Europeiska unionens råd

Bryssel 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

**LÄGESRAPPORT**

| | |
|---|---|
| från: | Rådets generalsekretariat |
| av den: | 17 oktober 2022 |
| till: | Delegationerna |
| Föreg. dok. nr: | 12930/22 |
| Ärende: | Rådets slutsatser om säkerheten i IKT-leveranskedjan<br>– Rådets slutsatser godkända av rådet vid mötet den 17 oktober 2022 |

För delegationerna bifogas rådets slutsatser om säkerheten i IKT-leveranskedjan, som godkändes av rådet vid dess möte den 17 oktober 2022.

**BILAGA**

**Rådets slutsatser om säkerheten i IKT-leveranskedjan**

EUROPEISKA UNIONENS RÅD,

SOM ERINRAR OM sina slutsatser om

– det gemensamma meddelandet av den 20 november 2017 till Europaparlamentet och rådet – *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*,

– uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU,

– 5G:s betydelse för den europeiska ekonomin och behovet av att minska säkerhetsriskerna i samband med 5G,

– att forma Europas digitala framtid,

– en återhämtning som främjar omställningen till en mer dynamisk, motståndskraftig och konkurrenskraftig europeisk industri,

– cybersäkerheten för uppkopplade enheter,

– rådets slutsatser om EU:s strategi för cybersäkerhet för ett digitalt decennium,

– utvecklingen av Europeiska unionens arbete på cyberområdet,

– Europeiska revisionsrättens särskilda rapport nr 03/2022 ”Utbyggnaden av 5G i EU: förseningar i nätutbyggnaden och säkerhetsproblem som fortfarande är olösta”,

SOM ERINRAR OM Europeiska rådets slutsatser

– av den 1–2 oktober 2020 om covid-19, den inre marknaden, industripolitik, digitala frågor och yttre förbindelser,

– av den 24–25 mars 2022 om Rysslands militära aggression mot Ukraina, säkerhet och försvar, energi, ekonomiska frågor, covid-19 och yttre förbindelser,

– av den 30–31 maj 2022 om Ukraina, livsmedelstrygghet, säkerhet, försvar och energi,

1. BETONAR, med tanke på geopolitikens ökande betydelse för cybersäkerhet, att Europeiska unionen och dess medlemsstater måste närma sig cybersäkerheten på ett övergripande och strategiskt sätt; Rysslands militära aggression mot Ukraina har radikalt förändrat Europeiska unionens strategiska och säkerhetsrelaterade förutsättningar och visat på behovet av att Europeiska unionen stärks och får större förmåga på säkerhets- och försvarsområdet; den har belyst att det är av yttersta vikt att på lämpligt sätt ta hänsyn till den geopolitiska miljön, inte bara när man reagerar på skadlig it-verksamhet, utan även när man bygger upp och upprätthåller motståndskraften inom informations- och kommunikationsteknik (IKT); detta är av särskild betydelse för leveranskedjorna för IKT-produkter och IKT-tjänster (IKT-leveranskedjor), som både kan äventyras på grundval av geopolitisk rivalitet, vilket illustreras av SolarWinds-attacken, och påverkas av geopolitiska spänningar och instabilitet, vilket framgår av hotet i samband med beroendet av ryska IKT-leverantörer vid tidpunkten för Rysslands militära aggression mot Ukraina,

2. NOTERAR att riskerna med anknytning till med IKT-leveranskedjan, som består av en rad sammanlänkade resurser och processer mellan ekonomiska aktörer (enligt definitionen i förordning (EU) 2019/1020), som börjar med anskaffning av råmaterial och sträcker sig genom tillverkning, bearbetning, hantering och leverans av IKT-produkter och IKT-tjänster, inbegripet tillhandahållande av stöd under IKT-produkters och IKT-tjänsters livscykel, kännetecknas av unika utmaningar och potentiellt långtgående konsekvenser; förutom riskerna i samband med att IKT-produkter inte är tillgängliga, till exempel på grund av brist på kritiska råvaror och halvledare som behövs för deras produktion, hotas leveranskedjorna för IKT-produkter och IKT-tjänster även på andra sätt; de kan i synnerhet vara utsatta för eller missbrukas av illvilliga aktörer på sofistikerade, ofta dolda sätt som påverkar de överförda och lagrade känsliga uppgifternas konfidentialitet, integritet och tillgänglighet,

