Svet
Evropske unije

Bruselj, 22. maj 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Prejemnik:	delegacije
Št. predh. dok.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Zadeva:	Sklepi Sveta o politiki EU za kibernetsko obrambo

V prilogi vam pošiljamo sklepe Sveta o politiki EU za kibernetsko obrambo, ki jih je Svet odobril na seji 22. maja 2023.

Sklepi Sveta o politiki EU za kibernetsko obrambo

1. Svet na podlagi okvira politike za kibernetsko obrambo iz leta 2014 in njegove posodobitve iz leta 2018 pozdravlja ambiciozno skupno sporočilo o politiki EU za kibernetsko obrambo za nadaljnje naložbe v naše sodobne in interoperabilne oborožene sile, najnovejše tehnologije in najsodobnejše zmogljivosti kibernetske obrambe ter krepitev partnerstev za reševanje skupnih izzivov. V času vse večje odvisnosti od digitalnih tehnologij je kibernetski prostor postal prostor strateške konkurence. Nujno je torej treba ohraniti odprt, svoboden, stabilen in varen kibernetski prostor. Uporaba kibernetskih operacij, ki omogočajo in spremljajo neizzvano in neupravičeno vojno agresijo Rusije proti Ukrajini, vpliva na svetovno stabilnost in varnost, predstavlja pomembno tveganje za zaostritev razmer in prispeva k že tako znatnemu povečanju zlonamernih kibernetskih dejavnosti zunaj konteksta oboroženih spopadov v zadnjih letih.

2. Vojna v Ukrajini je vzpostavila nove strateške razmere in potrdila, da morajo EU, njene države članice in njihovi partnerji dodatno okrepiti odpornost EU pri soočanju s kibernetskimi grožnjami ter povečati našo skupno kibernetsko varnost in kibernetsko obrambo pred zlonamernim ravnanjem in agresijo v kibernetskem prostoru. Skupno sporočilo o politiki EU za kibernetsko obrambo kaže našo odločenost, da zagotovimo takojšnje in dolgoročne ukrepe za zagotovitev svobodnega delovanja v kibernetskem prostoru in odzivov na akterje groženj, ki si med drugim prizadevajo posegati v omrežja in informacijske sisteme EU in njenih partnerjev, jih motiti ali uničiti. To skupno sporočilo dopolnjuje strategijo EU za kibernetsko varnost in je v skladu s strateškim kompasom pomemben korak k vseobsegajočemu pristopu EU k odpornosti, odzivanju, preprečevanju konfliktov, sodelovanju in stabilnosti v kibernetskem prostoru. Svet v zvezi s tem poudarja potrebo po ustreznih in usklajenih odzivih EU, njenih držav članic in njihovih partnerjev ter pričakuje tudi revizijo izvedbenih smernic iz zbirke orodij EU za kibernetsko diplomacijo, kar je še en ključen korak k oblikovanju stališča EU glede kibernetske varnosti.

3. Svet poudarja, da nedavni kibernetski napadi na evropsko kritično infrastrukturo, hitro razvijajoče se okolje kibernetskih groženj in hiter tehnološki razvoj kažejo tudi potrebo po okrepljenem civilno-vojaškem usklajevanju in sodelovanju, hkrati pa poudarja, da med civilnimi in vojaškimi skupnostmi ni hierarhije.
   Politika EU za kibernetsko obrambo omogoča EU in njenim državam članicam, da okrepijo svoje zmogljivosti za zaščito, odkrivanje, obrambo in odvračanje, pri čemer ustrezno uporabijo celo vrsto obrambnih možnosti, ki so na voljo civilnim in vojaškim skupnostim za širšo varnost in obrambo EU, v skladu z mednarodnim pravom, vključno s pravom o človekovih pravicah in mednarodnim humanitarnim pravom.

