Vijeće
Europske unije

Bruxelles, 19. studenoga 2018.
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	19. studenoga 2018.
Za:	Delegacije
Predmet:	Okvir za politiku kiberobrane EU-a (ažuriranje 2018.)

Za delegacije se u Prilogu nalazi Okvir za politiku kiberobrane EU-a (ažuriranje 2018.) koji je Vijeće donijelo na 3652. sastanku održanome 19. studenoga 2018.

PRILOG

OKVIR ZA POLITIKU KIBEROBRANE EU-A

(KAKO JE AŽURIRAN 2018.)

Područje primjene i ciljevi

Kako bi odgovorili na sigurnosne izazove koji se mijenjaju, EU i njegove države članice moraju ojačati kiberotpornost i razviti jake sposobnosti u području kibersigurnosti i kiberobrane.

Okvirom za politiku kiberobrane EU-a podupire se razvoj sposobnosti kiberobrane država članica EU-a te jačanje kiberzaštite sigurnosne i obrambene infrastrukture EU-a, ne dovodeći u pitanje nacionalno zakonodavstvo država članica i zakonodavstvo EU-a, uključujući, kad je ono definirano, područje primjene kiberobrane.

Kiberprostor je peto područje djelovanja, uz područja kopna, mora, zraka i svemira: uspješna provedba misija i operacija EU-a sve više ovisi o neometanom pristupu sigurnom kiberprostoru te su zbog toga potrebne jake i otporne kiberoperativne sposobnosti.

Cilj je ažuriranog okvira za politiku kiberobrane dodatno razviti politiku kiberobrane EU-a uzimanjem u obzir relevantnih foruma i područja politike te provedbe okvira za politiku kiberobrane od 2014. U okviru za politiku kiberobrane utvrđuju se prioritetna područja kiberobrane i razjašnjavaju uloge raznih europskih aktera, poštujući pritom u potpunosti odgovornosti i nadležnosti aktera Unije i država članica, kao i institucijski okvir EU-a i njegovu autonomiju u donošenju odluka.

Kontekst

U zaključcima Europskog vijeća o ZSOP-u iz prosinca 2013. te u zaključcima Vijeća o ZSOP-u iz studenoga 2013. pozivalo se na razvoj okvira za politiku kiberobrane EU-a na temelju prijedloga Visokog predstavnika i u suradnji s Europskom komisijom i Europskom obrambenom agencijom (EDA). Vijeće je okvir za politiku kiberobrane EU-a donijelo 18. studenoga 2014.[1] i otada se konkretnim rezultatima u okviru njegove provedbe znatno doprinijelo povećanju sposobnosti kiberobrane država članica. Kao dio godišnjeg izvješća iz 2017. o provedbi okvira za politiku kiberobrane[2] i uzimajući u obzir inicijative EU-a u području sigurnosti i obrane, posebno Koordinirano godišnje preispitivanje u području obrane (CARD), stalnu strukturiranu suradnju (PESCO), Europski fond za obranu (EDF) i pakt za civilni ZSOP kao i reviziju plana za razvoj sposobnosti (CDP) i plana razvoja civilnih sposobnosti iz 2018., države članice pozvale su na ažuriranje okvira za politiku kiberobrane EU-a.

Kibersigurnost je prioritet u okviru Globalne strategije EU-a za vanjsku i sigurnosnu politiku i u okviru razine ambicije EU-a[3]. U globalnoj strategiji ističe se potreba za povećanjem sposobnosti za zaštitu EU-a i njegovih građana te odgovora na vanjske krize. Globalnom strategijom naglašava se potreba za jačanjem EU-a kao sigurnosne zajednice. U tom kontekstu, naporima u području sigurnosti i obrane trebala bi se ojačati i strateška uloga EU-a i njegova sposobnost autonomnog djelovanja kada i gdje god je to potrebno te, prema mogućnosti, zajedno s partnerima. Ti ciljevi zahtijevaju bolju suradnju u razvoju sposobnosti, promicanjem učinkovitosti i interoperabilnosti civilnih i vojnih sposobnosti koji iz toga nastaju.

---

1 Dokument Vijeća 15585/14, 18.11.2014.
2 Dokument Vijeća 15870/17, 19.12.2017.
3 Zaključci Vijeća o provedbi globalne strategije EU-a u području sigurnosti i obrane, 14.11.2016.

Zajedničkim nizom prijedloga za provedbu Zajedničke izjave koju su predsjednik Europskog vijeća, predsjednik Europske komisije i glavni tajnik Organizacije sjevernoatlantskog ugovora potpisali u Varšavi 8. srpnja 2016.[4] obuhvaćena su konkretna djelovanja za proširenje suradnje EU-a i NATO-a u području kibersigurnosti i kiberobrane, među ostalim u kontekstu misija i operacija, kao i u vezi s razvojem sposobnosti kiberobrane, istraživanjima i tehnologijom, osposobljavanjem, obrazovanjem, vježbama i uključivanjem kiberpitanja u upravljanje krizama. Ta suradnja odvija se uz puno poštovanje načela otvorenosti, transparentnosti, uključivosti, uzajamnosti i autonomije EU-a u donošenju odluka. Tehničkim sporazumom između tima za hitne računalne intervencije EU-a (CERT-EU) i NATO-ove službe za odgovor na računalne incidente (NCIRC) potpisanim u veljači 2016. olakšava se razmjena tehničkih informacija u svrhu poboljšanja sprečavanja i otkrivanja kiberincidenata i odgovora na njih u objema organizacijama.