3. KONSTATERAR, med erkännande av att det behövs en allriskstrategi för att säkra IKT-tillgångar, att förslaget till direktiv om kritiska entiteters motståndskraft är relevant för att förbättra de kritiska entiteternas fysiska säkerhet och BETONAR att det, utöver att öka motståndskraften mot angrepp i leveranskedjan som utförs med hjälp av cybermedel, är lika viktigt att stärka IKT-leveranskedjornas övergripande motståndskraft och säkerhet mot alla olika hotfaktorer, såsom naturkatastrofer, systemfel, interna hot eller mänskliga fel, INSER i detta avseende att IKT-leveranskedjans säkerhet omfattar säkerställande av skyddet av IKT-produkter och IKT-tjänster som produceras, levereras, upphandlas och används i IKT-leveranskedjor, bland annat genom att enskilda komponenter och överförda data skyddas,

4. UPPMANAR, med utgångspunkt i lärdomarna från följderna av Europeiska unionens strategiska beroende av ryska fossila bränslen samt effekterna av störningarna i leveranskedjorna under covid-19-pandemin, särskilt när det gäller läkemedel och halvledare, där EU:s strategiska beroenden blottlades, medlemsstaterna att arbeta för att undvika liknande situationer med oönskat strategiskt beroende av IKT-produkter och IKT-tjänster; på grund av den tilltagande digitaliseringen av samhället och den ständigt ökande användningen av IKT i kritisk infrastruktur bör strategiska externa beroenden med anknytning till IKT-produkter och IKT-tjänster och deras leveranskedjor utvärderas kontinuerligt och, när så är lämpligt, åtgärdas,

5. ERINRAR OM att uppnåendet av strategiskt oberoende samtidigt som en öppen ekonomi bevaras är ett centralt mål för unionen, vilket inbegriper att identifiera och minska strategiska beroenden och öka motståndskraften inom de känsligaste industriella ekosystemen och specifika områdena, även på det digitala området; i detta ingår utveckling och utbyggnad av strategisk digital kapacitet och infrastruktur samt förstärkning av förmågan att göra självständiga tekniska val och, som en av de viktigaste pelarna, säkerställande av motståndskraftiga och säkra infrastrukturer, produkter och tjänster för att bygga upp förtroende för den digitala inre marknaden och inom det europeiska samhället, samtidigt som öppenhet, globalt samarbete med likasinnade partner och konkurrenskraft upprätthålls och de potentiella fördelarna med detta utnyttjas; Europeiska unionens grundläggande värden bevarar i synnerhet privatliv, säkerhet, jämlikhet, mänsklig värdighet, rättsstatsprincipen och ett öppet internet som förutsättningar för att uppnå ett samhälle, en ekonomi och en industri som är digitalt drivna och människocentrerade,

