikoleverandører af IKT-produkter og -tjenester, der anvendes til driften af kritiske net og systemer, udgør en strategisk trussel, der skal afbødes gennem passende politikker på både nationalt plan og EU-plan og gennem samarbejde mellem medlemsstaterne og med ligesindede internationale partnere, OPFORDRER med henblik på at lette afbødningen af denne strategiske risiko og støtte de koordinerede risikovurderinger af forsyningskæden NIS-samarbejdsgruppen TIL i samarbejde med Kommissionen og ENISA at udvikle en værktøjskasse med foranstaltninger til nedbringelse af kritiske risici i IKT-forsyningskæden (værktøjskasse til IKT-forsyningskæden). Værktøjskassen til IKT-forsyningskæden bør bygge på strategiske trusselsscenarier, der konstateres for IKT-forsyningskæder, og indeholde foranstaltninger, der kan træffes for at reagere på disse scenarier ved at trække på erfaringerne fra 5G-værktøjskassen og dem, der er indhøstet på nationalt plan. Den bør på en gennemsigtig måde supplere de koordinerede risikovurderinger af forsyningskæden for specifikke IKT-tjenester, -systemer eller -produkter i henhold til det kommende NIS 2-direktiv ved at tilbyde generiske foranstaltninger til nedbringelse af de risici, der kan justeres for specifikke IKT-tjenester, -systemer eller -produkter på en skalerbar måde, på grundlag af de risici, der konstateres i de individuelle koordinerede risikovurderinger af forsyningskæden,

22. UNDERSTREGER, at forsknings-, innovations-, investerings- og iværksætteraktiviteter på det digitale område og cybersikkerhedsområdet samt finansieringen af sådanne aktiviteter spiller en vigtig rolle med hensyn til at undgå eventuelle fremtidige uønskede strategiske afhængighedsforhold og styrke IKT-forsyningskædernes generelle modstandsdygtighed, FREMHÆVER i denne forbindelse betydningen og relevansen af både de strategiske opgaver og gennemførelsesopgaverne for Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre med hensyn til at bidrage til at maksimere virkningerne af investeringer for at styrke Unionens lederskab og åbne strategiske autonomi inden for cybersikkerhed, støtte Unionens teknologiske kapaciteter og færdigheder og for at øge Unionens globale konkurrenceevne, OPFORDRER i den forbindelse TIL en hurtig operationalisering af Netværket af Nationale Koordinationscentre, OPFORDRER Netværket af Nationale Koordinationscentre TIL at tage hensyn til sikkerhedsaspekterne i IKT-forsyningskæden, herunder f.eks. udvikling af sikker software, i deres strategiske dagsorden, samtidig med at sammenhæng og komplementaritet sikres og enhver form for dobbeltarbejde undgås, STØTTER en styrkelse af europæisk konkurrenceevne på cybersikkerhedsområdet gennem finansieringsprogrammer såsom Horisont Europa-programmet for forskning og innovation samt programmet for et digitalt Europa med henblik på at forstærke, opbygge og erhverve afgørende kapaciteter til EU's digitale økonomi, samfund og demokrati,

STØTTEMEKANISMER

23. TILSKYNDER TIL øgede incitamenter til finansiel støtte i forbindelse med foranstaltninger, der har til formål at styrke sikkerheden i IKT-forsyningskæden, OPFORDRER som en prioritet, også med henblik på den kommende gennemførelse af NIS 2-direktivet, Netværket af Nationale Koordinationscentre, Kommissionen og relevante interessenter TIL at undersøge mulighederne for at medtage aspekter vedrørende sikkerhed i IKT-forsyningskæden i de kommende indkaldelser inden for arbejdsprogrammerne for cybersikkerhed under programmet for et digitalt Europa og Horisont Europa-programmet eller andre relevante finansieringsmuligheder. Disse finansieringsmuligheder bør bl.a. have til formål at gøre det muligt for organisationerne at støtte opretholdelsen af et højt cybersikkerhedsniveau med hensyn til indkøb af IKT-produkter og -tjenester i hele forsyningskæden, navnlig i forbindelse med udskiftning af specifikke kritiske IKT-tjenester, -systemer eller -produkter, der anerkendes som indebærende en høj risiko i overensstemmelse med de fremtidige koordinerede risikovurderinger af forsyningskæden,

