Vijeće
Europske unije

Bruxelles, 22. svibnja 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**

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Za:	Delegacije
Br. preth. 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
Predmet:	Zaključci Vijeća o politici EU-a u području kiberobrane

Za delegacije se u Prilogu nalaze zaključci Vijeća o politici EU-a u području kiberobrane koje je Vijeće odobrilo na sastanku održanom 22. svibnja 2023.

Zaključci Vijeća o politici EU-a u području kiberobrane

1. Nadovezujući se na okvir za politiku kiberobrane iz 2014. i njegovo ažuriranje 2018., Vijeće pozdravlja ambicioznu Zajedničku komunikaciju o politici kiberobrane EU-a, čiji je cilj daljnje ulaganje u naše moderne i interoperabilne oružane snage, najnaprednije tehnologije, najsuvremenije kapacitete za kiberobranu i jačanju partnerstava za rješavanje zajedničkih izazova. Kiberprostor je postao područje strateškog nadmetanja u vrijeme sve veće ovisnosti o digitalnim tehnologijama. Stoga je ključno održavati ga otvorenim, slobodnim, stabilnim i sigurnim. Upotreba kiberoperacija, koje su omogućile i pratile ničim izazvani i neopravdani agresivni rat Rusije protiv Ukrajine, utječe na globalnu stabilnost i sigurnost, predstavlja velik rizik od eskalacije i doprinosi već znatnom povećanju zlonamjernih kiberaktivnosti izvan konteksta oružanih sukoba posljednjih godina.

2. Rat u Ukrajini pružio je novi strateški kontekst i potvrdio potrebu da EU, njegove države članice i njihovi partneri dodatno ojačaju otpornost EU-a pri suočavanju s kiberprijetnjama i poboljšaju našu zajedničku kibersigurnost i kiberobranu od zlonamjernog ponašanja i činova agresije u kiberprostoru. U Zajedničkoj komunikaciji o politici kiberobrane EU-a ističe se naša odlučnost da poduzmemo hitne i dugoročne mjere za osiguravanje slobode djelovanja u kiberprostoru i reagiramo u pogledu aktera koji predstavljaju prijetnju i koji, među ostalim, nastoje neovlašteno upadati u mrežne i informacijske sustave EU-a i njegovih partnera te ih ometati ili uništiti. Ova Zajednička komunikacija, kojom se dopunjuje Strategija EU-a za kibersigurnost i koja je usklađena sa Strateškim kompasom, važan je korak prema sveobuhvatnom pristupu EU-a otpornosti, odgovoru, sprečavanju sukoba, suradnji i stabilnosti u kiberprostoru. U tom kontekstu Vijeće ističe potrebu za odgovarajućim i dosljednim odgovorima EU-a, njegovih država članica i njihovih partnera te sa zanimanjem iščekuje reviziju smjernica za provedbu instrumentarija EU-a za kiberdiplomaciju kao još jedan ključan korak naprijed u razvoju položaja EU-a u pogledu kiberprostora.

3. Vijeće ističe da nedavni kibernapadi na europsku kritičnu infrastrukturu, kiberprijetnje koje se brzo razvijaju i brzi tehnološki razvoj također pokazuju da postoji potreba za pojačanom civilno-vojnom koordinacijom i suradnjom, istodobno naglašavajući da ne postoji hijerarhija između civilnih i vojnih zajednica.
   Politika EU-a u području kiberobrane omogućuje EU-u i njegovim državama članicama da ojačaju svoju sposobnost zaštite, otkrivanja, obrane i odvraćanja te da na odgovarajući način iskoriste puni raspon obrambenih mogućnosti dostupnih civilnim i vojnim zajednicama za širu sigurnost i obranu EU-a, u skladu s međunarodnim pravom, uključujući pravo o ljudskim pravima i međunarodno humanitarno pravo.