6. NOTERAR att det på grund av utvecklingen av cyberhotbilden, som de senaste åren har visat sig genom trenden med mycket verkningsfulla och sofistikerade attacker i leveranskedjan, till exempel genom SolarWinds-, Mimecast- eller Kaseya-attackerna, och som har uppstått tillsammans med utkontraktering av viktiga IKT-tjänster och intensifierats av det övergripande beroendet av IKT-produkter och IKT-tjänster som tillverkas, tillhandahålls eller underhålls av tredje part, är det i framtiden högst sannolikt att fler attacker i leveranskedjan med betydande skada för ekonomin och samhället kommer att inträffa, BETONAR mot bakgrund av detta vikten av att öka IKT-leveranskedjornas säkerhet och motståndskraft för att den inre marknaden ska fungera och behovet av att säkerställa tillgång, säkerhet och mångfald ska säkerställas när det gäller IKT-produkter och IKT-tjänster på den inre marknaden, KONSTATERAR därför att det finns ett behov av att maximera och rationalisera användningen av befintliga EU-instrument och EU-strategier för att uppnå dessa mål samt behovet av att kontinuerligt anpassa sig till den föränderliga cyberhotbilden genom att införa ytterligare lämpliga åtgärder och mekanismer, även i förhållande till eventuella säkerhetsrisker med ny och omstörtande teknik, UPPMANAR medlemsstaterna att i detta avseende följa den riskbaserade strategin för att hantera ny teknikutveckling,

7. KONSTATERAR att det är nödvändigt att förstå den ständigt föränderliga cyberhotbilden och komplexiteten i attackerna mot leveranskedjan för att effektivt minska de risker som är förknippade med IKT-leveranskedjor, BETONAR i detta avseende behovet av att anpassa sig till nya hot genom att aktivt och kontinuerligt övervaka, analysera och bedöma hotbilden i leveranskedjan, öka medvetenheten och bygga upp kunskap om hot och sårbarheter och proaktivt varna relevanta enheter på ett skräddarsytt sätt, VÄLKOMNAR det arbete som utförs av Europeiska unionens cybersäkerhetsbyrå (Enisa) när det gäller säkerhet i IKT-leveranskedjan, särskilt rapporten om hotbilden när det gäller attacker i leveranskedjan,

SEKTORSÖVERGRIPANDE INSTRUMENT OCH STRATEGIER

8. BEKRÄFTAR vikten av att medlemsstaterna överväger behovet av att diversifiera leverantörer av kritisk IKT för att undvika eller begränsa ett stort beroende av enskilda leverantörer, särskilt högriskleverantörer, eftersom det ökar exponeringen för konsekvenserna av potentiella störningar, INSER att undvikande av låsning till leverantörer och diversifiering av IKT-leverantörer är en av de viktiga komponenterna för att säkerställa stabilitet och säkerhet på den inre marknaden, FRAMHÅLLER behovet av att främja och genomföra lämpliga strategier som underlättar diversifiering av leverantörer och konkurrenskraft på ett teknikneutralt sätt, UPPMANAR dessutom till integrering av aspekter som rör förebyggande av låsning till leverantörer i EU-lagstiftningen, VÄRDESÄTTER förslaget till förordning om harmoniserade regler för rättvis tillgång till och användning av data (dataakten), som syftar till att öka interoperabiliteten mellan databehandlingstjänster och undanröja hinder för byte mellan leverantörer av databehandlingstjänster,

9. ÄR MEDVETET OM kopplingen mellan IKT-leveranskedjans säkerhet och offentlig upphandling, BETONAR behovet av att i förfarandena för offentlig upphandling ta tillräcklig hänsyn till vikten av IKT-leveranskedjans säkerhet genom att vid behov införa objektiva och riskbaserade urvalskriterier för anbudsgivarnas förmåga att säkerställa en hög säkerhetsnivå för de tjänster som tillhandahålls, EFTERLYSER en lämplig balans mellan å ena sidan allmänintresset av att offentliga medel används så effektivt och rättvist som möjligt och å andra sidan allmänintresset av att säkra informationssystem och säkerställa en väl fungerande inre marknad, UPPMANAR, för att underlätta genomförandet av relevanta regler för offentlig upphandling mot bakgrund av den ökande cybersäkerheten, kommissionen att senast det tredje kvartalet 2023 utarbeta metodriktlinjer för att uppmuntra de upphandlande myndigheterna att lägga lämpligt fokus på anbudsgivarnas och deras underleverantörers cybersäkerhetspraxis och att bedöma och vid behov lägga fram förslag för att se över eller komplettera relevant lagstiftning om offentlig upphandling,

