Svet
Evropske unije

Bruselj, 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

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	17. oktober 2022
Prejemnik:	delegacije
Št. predh. dok.:	12930/22
Zadeva:	Sklepi Sveta o varnosti dobavne verige IKT – sklepi Sveta, ki jih je Svet odobril na seji 17. oktobra 2022

V prilogi vam pošiljamo Sklepe Sveta o varnosti dobavne verige IKT, ki jih je Svet odobril na seji 17. oktobra 2022.

PRILOGA

Sklepi Sveta o varnosti dobavne verige IKT

SVET EVROPSKE UNIJE –

OB OPOZARJANJU na svoje sklepe o:

– Skupnem sporočilu Evropskemu parlamentu in Svetu z dne 20. novembra 2017: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“,

– krepitvi zmogljivosti in zmožnosti na področju kibernetske varnosti v EU,

– pomenu omrežij 5G za evropsko gospodarstvo in dejstvu, da je treba zmanjšati varnostna tveganja, povezana z njimi,

– oblikovanju digitalne prihodnosti Evrope,

– „okrevanju, ki pospešuje prehod k bolj dinamični, odpornejši in bolj konkurenčni industriji“,

– kibernetski varnosti povezanih naprav,

– strategiji EU za kibernetsko varnost v digitalnem desetletju,

– vzpostavitvi stališča Evropske unije glede kibernetskih vprašanj,

– Posebnem poročilu št. 03/2022 Evropskega računskega sodišča z naslovom „Uvajanje omrežij 5G v EU: zamude pri uvajanju omrežij in varnostna vprašanja, ki ostajajo nerešena“;

OB OPOZARJANJU na sklepe Evropskega sveta o:

– COVID-19, enotnem trgu, industrijski politiki in digitalni razsežnosti ter zunanjih odnosih z dne 1. in 2. oktobra 2020,

– ruski vojaški agresiji v Ukrajini, varnosti in obrambi, energiji, gospodarskih vprašanjih, COVID-19 in zunanjih odnosih z dne 24. in 25. marca 2022,

– Ukrajini, prehranski varnosti, varnosti in obrambi ter energiji z dne 30. in 31. maja 2022 –

1. glede na vse večji pomen geopolitike za kibernetsko varnost POUDARJA, da morajo Evropska unija in njene države članice kibernetsko varnost obravnavati celovito in strateško. Vojaška agresija Rusije v Ukrajini je popolnoma preobrazila strateško in varnostno okolje Evropske unije ter nakazala, da mora biti Evropska unija na področju varnosti in obrambe močnejša in zmogljivejša. Izpostavil je, da je izredno pomembno ustrezno upoštevati geopolitično okolje, ne le pri odzivanju na zlonamerne kibernetske dejavnosti, temveč tudi pri izgradnji in ohranjanju odpornosti informacijskih in komunikacijskih tehnologij (IKT). To je še posebej pomembno za dobavne verige proizvodov in storitev IKT (dobavne verige IKT), ki bi lahko bile ogrožene zaradi geopolitičnega rivalstva, kot je razvidno iz napada SolarWinds, ter bi jih prizadele geopolitične napetosti in nestabilnost, kot je razvidno iz grožnje, povezane z odvisnostjo od ruskih ponudnikov IKT v času vojaške agresije Rusije v Ukrajini;

2. UGOTAVLJA, da narava tveganj, povezanih z dobavno verigo IKT – ki jo sestavlja povezan sklop virov in procesov med gospodarskimi subjekti (kot so opredeljeni v Uredbi (EU) 2019/1020) ter se razteza vse od pridobivanja surovin pa do proizvodnje, obdelave in dostave proizvodov in storitev IKT ter ravnanja z njimi, vključno z zagotavljanjem podpore med življenjskim ciklom proizvodov in storitev IKT – prinaša edinstvene izzive in potencialno daljnosežne posledice. Poleg tveganj, povezanih z nerazpoložljivostjo proizvodov IKT, na primer zaradi pomanjkanja kritičnih surovin in polprevodnikov, potrebnih za njihovo proizvodnjo, so dobavne verige proizvodov in storitev IKT izpostavljene še drugim grožnjam. Zlasti jih lahko zlonamerni akterji izberejo za tarčo ali jih zlorabljajo na sofisticirane, pogosto prikrite načine, ki vplivajo na zaupnost, celovitost in razpoložljivost prenesenih in shranjenih občutljivih podatkov;