Trebalo bi podsjetiti na to da nekoliko politika EU-a doprinosi ciljevima politike kiberobrane kako je navedeno u ovom dokumentu, a ovim okvirom u obzir se uzimaju i relevantne uredbe, politike i tehnološka potpora u civilnoj domeni. Na primjer, u srpnju 2016. Europski parlament i Vijeće donijeli su Direktivu o sigurnosti mreža i podataka[5] (NIS) kojom će se povećati ukupna spremnost država članica za suočavanje s kiberprijetnjama te poboljšati suradnja diljem EU-a. Tom Direktivom utvrđuju se mjere s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava unutar Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta. Rok za prenošenje Direktive bio je 9. svibnja 2018.

---

[4] Zaključci Vijeća o provedbi Zajedničke izjave predsjednika Europskog vijeća, predsjednika Europske komisije i glavnog tajnika Organizacije sjevernoatlantskog ugovora (6. prosinca 2016., 15283/16; 5. prosinca 2017., 14802/17).

[5] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194, 19.7.2016., str. 1.

U prijedlog akta EU-a o kibersigurnosti iz rujna 2017. uključeni su novi mandat za agenciju EU-a za kibersigurnost (ENISA) i uspostava okvira za certifikaciju u cijelom EU-u. Nakon što bude uspostavljen, okvirom za certifikaciju trebalo bi se podupirati visoke standarde za IKT postupke, proizvode i usluge i trebao bi biti izvor konkurentske prednosti i povećati povjerenje potrošača i naručitelja. Komisija je u rujnu 2017. napravila još jedan korak u pripremi EU-a za slučaj prekograničnih kiberincidenata velikih razmjera („Nacrt”) i sada radi s državama članicama i drugim institucijama, agencijama i tijelima na razvoju europske suradnje u kiberkrizama, uspostavom praktične operacionalizacije i dokumentacije svih relevantnih aktera, procesa i postupaka u kontekstu postojećih mehanizama EU-a za upravljanje krizama i katastrofama, posebno aranžmanima za integrirani politički odgovor na krizu.

U zaključcima Vijeća o jačanju europskog sustava kiberotpornosti iz studenoga 2016. opisan je zajednički cilj doprinosa strateškoj autonomiji EU-a, kako je navedeno u zaključcima Vijeća iz studenoga 2016. o globalnoj strategiji Europske unije za vanjsku i sigurnosnu politiku, također i u kiberprostoru. Europsko vijeće tu je poruku ponovno potvrdilo u lipnju 2018. te naglasilo i potrebu da se ojačaju sposobnosti u odnosu na prijetnje u području kibersigurnosti koje dolaze izvan EU-a.

Vijeće je u 2017. donijelo okvir za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („alati za kiberdiplomaciju”)[6]. Očekuje se da će se tim okvirom poticati suradnja, olakšati ublažavanje prijetnji te dugoročno utjecati na ponašanje potencijalnih agresora. Okvir se koristi mjerama ZVSP-a, uključujući mjere ograničavanja, kako bi se spriječilo zlonamjerne kiberaktivnosti i odgovorilo na njih. Počinitelji zlonamjernih kiberativnosti trebaju odgovarati za svoja djelovanja te se države članice EU-a potiču da dodatno razviju svoju sposobnost koordiniranog odgovora na zlonamjerne kiberaktivnosti u skladu s alatima za kiberdiplomaciju. Države ne bi trebale provoditi ili svjesno podupirati aktivnosti u području informacijske i komunikacijske tehnologije u suprotnosti sa svojim obvezama prema međunarodnom pravu i ne bi trebale svjesno dopustiti da se njihovo državno područje upotrebljava za međunarodne prijestupe upotrebom informacijske i komunikacijske tehnologije.

Komisija i Visoki predstavnik / potpredsjednik Komisije u rujnu 2017. predstavili su zajedničku komunikaciju[7] o kiberpitanjima s ciljem ublažavanja rizika koji proizlaze iz novih prijetnji. To uključuje kiberobranu kao jedno od glavnih područja djelovanja, pri čemu je okvir za politiku kiberobrane jedan od stupova njezine konkretne provedbe[8].

U zaključcima Vijeća iz studenoga 2017. o kiberpitanjima prepoznate su sve čvršće veze između kibersigurnosti i kiberobrane i pozvano je na jačanje suradnje u području kiberobrane, među ostalim poticanjem suradnje između civilnih i vojnih zajednica za odgovor na incidente. Naglašeno je i da bi posebno ozbiljan kiberincident ili kiberkriza trebali biti dostatna osnova da se država članica pozove na klauzulu solidarnosti EU-a i/ili klauzulu o uzajamnoj pomoći.

---

6 Zaključci Vijeća o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („Alati za kiberdiplomaciju”), 9916/17, 7. lipnja 2017.

7 Zajednička komunikacija Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a (13. rujna 2017., JOIN (2017) 450 final).

8 Zaključci Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a (20. rujna 2017., 14435/17).

Stalna strukturirana suradnja (PESCO) pokrenuta je 11. prosinca 2017. Taj ambiciozan, obvezujući i uključiv okvir za suradnju uspostavljen je među 25 država članica i obuhvaća obvezu da se povećaju napori u suradnji u vezi s kiberobranom, kao i u vezi s povezanim projektima u okviru PESCO-a. Prvi niz projekata u okviru PESCO-a koje su u 2017. utvrdile države članice koje sudjeluju u PESCO-u obuhvaća dva projekta povezana s kiberobranom: „Timovi za brz odgovor na kiberincidente i uzajamna pomoć u području kibersigurnosti" i „Platforma za razmjenu informacija o odgovoru na kiberprijetnje i kiberincidente". Predviđen je sljedeći niz projekata u okviru PESCO-a. PESCO će razvijati sposobnosti kiberobrane te time ojačati suradnju među državama članicama sudionicama i povećati interoperabilnost.