10. KONSTATERAR att utländska direktinvesteringar som rör IKT-produkter och IKT-tjänster, samtidigt som de medför ekonomiska och sociala fördelar för medlemsstater, företag och medborgare, skulle kunna innebära risker för säkerheten och den allmänna ordningen och NOTERAR att EU:s system för granskning av utländska direktinvesteringar, tillsammans med respektive nationella granskningssystem, som tillhandahåller medel för att hantera sådana risker, också skulle kunna tillämpas som ett användbart verktyg för att skydda IKT-leveranskedjans säkerhet och motståndskraft genom att bidra till att eliminera högriskinvesteringar som kan påverka sådan säkerhet och motståndskraft; INSER att information som utbyts och delas genom denna mekanism kan hjälpa medlemsstaterna att bättre bedöma eventuella hot mot IKT-leveranskedjornas säkerhet och vidta nödvändiga åtgärder i enlighet därmed; UPPMANAR de berörda nationella aktörerna att när så är lämpligt även ta hänsyn till denna dimension av granskningssystemet,

11. BEKRÄFTAR, när det gäller försvar, sin uppmaning till kommissionen att under 2023, tillsammans med medlemsstaterna, bedöma riskerna för leveranskedjor för kritisk infrastruktur på olika områden, inbegripet det digitala området, med koppling till EU:s säkerhets- och försvarsintressen samt att undersöka alternativ för att öka cybersäkerheten i hela leveranskedjan för EU:s försvarstekniska och försvarsindustriella bas; UPPMANAR dessutom medlemsstaterna och kommissionen att reflektera över säkerheten i IKT-leveranskedjan vid genomförandet av åtagandena och åtgärderna i den strategiska kompassen,

12. ERKÄNNER vikten av råvaror av avgörande betydelse och alla typer av halvledare som grundläggande byggstenar för IKT-produkter och UPPMANAR till konstruktiva förhandlingar om förslaget till Europaparlamentets och rådets förordning om en ram med åtgärder för att stärka Europas halvledarekosystem (förordningen om halvledare) och förslaget till rådets förordning om ändring av förordning (EU) 2021/2085 om bildande av gemensamma företag, vad gäller det gemensamma företaget för halvledare,

IT-SPECIFIKA INSTRUMENT

13. NOTERAR särskilt när det gäller telekommunikationsinfrastruktur de framsteg som gjorts på unionsnivå för att förbättra säkerheten i leveranskedjan för 5G-nät, särskilt genom EU:s verktygslåda för 5G-säkerhet; UPPMANAR medlemsstaterna att utbyta ytterligare information om bästa praxis och metoder rörande genomförandet av åtgärderna enligt rekommendationerna i verktygslådan för 5G-säkerhet och i synnerhet att tillämpa relevanta begränsningar på högriskleverantörer när det gäller nyckeltillgångar som definieras som kritiska och känsliga i EU:s samordnade riskbedömning; FRAMHÅLLER att EU:s verktygslåda för 5G är ett smidigt riskbaserat instrument för att hantera identifierade säkerhetsutmaningar, som gör det möjligt att hantera 5G-cybersäkerhetsaspekter i tid och på ett effektivt sätt, samtidigt som medlemsstaternas befogenheter respekteras, och ERKÄNNER att den är ett värdefullt instrument för att, med full insyn, ytterligare förbättra säkerheten i leveranskedjan för telekommunikationsnät på ett samordnat sätt som kan tjäna som inspiration för riskbedömnings- och begränsningsverktyg med anknytning till andra viktiga sektorer; ERINRAR OM uppmaningen från berörda myndigheter att på grundval av riskbedömningar utarbeta rekommendationer till medlemsstaterna och kommissionen i syfte att stärka resiliensen hos kommunikationsnät och infrastrukturer inom Europeiska unionen, inbegripet det fortsatta genomförandet av EU:s verktygslåda för 5G,