3. ob priznavanju, da je za zaščito sredstev IKT potreben pristop, ki upošteva vse nevarnosti, POTRJUJE pomen predloga direktive o odpornosti kritičnih subjektov za izboljšanje fizične varnosti kritičnih subjektov ter POUDARJA, da je poleg krepitve odpornosti proti napadom na dobavne verige, ki se izvajajo s kibernetskimi sredstvi, enako pomembno krepiti splošno odpornost in varnost dobavnih verig IKT pred najrazličnejšimi dejavniki ogroženosti, kot so naravni dogodki, okvare sistema, notranje grožnje ali človeške napake. V zvezi s tem PRIZNAVA, da varnost dobavne verige IKT vključuje zagotavljanje zaščite proizvodov in storitev IKT, ki se proizvajajo, dobavljajo, naročajo in uporabljajo v dobavnih verigah IKT, med drugim tudi zaščito posameznih sestavnih delov in prenesenih podatkov;

4. na podlagi izkušenj iz posledic strateških odvisnosti Evropske unije od ruskih fosilnih goriv ter učinkov motenj v dobavnih verigah med pandemijo COVID-19, zlasti v zvezi s farmacevtskimi izdelki in polprevodniki, pri katerih so se pokazale strateške odvisnosti EU, SPODBUJA države članice, naj si prizadevajo za preprečevanje podobnih primerov neželenih strateških zunanjih odvisnosti v zvezi s proizvodi in storitvami IKT. Zaradi vse večje digitalizacije družbe in vse večje uporabe IKT v kritični infrastrukturi bi bilo treba stalno ocenjevati in, kjer je to ustrezno, odpravljati strateške zunanje odvisnosti, povezane s proizvodi in storitvami IKT ter njihovimi dobavnimi verigami;

5. OPOZARJA, da je doseganje strateške avtonomije ob hkratnem ohranjanju odprtega gospodarstva ključni cilj Unije, kar vključuje identificiranje in zmanjševanje strateških odvisnosti ter povečanje odpornosti najobčutljivejših industrijskih ekosistemov in posebnih področij, tudi digitalnega. To vključuje razvoj in uporabo strateških digitalnih zmogljivosti in infrastrukture ter krepitev sposobnosti sprejemanja avtonomnih tehnoloških odločitev in – kot enega glavnih stebrov – zagotavljanje odpornih in varnih infrastruktur, proizvodov in storitev zaradi krepitve zaupanja v enotni digitalni trg in znotraj evropske družbe, vse ob ohranjanju odprtosti, globalnega sodelovanja s podobno mislečimi partnerji in konkurenčnosti ter izkoriščanju morebitnih koristi vsega naštetega. Temeljne vrednote Evropske unije so usmerjene zlasti v ohranjanje zasebnosti, varnosti, enakosti, človekovega dostojanstva, pravne države in odprtega interneta kot predpogojev za doseganje na človeka osredotočene družbe, gospodarstva in industrije, katerih gonilo je digitalizacija;

6. UGOTAVLJA, da je zaradi razvoja dogodkov na področju kibernetskih groženj, kot se v zadnjih letih kažejo v vse pogostejših zelo učinkovitih in sofisticiranih napadih na dobavne verige, kot so napadi SolarWinds, Mimecast ali Kaseya, ki se pojavljajo skupaj z oddajanjem bistvenih storitev IKT v zunanje izvajanje ter so močnejši zaradi splošne odvisnosti od proizvodov in storitev IKT, ki jih proizvajajo, zagotavljajo ali servisirajo tretje strani, v prihodnosti zelo verjetno, da bo prišlo do še več napadov na dobavne verige z znatno škodo za gospodarstvo in družbo. Ob upoštevanju tega POUDARJA, da je zaradi delovanja enotnega trga pomembno krepiti varnost in odpornost dobavnih verig IKT, da pa je obenem treba zagotavljati razpoložljivost, varnost in raznolikost proizvodov in storitev IKT na enotnem trgu. Zato PRIZNAVA, da je treba čim bolj povečati in racionalizirati uporabo obstoječih instrumentov in pristopov EU za doseganje teh ciljev, pa tudi, da se je treba nenehno prilagajati spreminjajočim se kibernetskim grožnjam z uvedbo dodatnih ustreznih ukrepov in mehanizmov, tudi v zvezi z morebitnimi varnostnimi tveganji nastajajočih in prelomnih tehnologij. SPODBUJA države članice, naj v zvezi s tem uporabljajo pristop, ki temelji na tveganju, da bi se soočile z novimi tehnološkimi dosežki;