4. Iako je nacionalna sigurnost, među ostalim u području kibersigurnosti, i dalje isključiva odgovornost svake države članice, kako je navedeno u članku 4. stavku 2. UEU-a, Vijeće naglašava potrebu za znatnim pojedinačnim i suradničkim ulaganjem u jačanje otpornosti i uvođenje cjelokupnog spektra sposobnosti za kiberobranu te iskorištavanjem okvirâ EU-a za suradnju i financijskih poticaja. Vijeće naglašava potrebu za daljnjim jačanjem djelovanja država članica te institucija, tijela i agencija EU-a kako bi se zaštitili Unija, naši građani, institucije, tijela i agencije EU-a te misije i operacije ZSOP-a u kiberprostoru. Nadalje, naglašava da je važno osigurati otpornost EU-a u kiberprostoru razvojem sposobnosti za kiberobranu i jačanjem suradnje s pouzdanim privatnim ekosustavom.

I. **Zajedničko djelovanje za snažniju kiberobranu**

5. Vijeće ponovno ističe da je postupan, transparentan i uključiv proces bitan za jačanje povjerenja ključnog za daljnji razvoj okvira EU-a za odgovor na kiberkrize, koji treba provesti u skladu s planom za upravljanje kiberkrizama izrađenim u okviru Vijeća. Vijeće ponovno naglašava da je potrebno nastaviti jačati našu sposobnost zaštite i otkrivanja kibernapada te obranu i odvraćanje od njih poboljšanjem informiranosti o stanju, izgradnjom kapaciteta, razvojem sposobnosti, osposobljavanjem, vježbama i većom otpornosti te odlučnim odgovorom na kibernapade protiv EU-a, njegovih država članica, institucija, tijela i agencija EU-a, misija i operacija ZSOP-a upotrebom svih odgovarajućih sredstava. Vijeće pritom potiče visokog predstavnika i Komisiju da smanje složenost u području kibersigurnosti, izbjegnu nepotrebno udvostručavanje te osiguraju suradnju i sinergije s postojećim inicijativama. Potrebno je ojačati suradnju i koordinaciju među akterima u području kiberobrane unutar EU-a i država članica te među njima, između vojnih i civilnih kiberzajednica te između javnog i pouzdanog privatnog ekosustava. U tom kontekstu države članice potiču se da dodatno istraže i ojačaju civilno-vojne nacionalne koordinacijske mehanizme, olakšaju zajedničku dobrovoljnu razmjenu informacija, razmjenjuju stečena iskustva, doprinose razvoju interoperabilnih standarda te provode procjene rizika i oblikuju scenarije rizika, kao i zajedničke vježbe, osobito na europskoj razini, uz potpuno poštovanje odredaba Direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS 2).

6. Prepoznajući napore uložene u daljnje jačanje otpornosti Unije na temelju Direktive NIS 2 i Direktive o otpornosti kritičnih subjekata (CER), Vijeće ponavlja svoju preporuku o koordiniranom pristupu na razini EU-a za jačanje otpornosti kritične infrastrukture[1]. Poziva na donošenje mjera za daljnje jačanje otpornosti kritičnih subjekata, infrastrukture, digitalnih proizvoda i usluga, uz napomenu da je pravilna provedba Direktive NIS 2 i dalje najvažniji korak. Iako je to uglavnom civilna odgovornost, time se doprinosi i jačanju kiberobrane. U tom se kontekstu institucije, tijela i agencije EU-a, kao i države članice potiču da podupiru daljnji razvoj i uvođenje novih i postojećih koordinacijskih mehanizama na razini EU-a, procjena rizika, evaluacija i scenarija, zajedničke dobrovoljne razmjene informacija i vježbi, na način kojim se stvara dodana vrijednost i izbjegava nepotrebno udvostručavanje s postojećim inicijativama.

7. Kako bi se dodatno ojačalo povjerenje, konsolidirala suradnja i olakšala pravodobna razmjena informacija o kiberincidentima velikih razmjera koji utječu na obrambene sustave, Vijeće pozdravlja inicijativu u pogledu daljnjeg razvoja Konferencije zapovjednika EU-a za kiberprostor koju će organizirati svako predsjedništvo Vijeća EU-a, uz potporu Europske obrambene agencije (EDA) i sudjelovanje Europske službe za vanjsko djelovanje (ESVD). Vijeće potiče sve države članice da sudjeluju na tim sastancima. Kako bi se ojačala otpornost EU-a na kiberincidente velikih razmjera, Vijeće poziva mrežu organizacija EU-a za vezu za kiberkrize (EU-CyCLONe) i Konferenciju zapovjednika EU-a za kiberprostor da utvrde moguće načine suradnje i ostvarivanja koristi od zajedničke vojne i civilne perspektive.

