Svet
Evropske unije

Bruselj, 19. november 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

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Datum:	19. november 2018
Prejemnik:	delegacije
Zadeva:	Okvir EU za politiko kibernetske obrambe (posodobitev za leto 2018)

V prilogi vam pošiljamo okvir EU za politiko kibernetske obrambe (posodobitev za leto 2018), ki ga je Svet sprejel 19. novembra 2018 na 3652. seji.

PRILOGA

OKVIR EU ZA POLITIKO KIBERNETSKE OBRAMBE

(POSODOBITEV ZA LETO 2018)

Področje uporabe in cilji

Da bi se odzvale na spreminjajoče se varnostne izzive, morajo EU in njene države članice okrepiti kibernetsko odpornost ter razviti zanesljive zmogljivosti za kibernetsko varnost in obrambo.

Okvir EU za politiko kibernetske obrambe (v nadaljnjem besedilu: OPKO) podpira razvoj zmogljivosti držav članic EU za kibernetsko obrambo in krepitev kibernetske zaščite varnostne in obrambne infrastrukture EU brez poseganja v nacionalno zakonodajo držav članic in zakonodajo EU, vključno s področjem uporabe kibernetske obrambe, če je to opredeljeno.

Kibernetski prostor je peto področje dejavnosti, poleg področja kopnega, morja, zraka in vesolja: uspešno izvajanje misij in operacij EU je vse bolj odvisno od nemotenega dostopa do varnega kibernetskega prostora, za kar so potrebne zanesljive in odporne kibernetske operativne zmogljivosti.

Cilj posodobljenega OPKO je nadaljnji razvoj politike kibernetske obrambe EU ob upoštevanju ustreznih premikov v drugih zadevnih forumih in na področjih politike ter izvajanja OPKO od leta 2014. V OPKO so opredeljena prednostna področja kibernetske obrambe in pojasnjene vloge različnih evropskih akterjev ob polnem spoštovanju odgovornosti in pristojnosti akterjev Unije in držav članic, pa tudi institucionalnega okvira EU in njene avtonomije pri odločanju.

Ozadje

Evropski svet in Svet sta v sklepih o SVOP iz decembra 2013 oziroma novembra 2013 na podlagi predloga visokega predstavnika pozvala k oblikovanju okvira EU za politiko kibernetske obrambe v sodelovanju z Evropsko komisijo in Evropsko obrambno agencijo (EDA). Svet je 18. novembra 2014 sprejel okvir EU za politiko kibernetske obrambe[1], od takrat pa so konkretni dosežki pri njegovem izvajanju prispevali k znatni okrepitvi zmogljivosti držav članic za kibernetsko obrambo. Izhajajoč iz letnega poročila o izvajanju okvira za politiko kibernetske obrambe za leto 2017[2] in ob upoštevanju pobud EU na varnostnem in obrambnem področju, zlasti usklajenega letnega pregleda na področju obrambe (CARD), stalnega strukturnega sodelovanja (PESCO), Evropskega obrambnega sklada (EDF) in pakta o civilnih vidikih SVOP ter revidiranega načrta za razvoj zmogljivosti za leto 2018 in načrta za razvoj civilnih zmogljivosti, so države članice pozvale k posodobitvi okvira EU za politiko kibernetske obrambe.

Kibernetska varnost je prednostna naloga v okviru globalne strategije EU za zunanjo in varnostno politiko ter ravni ambicij EU[3]. V globalni strategiji je poudarjena potreba po povečanju zmogljivosti za zaščito EU in njenih državljanov ter odzivanje na zunanje krize. Izpostavljena je tudi potreba po okrepitvi EU kot varnostne skupnosti. Glede na to bi bilo treba s prizadevanji na varnostnem in obrambnem področju okrepiti tudi strateško vlogo in sposobnost EU, da ukrepa avtonomno, če in kadar je to potrebno, po možnosti v sodelovanju s partnerji. Ti cilji zahtevajo boljše sodelovanje pri razvoju zmogljivosti, pri čemer se spodbujata učinkovitost in interoperabilnost tako razvitih civilnih in vojaških zmogljivosti.

---

1 Dokument Sveta 15585/14, 18. 11. 2014.
2 Dokument Sveta 15870/17, 19. 12. 2017.
3 Sklepi Sveta o izvajanju globalne strategije EU na področju varnosti in obrambe, 14. 11. 2016.