4. Čeprav je nacionalna varnost, tudi na kibernetskem področju, še vedno v izključni pristojnosti vsake države članice, kot je navedeno v členu 4(2) PEU, Svet medtem poudarja, da je treba posamično in skupaj znatno vlagati v večjo odpornost in uporabo obrambnih zmogljivosti kibernetske obrambe v celotnem spektru ter spodbujati okvire EU za sodelovanje in finančne spodbude. Svet poudarja, da je treba dodatno okrepiti ukrepe držav članic ter institucij, organov, uradov in agencij EU, da bi zaščitili Unijo, naše državljane, institucije, organe, urade in agencije EU ter misije in operacije v okviru SVOP v kibernetskem prostoru. Poleg tega poudarja pomen krepitve odpornosti EU v kibernetskem prostoru z razvojem zmogljivosti kibernetske obrambe in krepitvijo sodelovanja z zaupanja vrednim zasebnim ekosistemom.

I. **Skupno ukrepanje za močnejšo kibernetsko obrambo**

5. Svet ponovno poudarja, da je postopen, pregleden in vključujoč proces bistvenega pomena za krepitev zaupanja, ki je ključnega pomena za nadaljnji razvoj okvira EU za krizno upravljanje na področju kibernetske varnosti, ki ga je treba izvesti v skladu z načrtom za obvladovanje kibernetskih kriz, ki ga je pripravil Svet. Svet ponovno poudarja, da je treba z uporabo vseh ustreznih sredstev še naprej krepiti naše zmogljivosti za zaščito in obrambo pred kibernetskimi napadi, njihovo odkrivanje ter odvračanje od njih z izboljšanim situacijskim zavedanjem, krepitvijo in razvojem zmogljivosti, usposabljanjem, vajami, okrepljeno odpornostjo ter odločnim odzivanjem na kibernetske napade zoper EU, njene države članice in institucije, organe, urade in agencije EU, misije in operacije v okviru SVOP. Pri tem poziva visokega predstavnika in Komisijo, naj zmanjšata zapletenost na kibernetskem področju, se izogneta nepotrebnemu podvajanju ter zagotovita sodelovanje in sinergije z obstoječimi pobudami. Okrepiti je treba sodelovanje in usklajevanje med akterji kibernetske obrambe v EU in državah članicah ter med njimi, med vojaškimi in civilnimi kibernetskimi skupnostmi ter med javnim in zaupanja vrednim zasebnim ekosistemom. Države članice se v tem smislu spodbuja, naj nadalje preučijo in okrepijo civilno-vojaške nacionalne mehanizme usklajevanja, olajšajo skupno prostovoljno izmenjavo informacij, izmenjujejo pridobljene izkušnje, prispevajo k razvoju interoperabilnih standardov ter izvajajo ocene tveganja in oblikovanje scenarijev tveganja, pa tudi skupne vaje, zlasti na evropski ravni, ob polnem spoštovanju določb direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS2).

6. Svet ob priznavanju prizadevanj za nadaljnjo krepitev odpornosti Unije na podlagi direktive NIS2 in direktive o odpornosti kritičnih subjektov ponovno poudarja svoje priporočilo o usklajenem pristopu na ravni EU za krepitev odpornosti kritične infrastrukture[1]. Poziva k ukrepom za nadaljnjo krepitev odpornosti kritičnih subjektov, infrastrukture, digitalnih proizvodov in storitev, hkrati pa ugotavlja, da je pravilno izvajanje direktive NIS2 še vedno najpomembnejši korak. Čeprav gre pretežno za civilno odgovornost, to prispeva tudi k močnejši kibernetski obrambi. V zvezi s tem se institucije, organe, urade in agencije EU ter države članice spodbuja, naj podprejo nadaljnji razvoj in uporabo novih in obstoječih usklajevalnih mehanizmov EU, ocen tveganja, vrednotenj in scenarijev, skupne prostovoljne izmenjave informacij in vaj na način, ki prinaša dodano vrednost in preprečuje nepotrebno podvajanje z obstoječimi pobudami.

7. Da bi dodatno okrepili zaupanje, utrdili sodelovanje in olajšali pravočasno izmenjavo informacij o pomembnih kibernetskih incidentih in kibernetskih incidentih velikih razsežnosti, ki vplivajo na obrambne sisteme, Svet pozdravlja pobudo za nadaljnji razvoj konference poveljnikov kibernetske varnosti EU, ki jo bo organiziralo vsako predsedstvo Sveta EU ob podpori Evropske obrambne agencije (EDA) in sodelovanju Evropske službe za zunanje delovanje (ESZD). Svet spodbuja vse države članice, naj se udeležijo teh srečanj. Svet poziva organizacijsko mrežo za povezovanje v kibernetski krizi (EU-CyCLONe) in konferenco kibernetskih poveljnikov EU, da za okrepitev odpornosti EU na kibernetske incidente velikih razsežnosti opredelita možne načine sodelovanja in izkoristita skupno vojaško in civilno perspektivo.