[1] Prijedlog preporuke Vijeća o koordiniranom pristupu Unije jačanju otpornosti kritične infrastrukture, COM(2022) 551.

8. Kako bi se potaknuo odlučniji i koordiniraniji odgovor na razini EU-a, Vijeće pozdravlja uspostavu operativne mreže za vojne timove EU-a za hitne računalne intervencije (MICNET) i sa zanimanjem iščekuje da dosegne početnu operativnu sposobnost do sredine 2024. kako bi se poboljšala razmjena tehničkih informacija o kiberincidentima koji utječu na obrambene sustave među državama članicama sudionicama. Vijeće potiče sve države članice da sudjeluju u MICNET-u kako bi se osigurala djelotvornost te mreže. Nadalje, Vijeće poziva države članice da iskoriste iskustva stečena u okviru mreže timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi) te snažno potiče stvaranje djelotvornog mehanizma za suradnju i koordinaciju između tih dviju mreža u odgovarajućem trenutku, uz potpuno poštovanje mehanizama upravljanja i izbornih jedinica svakog subjekta.

9. S obzirom na povećanje zlonamjernih kiberaktivnosti državnih i nedržavnih aktera usmjerenih na misije i operacije ZSOP-a EU-a, Vijeće poziva EU i njegove države članice da ojačaju svoje sposobnosti za obranu i osiguravanje misija i operacija ZSOP-a. U tom pogledu Vijeće pozdravlja ciljeve daljnjeg poboljšanja zaštite vojnih mreža i struktura EU-a, u skladu s, među ostalim, vojnom vizijom i strategijom EU-a o kiberprostoru kao području operacija[2].

[2] EEAS(2021) 706 REV 4

10. Vijeće ponovno ističe zaključke Vijeća iz svibnja 2022.[3] i potrebu za ulaganjem u našu uzajamnu pomoć na temelju članka 42. stavka 7. UEU-a, kao i klauzule solidarnosti iz članka 222. UFEU-a. Vijeće naglašava važnost daljnjeg produbljivanja zajedničkog razumijevanja EU-a i njegovih država članica o provedbi članka 42. stavka 7., među ostalim u složenim scenarijima koji uključuju kibernapad, u skladu s relevantnim načelima međunarodnog prava. Pozdravlja mogućnost da, na izričit zahtjev dotične države članice ili više njih, EU u slučaju kibernapada pruži potporu, ne dovodeći u pitanje posebnu prirodu sigurnosne i obrambene politike određenih država članica.

11. Vijeće ističe napredak postignut u projektu u okviru PESCO-a koji se odnosi na Timove za brz odgovor na kiberincidente i uzajamnu pomoć u području kibersigurnosti (CRRT-ovi) te njegovu spremnost da na zahtjev djeluje kao sposobnost za potrebe država članica i EU-a, potporu misijama i operacijama ZSOP-a i pružanje pomoći partnerima EU-a. Vijeće pozdravlja daljnji razvoj sposobnosti CRRT-ova u okviru PESCO-a, nacionalnih timova za odgovor na kiberincidente i, prema potrebi, dodatnih sposobnosti za odgovor na incidente kao što su budući timovi za brzi odgovor na hibridne prijetnje kako su predviđeni u Strateškom kompasu, među ostalim poticanjem njihove koordinacije i suradnje na razini EU-a.

[3] Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora, 23. svibnja 2022., 9364/22.