Skupni sklop predlogov za izvajanje skupne izjave, ki so jo 8. julija 2016 v Varšavi podpisali predsednik Evropskega sveta, predsednik Evropske komisije in generalni sekretar Organizacije Severnoatlantske pogodbe[4], vsebuje tudi konkretne ukrepe za razširitev sodelovanja EU in NATO pri kibernetski varnosti in obrambi, tudi v okviru misij in operacij, pa tudi v povezavi z razvojem zmogljivosti kibernetske obrambe, raziskavami in tehnologijo, usposabljanjem, izobraževanjem, vajami in vključevanjem kibernetskih vidikov v krizno upravljanje. Sodelovanja poteka ob popolnem spoštovanju načel odprtosti, preglednosti, vključevanja, vzajemnosti in avtonomnega odločanja EU. Tehnični dogovor med skupino EU za odzivanje na računalniške grožnje (CERT-EU) in službo zveze NATO za odzivanje na incidente na področju računalniške varnosti, ki je bil podpisan februarja 2016, lajša izmenjavo tehničnih informacij, da bi izboljšali preprečevanje in odkrivanje kibernetskih incidentov ter odziv nanje v obeh organizacijah.

Treba je opozoriti, da k uresničevanju ciljev politike kibernetske obrambe, določenih v tem dokumentu, prispevajo različne politike EU in da se v tem okviru upošteva tudi ustrezna regulativna, politična in tehnološka podpora na civilnem področju. Na primer, Evropski parlament in Svet sta julija 2016 sprejela direktivo o varnosti omrežij in informacij[5], s katero se bo izboljšala splošna pripravljenost držav članic na kibernetske grožnje ter okrepilo sodelovanje na ravni EU. Ta direktiva določa ukrepe za doseganje visoke skupne ravni varnosti omrežij in informacijskih sistemov v Uniji, da bi izboljšali delovanje notranjega trga. Rok za prenos te direktive je bil 9. maj 2018.

---

4 Sklepi Sveta o izvajanju Skupne izjave predsednika Evropskega sveta, predsednika Evropske komisije in generalnega sekretarja Organizacije Severnoatlantske pogodbe (6. december 2016, 15283/16; 5. december 2017, 14802/17).

5 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, UL L 194, 19.7.2016, str. 1.

V predlog za uredbo EU o kibernetski varnosti iz septembra 2017 je vključen nov mandat za Agencijo EU za kibernetsko varnost (ENISA) in vzpostavitev vseevropskega okvira za certificiranje. Okvir za certificiranje naj bi, potem ko bo vzpostavljen, podpiral visoke standarde za postopke, izdelke in storitve IKT, poleg tega naj bi doprinesel h konkurenčni prednosti ter večjemu zaupanju potrošnikov in naročnikov. Komisija je poleg tega septembra 2017 sprejela še en ukrep, s katerim naj bi EU pripravili na velike čezmejne kibernetske incidente („načrt“), in sedaj skupaj z državami članicami in drugimi institucijami, agencijami in organi razvija evropsko sodelovanje na področju kibernetskih kriz, pri čemer se vzpostavlja praktično delovanje in dokumentiranje vseh zadevnih akterjev, procesov in postopkov v okviru obstoječih mehanizmov EU za krizno upravljanje in mehanizmov obvladovanja nesreč, zlasti ureditev za enotno politično odzivanje na krize.

V sklepih Sveta o krepitvi evropske kibernetske odpornosti iz novembra 2016 je bil orisan skupni cilj prispevanja k strateški avtonomnosti EU, kot je bil naveden v sklepih Sveta iz novembra 2016 o globalni strategiji za zunanjo in varnostno politiko Evropske unije, tudi v kibernetskem prostoru. Evropski svet je to sporočilo junija 2018 znova potrdil in še poudaril, da je treba okrepiti zmogljivosti za odziv na kibernetske grožnje iz držav zunaj EU.