7. POTRJUJE, da je razumevanje nenehno spreminjajočih se kibernetskih groženj in kompleksnosti napadov na dobavne verige bistveno za učinkovito zmanjševanje tveganj, povezanih z dobavnimi verigami IKT. V zvezi s tem POUDARJA, da se je treba novim grožnjam prilagoditi z dejavnim in stalnim spremljanjem, analiziranjem in ocenjevanjem narave groženj v dobavni verigi, ozaveščanjem in pridobivanjem znanja o grožnjah in ranljivostih ter proaktivnim in prilagojenim opozarjanjem ustreznih subjektov. Pozdravlja delo Agencije Evropske unije za kibernetsko varnost (ENISA) v zvezi z varnostjo dobavne verige IKT, zlasti njeno poročilo o naravi groženj za napade na dobavne verige;

MEDSEKTORSKI INSTRUMENTI IN PRISTOPI

8. PONOVNO POTRJUJE, kako pomembno je, da države članice razmislijo o potrebi po diverzifikaciji dobaviteljev in ponudnikov ključnih IKT, da bi preprečile ali omejile ustvarjanje velikih odvisnosti od posameznih dobaviteljev in ponudnikov, zlasti dobaviteljev in ponudnikov z visokim tveganjem, saj to povečuje izpostavljenost posledicam morebitnih motenj. PRIZNAVA, da je izogibanje vezanosti na ponudnika ter diverzifikacija dobaviteljev in ponudnikov IKT eden od pomembnih elementov za zagotavljanje stabilnosti in varnosti notranjega trga. IZPOSTAVLJA, da je treba spodbujati in izvajati ustrezne strategije za spodbujanje diverzifikacije ponudnikov in konkurenčnosti na tehnološko nevtralen način. Poleg tega SPODBUJA vključitev vidikov, povezanih s preprečevanjem vezanosti na ponudnika, v zakonodajo EU. V zvezi s tem JE SEZNANJEN s predlogom uredbe o usklajenih pravilih o pravičnem dostopu do podatkov in njihovi uporabi (akt o podatkih), katere cilj je povečati interoperabilnost storitev obdelave podatkov in odpraviti ovire za zamenjavo ponudnikov storitev obdelave podatkov;

9. PRIZNAVA povezavo med varnostjo dobavne verige IKT in javnimi naročili. POUDARJA, da morajo postopki javnega naročanja ustrezno upoštevati pomen varnosti dobavne verige IKT, tako da se, kjer je to ustrezno, uvedejo objektivna izbirna merila, ki temeljijo na tveganju in se nanašajo na sposobnost ponudnikov, da zagotovijo visoko raven varnosti ponujenih storitev. POZIVA k iskanju pravega ravnovesja med javnim interesom za najučinkovitejšo in najpravičnejšo uporabo javnih sredstev na eni strani ter javnim interesom za zaščito informacijskih sistemov in zagotavljanje nemotenega delovanja enotnega trga na drugi strani. Za lažje izvajanje ustreznih pravil o javnem naročanju ob upoštevanju povečanja kibernetske varnosti POZIVA Komisijo, naj do tretjega četrtletja leta 2023 pripravi metodološke smernice, da bi javne naročnike spodbudila, naj se ustrezno osredotočijo na prakse ponudnikov in njihovih podizvajalcev na področju kibernetske varnosti, pa tudi ocenijo zadevno zakonodajo o javnem naročanju in po potrebi pripravijo predloge za njeno revizijo ali dopolnitev;