U ažuriranom planu za razvoj sposobnosti (CDP) koji je Upravljački odbor EDA-e odobrio u lipnju 2018. kiberobrana je utvrđena kao ključni element, prepoznajući potrebu za obrambenim kiberoperacijama u svim operativnim kontekstima, na temelju sofisticirane trenutačne i prognostičke svijesti o stanju u vezi s kiberporstorom, uključujući sposobnost kombiniranja velike količine podataka i obavještajnih podataka iz različitih izvora u svrhu pružanja potpore brzom donošenju odluka i povećanoj automatizaciji procesa prikupljanja i analize podataka te potpore donošenju odluka. U planu za razvoj sposobnosti iz 2018. utvrđuju se prioriteti u vezi sa sposobnošću kiberobrane u sljedećim područjima: suradnji i sinergijama s relevantnim akterima u svim područjima kiberobrane i kibersigurnosti; aktivnostima istraživanja i tehnologije u području kiberobrane; okvirima inženjeringa sustava za kiberoperacije; obrazovanju, osposobljavanju, vježbama i evaluaciji (ETEE); rješavanju izazova u vezi s kiberobranom u zraku, svemiru, na moru i na kopnu.

Konačno, tijekom posljednjih godina jasna je postala potreba da međunarodna zajednica spriječi sukobe, surađuje i stabilizira kiberprostor. EU u bliskoj suradnji s drugim međunarodnim organizacijama, posebno UN-om, OESS-om i Regionalnim forumom ASEAN-a, promiče strateški okvir za sprečavanje sukoba, suradnju i stabilnost u kiberprostoru koji obuhvaća i. primjenu međunarodnog prava, osobito Povelje UN-a u cjelini, u kiberprostoru, ii. poštovanje univerzalnih neobvezujućih normi, pravila i načela za odgovorno postupanje država te iii. razvoj i primjenu regionalnih mjera za izgradnju povjerenja. Okvirom za politiku kiberobrane također bi se trebao podupirati taj pothvat.

Prioriteti

U ažuriranom okviru za politiku kiberobrane utvrđeno je šest prioritetnih područja. Ovaj okvir politike u prvom je redu usmjeren na razvoj sposobnosti kiberobrane, kao i na zaštitu EU-ovih komunikacijskih i informacijskih mreža ZSOP-a. Druga prioritetna područja uključuju osposobljavanje i vježbe, istraživanje i tehnologiju, civilno-vojnu suradnju i međunarodnu suradnju. U području osposobljavanja naglasak je stavljen na unapređenje osposobljavanja država članica u području kiberobrane i osposobljavanja lanca zapovjedništva ZSOP-a u području osvješćivanja u pogledu kiberpitanja. Važno je i da se u vježbama prikladno sagleda kiberdimenzija kako bi se poboljšala sposobnost EU-a da reagira na kiberkrize i hibridne krize s ciljem poboljšanja postupaka donošenja odluka i dostupnosti informacija. Kiberprostor je domena koja se brzo razvija i potrebno je poduprijeti nova tehnološka kretanja, i u civilnoj i u vojnoj domeni. Civilno-vojna suradnja u kiberpodručju ključna je kako bi se osigurao dosljedan odgovor na kiberprijetnje. Naposljetku, poboljšanjem suradnje s međunarodnim partnerima moglo bi se pomoći poboljšati kibersigurnost unutar EU-a i izvan njega te promicati načela i vrijednosti EU-a.

U ovom okviru navode se prijedlozi i mogućnosti za koordinaciju među relevantnim institucijama, tijelima i agencijama EU-a. U njemu se također odražava važna uloga privatnog sektora za razvoj tehnologija za kibersigurnost i kiberobranu.

Osim toga, okvirom za politiku kiberobrane dodatno se podupire integracija kiberobrane u mehanizme Unije za upravljanje krizama pri čemu za suočavanje s učincima kiberkrize primjenjive mogu biti relevantne odredbe Ugovora o EU-u i Ugovora o funkcioniranju EU-a[9].

1. Potpora razvoju sposobnosti kiberobrane država članica

Razvojem sposobnosti i tehnologija kiberobrane trebalo bi obuhvatiti sve aspekte razvoja sposobnosti, uključujući doktrinu, vodstvo, organizaciju, osoblje, osposobljavanje, industriju, tehnologiju, infrastrukturu, logistiku i interoperabilnost. U tu svrhu države članice trebale bi pojačati svoje napore radi postizanja učinkovite sposobnosti kiberobrane. ESVD, Komisija i EDA trebali bi surađivati i pružiti potporu tim naporima.

Potrebna je kontinuirana procjena ranjivosti informacijskih infrastruktura koje podupiru misije i operacije ZSOP-a, kao i razumijevanje učinkovitosti zaštite u gotovo stvarnom vremenu. S operativnog stajališta, jedno od glavnih područja na koje su usmjerene aktivnosti kiberobrane bit će na zadržavanju dostupnosti, cjelovitosti i povjerljivosti komunikacijskih i informacijskih mreža ZSOP-a, osim ako je drugačije navedeno u okviru mandata operacija ili misija. Nadalje, ESVD će u suradnji s državama članicama dodatno integrirati kibersposobnosti u misije i operacije ZSOP-a.

Počinitelji zlonamjernih kiberaktivnosti trebaju odgovarati za svoja djelovanja. Važno je da države članice EU-a, uz potporu ESVD-a, potiču uzajamnu suradnju kako bi se odgovorilo na zlonamjerne kiberaktivnosti. Alati za kiberdiplomaciju razvijeni su kako bi se pomoglo u ostvarenju takvog uzajamnog odgovora. ESVD i EDA organizirat će redovite vježbe na temelju alata za kiberdiplomaciju u kojima države članice EU-a mogu to vježbati.

[9] Članak 222. UFEU-a i članak 42. stavak 7. UEU-a, uzimajući u obzir članak 17. UEU-a.