14. NOTERAR vikten av driftskompatibla strategier som kan hantera låsning till leverantörer och sprida koncentrationsrisker, samtidigt som säkerheten i leveranskedjan förbättras över hela spektrumet av IKT-infrastruktur och IKT-tjänster; ÄR MEDVETET OM de potentiella fördelarna med Open RAN-konceptet i detta avseende, särskilt när det gäller 5G-nät, och ERINRAR samtidigt om den rapport om cybersäkerhet i Open RAN som offentliggjorts av samarbetsgruppen för nät- och informationssäkerhet och noterar att detta koncept fortfarande håller på att utvecklas och att dess säkerhet, transparens och standardisering befinner sig i ett tidigt mognadsskede, samt BETONAR vikten av att bedöma riskerna inför varje övergång till nya standarder eller arkitekturer,

15. FRAMHÅLLER betydelsen av befintliga och kommande övergripande lagstiftningsinstrument för cybersäkerhet, särskilt förordningen om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten), det kommande direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2), förslaget till förordning om fastställande av åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer samt förslaget till förordning om övergripande cybersäkerhetskrav för produkter med digitala inslag (rättsakten om cyberresiliens), för att öka säkerheten i IKT-leveranskedjan; NOTERAR dessutom den viktiga utvecklingen av sektorsspecifika cybersäkerhetsbestämmelser, särskilt den framtida förordningen om digital operativ motståndskraft för finanssektorn (DORA-förordningen), som omfattar en tillsynsram för tredjepartsleverantörer av IKT-tjänster som är viktiga för finansiella enheter; genom dessa förordningar införs allmänna skyldigheter i fråga om säkerhet i leveranskedjan samt detaljerade och specifika krav som är relevanta för den berörda sektorn; BETONAR samtidigt att leverantörerna ofta tillhandahåller sina produkter och tjänster inom olika sektorer snarare än till en enda bransch; det är därför mycket viktigt att se till att säkerhetskraven i leveranskedjan i möjligaste mån anpassas till alla berörda sektorer, särskilt de som omfattas av det framtida NIS 2-direktivet, för att undvika skillnader mellan de skyldigheter som åläggs leverantörerna och för att minska bördan för operatörer inom kritiska sektorer att bedöma leverantörernas efterlevnad av dessa skyldigheter, samtidigt som hänsyn tas till sektorsspecifika särdrag,

16. VÄLKOMNAR förslaget till rättsakt om cyberresiliens som ett viktigt lagstiftningsinstrument för att främja en säker utveckling av produkter med digitala inslag och för att säkerställa att cybersäkerhet beaktas under hela livscykeln för produkter med digitala inslag; NOTERAR att förslaget till rättsakt om cyberresiliens har potential att avsevärt bidra till att stärka säkerheten inom IKT-leveranskedjan; UPPMANAR TILL konstruktiva förhandlingar och ett snabbt antagande av akten;

17. ÄR i detta avseende MEDVETET OM det pågående arbete som leds av Enisa, tillsammans med medlemsstaterna och andra parter, för att förse EU med certifieringssystem för IKT-produkter, IKT-tjänster och IKT-processer i enlighet med cybersäkerhetsakten, vilket bör bidra till att höja den övergripande cybersäkerhetsnivån på den digitala inre marknaden; UPPMANAR alla berörda parter att delta i det förberedande arbetet med enskilda europeiska certifieringssystem för att bygga upp förtroendet för säkra IKT-produkter, IKT-processer och IKT-tjänster och stärka deras resiliens och UPPMANAR kommissionen att snabbt utarbeta genomförandeakter om de europeiska certifieringssystemen efter slutförandet av det förberedande arbetet, särskilt det gemensamma kriteriebaserade europeiska systemet för cybersäkerhetscertifiering; KONSTATERAR att de europeiska certifieringssystemen vid behov bör omfatta krav på säkerhet i leveranskedjan, även med avseende på förbindelserna med leverantörer,