[1] Predlog priporočila Sveta o usklajenem pristopu Unije za krepitev odpornosti kritične infrastrukture, COM(2022) 551.

8. Svet pozdravlja vzpostavitev mreže vojaških skupin EU za odzivanje na izredne računalniške razmere (MICNET) in pričakuje, da bo dosegla začetno operativno zmogljivost do sredine leta 2024, da bi spodbudili odločnejši in bolj usklajen odziv na ravni EU in da bi se izboljšala izmenjava tehničnih informacij o kibernetskih incidentih, ki vplivajo na obrambne sisteme, med sodelujočimi državami članicami. Svet spodbuja vse države članice, naj sodelujejo v MICNET, da se zagotovi njena učinkovitost. Poleg tega Svet poziva države članice, naj se oprejo na izkušnje, pridobljene v okviru mreže skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT), in odločno spodbuja vzpostavitev učinkovitega mehanizma za sodelovanje in usklajevanje med obema mrežama ob ustreznem času, ob polnem spoštovanju mehanizmov upravljanja in uporabnikov vsakega subjekta.

9. Glede na povečanje števila zlonamernih kibernetskih dejavnosti državnih in nedržavnih akterjev v misijah in operacijah v okviru SVOP Svet poziva EU in njene države članice, naj okrepijo svoje zmogljivosti za obrambo in varovanje misij in operacij v okviru SVOP. V zvezi s tem pozdravlja cilje, da se doseže nadaljnji napredek pri zaščiti vojaških mrež in struktur EU, med drugim v skladu z vojaško vizijo in strategijo EU za kibernetski prostor kot področje operacij[2].

[2] EEAS(2021) 706 REV4

10. Svet ponovno poudarja sklepe Sveta iz maja 2022[3] in potrebo po vlaganju v našo medsebojno pomoč na podlagi člena 42(7) PEU ter solidarnostno klavzulo iz člena 222 PDEU. Svet poudarja pomen nadaljnjega poglabljanja skupnega razumevanja EU in držav članic glede izvajanja člena 42(7), vključno z zapletenimi scenariji, ki vključujejo kibernetski napad, v skladu z ustreznimi načeli mednarodnega prava. Pozdravlja možnost podpore EU ob kibernetskem napadu na izrecno zahtevo zadevne države članice ali zadevnih držav članic, brez poseganja v posebni značaj varnostne in obrambne politike katere koli od držav članic.

11. Svet poudarja napredek, dosežen pri projektu PESCO – enote za hitro odzivanje na kibernetske grožnje in medsebojna pomoč na področju kibernetske varnosti (CRRT), ter njegovo pripravljenost, da na zahtevo deluje kot zmogljivost za potrebe držav članic in EU, podpira misije in operacije v okviru SVOP ter zagotavlja pomoč partnericam EU. Svet pozdravlja nadaljnji razvoj zmogljivosti PESCO CRRT, nacionalnih skupin za odzivanje na kibernetske grožnje in po potrebi dodatnih zmogljivosti za odzivanje na incidente, kot so prihodnje skupine za hitro odzivanje na hibridne grožnje, kot so predvidene v strateškem kompasu, tudi s spodbujanjem njihovega usklajevanja in sodelovanja na ravni EU.

[3] Sklepi Sveta o vzpostavitvi stališča Evropske unije glede kibernetskih vprašanj, 23. maj 2022, 9364/22.