S obzirom na to da je u nacionalnom zakonodavstvu država članica kao i u zakonodavstvu EU-a područje primjene kiberobrane široko i raznoliko, ako je definirano, potrebno je razviti zajedničko skupno razumijevanje područja primjene kiberobrane.

Budući da se vojne operacije ZSOP-a oslanjaju na zapovjednu, nadzornu, komunikacijsku i računalnu (C4) infrastrukturu koju osiguravaju države članice, potreban je određeni stupanj strateške konvergencije prilikom planiranja zahtjeva za informacijsku infrastrukturu u području kiberobrane.

Polazeći od rada projektnog tima EDA-e za kiberobranu radi razvoja sposobnosti kiberobrane, EDA i države članice će:

- upotrebljavati plan razvoja sposobnosti i druge instrumente poput CARD-a za olakšavanje i podupiranje suradnje među državama članicama kako bi se povećao stupanj konvergencije u planiranju zahtjeva za kiberobranu država članica na strateškoj razini, posebice u pogledu praćenja, svijesti o stanju, sprečavanja, otkrivanja i zaštite, razmjene informacija, forenzičkih mogućnosti i mogućnosti analize zlonamjernih softvera, stečenih iskustava, sprečavanja širenja štete, sposobnosti dinamičkog obnavljanja, pohrane distribuiranih podataka i sigurnosnih kopija podataka;
- podupirati postojeće i buduće projekte udruživanja i dijeljenja povezane s kiberobranom za vojne operacije (npr. u forenzici, pri razvoju interoperabilnosti, određivanju standarda);
- razviti standardni niz ciljeva i zahtjeva za određivanje minimalne razine kibersigurnosti i povjerenja koju trebaju postići države članice oslanjajući se na postojeće iskustvo diljem EU-a.

ESVD i EDA će:

- olakšati razmjene među državama članicama u vezi s nacionalnim doktrinama kiberobrane i programima zapošljavanja, zadržavanja i pričuvnika usmjerenima na kiberobranu.

EDA će:

- proučiti različita područja primjene vojnih zahtjeva u području kiberobrane u nacionalnom zakonodavstvu i najboljoj praksi država članica. Glavni cilj proučavanja bit će razviti arhitekturu poduzeća za kiberobranu, kako bi se uključili područje primjene, funkcionalnosti i zahtjevi koje države članice upotrebljavaju u domeni na temelju nacionalnog zakonodavstva i zakonodavstva EU-a.

Države članice na dobrovoljnoj će osnovi:

- poboljšati suradnju među svojim vojnim timovima za hitne računalne intervencije (CERT) kako bi se poboljšalo sprečavanje incidenata i postupanje s njima;
- iskoristiti PESCO kako bi se dodatno poboljšala suradnja u vezi s kiberobranom, uključujući nove projekte;
- iskoristiti Europski fond za obranu kako bi se zajednički razvile sposobnosti kiberobrane;
- razviti zajedničko razumijevanje o primjeni klauzule o uzajamnoj pomoći u kiberpodručju, uz očuvanje njezine fleksibilnosti;
- razviti osnovne zahtjeve za kiberobranu u vezi s informacijskom infrastrukturom;
- u mjeri u kojoj poboljšanje sposobnosti kiberobrane ovisi o civilnoj mreži i civilnoj stručnosti u području informacijske sigurnosti, iskoristiti stručnost ENISA-e, tijela država članica okupljenih u skupinu za suradnju u području NIS-a i drugih mogućih subjekata na razini EU-a sa stručnošću u području civilne kibersigurnosti.

Države članice, ESVD / Vojni stožer EU-a, Europska akademija za sigurnost i obranu (ESDO) i EDA će:

- razmotriti osmišljavanje osposobljavanja u području kiberobrane s ciljem certifikacije borbenih skupina EU-a.

Komisija, u suradnji s državama članicama, će:

- razmotriti kiberobranu u programima rada Europskog programa industrijskog razvoja u području obrane i Europskog fonda za obranu.

2. Jačanje zaštite komunikacijskih i informacijskih sustava ZSOP-a kojima se koriste subjekti EU-a

Ne dovodeći u pitanje ulogu tima za hitne računalne intervencije institucija, tijela i agencija EU-a (CERT-EU) kao središnje koordinacijske strukture EU-a za rješavanje kiberincidenata za sve institucije, tijela i agencije Unije i u okviru relevantnih pravila koja se odnose na proračun Unije, ESVD će razviti prikladno i autonomno razumijevanje pitanja sigurnosti i mrežne obrane te razviti vlastite kapacitete sigurnosti informacijske tehnologije. Nastojat će povećati otpornost mreža ESVD-a za ZSOP s naglaskom na sprečavanju, otkrivanju, rješavanju incidenata, svijesti o stanju, razmjeni informacija i mehanizmima ranog upozoravanja.

Zaštita komunikacijskih i informacijskih sustava ESVD-a i razvoj kapaciteta sigurnosti informacijske tehnologije (IT) vodi Glavna uprava ESVD-a za proračun i administraciju (BA). Dodatne namjenske resurse i potporu pružat će i Vojni stožer Europske unije (EUMS), Uprava za upravljanje krizama i planiranje (CMPD) i služba za civilno planiranje i provođenje (CPCC). Ti kapaciteti sigurnosti informacijske tehnologije obuhvaćat će klasificirane i neklasificirane sustave te biti sastavni dio postojećih operativnih subjekata.

Postoji i potreba za pojednostavnjenjem sigurnosnih pravila za informacijske sustave koje pružaju razni institucijski dionici EU-a tijekom obavljanja misija i operacija ZSOP-a. U tom bi se kontekstu mogao razmotriti jedinstveni zapovjedni lanac radi povećanja otpornosti mreža koje se upotrebljavaju za ZSOP.