Svet je leta 2017 sprejel okvir za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“)[6], ki naj bi spodbudil sodelovanje, omogočil zmanjšanje groženj in vplival na vedenje morebitnih napadalcev na dolgi rok. Na podlagi tega okvira se za preprečevanje zlonamernih kibernetskih dejavnosti in odziv nanje uporabljajo ukrepi SZVP, vključno z omejevalnimi ukrepi. Storilci zlonamernih kibernetskih dejavnosti morajo zanje odgovarjati, države članice EU pa so pozvane k nadaljnjemu razvoju zmožnosti, da se na takšne dejavnosti odzovejo usklajeno ob upoštevanju zbirke orodij za kibernetsko diplomacijo. Države ne bi smele izvajati ali namenoma podpirati dejavnosti informacijske in komunikacijske tehnologije, ki so v nasprotju z njihovimi obveznostmi po mednarodnem pravu, in ne bi smele zavestno dopustiti, da se z uporabo informacijske in komunikacijske tehnologije na njihovem ozemlju krši mednarodno pravo.

Komisija in VP/PP sta septembra 2017 predstavili skupno sporočilo[7] o kibernetski varnosti, da bi ublažili tveganja, ki izhajajo iz novih groženj. V tem sporočilu je kibernetska obramba navedena kot eno glavnih področij ukrepanja, OPKO pa kot eden od stebrov njenega konkretnega izvajanja[8].

Svet je v sklepih iz novembra 2017 o kibernetskih vprašanjih priznal vse tesnejšo povezanost med kibernetsko varnostjo in obrambo ter pozval k pospešitvi sodelovanja pri kibernetski obrambi, tudi s spodbujanjem sodelovanja med civilnimi in vojaškimi akterji, ki se odzivajo na incidente. Poudaril je tudi, da bi posebno hud kibernetski incident ali kriza lahko bila zadosten razlog, da država članica uveljavi solidarnostno klavzulo EU in/ali klavzulo o vzajemni pomoči.

---

6 Sklepi Sveta o okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“), 9916/17, 7. junij 2017.

7 Skupno sporočilo Evropskemu parlamentu in Svetu: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“ (13. september 2017, JOIN (2017) 450 final).

8 Sklepi Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU (20. november 2017, 14435/17)“.

11. decembra 2017 je bilo vzpostavljeno stalno strukturno sodelovanje (PESCO). Ta ambiciozen, zavezujoč in vključujoč okvir sodelovanja vključuje 25 držav članic, vsebuje pa tudi zavezo za povečanje prizadevanj v okviru sodelovanja pri kibernetski obrambi in tudi pri zadevnih projektih PESCO. Prvi sklop projektov PESCO, ki so jih leta 2017 določile države članice, sodelujoče pri PESCO, vključuje dva projekta, ki sta povezana s kibernetsko obrambo in se nanašata na „enote za hitro odzivanje na kibernetske grožnje in medsebojno pomoč na področju kibernetske varnosti“ in „platformo za izmenjavo informacij v zvezi s kibernetskimi grožnjami in odzivanjem na incidente“. Predvideni so še drugi sklopi projektov PESCO. V okviru PESCO se bodo razvijale zmogljivosti kibernetske obrambe, s čimer se bo krepilo sodelovanje med sodelujočimi državami članicami in povečala interoperabilnost.

V posodobljenem načrtu za razvoj zmogljivosti EU, ki ga je junija 2018 potrdil usmerjevalni odbor EDA, je kibernetska obramba označena kot ključni element, pri čemer se priznava potreba po obrambnih kibernetskih operacijah v vseh operativnih kontekstih, na podlagi dobro razvitega spremljanja trenutnih razmer v kibernetskem prostoru z možnostjo predvidevanja dogodkov, vključno s sposobnostjo kombiniranja velikih količin podatkov in obveščevalnih informacij iz številnih virov za podporo hitremu odločanju ter z večjo avtomatizacijo procesov zbiranja in analiziranja podatkov ter podpore odločanju. V načrtu za razvoj zmogljivosti za leto 2018 so v zvezi z zmogljivostmi za kibernetsko obrambo opredeljene prednostne naloge na naslednjih področjih: sodelovanje in sinergije z ustreznimi akterji na vseh področjih kibernetske obrambe in kibernetske varnosti; raziskave in tehnologija na področju kibernetske obrambe; okviri sistemskega inženiringa za kibernetske operacije; izobraževanje, usposabljanje, vaje in ocenjevanje; reševanje izzivov na področju kibernetske obrambe v zraku, vesolju, na morju in kopnem.