10. PRIZNAVA, da bi lahko neposredne tuje naložbe, povezane s proizvodi in storitvami IKT, čeprav sicer državam članicam, podjetjem in državljanom zagotavljajo gospodarske in socialne koristi, vključevale tveganja za varnost in javni red, ter UGOTAVLJA, da bi se lahko mehanizem EU za pregled neposrednih tujih naložb skupaj z ustreznimi nacionalnimi sistemi pregleda, ki zagotavljajo sredstva za obravnavanje takih tveganj, uporabljal tudi kot koristno orodje za zagotavljanje varnosti in odpornosti dobavne verige IKT, saj bi prispeval k odpravi naložb z visokim tveganjem, ki bi lahko vplivale na tako varnost in odpornost. SE ZAVEDA, da lahko informacije, ki se izmenjujejo in delijo prek tega mehanizma, državam članicam pomagajo bolje oceniti morebitne grožnje za varnost dobavnih verig IKT in v skladu s tem sprejeti potrebne ukrepe. POZIVA ustrezne nacionalne akterje, naj, kjer je to ustrezno, upoštevajo tudi to razsežnost mehanizma pregleda;

11. kar zadeva obrambo, PONOVNO POTRJUJE svoj poziv Komisiji, naj leta 2023 skupaj z državami članicami oceni tveganja za dobavne verige kritične infrastrukture na različnih področjih, vključno z digitalnim področjem, ki so povezana z varnostnimi in obrambnimi interesi EU, ter preuči možnosti za povečanje kibernetske varnosti v celotni dobavni verigi tehnološke in industrijske baze obrambe EU. Poleg tega POZIVA države članice in Komisijo, naj pri izvajanju zavez in ukrepov strateškega kompasa razmislijo o varnosti dobavne verige IKT;

12. ob priznavanju pomena kritičnih surovin in vseh vrst polprevodnikov kot osnovnih gradnikov proizvodov IKT SPODBUJA konstruktivna pogajanja o predlogu uredbe o vzpostavitvi okvira ukrepov za okrepitev evropskega polprevodniškega ekosistema (akt o čipih) in predlogu uredbe Sveta o spremembi Uredbe Sveta (EU) 2021/2085 o ustanovitvi skupnih podjetij v okviru Obzorja Evropa v zvezi s Skupnim podjetjem za čipe;

INSTRUMENTI, SPECIFIČNI ZA KIBERNETSKO VARNOST

13. zlasti v zvezi s telekomunikacijsko infrastrukturo JE SEZNANJEN z dosežki na ravni Unije pri izboljšanju varnosti dobavne verige omrežij 5G, predvsem prek zbirke orodij EU za varnost 5G. POZIVA države članice, naj še naprej izmenjujejo informacije o najboljših praksah in metodologijah v zvezi z izvajanjem ukrepov, priporočenih v zbirki orodij EU za varnost 5G, zlasti pa naj v zvezi s ključnimi sredstvi, ki so v usklajeni oceni tveganja v EU opredeljena kot kritična in občutljiva, uporabljajo zadevne omejitve za dobavitelje in ponudnike z visokim tveganjem. IZPOSTAVLJA, da je zbirka orodij EU za varnost 5G prožen na tveganju temelječ instrument za obravnavanje identificiranih varnostnih izzivov, ki omogoča pravočasno in učinkovito obravnavanje vidikov kibernetske varnosti tehnologije 5G ob spoštovanju pristojnosti držav članic, in SE ZAVEDA, da je dragocen instrument za nadaljnje usklajeno izboljšanje varnosti – ob popolni preglednosti – dobavne verige telekomunikacijskih omrežij, kar bi lahko služilo kot navdih za orodja za ocenjevanje in zmanjševanje tveganj, povezana z drugimi ključnimi sektorji. PONAVLJA poziv ustreznim organom, naj na podlagi ocen tveganja oblikujejo priporočila za države članice in Komisijo, da bi okrepili odpornost komunikacijskih omrežij in infrastruktur v Evropski uniji, vključno z nadaljnjim izvajanjem zbirke orodij EU za varnost 5G;