12. Vijeće pozdravlja rad projekta u okviru PESCO-a koji se odnosi na Koordinacijski centar za kibernetičko i informacijsko područje (CIDCC), usmjeren na pružanje vojne sposobnosti za prikupljanje i analizu informacija koje su relevantne za dobivanje zajedničke operativne slike o kiberprostoru. Vijeće nadalje pozdravlja prijedlog da se dokaz koncepta, pokaže li se uspješnim kao centar za koordinaciju informacija, od 2025. nadalje integrira u Koordinacijski centar za kiberobranu EU-a (EUCDCC), čime bi se poboljšala koordinacija i informiranost o stanju, posebno kad su posrijedi zapovjednici misija i operacija ZSOP-a EU-a, te ojačala šira struktura zapovjedništva i nadzora EU-a. Vijeće poziva visokog predstavnika da predstavi koncept i plan za osnivanje EUCDCC-a, polazeći od iskustava sličnih međunarodnih subjekata, utvrđujući potrebne resurse, izbjegavajući nepotrebno udvostručavanje i nastojeći ostvariti komplementarnost sa širim okvirom EU-a za kibersigurnost.

13. Vijeće ističe važnost strateške obavještajne suradnje u vezi s kiberprijetnjama i kiberaktivnostima te poziva države članice da putem svojih nadležnih tijela i dalje doprinose radu Obavještajnog i situacijskog centra EU-a (EU INTCEN), Obavještajne uprave EUMS-a i država članica u okviru Službe za jedinstvenu obavještajnu analizu (SIAC). Vijeće nadalje ističe važnost jačanja naših kapaciteta za prikupljanje obavještajnih podataka o kiberprijetnjama kako bismo poboljšali svoju kiberotpornost i svoj odgovor te pružili učinkovitu potporu svojim civilnim i vojnim misijama i operacijama ZSOP-a, kao i svojim oružanim snagama i kapacitetima SIAC-a u kiberpodručju, na temelju dobrovoljnih obavještajnih doprinosa država članica i ne dovodeći u pitanje njihove nadležnosti.

14. Vijeće prima na znanje centar Europske komisije za situaciju i analizu u kiberprostoru, čiji je cilj poboljšati informiranost Komisije o stanju. Vijeće naglašava važnost uspostave uzajamno korisne suradnje između tog centra i drugih institucija, tijela, ureda i agencija, osobito Agencije Europske unije za kibersigurnost (ENISA) i tima za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU). Vijeće ističe važnost toga da se pri razvoju informiranosti o stanju osigurava bliska suradnja s mrežama EU-a za suradnju i poštuje povjerljivost. Vijeće napominje da je potrebno ojačati zajedničku informiranost o stanju na razini EU-a i dodatno razviti okvir EU-a za odgovor na kiberkrize, uz istodobno izbjegavanje nepotrebnog udvostručavanja napora.

15. Vijeće podsjeća na to da su obrazovanje, osposobljavanje i vježbe u području kibersigurnosti ključni za osiguravanje pripravnosti i učinkovitosti te pozdravlja nacionalne aktivnosti, kao i one koje pruža EU putem Europske akademije za sigurnost i obranu, Europske obrambene agencije (EDA), ENISA-e i tekućih projekata u okviru PESCO-a, kao što su Mreža kiberpoligona (CRF) i Kiberakademija i inovacijski centar EU-a (EU CAIH). S ciljem daljnjeg jačanja tih napora, Vijeće sa zanimanjem iščekuje uspostavu okvirnog projekta EDA-e CyDef-X za sinkronizaciju i podupiranje vježbi u području kiberobrane. Vijeće potiče EDA-u da u bliskoj suradnji s državama članicama i ESVD-om istraži na koji bi se način projektom CyDef-X mogle dodatno poduprijeti vježbe kao što je CYBER PHALANX, među ostalim u okviru uzajamne pomoći na temelju članka 42. stavka 7. UEU-a i klauzule solidarnosti iz članka 222. UFEU-a, kao i s Komisijom i ENISA-om u pogledu civilnih vježbi. Nadalje, Vijeće potiče upotrebu i daljnji razvoj, u okviru projekta CyDef-X, postojećih okruženja za testiranje i vježbe u području kiberobrane, kao što je Mreža kiberpoligona. Kako bi se osigurao fleksibilan i učinkovit postupak donošenja odluka u slučaju kiberkrize, Vijeće ističe važnost održavanja redovitih simulacijskih vježbi za razinu odlučivanja država članica.