Radi bolje koordinacije i kako bi se povećala zaštita i otpornost komunikacijskih i informacijskih sustava i mreža ZSOP-a, u 2017. osnovan je unutarnji Odbor ESVD-a za upravljanje kiberpitanjima pod glavnim tajnikom ESVD-a.

ESVD/BA će:

- ojačati kapacitet sigurnosti informacijske tehnologije unutar ESVD-a na temelju postojećih tehničkih sposobnosti i postupaka s naglaskom na sprečavanju, otkrivanju, rješavanju incidenata, svijesti o stanju, razmjeni informacija i mehanizmima ranog upozoravanja. Dodatno će se ojačati strategija suradnje s CERT-EU-om i postojećim sposobnostima kibersigurnosti EU-a.

ESDV/BA će, u suradnji s EUMS-om, MPCC-om, CMPD-om i CPCC-om:

- razvijati koherentnu politiku i smjernice za sigurnost informacijske tehnologije, također uzimajući u obzir tehničke zahtjeve u vezi s kiberobranom u kontekstu ZSOP-a za strukture, misije i operacije, imajući na umu postojeće okvire i politike suradnje u EU-u za postizanje usklađenosti pravila, politika i organizacije.

ESVD/Služba za jedinstvenu obavještajnu analizu (SIAC) će:

- na temelju stečenih iskustava iz postojećih struktura poboljšati svoje procjenjivanje kiberprijetnji i obavještajnu sposobnost prepoznavanja novih kiberrizika i pružati redovite procjene rizika na temelju strateške procjene prijetnji i informacija o incidentima u gotovo stvarnom vremenu koje se koordiniraju među relevantnim strukturama EU-a i koje su dostupne uz različite stupnjeve tajnosti.

ESVD/SIAC i CERT-EU će:

- promicati razmjenu informacija o kiberprijetnjama u stvarnom vremenu između država članica i relevantnih subjekata EU-a. U tu svrhu razvijat će se mehanizmi za razmjenu informacija i mjere za izgradnju povjerenja kod relevantnih nacionalnih i europskih tijela putem dobrovoljnog pristupa koji se temelji na postojećoj suradnji.

ESVD/EUMS i MPCC će:

- dodatno razvijati i integrirati u planiranje na strateškoj razini koncept kiberobrane za vojne operacije i misije ZSOP-a;
- razvijati, u suradnji s operativnim stožerom, opće standardne postupke u vezi s kiberpitanjima na operativnoj razini.

ESVD/CPCC i CPMD će:

- dalje razvijati i integrirati u strateško planiranje koncept o kiberobrani za civilne misije ZSOP-a;
- jačati sposobnosti kiberobrane civilnih misija ZSOP-a na temelju postojeće infrastrukture i promicanjem normizacije i usklađivanja tehnologija koje se upotrebljavaju u okviru misija i operacija ZSOP-a, koristeći se, prema potrebi, stručnošću CERT-EU-a, ENISA-e i EDA-e;
- u postupku jačanja civilnog ZSOP-a, dodatno istražiti moguću potporu civilnih misija ZSOP-a državama domaćinima u pogledu kibersigurnosti.

ESVD će:

- dalje razvijati zajedničke zahtjeve za vojne i civilne misije i operacije ZSOP-a;
- jačati koordinaciju kiberobrane radi provedbe ciljeva povezanih sa zaštitom mreža kojima se služe institucijski akteri EU-a koji podupiru ZSOP, oslanjajući se na postojeća iskustva diljem EU-a;
- redovito preispitivati zahtjeve za resurse i druge bitne odluke o politikama na temelju promjenjive situacije u pogledu prijetnji, savjetujući se s državama članicama i drugim institucijama EU-a.

3. Promicanje civilno-vojne suradnje

Kiberprostor je područje koje se brzo razvija: tehnološki razvoj treba ojačati sigurnosnim sustavima u civilnom i vojnom području. U mjeri u kojoj je to moguće trebalo bi predvidjeti koordinaciju civilnog i vojnog područja u slučajevima kada se sličnim tehnološkim razvojem pronađu rješenja za civilne i vojne primjene. U drugim slučajevima, vojne sposobnosti i sustavi oružja toliko su posebni da ih nije moguće dijeliti s civilnim tehnologijama. Ne dovodeći u pitanje unutarnju organizaciju i zakonodavstvo država članica, civilno-vojna suradnja u kiberdomeni može se uzeti u obzir, među ostalim, za razmjenu najboljih praksi, razmjenu informacija i mehanizme ranog upozoravanja, procjene rizika reagiranja na incidente i podizanje svijesti te za osposobljavanje i vježbe.

Poboljšanje civilne kibersigurnosti važan je čimbenik koji doprinosi općoj sigurnosnoj otpornosti mreža i podataka. Direktivom o sigurnosti mreža i podataka (NIS) povećava se spremnost na nacionalnoj razini i jača suradnja među državama članicama na razini Unije i na strateškoj i na operativnoj razini. Ta suradnja obuhvaća i nacionalna tijela koja nadziru politike kibersigurnosti kao i nacionalne timove za hitne računalne intervencije (CERT-ovi) te CERT-EU. Suradnja između civilnih i vojnih CERT-ova trebala bi se ojačati vodeći računa o tim promjenama. Novim europskim aktom o kibersigurnosti želi se poboljšati europska otpornost na kibernapade te osigurati okvir za kibersigurnosnu certifikaciju za proizvode i usluge, povećavajući time povjerenje u civilnu digitalnu sferu.