12. Svet pozdravlja delo centra za usklajevanje na kibernetskem in informacijskem področju (CIDCC), tj. projekta PESCO, katerega cilj je zagotoviti vojaške zmogljivosti za zbiranje in analizo informacij, relevantnih za oblikovanje skupnega razumevanja za delovanje na kibernetskem področju. Poleg tega pozdravlja predlog, da se potrditev koncepta – če se to izkaže za uspešno kot center za usklajevanje informacij – od leta 2025 dalje vključi v center EU za koordinacijo kibernetske obrambe (EUCDCC), s čimer bi izboljšali usklajevanje in situacijsko zavedanje, zlasti poveljnikov misij in operacij EU v okviru SVOP, ter okrepili širšo strukturo poveljevanja in nadzora EU. Svet poziva visokega predstavnika, naj predstavi koncept in časovni načrt za ustanovitev EUCDCC, pri čemer naj upošteva izkušnje podobnih mednarodnih subjektov, opredeli potrebne vire, se izogiba nepotrebnemu podvajanju in si prizadeva za dopolnjevanje s širšim okvirom EU za kibernetsko varnost.

13. Svet poudarja pomen strateškega obveščevalnega sodelovanja v zvezi s kibernetskimi grožnjami in dejavnostmi ter poziva države članice, naj prek svojih pristojnih organov še naprej prispevajo k delu EU INTCEN, obveščevalnega direktorata VŠEU in držav članic v okviru Enotne zmogljivosti za analizo obveščevalnih podatkov (SIAC). Poleg tega poudarja, kako pomembno je okrepiti naše zmogljivosti na področju kibernetske obveščevalne dejavnosti, da bi okrepili našo kibernetsko odpornost in odzivanje ter zagotovili učinkovito podporo našim civilnim in vojaškim misijam in operacijam v okviru SVOP, pa tudi našim oboroženim silam in zmogljivostim SIAC na kibernetskem področju, in sicer na podlagi prostovoljnih prispevkov držav članic v zvezi z obveščevalno dejavnostjo in brez poseganja v njihove pristojnosti.

14. Svet je seznanjen s centrom Evropske komisije za kibernetske razmere in analizo, katerega cilj je izboljšati situacijsko zavedanje v Komisiji. Svet poudarja pomen vzpostavitve obojestransko koristnega sodelovanja med tem centrom ter drugimi institucijami, organi, uradi in agencijami EU, zlasti ENISA in CERT-EU. Izpostavlja pomen zagotavljanja tesnega sodelovanja z mrežami EU za sodelovanje pri razvoju situacijskega zavedanja, pa tudi spoštovanja zaupnosti. Ugotavlja, da je treba okrepiti skupno situacijsko zavedanje na ravni EU in nadalje razvijati okvir EU za krizno upravljanje na področju kibernetske varnosti in pri tem preprečiti nepotrebno podvajanje dela.

15. Svet opozarja, da so izobraževanje, usposabljanje in vaje na kibernetskem področju bistveni za zagotavljanje pripravljenosti in učinkovitosti, ter pozdravlja nacionalne dejavnosti in dejavnosti, ki jih zagotavlja EU v okviru Evropske akademije za varnost in obrambo (EAVO), EDA, ENISA in tekočih projektov PESCO, kot sta Zveza virtualnih poligonov za kibernetsko varnost ter akademsko in inovacijsko vozlišče EU za kibernetsko varnost (CAIH). Da bi ta prizadevanja še okrepili, Svet z zanimanjem pričakuje vzpostavitev okvirnega projekta EDA CyDef-X za usklajevanje in podporo vajam na področju kibernetske obrambe. Svet spodbuja EDA, naj v tesnem sodelovanju z državami članicami in ESZD preuči, kako bi lahko s projektom CyDef-X dodatno podprli vaje, kot je CYBER PHALANX, vključno z medsebojno pomočjo na podlagi člena 42(7) PEU in solidarnostno klavzulo iz člena 222 PDEU, pa tudi s Komisijo in agencijo ENISA v zvezi s civilnimi vajami. Svet se poleg tega zavzema za to, da se v okviru projekta CyDef-X uporabijo in nadalje razvijajo obstoječa okolja za testiranje in vaje na področju kibernetske obrambe, kot je Zveza virtualnih poligonov za kibernetsko varnost. Da bi zagotovili prožen in učinkovit postopek odločanja v primeru kibernetske krize, Svet poudarja, da je pomembno organizirati redne simulacijske vaje na ravni odločanja držav članic.