16. Vijeće prima na znanje Prijedlog zakona o kibersigurnosti i namjeru da se ojačaju sposobnosti za otkrivanje kiberprijetnji i kiberincidenata u EU-u i odgovor na njih. Vijeće naglašava da prijedlozi u tom području mogu biti učinkoviti samo ako su usklađeni s okvirima i potrebama država članica u području upravljanja krizama. Vijeće naglašava važnost testiranja kritične infrastrukture na potencijalne ranjivosti, ako se to ocijeni korisnim, kao nacionalne nadležnosti, uzimajući u obzir dostupne procjene rizika EU-a.

17. Vijeće prima na znanje prijedlog Komisije o uspostavi Mehanizma za hitne situacije u području kibersigurnosti, kojim bi se mogla poduprijeti dostupnost kibersigurnosnih usluga od pouzdanih privatnih pružatelja kako bi na zahtjev pomogli državama članicama u slučaju kiberincidenata velikih razmjera, no istodobno ističe potrebu za jačanjem europske industrije kibersigurnosti uz potporu Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC) kao ključnog stupa za operativnost tog mehanizma. Vijeće ističe ključnu ulogu svake države članice u praćenju i procjeni vlastitih nacionalnih potreba.

II. **Osiguravanje obrambenog ekosustava EU-a**

18. Vijeće podsjeća na to da potiče države članice da dodatno razviju vlastite sposobnosti za provedbu operacija kiberobrane, što prema potrebi uključuje obrambene mjere za zaštitu i otkrivanje kibernapada te obranu i odvraćanje od njih. Budući da se Direktiva NIS 2 ne primjenjuje na subjekte javne uprave koji provode svoje aktivnosti u području obrane, Vijeće poziva EDA-u da, prema potrebi uz potporu Komisije i ESVD-a, pomogne državama članicama u razvoju pravno neobvezujućih dobrovoljnih preporuka nadahnutih Direktivom NIS 2 kako bi se povećala kibersigurnost u obrambenoj zajednici, te poziva sve države članice da se aktivno uključe u te napore. Kod tih bi preporuka trebalo imati na umu slične napore koji se poduzimaju u drugim okvirima.

19. Kako je navedeno u Strateškom kompasu, kapaciteti EU-a za djelovanje ovise o njegovoj sposobnosti da smanji strateške ovisnosti u svojim sposobnostima za kiberobranu i lancima opskrbe, kao i o razvoju najsuvremenijih tehnologija za kiberobranu i ovladavanju njima. To uključuje jačanje europske obrambene tehnološke i industrijske baze (EDTIB) diljem EU-a i njezine sposobnosti suradnje s partnerima istomišljenicima diljem svijeta, na uzajamnoj osnovi, kako bi se osigurale obostrane koristi. Vijeće stoga poziva da industrije kibersigurnosti i kiberobrane blisko surađuju kako bi stvorile sinergiju s ciljem razvoja i postizanja punog spektra sposobnosti za kiberobranu. Vijeće poziva Komisiju da daljnjim ulaganjima i mjerama politike te, prema potrebi, u bliskoj suradnji s ECCC-om, dodatno podupre razvoj snažne, fleksibilne, globalno konkurentne i inovativne europske obrambene tehnološke i industrijske baze, što uključuje mala i srednja poduzeća (MSP-ove).

20. S obzirom na važnost interoperabilnosti i zajedničkih obilježja sposobnosti za kiberobranu, među ostalim kad je posrijedi zajednički razvoj sposobnosti za kiberobranu sljedeće generacije, Vijeće poziva EDA-u i Vojni stožer EU-a da rade na skupu zahtjeva za interoperabilnost kiberobrane EU-a, koji bi se temeljili na postojećim načelima, procesima i standardima utvrđenima prije svega u okviru Organizacije sjevernoatlantskog ugovora (NATO) i bili usklađeni s njima. Nadalje, Vijeće poziva države članice da u okviru Europskog odbora za normizaciju u području obrane te u bliskoj suradnji sa svim relevantnim dionicima, uključujući prema potrebi europske organizacije za normizaciju i NATO, istraže bi li mogli biti potrebni posebni dobrovoljni standardi za obrambene sustave.