14. OPOZARJA na pomen interoperabilnih pristopov, s katerimi se je mogoče odzvati na vezanost na ponudnika in zmanjšati tveganje koncentracije, obenem pa izboljšati varnost dobavne verige v celotnem spektru infrastrukture in storitev IKT. Zlasti glede omrežij 5G SE ZAVEDA morebitnih koristi koncepta odprtega radijskega dostopovnega omrežja v zvezi s tem, obenem pa OPOZARJA na poročilo o kibernetski varnosti odprtega radijskega dostopovnega omrežja, ki ga je objavila Skupina za sodelovanje na področju varnosti omrežij in informacij in v katerem je navedeno, da se ta koncept še razvija, njegova varnost, preglednost in standardizacija pa so v zgodnji fazi zrelosti, ter POUDARJA, da je treba pred kakršnim koli prehodom na nove standarde ali strukture oceniti tveganja;

15. IZPOSTAVLJA pomen obstoječih in prihodnjih horizontalnih zakonodajnih instrumentov na področju kibernetske varnosti, zlasti uredbe o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (akt o kibernetski varnosti), prihodnje direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (revidirana direktiva o varnosti omrežij in informacij), predloga uredbe o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije ter predloga uredbe o horizontalnih zahtevah glede kibernetske varnosti za proizvode z digitalnimi elementi (akt o kibernetski odpornosti), za povečanje varnosti dobavne verige IKT. Poleg tega UGOTAVLJA pomemben razvoj na področju sektorskih predpisov o kibernetski varnosti, zlasti prihodnje uredbe o digitalni operativni odpornosti v finančnem sektorju (DORA), ki vključuje okvir nadzora za tretje ponudnike storitev IKT, ki so ključni za finančne subjekte. S temi predpisi se uvajajo splošne obveznosti v zvezi z varnostjo dobavne verige ter podrobne in specifične zahteve, pomembne za zadevni sektor. Obenem POUDARJA, da dobavitelji ali ponudniki svoje proizvode in storitve pogosto dobavljajo različnim sektorjem, ne pa eni sami panogi. Zato je zelo pomembno zagotoviti, da so zahteve glede varnosti dobavne verige čim bolj usklajene v vseh zadevnih sektorjih, zlasti tistih, ki jih zajema prihodnja revidirana direktiva o varnosti omrežij in informacij, da bi se izognili razlikam med obveznostmi, naloženimi dobaviteljem ali ponudnikom, pa tudi zmanjšali breme za operaterje v kritičnih sektorjih, ki ob upoštevanju sektorskih posebnosti ocenjujejo izpolnjevanje navedenih obveznosti s strani dobaviteljev ali ponudnikov;

16. POZDRAVLJA predlog akta o kibernetski odpornosti kot pomemben zakonodajni instrument za spodbujanje varnega razvoja proizvodov z digitalnimi elementi in za zagotavljanje, da se kibernetska varnost upošteva v celotnem življenjskem ciklu proizvodov z digitalnimi elementi. UGOTAVLJA, da bi lahko predlog akta o kibernetski odpornosti znatno prispeval h krepitvi varnosti dobavne verige IKT. SPODBUJA konstruktivna pogajanja in pravočasno sprejetje akta;

17. v zvezi s tem SE SEZNANJA z delom, ki ga agencija ENISA trenutno opravlja v sodelovanju z državami članicami in drugimi deležniki, da bi EU zagotovila certifikacijske sheme za proizvode, storitve in postopke IKT v skladu z aktom o kibernetski varnosti, ki bi morale prispevati k dvigu splošne ravni kibernetske varnosti na enotnem digitalnem trgu. SPODBUJA vse deležnike, naj sodelujejo pri pripravljalnem delu za posamezne evropske certifikacijske sheme, da bi vzpostavili zaupanje v varne proizvode, postopke in storitve IKT ter okrepili njihovo odpornost, Komisijo pa POZIVA, naj po zaključku pripravljalnega dela hitro pripravi izvedbene akte o evropskih certifikacijskih shemah, zlasti evropsko certifikacijsko shemo za kibernetsko varnost, ki temelji na skupnih merilih. UGOTAVLJA, da bi morale evropske certifikacijske sheme po potrebi vključevati zahteve glede varnosti dobavne verige, tudi kar zadeva odnose z dobavitelji in ponudniki;