EDA-u, Agenciju Europske unije za mrežnu i informacijsku sigurnost (ENISA), Europski centar za kiberkriminalitet (EC3) i CERT-EU, zajedno s drugim relevantnim tijelima i agencijama EU-a, u skladu s njihovim mandatima i bez preklapanja s nadležnostima država članica, kao i države članice, potiče se da dalje unapređuju svoju suradnju u sljedećim područjima:

- razvijanju zajedničkih profila sposobnosti u području kibersigurnosti i kiberobrane koji se temelje na međunarodnim najboljim praksama i certificiranju koje upotrebljavaju institucije, tijela i agencije EU-a, uzimajući u obzir i standarde certificiranja privatnog sektora;
- doprinosu daljnjem razvoju i prilagodbi organizacijskih i tehničkih standarda kibersigurnosti i kiberobrane iz javnog sektora za upotrebu u sektoru obrane i sigurnosti; prema potrebi, nadovezivanju na rad ENISA-e i EDA-e;
- uspostavi ili daljem razvoju radnih mehanizama i aranžmana za razmjenu najbolje prakse, posebno u vezi s obrazovanjem, osposobljavanjem i vježbama, kao i područjem istraživanja i tehnologije te drugim područjima, osiguravajući civilno-vojne sinergije;
- iskorištavanju postojećih iskustava EU-a u sposobnostima za sprečavanje, istragu i forenziku u području kiberkriminaliteta i njihovoj pojačanoj upotrebi pri razvoju sposobnosti kiberobrane.

Države članice na dobrovoljnoj će osnovi:

- jačati suradnju između civilnih i vojnih CERT-ova među državama članicama.

ESVD, Komisija i države članice će:

- uključiti kiberobranu u postupke upravljanja katastrofama i krizama EU-a (postupkom izrade nacrta).

4. Istraživanje i tehnologija

Operatori infrastrukture i usluga informacijskih i komunikacijskih tehnologija u civilne i obrambene svrhe suočavaju se sa sličnim izazovima u vezi s kibersigurnošću, što proizlazi iz zajedničkih zahtjeva za tehnološkom i operativnom sposobnošću. Predviđene su zajedničke potrebe u istraživanju i tehnologiji i zajednički zahtjevi za sustave kako bi se poboljšala interoperabilnost sustava na dulji rok te smanjili troškovi razvoja rješenja. Postizanje ekonomije razmjera nužno je za suočavanje sa sve većim brojem prijetnji i slabih točaka. To bi zauzvrat trebalo olakšati očuvanje i rast konkurentne industrije kiberobrane u Europi.

Razvoj sposobnosti kiberobrane sadrži važnu dimenziju istraživanja i tehnologije. Unutar okvira Plana za istraživanje kibernetičke obrane (CDRA) EDA je predvidjela stabilnu osnovu za određivanje prioriteta budućih troškova za istraživanje i tehnologiju unutar međuvladinog okvira. Naknadnim strateškim planom istraživanja koji je izrađen u okviru relevantne *Ad hoc* radne skupine EDA-e omogućuje se informirano određivanje prioriteta u vezi s tehnologijama povezanima s kiberpodručjem koje su potrebne u vojne svrhe te se pritom utvrđuju mogućnosti za napore i ulaganja dvojne namjene, bilo da je riječ o kontekstu financiranja na nacionalnoj ili multinacionalnoj razini ili razini EU-a.

Razvoj tehnoloških sposobnosti u Europi ključan je za ublažavanje prijetnji i slabih točaka. Industrija će i dalje biti glavni pokretač tehnologije i inovacija povezanih s kiberobranom. Kriptografija, sigurni ugrađeni sustavi, otkrivanje zlonamjernih softvera, tehnika simulacije i vizualizacije, zaštita mrežnih i komunikacijskih sustava, tehnologija identifikacije i autentifikacije neka su od područja kojima se je potrebno baviti. Isto je tako važno poticati konkurentan opskrbni lanac europske industrijske kibersigurnosti podupiranjem uključivanja malih i srednjih poduzeća (MSP-a).

Osiguravanje da Europa može držati korak s međunarodnim konkurentima u odnosu na sposobnosti u području kibertehnologije također ovisi o našoj sposobnosti za poticanje revolucionarnih inovacija, putem nacionalnih instrumenata i instrumenata EU-a poput Europskog vijeća za inovacije.

Kako bi olakšale civilno-vojnu suradnju u razvoju sposobnosti kiberobrane i osnažile europsku obrambenu tehnološku i industrijsku bazu[10] te kako bi doprinijele strateškoj autonomiji EU-a u području kiberprostora, kada i gdje je to potrebno i kad je moguće s partnerima,

EDA, Komisija i države članice će:

- raditi na postizanju sinergija između napora koji se ulažu u istraživanje i tehnologiju u vojnom sektoru i civilnih programa za istraživanje i razvoj, a posebice onih koji se odnose na revolucionarne inovacije, te razmotriti dimenziju kibersigurnosti i kiberobrane pri provedbi pripremnog djelovanja za istraživanje u području obrane;
- razmjenjivati istraživačke programe za područje kibersigurnosti (npr. strateški plan istraživanja u području kibersigurnosti Europske obrambene agencije) kao i planove i djelovanja koji će proizaći iz toga. U tu svrhu izradit će se međusektorski istraživački program za područje kiberobrane uz blisku suradnju s Komisijom i državama članicama;
- doprinositi poboljšavanju integracije dimenzija kibersigurnosti i kiberobrane u programima dvojne namjene sa sigurnosnom i obrambenom dimenzijom, npr. programu istraživanja i razvoja upravljanja zračnim prometom na jedinstvenom europskom nebu (SESAR).

[10] Komunikacija „Prema konkurentnijem i učinkovitijem sektoru obrane i sigurnosti”, COM (2013) 542.