16. Svet je seznanjen s predlogom akta o kibernetski solidarnosti in namero, da se okrepijo zmogljivosti za odkrivanje kibernetskih groženj in incidentov v EU ter odzivanje nanje. Poudarja, da so lahko predlogi na tem področju učinkoviti le, če so usklajeni z okviri in potrebami držav članic glede kriznega upravljanja. Poudarja, da je treba preveriti, ali ima kritična infrastruktura morebitne ranljivosti, če je ocenjena kot koristna, in sicer v okviru nacionalne pristojnosti, pri čemer se upoštevajo razpoložljive ocene tveganja na ravni EU.

17. Svet je seznanjen s predlogom Komisije za vzpostavitev mehanizma za kibernetske izredne razmere, s katerim bi se lahko podpirala razpoložljivost storitev kibernetske varnosti, ki jih nudijo zaupanja vredni zasebni ponudniki, da bi na zahtevo pomagali državam članicam v primeru kibernetskih incidentov velikih razsežnosti, hkrati pa poudarja, da je treba okrepiti evropsko industrijo kibernetske varnosti, in sicer s podporo ECCC kot ključnega stebra za delovanje tega mehanizma. Svet izpostavlja ključno vlogo vsake države članice pri spremljanju in ocenjevanju nacionalnih potreb.

II. **Zaščita obrambnega ekosistema EU**

18. Svet ponovno poziva države članice, naj še naprej razvijajo lastne zmogljivosti za izvajanje operacij kibernetske obrambe, po potrebi tudi s proaktivnimi obrambnimi ukrepi za zaščito in obrambo pred kibernetskimi napadi, njihovo odkrivanje ter odvračanje od njih. Glede na to, da se direktiva NIS2 ne uporablja za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju obrambe, Svet poziva EDA, naj ob ustrezni podpori Komisije in ESZD državam članicam pomaga pri oblikovanju pravno nezavezujočih prostovoljnih priporočil na podlagi direktive NIS2 za povečanje kibernetske varnosti v obrambni skupnosti, ter poziva vse države članice, naj dejavno sodelujejo pri teh prizadevanjih. Ta priporočila bi morala upoštevati podobna prizadevanja v drugih okvirih.

19. Kot je priznano v strateškem kompasu, je sposobnost EU za ukrepanje odvisna od njene sposobnosti, da zmanjša strateške odvisnosti v okviru svojih zmogljivostih kibernetske obrambe in dobavnih verigah, ter od razvoja in obvladovanja najnovejših tehnologij na področju kibernetske obrambe. To vključuje krepitev tehnološke in industrijske baze evropske obrambe (EDTIB) po vsej EU ter njeno zmožnost sodelovanja na vzajemni osnovi s podobno mislečimi partnerji po svetu, da se zagotovijo vzajemne koristi. Svet zato poziva k tesnemu sodelovanju med sektorjema kibernetske varnosti in kibernetske obrambe, da bi ustvarili sinergije ter tako razvili in zagotovili zmogljivosti kibernetske obrambe v celotnem spektru. Svet poziva Komisijo, naj po potrebi v tesnem sodelovanju z ECCC še naprej podpira razvoj močne, prožne, globalno konkurenčne in inovativne industrijske in tehnološke baze evropske kibernetske obrambe, vključno z malimi in srednjimi podjetji (MSP), in sicer z nadaljnjimi naložbami in ukrepi politike.

20. Glede na pomen interoperabilnosti in skupnega razvoja zmogljivosti kibernetske obrambe, tudi v zvezi s skupnim razvojem zmogljivosti za kibernetsko obrambo naslednje generacije, Svet poziva EDA in Vojaški štab EU, naj oblikujeta sklop zahtev EU glede interoperabilnosti na področju kibernetske obrambe, ki bi temeljile na obstoječih načelih, postopkih in standardih, določenih zlasti v okviru Organizacije Severnoatlantske pogodbe (NATO), in bi bile združljive z njimi. Poleg tega Svet poziva države članice, naj v okviru evropskega odbora za standardizacijo na področju obrambe v tesnem sodelovanju z vsemi ustreznimi deležniki, po potrebi tudi z evropskimi organizacijami za standardizacijo in Natom, preučijo, ali bi bili potrebni posebni prostovoljni standardi za obrambne sisteme.