18. IZPOSTAVLJA, da bo treba temeljito izvajati vse prihodnje določbe revidirane direktive o varnosti omrežij in informacij, povezane z varnostjo dobavne verige IKT. V zvezi s tem POUDARJA pomen usklajenih ocen tveganja v EU za kritične dobavne verige (usklajene ocene tveganja za dobavne verige), nacionalnih politik o varnosti dobavne verige in varnostnih ukrepov, povezanih z dobavno verigo. UGOTAVLJA, da je treba pozornost nameniti ne le primarnim dobaviteljem ali ponudnikom, temveč tudi ustreznim podizvajalcem, kar zadeva tveganja za varnost primarnega dobavitelja ali ponudnika ali končne stranke. Da bi olajšali izvajanje ukrepov za obvladovanje tveganj v dobavni verigi, SPODBUJA agencijo ENISA, naj s pomočjo Skupine za sodelovanje na področju varnosti omrežij in informacij izvede pregled najboljših praks, ki so na voljo za obvladovanje tveganj v dobavni verigi, ter jih združi v metodološke smernice. Poleg tega SPODBUJA agencijo ENISA, naj spremlja naložbe subjektov, ki jih ureja prihodnja revidirana direktiva o varnosti omrežij in informacij, v varnost dobavne verige IKT;

19. IZPOSTAVLJA tudi koristi in tveganja uporabe ponudnikov upravljanih storitev in ponudnikov upravljanih varnostnih storitev v okviru varnosti dobavne verige. Čeprav lahko uporaba teh ponudnikov znatno izboljša varnost v organizacijah in vodi k višjim ravnem kibernetske varnosti, pa lahko upravljanje sistemov in storitev IKT na daljavo skupaj s privilegiranim dostopom do okolja strank IKT, ki bi ga ponudniki upravljanih storitev in ponudniki upravljanih varnostnih storitev morebiti potrebovali, v primeru ponudnikov upravljanih storitev in ponudnikov upravljanih varnostnih storitev, katerih varnost je ogrožena, povzročita vplivne kaskadne učinke na veliko število strank. Zato je izjemno pomembno, da ponudniki upravljanih storitev in ponudniki upravljanih varnostnih storitev ohranjajo visoko raven svoje notranje varnosti in varnosti storitev, ki jih ponujajo, ter da imajo do svojih strank transparenten pristop glede varnosti storitev, ki jih zagotavljajo. V zvezi s tem POZDRAVLJA njihovo prihodnjo vključitev v področje uporabe prihodnje revidirane direktive o varnosti omrežij in informacij;

20. glede izvajanja mehanizma za usklajene ocene tveganja za dobavne verige v skladu s prihodnjo revidirano direktivo o varnosti omrežij in informacij UGOTAVLJA, da so v zvezi s tem pomembni netehnični dejavniki tveganja, kot je neupravičen vpliv tretje države na dobavitelje in ponudnike storitev, ter SE v zvezi s tem SEZNANJA z dejavniki, ki se lahko uporabijo za oceno profila tveganja, kot je navedeno v usklajeni oceni tveganja kibernetske varnosti omrežij 5G na ravni EU. POZIVA Komisijo, naj po posvetovanju s Skupino za sodelovanje na področju varnosti omrežij in informacij ter agencijo ENISA do drugega četrtletja leta 2023 ugotovi, katere specifične storitve, sistemi ali proizvodi IKT bi lahko bili predmet prednostnih usklajenih ocen tveganja za dobavne verige;

21. UGOTAVLJA, da odvisnosti od dobaviteljev proizvodov in ponudnikov storitev IKT z visokim tveganjem, ki se uporabljajo za delovanje kritičnih omrežij in sistemov, predstavljajo strateško grožnjo, ki jo je treba ublažiti z ustreznimi politikami na nacionalni ravni in ravni EU ter s sodelovanjem med državami članicami in s podobno mislečimi mednarodnimi partnerji. Da bi olajšali ublažitev tega strateškega tveganja in podprli usklajene ocene tveganja za dobavne verige, POZIVA Skupino za sodelovanje na področju varnosti omrežij in informacij, naj v sodelovanju s Komisijo in agencijo ENISA razvije nabor ukrepov za zmanjšanje tveganj v kritični dobavni verigi IKT (nabor orodij za dobavno verigo IKT). Nabor orodij za dobavno verigo IKT bi moral temeljiti na strateških scenarijih groženj, identificiranih za dobavne verige IKT, ter zagotavljati ukrepe za odzivanje na te scenarije na podlagi izkušenj iz zbirke orodij EU za varnost 5G in izkušenj, pridobljenih na nacionalni ravni. Na pregleden način bi moral dopolnjevati usklajene ocene tveganja za dobavne verige za specifične storitve, sisteme ali proizvode IKT v skladu s prihodnjo revidirano direktivo o varnosti omrežij in informacij, in sicer s ponujanjem splošnih ukrepov za zmanjšanje tveganj, ki jih je mogoče na nadgradljiv način prilagoditi posameznim storitvam, sistemom ali proizvodom IKT na podlagi tveganj, ugotovljenih v posameznih usklajenih ocenah tveganja za dobavne verige;