Poleg tega se je v zadnjih nekaj letih pojavila potreba, da mednarodna skupnost preprečuje konflikte v kibernetskem prostoru, sodeluje in stabilizira kibernetski prostor. EU v tesnem sodelovanju z drugimi mednarodnimi organizacijami, zlasti z ZN, OVSE in regionalnim forumom ASEAN, spodbuja strateški okvir za preprečevanje konfliktov, sodelovanje in stabilnost v kibernetskem prostoru, ki vključuje: (i) uporabo mednarodnega prava, zlasti vseh določb Ustanovne listine ZN, v kibernetskem prostoru; (ii) spoštovanje univerzalnih nezavezujočih standardov, pravil in načel odgovornega ravnanja držav; (iii) razvoj in izvajanje regionalnih ukrepov za krepitev zaupanja. Ta prizadevanja bi moral podpreti tudi okvir politike kibernetske obrambe.

Prednostne naloge

V posodobljenem OPKO je določenih šest prednostnih področij. Glavni poudarek tega okvira politike je na razvoju zmogljivosti kibernetske obrambe ter na zaščiti komunikacijskih in informacijskih omrežij EU za SVOP. Druga prednostna področja so med drugim usposabljanje in vaje, raziskave in tehnologija, civilno-vojaško sodelovanje in mednarodno sodelovanje. Na področju usposabljanja je poudarek na nadgradnji usposabljanja v državah članicah na področju kibernetske obrambe in usposabljanja na področju kibernetske ozaveščenosti v liniji poveljevanja SVOP. Pomembno je tudi, da se kibernetska razsežnost ustrezno obravnava v vajah, da bi z izboljšanjem postopkov odločanja in razpoložljivosti informacij izboljšali zmožnost EU za odzivanje na kibernetske in hibridne krize. Kibernetski prostor se hitro razvija, zato je treba podpirati nov tehnološki razvoj na civilnem in vojaškem področju. Civilno-vojaško sodelovanje na kibernetskem področju je ključno za usklajen odziv na kibernetske grožnje. Okrepljeno sodelovanje z mednarodnimi partnerji bi navsezadnje lahko pripomoglo tudi k boljši kibernetski varnosti v EU in zunaj nje ter k uveljavljanju načel in vrednot EU.

V tem okviru so navedeni predlogi in možnosti za usklajevanje med ustreznimi institucijami, organi in agencijami EU. Upoštevana je tudi pomembna vloga zasebnega sektorja za razvoj tehnologij na področju kibernetske varnosti in kibernetske obrambe.

V OPKO se poleg tega dodatno podpira vključevanje kibernetske obrambe v mehanizme kriznega upravljanja Unije z namenom obvladovanja posledic kibernetskih kriz, pri čemer se lahko uporabljajo ustrezne določbe Pogodbe o EU in Pogodbe o delovanju EU[9].

1. Podpiranje razvoja zmogljivosti kibernetske obrambe v državah članicah

Pri razvoju zmogljivosti in tehnologij kibernetske obrambe bi morali upoštevati vse vidike razvoja zmogljivosti, vključno z doktrino, vodenjem, organizacijo, osebjem, usposabljanjem, industrijo, tehnologijo, infrastrukturo, logistiko in interoperabilnostjo. V ta namen bi morale države članice okrepiti prizadevanja za razvoj učinkovitih zmogljivosti kibernetske obrambe. ESZD, Komisija in EDA bi morale sodelovati in podpreti ta prizadevanja.

Potrebno je stalno ocenjevanje šibkih točk informacijskih infrastruktur, ki podpirajo misije in operacije v okviru SVOP, hkrati z razumevanjem učinkovitosti zaščite v skoraj realnem času. Z operativnega stališča bo eno od glavnih prednostnih področij dejavnosti kibernetske obrambe ohranjanje dostopnosti, celovitosti in zaupnosti komunikacijskih in informacijskih omrežij SVOP, razen če je v mandatu operacij ali misij določeno drugače. Poleg tega bo ESZD v sodelovanju z državami članicami še dodatno vključevala kibernetske zmogljivosti v misije in operacije v okviru SVOP.

Storilci zlonamernih kibernetskih dejavnosti morajo zanje odgovarjati. Pri tem je pomembno, da države članice EU ob podpori ESZD spodbujajo vzajemno sodelovanje pri odzivanju na zlonamerne kibernetske dejavnosti. Da bi pripomogli k takšnemu vzajemnemu odzivu, je bila razvita zbirka orodij za kibernetsko diplomacijo. ESZD in EDA bosta na podlagi te zbirke organizirali redne vaje, v okviru katerih se bodo države članice EU lahko urile na tem področju.