21. Vijeće pozdravlja napore Komisije da predstavi plan za promicanje upotrebe postojećih standarda za civilnu kibersigurnost i kiberobranu, kao i razvoj novih dobrovoljnih standarda. Vijeće ističe potrebu za usklađivanjem standarda kibersigurnosti i kiberobrane, prema potrebi. Vijeće uviđa da bi takvi dobrovoljni standardi mogli biti korisni za industriju kibersigurnosti i kiberobrane EU-a te poziva na bližu suradnju civilnih tijela za normizaciju i tijela za normizaciju u području obrane.

22. Vijeće poziva na brz razvoj preporuka utemeljenih na mapiranju postojećih alata za sigurnu komunikaciju u kiberpodručju, provedenom od strane Komisije i relevantnih institucija. Preporuke bi, prema potrebi, trebale biti usklađene s postojećim inicijativama za razmjenu informacija i uzimati u obzir i rizike koje nove i disruptivne tehnologije predstavljaju za aktualne metode šifriranja.

23. Nadalje, Vijeće pozdravlja početni rad Komisije, visokog predstavnika i Skupine za suradnju NIS na procjeni rizika i razvoju scenarija, na zahtjev Vijeća, koji su isprva bili povezani s energetskim sektorom i sektorom telekomunikacija. Vijeće potvrđuje da se pripremaju i ciljane procjene kibersigurnosnih rizika za komunikacijsku infrastrukturu i mreže u EU-u. Vijeće ponovno ističe da je od iznimne važnosti postojanje zajedničkog razumijevanja među državama članicama, ali i institucijama, tijelima i agencijama EU-a, o mogućim učincima kiberincidenata. Vijeće stoga poziva navedene aktere da osiguraju da se procjene rizika, scenariji i naknadne preporuke uzmu u obzir pri utvrđivanju i prioritizaciji mjera i potpore na razini EU-a i, prema potrebi, na nacionalnoj razini. Vijeće, osim toga, poziva da svi relevantni akteri razmotre scenarije rizika u postupcima procjene rizika, kao i pri razvoju vježbi u području kibersigurnosti.

III. **Ulaganje u sposobnosti za kiberobranu**

24. Vijeće potiče države članice da povećaju svoja ulaganja u izgradnju, održavanje i daljnji razvoj interoperabilnih sposobnosti za kiberobranu. Vijeće podupire razradu niza dobrovoljnih obveza za daljnji razvoj nacionalnih sposobnosti za kiberobranu, imajući na umu slične napore poduzete u drugim okvirima.

25. Vijeće poziva države članice i EDA-u da iskoriste mogućnost revizije plana za razvoj sposobnosti kako bi postavile visoku razinu ambicije u pogledu razvoja suradničke kiberobrane na razini EU-a. Vijeće dodatno potiče države članice da na temelju ažuriranog skupa prioriteta i svojih obveza u okviru PESCO-a povećaju svoju razinu sudjelovanja u suradničkim projektima EU-a za razvoj sposobnosti za kiberobranu, i prepoznaje izravnu korist suradničkih projekata na razini EU-a za potporu razvoju nacionalnih sposobnosti za kiberobranu.

26. Vijeće pozdravlja suradničke istraživačke napore na razini EU-a koji se ulažu u razmatranje moguće primjene novih i disruptivnih tehnologija u obrambenim sustavima, uz napomenu da je potrebno osigurati da se rezultati tog tehnološkog razvoja brzo uključe u postojeće i buduće sposobnosti. Vijeće potiče države članice i industriju EU-a da na najbolji način iskoriste mogućnosti suradničkog istraživanja na razini EU-a, primjerice u okviru EDA-e, tekućih projekata PESCO-a, kao što je Kiberakademija i inovacijski centar EU-a (EU CAIH), Europskog fonda za obranu i, prema potrebi, Obzora Europa i programa Digitalna Europa za projekte dvojne namjene. Nadalje, Vijeće pozdravlja iskorištavanje namjenskih okvira za potporu inovacijama u području obrane unosom *start-up* poduzeća iz civilnih sektora (*spin-in*), posebno programa EU-a za inovacije u području obrane i Centra za europske inovacije u području obrane. Nadalje, Vijeće potiče Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC) i EDA-u da uspostave radni dogovor kako bi se olakšala razmjena informacija između njihovih zaposlenika o civilnim prioritetima, prioritetima dvojne namjene i prioritetima u području obrambene tehnologije, s ciljem stvaranja sinergije i izbjegavanja udvostručavanja.