21. Svet pozdravlja prizadevanja Komisije, da predstavi načrt za spodbujanje uporabe obstoječih standardov za uporabo na področju civilne kibernetske varnosti in kibernetske obrambe ter razvoj novih prostovoljnih standardov. Poudarja, da je treba po potrebi uskladiti standarde kibernetske varnosti in kibernetske obrambe. Priznava, da bi lahko bili takšni prostovoljni standardi koristni za sektorja kibernetske varnosti in kibernetske obrambe v EU, ter poziva k tesnejšemu sodelovanju med civilnimi in obrambnimi organi za standardizacijo.

22. Svet poziva k hitremu oblikovanju priporočil na podlagi pregleda obstoječih orodij za varno komunikacijo na kibernetskem področju, ki ga pripravijo Komisija in ustrezne institucije. Kadar je mogoče, bi morala biti priporočila usklajena z obstoječimi pobudami za izmenjavo informacij, upoštevati pa bi morala tudi tveganja, ki jih za sedanje metode šifriranja predstavljajo nastajajoče in prelomne tehnologije.

23. Svet poleg tega pozdravlja začetno delo, ki so ga na zahtevo Sveta opravili Komisija, visoki predstavnik in Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, v zvezi z oceno tveganja in scenariji, ki so se prvotno nanašali na energetski in telekomunikacijski sektor. Svet ugotavlja, da se pripravljajo tudi ciljno usmerjene ocene tveganj glede kibernetske varnosti za komunikacijsko infrastrukturo in omrežja v EU. Ponovno poudarja, da je izjemno pomembno skupno razumevanje možnih vplivov kibernetskih incidentov med državami članicami, pa tudi med institucijami, organi in agencijami EU. Svet zato navedene akterje poziva, naj zagotovijo, da se ocene tveganja, scenariji in naknadna priporočila upoštevajo pri opredeljevanju in prednostnem razvrščanju ukrepov in podpore na ravni EU in po potrebi na nacionalni ravni. Poleg tega poziva, naj vsi zadevni akterji v postopkih ocenjevanja tveganja in pri razvoju kibernetskih vaj upoštevajo scenarije tveganja.

III. **Naložbe v zmogljivosti kibernetske obrambe**

24. Svet spodbuja države članice, naj povečajo svoje naložbe za izgradnjo, vzdrževanje in nadaljnji razvoj interoperabilnih zmogljivosti kibernetske obrambe. Svet podpira oblikovanje sklopa prostovoljnih zavez za nadaljnji razvoj nacionalnih zmogljivosti kibernetske obrambe, pri čemer upošteva dejstvo, da podobna prizadevanja potekajo tudi v drugih okvirih.

25. Svet poziva države članice in EDA, naj izkoristijo priložnost za revizijo načrta za razvoj zmogljivosti in določijo visoko raven ambicij pri razvoju skupne kibernetske obrambe na ravni EU. Svet nadalje spodbuja države članice, naj gradijo na posodobljenem sklopu prednostnih nalog in svojih zavezah v okviru PESCO, da bi povečale svojo raven sodelovanja pri skupnih projektih EU za razvoj zmogljivosti kibernetske obrambe, pri tem pa priznava neposredne koristi skupnih projektov na ravni EU za podporo razvoju nacionalnih zmogljivosti za kibernetsko obrambo.

26. Svet pozdravlja skupna raziskovalna prizadevanja na ravni EU za preučitev možnih uporab nastajajočih in prelomnih tehnologij v obrambnih sistemih, pri čemer poudarja, da je treba te tehnološke dosežke tudi hitro vključiti v obstoječe in prihodnje zmogljivosti. Svet spodbuja države članice in industrijo EU, naj kar najbolje izkoristijo priložnosti za skupne raziskave na ravni EU, na primer v okviru EDA, tekočih projektov PESCO, kot je akademsko in inovacijsko vozlišče EU za kibernetsko varnost (EU CAIH), Evropskega obrambnega sklada ter po potrebi programa Obzorje Evropa in programa Digitalna Evropa za projekte z dvojno rabo. Poleg tega Svet pozdravlja uporabo namenskih okvirov za podporo obrambnim inovacijam z uporabo vnosov s civilnega področja, predvsem obrambnoinovacijske sheme EU in vozlišča za inovacije na področju evropske obrambe. Poleg tega Svet spodbuja Evropski kompetenčni center za kibernetsko varnost (ECCC) in EDA, naj pripravita delovni dogovor za lažjo izmenjavo informacij med osebjem zadevnih organov o prednostnih nalogah na področju civilne tehnologije, tehnologije z dvojno rabo in obrambne tehnologije, da bi se ustvarile sinergije in preprečilo podvajanje.