18. FRAMHÅLLER behovet av ett grundligt genomförande av alla kommande NIS 2-bestämmelser om säkerhet i leveranskedjan för informations- och kommunikationsteknik; UNDERSTRYKER i detta avseende relevansen av EU:s samordnade riskbedömningar av kritiska leveranskedjor (samordnade riskbedömningar av leveranskedjan), nationell politik för säkerhet i leveranskedjan och säkerhetsåtgärder som rör leveranskedjan; NOTERAR att uppmärksamhet bör ägnas inte bara de primära leverantörerna utan även de relevanta underleverantörerna när det gäller risker för säkerheten för den primära leverantören eller slutkunden; UPPMANAR Enisa att med bistånd av samarbetsgruppen för nät- och informationssäkerhet göra en inventering av bästa tillgängliga praxis för riskhantering i leveranskedjan och sammanställa den i metodriktlinjer i syfte att underlätta genomförandet av riskhanteringsåtgärder i leveranskedjan, UPPMANAR dessutom Enisa att övervaka investeringar i IKT-leveranskedjans säkerhet för de enheter som omfattas av det kommande NIS 2-direktivet,

19. FRAMHÅLLER även fördelarna och riskerna med att använda leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster i samband med säkerheten i leveranskedjan; användningen av dessa leverantörer kan avsevärt förbättra säkerheten inom organisationer och leda till högre cybersäkerhetsnivåer, men förvaltning av IKT-system och IKT-tjänster på avstånd i kombination med privilegierad tillgång till kundernas IKT-miljö, som leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster kan behöva, kan, när det är fråga om leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster med bristande säkerhet, leda till kaskadeffekter med omfattande följder för ett stort antal kunder; det är därför av yttersta vikt att leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster upprätthåller en hög nivå av intern säkerhet och säkerhet vad gäller de tjänster som de tillhandahåller och har ett öppet förhållningssätt gentemot sina kunder när det gäller säkerheten i de tjänster som de tillhandahåller, VÄLKOMNAR i detta avseende att dessa i framtiden inkluderas i tillämpningsområdet för det kommande NIS 2-direktivet,

20. NOTERAR, när det gäller genomförandet av mekanismen för samordnade riskbedömningar av leveranskedjan i enlighet med det kommande NIS 2-direktivet, relevansen av icke-tekniska riskfaktorer i detta sammanhang, såsom en tredjestats otillbörliga påverkan av leverantörer och tjänsteleverantörer, och ÄR i detta sammanhang MEDVETET OM de faktorer som kan användas för att bedöma den riskprofil som nämns i EU:s samordnade riskbedömning av 5G-nätens cybersäkerhet, UPPMANAR kommissionen att senast under andra kvartalet 2023, efter samråd med samarbetsgruppen för nät- och informationssäkerhet och Enisa, fastställa vilka specifika IKT-tjänster, IKT-system eller IKT-produkter som kan prioriteras för att bli föremål för samordnade riskbedömningar av leveranskedjan,

21. NOTERAR att beroendet av högriskleverantörer av IKT-produkter och IKT-tjänster som används för driften av kritiska nätverk och system utgör ett strategiskt hot som måste minskas genom lämplig politik på både nationell nivå och EU-nivå och genom samarbete mellan medlemsstaterna och med likasinnade internationella partner, UPPMANAR, för att underlätta begränsningen av denna strategiska risk och stödja de samordnade riskbedömningarna av leveranskedjan, samarbetsgruppen för nät- och informationssäkerhet att i samarbete med kommissionen och Enisa utveckla en verktygslåda med åtgärder för att minska kritiska IKT-risker i leveranskedjan (verktygslådan för IKT-leveranskedjan); verktygslådan för IKT-leveranskedjan bör bygga på strategiska hotscenarier som identifierats för IKT-leveranskedjor och tillhandahålla åtgärder för att hantera dessa scenarier genom att utnyttja erfarenheterna från 5G-verktygslådan och den nationell nivån; den bör på ett transparent sätt komplettera de samordnade riskbedömningarna av leveranskedjan för specifika IKT-tjänster, IKT-system eller IKT-produkter enligt det kommande NIS 2-direktivet genom att erbjuda generiska riskreduceringsåtgärder som kan anpassas till specifika IKT-tjänster, IKT-system eller IKT-produkter på ett skalbart sätt på grundval av de risker som identifierats i de individuella samordnade riskbedömningarna av leveranskedjan,