27. Vijeće pozdravlja namjeru Komisije da u suradnji s EDA-om i ECCC-om izradi tehnološki plan za ključne kibertehnologije u skladu s njihovim mandatima, s državama članicama i uz savjetovanje s relevantnim dionicima, kao što je industrija, koja utvrđivanjem ključne kibertehnologije i mapiranjem tehnološkog razvoja i strateških ovisnosti pruža načine za smanjenje tih ovisnosti, čime se podupiru strateška autonomija i tehnološka suverenost EU-a, uz istodobno očuvanje otvorenoga gospodarstva. Vijeće napominje da tehnološki plan za ključne kibertehnologije može poslužiti kao temelj za strateške prioritete financijskih instrumenata EU-a, pri čemu je u skladu s odgovarajućim modalitetima koji su za njih uspostavljeni. Vijeće podsjeća da bi EU trebao provoditi ambicioznu i odlučnu europsku industrijsku politiku kako bi se stvorilo održivo, privlačno i konkurentno poslovno okruženje koje ujedno može omogućiti rast europskih subjekata u području kibersigurnosti.

28. Vijeće cijeni namjeru da se riješi problem znatnog nedostatka vještina u području kibersigurnosti privlačenjem novih stručnjaka, uključujući žene, usavršavanjem i prekvalifikacijom te ulaganjem u osposobljavanje i vježbe te organizacijom osposobljavanja i vježbi radi izgradnje raznolike i uključive radne snage u području kibersigurnosti. Prepoznajući izazove s kojima se EU suočava u pogledu ljudskog kapitala u području kibersigurnosti i kiberobrane, Vijeće pozdravlja inicijativu Akademije za vještine u području kibersigurnosti, koja može koristiti i radnoj snazi u području kiberobrane.

29. Vijeće poziva države članice da razmjenjuju informacije o najboljoj praksi za razvoj kvalificiranih stručnjaka za kibersigurnost, iskorištavajući sinergiju između vojnih i civilnih inicijativa te inicijativa za izvršavanje zakonodavstva te poziva Europsku akademiju za sigurnost i obranu, uz potporu i stručno znanje EDA-e i ENISA-e, da razmotri mogućnosti za poboljšanje razmjene najbolje prakse i daljnje sinergije između vojnih i civilnih područja u pogledu osposobljavanja i razvoja vještina u području kiberobrane.

30. Vijeće naglašava važnost zajedničkog razumijevanja sastava radne snage u području kibersigurnosti i povezanih vještina kako bi se utvrdili i uklonili nedostaci na tržištu rada u području kibersigurnosti, kao i potrebu za uključivanjem svih dionika, uključujući države članice i industriju. Vijeće prima na znanje da bi se uspostavom pokazatelja za praćenje tržišta rada u području kibersigurnosti pomoglo u utvrđivanju potreba za vještinama u području kibersigurnosti i primjerenom usmjeravanju sredstava, a istodobno bi se doprinijelo ispunjavanju obveza povezanih s politikama, posebno onih koje proizlaze iz Direktive NIS 2. Vijeće pozdravlja prijedlog okvira za certifikaciju vještina u području kiberobrane i poziva visokog predstavnika, u svojstvu voditelja Europske akademije za sigurnost i obranu, da ga razvije, u suradnji s ESVD-om, Komisijom i državama članicama, poticanjem civilnih inicijativa.