Komisija će:

- razmotriti osnivanje Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara kako bi podržala tehnološke i industrijske sposobnosti u području kibersigurnosti te povećala konkurentnost industrije kibersigurnosti u Uniji, osiguravanjem komplementarnosti i izbjegavanjem udvostručenja unutar mreže centara za stručnost u području kibersigurnosti te s drugim agencijama EU-a. Centrom bi se, među ostalim, trebala poboljšati suradnja između civilnih i obrambenih tehnologija i primjena te bi trebao blisko i u punoj komplementarnosti surađivati s Europskom obrambenom agencijom u području kiberobrane;
- podržavati razvoj industrijskih ekosustava i inovacijskih klastera kojima se obuhvaća cijeli vrijednosni lanac sigurnosti koristeći se akademskim znanjem, inovacijama MSP-a i industrijskom proizvodnjom.

Komisija će u suradnji s državama članicama:

- uzeti u obzir pitanja kiberobrane u pozivima za podnošenje prijedloga za pripremno djelovanje Unije za istraživanja u području obrane;
- uzeti u obzir područje kiberobrane u temama koje se trebaju razmotriti u kontekstu Europskog fonda za obranu;
- podržavati usklađenost politike EU-a kako bi osiguralo da politika i tehnički aspekti kiberzaštite EU-a ostanu u središtu tehnoloških inovacija te da su usklađeni diljem EU-a (sposobnost analize i procjene kiberprijetnji, integrirana sigurnost (*security by design*), upravljanje ovisnostima kod pristupa tehnologiji itd.).

5. Poboljšanje mogućnosti obrazovanja, osposobljavanja i vježbi

Kako bi se povećala spremnost za suočavanje s kiberprijetnama i razvila zajednička kultura kiberobrane diljem EU-a, što bi koristilo i misijama i operacijama EU-a, potrebno je poboljšati i proširiti mogućnosti osposobljavanja u području kiberobrane. Ključno je da se proračuni za obrazovanje i osposobljavanje upotrebljavaju učinkovito te da se istodobno njima pruža najbolja moguća kvaliteta. Udruživanje i dijeljenje pri obrazovanju i osposobljavanju u području kiberobrane na europskoj razini bit će od ključne važnosti.

Europska akademija za sigurnost i obranu (EASO), ESVD, EDA, Komisija i države članice će:

- na temelju EDA-ine analize potreba za osposobljavanjem u području kiberobrane i iskustava prikupljenih tijekom osposobljavanja u području kibersigurnosti koje organizira EASO, uspostaviti program osposobljavanja i obrazovanja ZSOP-a za različite korisnike, među ostalim ESVD, osoblje misija i operacija ZSOP-a i dužnosnike država članica kojim bi se trebalo razmotriti i pitanje zadržavanja kvalificiranog osoblja u kratkoročnom, srednjoročnom i dugoročnom razdoblju;
- predložiti uspostavu dijaloga o standardima osposobljavanja i certifikaciji u području kiberobrane s državama članicama, institucijama EU-a, trećim zemljama i drugim međunarodnim organizacijama te privatnim sektorom;
- raditi s europskim pružateljima usluga osposobljavanja u privatnom sektoru te akademskim institucijama da bi se poboljšale kompetencije i vještine osoblja koje sudjeluje u misijama i operacijama ZSOP-a.

EASO će:

- dodatno razviti platformu za obrazovanje, osposobljavanje, evaluaciju i vježbe u području kiberpitanja uspostavljenu pri EASO-u (platforma ETEE u području kiberpitanja);
- stvoriti sinergije s programima osposobljavanja drugih dionika poput ENISA-e, Europola, Europske policijske akademije (CEPOL) i NATO-ova Centra izvrsnosti za suradnju u području kiberobrane;
- istražiti mogućnost zajedničkih programa osposobljavanja u području kiberobrane EASO-a i NATO-a, otvorenih za sve države članice EU-a kako bi se poticala zajednička kultura kiberobrane.

Komisija će:

- procijeniti opcije unapređenja mogućnosti osposobljavanja i obrazovanja u okviru država članica utvrđenih kiberplatformom ETEE.

EDA će:

- dalje razvijati tečajeve EDA-e u suradnji s EASO-om da bi se zadovoljili zahtjevi država članica za obrazovanjem, osposobljavanjem i vježbama u području kiberobrane;
- podupirati platformu ETEE u području kiberpitanja, među ostalim postupnim uključivanjem modula za obrazovanje, osposobljavanje, evaluaciju i vježbe u području kiberpitanja razrađenih u okviru EDA-e.

ESVD i države članice će:

- slijediti ustanovljene EASO-ove mehanizme certifikacije za programe osposobljavanja u bliskoj suradnji s relevantnim službama u institucijama, tijelima i agencijama EU-a na temelju postojećih standarda i znanja. razmotriti mogućnost uspostave posebnih modula iz kiberpodručja unutar okvira inicijative Vojni Erasmus.

Postoji potreba za poboljšanjem mogućnosti vježbi u području kiberobrane za vojne i civilne sudionike ZSOP-a. Zajedničke vježbe služe kao alat za razvoj zajedničkog znanja i razumijevanja kiberobrane. Time će se nacionalnim snagama omogućiti da pojačaju spremnost za djelovanje u multinacionalnom okružju. Održavanjem zajedničkih vježbi u području kiberobrane također se povećava interoperabilnost i povjerenje.