22. POUDARJA pomembno vlogo, ki jo imajo raziskovalne, inovacijske, naložbene in podjetniške dejavnosti na digitalnem področju in področju kibernetske varnosti, pa tudi financiranje takih dejavnosti, da bi preprečili morebitne neželene strateške odvisnosti v prihodnosti in okrepili splošno odpornost dobavnih verig IKT. V zvezi s tem POUDARJA vlogo in pomen tako strateških kot izvedbenih nalog Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost (ECCC) ter mreže nacionalnih koordinacijskih centrov pri prispevanju k čim večji učinkovitosti naložb za okrepitev vodilnega položaja Unije in njene odprte strateške avtonomije na področju kibernetske varnosti, za podporo tehnološkim zmogljivostim in znanjem Unije ter za povečanje svetovne konkurenčnosti Unije. V zvezi s tem POZIVA k hitri operacionalizaciji ECCC. POZIVA ECCC, naj v svoji strateški agendi upošteva vidike varnosti dobavne verige IKT, vključno na primer z varnim razvojem programske opreme, pri tem pa zagotovi doslednost in dopolnjevanje ter prepreči morebitno podvajanje prizadevanj. PODPIRA krepitev evropske konkurenčnosti na področju kibernetske varnosti s programi financiranja, kot sta program Obzorje Evropa za raziskave in inovacije ter program Digitalna Evropa za krepitev, gradnjo in pridobivanje bistvenih zmogljivosti za digitalno gospodarstvo, družbo in demokracijo EU;

PODPORNI MEHANIZMI

23. SE ZAVZEMA ZA povečanje spodbud za finančno podporo, povezanih z ukrepi za krepitev varnosti dobavne verige IKT. POZIVA ECCC, Komisijo in ustrezne deležnike, naj, tudi glede na prihodnje izvajanje revidirane direktive o varnosti omrežij in informacij, prednostno preučijo možnosti za vključitev vidikov varnosti dobavne verige IKT v prihodnje razpise v okviru delovnih programov za kibernetsko varnost v sklopu programa Digitalna Evropa in programa Obzorje Evropa ali katere koli druge ustrezne možnosti financiranja. Te možnosti financiranja bi morale biti med drugim namenjene omogočanju organizacijam, da podpirajo ohranjanje visoke ravni kibernetske varnosti v smislu javnega naročanja proizvodov in storitev IKT v celotni dobavni verigi, zlasti v zvezi z zamenjavo specifičnih kritičnih storitev, sistemov ali proizvodov IKT, ki so v skladu s prihodnjimi usklajenimi ocenami tveganja za dobavne verige označeni kot storitve, sistemi ali proizvodi z visokim tveganjem;

24. SE ZAVEDA, da globalizacija in specializacija storitev IKT ter vse večja odvisnost od proizvodov in storitev tretjih strani povzročajo potrebo po tesnem sodelovanju v EU in na mednarodni ravni pri izmenjavi znanja in strokovnega znanja med ustreznimi deležniki, ter jih SPODBUJA, naj zavzamejo trdno in usklajeno stališče, ki bo na celovit način zagotavljalo varnost dobavne verige IKT. PRIZNAVA tudi, da je treba nadalje preučiti ustrezne najsodobnejše pristope in tehnike, tako za ustrezno osnovno kibernetsko higieno kot za dolgoročne rešitve za vzpostavitev varnih in odpornih dobavnih verig IKT, ter najprimernejše načine za njihovo spodbujanje in morebitno vključitev v politike ali druge pobude. V zvezi s tem PRIZNAVA, da bi bilo treba posebno pozornost nameniti preučitvi koristi in slabosti sistematičnih rešitev, kot so načela ničelnega zaupanja, nomenklatura programske opreme in podobne dolgoročne rešitve. PRIPOROČA, naj se v ta namen uporabi Skupina za sodelovanje na področju varnosti omrežij in informacij;