22. BETONAR den viktiga roll som forskning, innovation, investeringar och entreprenörsverksamhet spelar på det digitala området och cybersäkerhetsområdet samt finansieringen av sådan verksamhet när det gäller att undvika eventuella framtida oönskade strategiska beroenden och stärka IKT-leveranskedjornas övergripande motståndskraft, UNDERSTRYKER i detta sammanhang rollen och relevansen av både de strategiska uppgifterna och genomförandeuppgifterna för Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (ECCC) och nätverket av nationella samordningscentrum när det gäller att bidra till att maximera effekterna av investeringar för att stärka unionens ledarskap och öppna strategiska oberoende på cybersäkerhetsområdet och unionens stödjande tekniska kapacitet och kompetens och att öka unionens globala konkurrenskraft, EFTERLYSER i detta avseende ett snabbt operationellt genomförande av ECCC, UPPMANAR ECCC att i sin strategiska agenda ta hänsyn till säkerhetsaspekterna i IKT-leveranskedjan, inbegripet till exempel säker programvaruutveckling, samtidigt som konsekvens och komplementaritet säkerställs och dubbelarbete undviks, STÖDER stärkandet av den europeiska konkurrenskraften på cybersäkerhetsområdet genom finansieringsprogram, såsom Horisont Europa-programmet för forskning och innovation samt programmet för ett digitalt Europa för att stärka, bygga upp och förvärva nödvändig kapacitet för EU:s digitala ekonomi, samhälle och demokrati,

STÖDMEKANISMER

23. UPPMANAR till ökade ekonomiska stödincitament i samband med åtgärder som syftar till att stärka säkerheten i IKT-leveranskedjan, UPPMANAR, som en prioriterad fråga, även med tanke på det kommande genomförandet av NIS 2-direktivet, ECCC, kommissionen och relevanta intressenter att undersöka alternativ för att inkludera säkerhetsaspekter på IKT-leveranskedjan i de kommande ansökningsomgångarna inom arbetsprogrammen för cybersäkerhet inom ramen för programmet för ett digitalt Europa och Horisont Europa-programmet, eller andra relevanta finansieringsmöjligheter; dessa finansieringsmöjligheter bör bland annat syfta till att göra det möjligt för organisationerna att stödja upprätthållandet av en hög cybersäkerhetsnivå när det gäller upphandling av IKT-produkter och IKT-tjänster i hela leveranskedjan, särskilt när det gäller ersättning av specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter som erkänns som högriskprodukter i enlighet med framtida samordnade riskbedömningar av leveranskedjan,

24. KONSTATERAR att globaliseringen och specialiseringen av IKT-tjänster och det ökade beroendet av tredjepartsprodukter och tredjepartstjänster medför ett behov av ett nära samarbete inom EU och internationellt för att dela kunskap och expertis mellan berörda parter och UPPMANAR dessa att finna en stark och samordnad ståndpunkt som säkerställer säkerheten i IKT-leveranskedjan på ett övergripande sätt, INSER också behovet av att ytterligare utforska relevanta moderna strategier och tekniker, både för lämpliga grundläggande it-hygieniska och långsiktiga lösningar för att uppnå säkra och motståndskraftiga IKT-leveranskedjor samt de lämpligaste sätten att främja dessa och eventuellt införliva dem i politik eller andra initiativ, ERKÄNNER i detta avseende att särskild uppmärksamhet bör ägnas åt att undersöka fördelarna och nackdelarna med systematiska lösningar, såsom nollförtroende-principerna, materiallista för programvara och liknande långsiktiga lösningar, REKOMMENDERAR att samarbetsgruppen för nät- och informationssäkerhet används för detta ändamål,