IV. **Sklapanje partnerstava za rješavanje zajedničkih pitanja**

31. Vijeće poziva visokog predstavnika i Komisiju da ojačaju i unaprijede suradnju te istraže uzajamno korisna i prilagođena partnerstva u pogledu politika kiberobrane, među ostalim u pogledu izgradnje sposobnosti za kiberobranu u okviru Europskog instrumenta mirovne pomoći (EPF). U tu bi svrhu kiberobranu trebalo dodati kao stavku u dijaloge i savjetovanja EU-a o kibersigurnosti te u sveukupna savjetovanja o sigurnosti i obrani s partnerima. Osim toga, trebalo bi poboljšati dijaloge i suradnju s privatnim sektorom. Vijeće naglašava da bi međunarodna suradnja u području kibersigurnosnih normi i certifikacije bila dodana vrijednost za europsku industriju. Stoga pozdravlja predanost Komisije da to učini ključnim dijelom dijaloga EU-a s trećim zemljama i međunarodnim organizacijama o kibersigurnosti.

32. Vijeće naglašava važnost međunarodne suradnje za sprečavanje ili smanjenje rizika od sukoba u kiberprostoru, posebno daljnjim razvojem i operacionalizacijom mjera za izgradnju povjerenja na regionalnoj i međunarodnoj razini, među ostalim u UN-u, te daljnjim poticanjem upotrebe postojećih mjera za izgradnju povjerenja u kiberpodručju, kao u Organizaciji za europsku sigurnost i suradnju (OESS), među ostalim u vrijeme međunarodnih napetosti.

    EU i njegove države članice naglašavaju da se postojeće međunarodno pravo primjenjuje u kiberprostoru i naglašava važnost stalnih napora za očuvanje i promicanje okvira UN-a za odgovorno ponašanje država i rada na njegovoj provedbi, među ostalim uspostavom Programa djelovanja za poticanje odgovornog ponašanja država u kiberprostoru.

33. U skladu sa zajedničkim izjavama o suradnji EU-a i NATO-a Vijeće poziva visokog predstavnika, također u svojstvu voditelja Europske akademije za sigurnost i obranu, i Komisiju, da dodatno ojačaju, prodube i prošire partnerstvo u kiberpodučju s NATO-om uz puno poštovanje načela uključivosti, uzajamnosti, obostrane otvorenosti i transparentnosti, kao i autonomije obiju organizacija u donošenju odluka. Uzimajući u obzir potrebu za osiguravanjem komplementarnih i koordiniranih napora uz najveću moguću uključenost država članica koje nisu dio NATO-a i izbjegavanjem nepotrebnih udvostručavanja, Vijeće poziva na uspostavu veza na relevantnim razinama između EU-a i NATO-a u području osposobljavanja, obrazovanja, informiranosti o stanju, vježbi i platformi za istraživanje i razvoj te na traženje potencijalne sinergije između odgovarajućih dobrovoljnih obveza u pogledu razvoja nacionalnih sposobnosti za kiberobranu i okvirâ za upravljanje krizama, zaštite ključne infrastrukture i poboljšanja razmjene u području informiranosti o stanju, koordiniranih odgovora na zlonamjerne kiberaktivnosti, kao i napora za izgradnju kapaciteta u trećim zemljama. To uključuje tehnički dogovor između NATO-ove službe za odgovor na računalne incidente (NCIRC) i tima za hitne računalne intervencije (CERT-EU) te pojačani politički dijalog o pitanjima kiberobrane na svim razinama.

V. **Zaključak**

34. Nadovezujući se na Zaključke Vijeća o politici EU-a u području kiberobrane, Vijeće poziva visokog predstavnika i Komisiju da do drugog tromjesečja 2023. izrade plan provedbe te politike kako bi ga države članice odobrile. Vijeće također poziva države članice da dobrovoljno navedu svoje ambicije i djelovanja u pogledu kiberobrane u kontekstu politike kiberobrane EU-a te da u potpunosti iskoriste pravno neobvezujuće dobrovoljne preporuke i obveze kako bi pojačale svoje nacionalne i multinacionalne napore u području kiberobrane s ciljem maksimalnog povećanja učinka na razini EU-a. Visoki predstavnik, Komisija i države članice pozivaju se da počevši od drugog tromjesečja 2024. svake godine izvješćuju i raspravljaju o napretku u provedbi elemenata Zajedničke komunikacije i njezina provedbenog plana.