24. ANERKENDER, at globaliseringen og specialiseringen af IKT-tjenester og den øgede afhængighed af tredjepartsprodukter og -tjenester skaber et behov for tæt samarbejde inden for EU og på internationalt plan om udveksling af viden og ekspertise blandt relevante interessenter, og TILSKYNDER dem TIL at nå frem til en stærk og koordineret holdning, der garanterer sikkerheden i IKT-forsyningskæden på fyldestgørende vis, ANERKENDER også behovet for yderligere at undersøge relevante avancerede tilgange og teknikker, både til passende grundlæggende cyberhygiejne og langsigtede løsninger for at opnå sikre og modstandsdygtige IKT-forsyningskæder samt de mest hensigtsmæssige metoder til at fremme og potentielt indarbejde dem i politikker eller andre initiativer, ANERKENDER i den forbindelse, at der bør lægges særlig vægt på at undersøge fordelene og ulemperne ved systematiske løsninger såsom nultillidsprincipperne, softwarestyklister og lignende langsigtede løsninger, HENSTILLER, at NIS-samarbejdsgruppen anvendes til dette formål,

25. NOTERER SIG fordelene ved overvågning og effektiv udveksling af oplysninger om cyberhændelser og -trusler med henblik på forebyggelse, detektering og afbødning af virkninger af angreb i forsyningskæden, FREMHÆVER behovet for fortsat at opbygge tillid og tiltro mellem medlemsstaterne med henblik på effektiv udveksling af sådanne oplysninger, MINDER i denne forbindelse OM Kommissionens forslag om at støtte medlemsstaterne i at oprette og styrke sikkerhedsoperationscentre (SOC'er) med henblik på at opbygge et netværk af SOC'er i hele EU for yderligere at overvåge og foregribe advarsler om angreb mod netværk, MINDER OM behovet for komplementaritet og koordinering inden for eksisterende netværk og mekanismer, og FREMHÆVER navnlig i denne forbindelse den rolle, som netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er) spiller, og behovet for yderligere at undersøge disse netværks potentiale til at fremme en effektiv, sikker og pålidelig informationsudvekslingskultur, MINDER OM den indsats, som medlemsstaterne med støtte fra EU har gjort for at oprette sektorielle, nationale og regionale CSIRT'er, og nationale eller europæiske informationsudvekslings- og analysecentre (ISAC'er) som led i et effektivt netværk af cybersikkerhedspartnerskaber i Unionen,

26. FREMHÆVER på grund af den indbyrdes forbundne og globale karakter af trusler mod IKT-forsyningskæden betydningen af at tage stilling til og forbedre sikkerheden i IKT-forsyningskæden på globalt plan, HENSTILLER på denne baggrund, at der anvendes digitale partnerskaber, cyberdialoger og andre relevante EU-initiativer, herunder, hvor det er relevant, frihandelsaftaler, til at fremme risikobaserede evalueringer af IKT-produktleverandører og udbydere af IKT-tjenester, brugen af pålidelige leverandører og til anvendelsen af et sikkert og innovativt digitalt økosystem baseret på åbne, interoperable og gennemsigtige standarder, GENTAGER desuden visionen for Global Gateway-partnerskaberne samt Handels- og Teknologirådet mellem EU og USA, og aktiviteterne inden for dets arbejdsgrupper, om at fremme brugen af pålidelige leverandører/leverandører, der ikke er højrisikoleverandører, og udvikle en finansieringsmekanisme, der vil sætte projekter i stand til at gøre IKT-infrastruktur og -tjenester i tredjelande mere sikre, modstandsdygtige og pålidelige, herunder ved at afstå fra at finansiere indkøb fra upålidelige leverandører/højrisikoleverandører på en teknologineutral måde,

27. BEKRÆFTER PÅ NY sit tilsagn om at bidrage til og fremme et åbent, frit, globalt, stabilt og sikkert cyberspace og overholde de normer, regler og principper for ansvarlig statslig adfærd i cyberspace, der er fastsat inden for FN's rammer, MINDER, navnlig med hensyn til sikkerhed i IKT-forsyningskæden, OM den norm, som er godkendt af GGE og OEWG, og som tilskynder staterne til at tage rimelige skridt for at sikre forsyningskædens integritet, herunder gennem udvikling af objektive samarbejdsforanstaltninger, således at slutbrugerne kan have tiltro til IKT-produkters sikkerhed, og bestræbe sig på at forhindre udbredelse af ondsindede IKT-værktøjer og -teknikker og brug af skadelige skjulte funktioner, og SLÅR TIL LYD FOR en bred gennemførelse heraf.