27. Svet pozdravlja namero Komisije, da v sodelovanju z EDA in ECCC v skladu z njunima mandatoma pripravi tehnološki kažipot za kritične kibernetske tehnologije, skupaj z državami članicami in ob posvetovanju z ustreznimi deležniki, kot je industrija, ki z opredelitvijo kritičnih kibernetskih tehnologij, trasiranjem tehnološkega razvoja in strateških odvisnosti zagotavlja načine za zmanjšanje teh odvisnosti v podporo strateški avtonomiji in tehnološki suverenosti EU, hkrati pa ohranja odprto gospodarstvo. Svet ugotavlja, da bi lahko tehnološki kažipot za kritične kibernetske tehnologije prispeval k strateškim prednostnim nalogam za instrumente financiranja EU, hkrati pa bi bil v skladu z ustreznimi načini, ki veljajo zanje. Svet opozarja, da bi si morala EU prizadevati za ambiciozno in odločno evropsko industrijsko politiko, da bi ustvarila trajnostno, privlačno in konkurenčno poslovno okolje, ki bi lahko omogočilo tudi razvoj evropskih subjektov na kibernetskem področju.

28. Svet ceni namero, da se odpravi velika vrzel v spretnostih na področju kibernetske varnosti s privabljanjem novih strokovnjakov in tudi strokovnjakinj, izpopolnjevanjem in preusposabljanjem ter vlaganjem v usposabljanja in vaje za oblikovanje raznolike in vključujoče kibernetske delovne sile ter njihovo organizacijo. Svet se zaveda izzivov, s katerimi se EU sooča v zvezi s človeškim kapitalom na področju kibernetske varnosti in kibernetske obrambe, zato pozdravlja pobudo „akademija za veščine kibernetske varnosti“, ki bi lahko pomagala zaposlenim na področju kibernetske obrambe.

29. Svet poziva države članice, naj si izmenjujejo informacije o najboljših praksah za razvoj usposobljenih strokovnjakov za kibernetsko varnost, pri čemer naj izkoristijo sinergije med vojaškimi in civilnimi pobudami ter pobudami na področju kazenskega pregona, ter poziva EAVO, naj s podporo in strokovnim znanjem EDA in ENISA preuči možnosti za izboljšanje izmenjave najboljših praks in nadaljnje sinergije med vojaškim in civilnim področjem v zvezi z usposabljanjem in razvojem spretnosti na področju kibernetske obrambe.

30. Svet poudarja pomen skupnega razumevanja sestave delovne sile na področju kibernetske varnosti ter s tem povezanih znanj in spretnosti, da bi opredelili in odpravili vrzeli na trgu dela na področju kibernetske varnosti, ter dejstvo, da je treba vključiti vse deležnike, vključno z državami članicami in industrijo. Svet priznava, da bi določitev kazalnikov za spremljanje trga dela na področju kibernetske varnosti pripomogla k ustrezni opredelitvi potreb po spretnostih na področju kibernetske varnosti ter neposrednem financiranju, hkrati pa bi prispevala k izpolnjevanju obveznosti, povezanih s politiko, posebej tistih, ki izhajajo iz direktive NIS2. Svet pozdravlja predlog okvira za certificiranje spretnosti na področju kibernetske obrambe ter poziva visokega predstavnika kot vodjo EAVO, naj si v sodelovanju z ESZD, Komisijo in državami članicami ter spodbujanjem civilnih pobud prizadeva za napredek na tem področju.