25. OPOZARJA na koristi, ki jih imata spremljanje in učinkovita izmenjava informacij o kibernetskih incidentih in grožnjah za preprečevanje, odkrivanje in blažitev učinkov napadov na dobavne verige. POUDARJA, da je treba še naprej krepiti zaupanje med državami članicami za učinkovito izmenjavo takih informacij. V zvezi s tem OPOZARJA na predlog Komisije, da bi države članice podprli pri vzpostavljanju in krepitvi centrov za varnostne operacije, tako da bi se vzpostavila mreža centrov za varnostne operacije po vsej EU, kar bi omogočilo nadaljnje spremljanje in predvidevanje znakov napadov na omrežja. OPOZARJA na potrebo po dopolnjevanju in usklajevanju znotraj obstoječih mrež in mehanizmov, v zvezi s tem pa zlasti IZPOSTAVLJA vlogo mreže skupin za odzivanje na incidente na področju računalniške varnosti ter potrebo po nadaljnjem preučevanju potenciala te mreže za spodbujanje učinkovite, varne in zanesljive kulture izmenjave informacij. OPOZARJA na prizadevanja držav članic, da bi ob podpori EU ustanovile sektorske, nacionalne in regionalne skupine za odzivanje na incidente na področju računalniške varnosti ter nacionalne ali evropske centre za izmenjavo in analizo informacij, ki bi bili del učinkovite mreže partnerstev na področju kibernetske varnosti v Uniji;

26. zaradi medsebojno povezane in globalne narave groženj v dobavni verigi IKT IZPOSTAVLJA pomen pristopa k varnosti dobavne verige IKT in njene krepitve na globalni ravni. V zvezi s tem PRIPOROČA uporabo digitalnih partnerstev, kibernetskih dialogov in drugih ustreznih pobud EU, vključno, kjer je to ustrezno, s sporazumi o prosti trgovini, s katerimi bi spodbujali ocenjevanja dobaviteljev proizvodov IKT in ponudnikov storitev IKT, ki temeljijo na tveganju, uporabo zaupanja vrednih dobaviteljev ali ponudnikov ter uporabo varnega in inovativnega digitalnega ekosistema, ki temelji na odprtih, interoperabilnih in preglednih standardih. Poleg tega PONOVNO POTRJUJE vizijo partnerstev Global Gateway, pa tudi Sveta EU-ZDA za trgovino in tehnologijo in dejavnosti v okviru njegovih delovnih skupin, da bi spodbudili uporabo zaupanja vrednih dobaviteljev ali ponudnikov/dobaviteljev ali ponudnikov brez visokega tveganja ter razvili mehanizem financiranja, ki bi omogočil projekte, s katerimi bi infrastruktura in storitve IKT v tretjih državah postale varnejše, odpornejše in bolj zaupanja vredne na tehnološko nevtralen način, tudi tako, da se ne bi financirali nakupi od nezanesljivih dobaviteljev/dobaviteljev z visokim tveganjem;

27. PONOVNO POTRJUJE svojo zavezo, da bo prispeval k odprtemu, svobodnemu, globalnemu, stabilnemu in varnemu kibernetskemu prostoru in ga spodbujal ter da bo spoštoval norme, pravila in načela odgovornega ravnanja držav v kibernetskem prostoru, določene v okviru ZN. Zlasti v zvezi z varnostjo dobavne verige IKT OPOZARJA na normo, ki sta jo podprli skupina vladnih strokovnjakov pod okriljem ZN in odprta delovna skupina, s katero se države spodbujajo, naj sprejmejo razumne ukrepe za zagotovitev celovitosti dobavne verige, tudi z oblikovanjem objektivnih ukrepov sodelovanja, da bi končni uporabniki lahko zaupali v varnost proizvodov IKT, in si prizadevajo za preprečevanje širjenja zlonamernih orodij in tehnik IKT ter uporabe škodljivih skritih funkcij, ter SPODBUJA k njenemu širokemu izvajanju.