ESVD, EDA, CERT-EU i države članice usmjerit će se na promicanje elemenata kiberobrane u vježbama ZSOP-a kao i u drugim vježbama te će:

- integrirati dimenziju kiberobrane u postojeće scenarije vježbi za *MILEX* i *MULTILAYER*;
- redovito organizirati strateške/političke vježbe kao što su *CYBRID 2017*, u koordinaciji s usporednom i koordiniranom vježbom koju vodi EU (PACE), i tehničko-operativne vježbe poput *DEFNET-a*;
- razvijati, prema potrebi, namjenske vježbe EU-a u okviru ZSOP-a u području kiberobrane i istražiti mogućnost suradnje s paneuropskim vježbama u području kibersigurnosti poput *Cyber Europe* koju organizira ENISA;
- i dalje sudjelovati u drugim multinacionalnim vježbama iz područja kiberobrane, kao što je *Locked Shields*;
- pozivati relevantne međunarodne partnere na vježbe, poput NATO-a, u skladu s EU-ovim okvirom politike u području vježbi;
- organizirati redovite vježbe na temelju alata za kiberdiplomaciju na kojima države članice EU-a mogu vježbati reagiranje na zlonamjerne kiberaktivnosti.

6. Unapređivanje suradnje s relevantnim međunarodnim partnerima

U okviru međunarodne suradnje postoji potreba za osiguravanjem dijaloga s međunarodnim partnerima, posebno s NATO-om i drugim međunarodnim organizacijama, kako bi se pridonijelo razvoju djelotvornih sposobnosti kiberobrane. Trebalo bi raditi na pojačanom angažmanu u vezi s radom ostvarenim unutar okvira Organizacije za europsku sigurnost i suradnju (OESS) i Ujedinjenih naroda (UN) s ciljem daljeg razvoja strateškog okvira za sprečavanje sukoba, suradnju i stabilnost u kiberprostoru.

Postoji politička volja u EU-u za daljnjom suradnjom s NATO-om u području kiberobrane na razvoju jakih i stabilnih sposobnosti kiberobrane kako se zahtijeva Zajedničkom izjavom koju su predsjednik Europskog vijeća, predsjednik Europske komisije i glavni tajnik Organizacije sjevernoatlantskog ugovora potpisali 8. srpnja 2016. u Varšavi. Redovita savjetovanja među osobljem, uzajamno obavještavanje te mogući sastanci Skupine za političko-vojna pitanja i relevantnih odbora NATO-a pomoći će u izbjegavanju nepotrebna udvostručenja napora te jamčenju koherentnosti i komplementarnosti napora, u skladu s navedenim okvirom.

ESVD i EDA, zajedno s državama članicama, dalje će razvijati suradnju u području kiberobrane između EU-a i NATO-a poštujući institucijski okvir i autonomiju u donošenju odluka tih organizacija te će:

- pojačati aktualne aktivnosti u okviru provedbe Zajedničke izjave predsjednika Europskog vijeća, predsjednika Europske komisije i glavnog tajnika Organizacije sjevernoatlantskog ugovora;
- razmjenjivati najbolje prakse u upravljanju kriznim situacijama te u vojnim i civilnim misijama i operacijama u području kiberobrane;
- raditi na usklađenosti rezultata pri razvoju zahtjeva sposobnosti kiberobrane kada se oni preklapaju, a posebno pri razvoju sposobnosti kiberobrane na dulji rok;
- dalje primjenjivati okvir za suradnju EDA-e s NATO-ovim Centrom izvrsnosti za suradnju u području kiberobrane kao početnu platformu za pojačanu suradnju u multinacionalnim projektima kiberobrane, a na temelju odgovarajućih procjena.

EASO, ESVD i EDA će:

- unapređivati suradnju u konceptima osposobljavanja i obrazovanja u području kiberobrane te u vježbama;
- osiguravati uzajamno sudjelovanje osoblja u vježbama u skladu s dogovorenim okvirom.

CERT-EU će:

- dalje iskoristiti tehnički sporazum između CERT-EU-a i NCIRC-a (NATO-ove službe za odgovor na računalne incidente) kako bi se poboljšali svijest o stanju, razmjena informacija i mehanizmi ranog upozoravanja te predvidjele prijetnje koje bi mogle naštetiti objema organizacijama.

Što se tiče drugih međunarodnih organizacija i relevantnih međunarodnih partnera EU-a, ESVD i države članice će, po potrebi:

- slijediti strateški razvoj i savjetovati se u vezi s pitanjima kiberobrane s međunarodnim partnerima (međunarodnim organizacijama i trećim zemljama);
- istražiti mogućnosti suradnje u pitanjima kiberobrane, među ostalim s trećim zemljama koje sudjeluju u misijama i operacijama ZSOP-a;
- promicati u relevantnim međunarodnim organizacijama, a posebno u UN-u, OESS-u i Regionalnom forumu ASEAN-a, primjenu postojećeg međunarodnog prava, osobito Povelje UN-a u cjelini, razvoj i primjenu univerzalnih neobvezujućih normi za odgovorno postupanje država te regionalnih mjera za izgradnju povjerenja među državama kako bi se povećala transparentnost i smanjio rizik pogrešnog doživljavanja postupanja države.

Komisija i ESVD će:

- ako je to relevantno, podupirati izgradnju kibersposobnosti za partnere EU-a s pomoću izmijenjenog instrumenta za doprinos stabilnosti i miru.

Daljnje mjere

U okviru ESVD-ove koordinacije provedbe okvira za politiku kiberobrane ESVD/EDA/Komisija trebali bi godišnje izvješće o napretku koje sadrži šest spomenutih područja predstaviti Skupini za političko-vojna pitanja, uz sudjelovanje članova Horizontalne radne skupine za kiberpitanja, te Političkom i sigurnosnom odboru, kako bi se procijenila provedba okvira za politiku kiberobrane. Pružit će se i polugodišnja usmena prezentacija.

Od ključne je važnosti da se, ovisno o tome kako se kiberprijetnja razvija, utvrde nove potrebe za kiberobranom te potom uključe u okvir za politiku kiberobrane. Sljedeća revizija okvira za politiku kiberobrane trebala bi se predstaviti najkasnije do sredine 2022., uz blisko savjetovanje s državama članicama.