IV. **Partnerstva pri reševanju skupnih izzivov**

31. Svet poziva visokega predstavnika in Komisijo, naj okrepita in nadgradita sodelovanje ter preučita vzajemno koristna in ustrezno prilagojena partnerstva na področju politik kibernetske obrambe, vključno s krepitvijo zmogljivosti kibernetske obrambe prek Evropskega mirovnega instrumenta. V ta namen bi bilo treba kibernetsko obrambo kot točko v dialogih in posvetovanjih EU o kibernetski varnosti dodati k splošnim varnostnim in obrambnim posvetovanjem s partnerji. Poleg tega bi bilo treba okrepiti dialoge in sodelovanje z zasebnim sektorjem. Svet poudarja, da bi mednarodno sodelovanje v zvezi s standardi in certificiranjem kibernetske varnosti pomenilo dodano vrednost za evropsko industrijo. Zato pozdravlja zavezo Komisije, da bo to postalo pomemben del dialogov EU s tretjimi državami in mednarodnimi organizacijami o kibernetski varnosti.

32. Svet poudarja pomen mednarodnega sodelovanja za preprečevanje ali zmanjšanje nevarnosti konfliktov v kibernetskem prostoru, še posebej z nadaljnjim razvojem in operacionalizacijo ukrepov za krepitev zaupanja na regionalni in mednarodni ravni, vključno z ZN, ter z nadaljnjim spodbujanjem uporabe obstoječih kibernetskih ukrepov za krepitev zaupanja, kot v okviru Organizacije za varnost in sodelovanje v Evropi (OVSE), tudi v času mednarodnih napetosti.

    EU in njene države članice poudarjajo, da se v kibernetskem prostoru uporablja veljavno mednarodno pravo, in poudarjajo, da je treba še naprej ohranjati in spodbujati okvir ZN za odgovorno ravnanje držav ter si prizadevati za njegovo izvajanje, tudi z vzpostavitvijo akcijskega programa za spodbujanje odgovornega ravnanja držav v kibernetskem prostoru.

33. Svet v skladu s skupnimi izjavami o sodelovanju med EU in Natom poziva visokega predstavnika, tudi v njegovi vlogi vodje EDA, ter Komisijo, naj dodatno okrepita, poglobita in razširita partnerstvo z Natom na kibernetskem področju ob vsestranskem spoštovanju načel vključenosti, vzajemnosti, obojestranske odprtosti in preglednosti ter avtonomije odločanja obeh organizacij. Svet ob upoštevanju dejstva, da je treba zagotavljati komplementarnost in usklajenost prizadevanj z največjo možno vključenostjo držav članic, ki niso članice Nata, in preprečiti nepotrebna podvajanja, poziva k vzpostavitvi povezav med EU in Natom na ustreznih ravneh na področju usposabljanja, izobraževanja, situacijskega zavedanja, vaj ter raziskovalnih in razvojnih platform, ter k iskanju morebitnih sinergij med zadevnimi prostovoljnimi zavezami za razvoj nacionalnih zmogljivosti za kibernetsko obrambo in okviri za krizno upravljanje, zaščito kritične infrastrukture, izboljšanjem izmenjave situacijskega zavedanja, usklajenimi odzivi na zlonamerne kibernetske dejavnosti in prizadevanji za krepitev zmogljivosti v tretjih državah. To vključuje tehnični dogovor med službo Nata za odzivanje na računalniške incidente (NCIRC) in skupino EU za odzivanje na računalniške grožnje (CERT-EU) ter okrepljen politični dialog o vprašanjih kibernetske obrambe na vseh ravneh.

V. **Zaključek**

34. Svet na podlagi sklepov Sveta o politiki EU za kibernetsko obrambo poziva visokega predstavnika in Komisijo, naj do drugega četrtletja leta 2023 pripravita izvedbeni načrt, da bi ga države članice odobrile. Svet tudi poziva države članice, naj prostovoljno izrazijo svoje ambicije in ukrepe v zvezi s kibernetsko obrambo v okviru politike EU za kibernetsko obrambo ter v celoti izkoristijo pravno nezavezujoča prostovoljna priporočila in zaveze za okrepitev nacionalnih in večnacionalnih prizadevanj na področju kibernetske obrambe, da bi čim bolj povečale učinek na ravni EU. Visoki predstavnik, Komisija in države članice naj od drugega četrtletja leta 2024 vsako leto poročajo in razpravljajo o napredku pri izvajanju elementov skupnega sporočila in njegovega izvedbenega načrta.