25. NOTERAR fördelarna med övervakning och effektivt utbyte av information om cyberincidenter och cyberhot när det gäller att förebygga, upptäcka och mildra effekterna av attacker i leveranskedjan, BETONAR behovet av att fortsätta att bygga upp tillit och förtroende mellan medlemsstaterna för ett effektivt utbyte av sådan information, ERINRAR i det avseendet OM kommissionens förslag om att stödja medlemsstaterna i deras arbete med att inrätta och stärka säkerhetscentrum i syfte att bygga upp ett nätverk av sådana centrum i hela EU, för att ytterligare övervaka och förutse signaler som tyder på möjliga angrepp på nät, ERINRAR OM behovet av komplementaritet och samordning inom befintliga nätverk och mekanismer, och FRAMHÅLLER i detta avseende framför allt CSIRT-nätverkets roll och behovet av att ytterligare utforska dessa nätverks potential för att främja en effektiv, säker och tillförlitlig kultur för informationsutbyte, ERINRAR OM de insatser som gjorts av medlemsstaterna, med stöd av EU, för att inrätta sektoriella, nationella och regionala it-incidentcentrum (CSIRT) och nationella eller europeiska informations- och analyscentraler som en del av ett effektivt nätverk av cybersäkerhetspartnerskap i unionen,

26. BETONAR, på grund av att hoten mot IKT-leveranskedjan är sammanlänkade och globala till sin karaktär, vikten av att närma sig och förbättra säkerheten i IKT-leveranskedjan på global nivå, REKOMMENDERAR därför att man använder digitala partnerskap, cyberdialoger och andra relevanta EU-initiativ inbegripet, när så är lämpligt, frihandelsavtal, för att främja riskbaserade utvärderingar av IKT-produktleverantörer och IKT-tjänsteleverantörer, användning av tillförlitliga leverantörer och för att använda ett säkert och innovativt digitalt ekosystem baserat på öppna, driftskompatibla och transparenta standarder, UPPREPAR dessutom visionen för Global Gateway-partnerskapen och handels- och teknikrådet mellan EU och USA, och verksamhet inom dess arbetsgrupper, för att främja användningen av leverantörer som är betrodda eller inte är högriskleverantörer och utveckla en finansieringsmekanism för att möjliggöra projekt som gör IKT-infrastruktur och IKT-tjänster i tredjestater säkrare, mer motståndskraftiga och mer betrodda, bland annat genom att på ett teknikneutralt sätt avstå från att finansiera inköp från leverantörer som inte är betrodda/medför hög risk,

27. BEKRÄFTAR sitt åtagande att bidra till och främja en öppen, fri, global, stabil och säker cyberrymd och att följa de normer, regler och principer för ansvarsfullt statligt beteende i cyberrymden som fastställs i FN:s ram, ERINRAR, särskilt när det gäller säkerheten i IKT-leveranskedjan, om den norm som godkänts av FN:s grupp med myndighetsexperter och den öppna arbetsgruppen och som uppmuntrar staterna att vidta rimliga åtgärder för att säkerställa leveranskedjans integritet, bland annat genom utveckling av objektiva samarbetsåtgärder, så att slutanvändarna kan ha förtroende för IKT-produkters säkerhet, och att sträva efter att förhindra spridning av skadliga IKT-verktyg och skadlig IKT-teknik och användning av skadliga dolda funktioner, och FÖRORDAR ett brett genomförande av detta.