[9] Člen 222 PDEU in člen 42(7) PEU ob ustreznem upoštevanju člena 17 PEU.

Glede na to, da je področje uporabe kibernetske obrambe v nacionalnih zakonodajah držav članic in v zakonodaji EU široko in razvejano, v primeru ko in če je opredeljeno, obstaja potreba, da se oblikuje skupno razumevanje področja uporabe kibernetske obrambe.

Ker so vojaške operacije v okviru SVOP odvisne od infrastrukture poveljevanja, kontrole, komunikacij in računalnikov (C4), ki jo zagotavljajo države članice, je pri načrtovanju zahtev s področja kibernetske obrambe za informacijsko infrastrukturo potrebna določena stopnja strateške konvergence.

EDA in države članice bodo na podlagi dela projektne skupine EDA za kibernetsko obrambo z namenom razvoja zmogljivosti kibernetske obrambe:

- uporabljale načrt za razvoj zmogljivosti in druge instrumente, na primer CARD, s katerimi se olajšuje in podpira sodelovanje med državami članicami, da bi izboljšale stopnjo konvergence pri načrtovanju zahtev držav članic s področja kibernetske obrambe na strateški ravni, zlasti na področju spremljanja, poznavanja razmer, preprečevanja, odkrivanja in zaščite, izmenjave informacij, forenzike in zmogljivosti za analizo zlonamerne programske opreme, pridobljenih izkušenj, omejevanja škode, zmogljivosti za dinamično obnovitev, porazdeljenega shranjevanja podatkov in varnostnega kopiranja podatkov;
- podpirale obstoječe in prihodnje projekte združevanja in skupne uporabe, ki so povezani s kibernetsko obrambo, za vojaške operacije (npr. na področju forenzike, razvoja interoperabilnosti, določanja standardov);
- ob uporabi že pridobljenih izkušenj iz celotne EU razvile standardni nabor ciljev in zahtev, s katerimi bi opredelili najmanjšo raven kibernetske varnosti in zaupanja, ki jo morajo doseči države članice.

ESZD in EDA bosta:

- olajšali izmenjave med državami članicami na področju nacionalnih doktrin kibernetske obrambe ter v kibernetsko obrambo usmerjenih programov zaposlovanja, zadrževanja in rezervistov.

EDA bo:

- v študiji preučila različna področja uporabe vojaških zahtev s področja kibernetske obrambe v nacionalnih zakonodajah držav članic ter najboljše prakse. Glavni cilj študije bo razvoj arhitekture podjetja za kibernetsko obrambo, ki bo vključevala področje uporabe, funkcionalnosti in zahteve, ki se uporabljajo na tem področju v državah članicah na podlagi nacionalnih zakonodaj in zakonodaje EU.

Države članice bodo prostovoljno:

- okrepile sodelovanje med vojaškimi skupinami CERT, da bi izboljšali preprečevanje in obravnavanje incidentov;
- izkoristile možnosti PESCO, da bi dodatno okrepili sodelovanje pri kibernetski obrambi, tudi pri novih projektih;
- izkoristile možnosti Evropskega obrambnega sklada, da bi skupaj razvijali zmogljivosti kibernetske obrambe;
- oblikovale skupno razumevanje uporabe klavzule o vzajemni pomoči na kibernetskem področju ob ohranitvi njene prožnosti;
- oblikovale osnovne zahteve s področja kibernetske varnosti za informacijsko infrastrukturo;
- kolikor je izboljšanje zmogljivosti kibernetske obrambe odvisno od civilnega strokovnega znanja s področja varnosti omrežij in informacij, izkoristile strokovno znanje agencije ENISA, organov držav članic v okviru skupine za sodelovanje glede varnosti omrežij in informacij ter drugih morebitnih subjektov na ravni EU, ki imajo strokovno znanje s področja civilne kibernetske varnosti.

Države članice, ESZD/Vojaški štab EU, ESZD in EDA bodo:

- razmislili o razvoju usposabljanja s področja kibernetske obrambe v luči certificiranja bojnih skupin EU.

Komisija bo v sodelovanju z državami članicami:

- upoštevala kibernetsko obrambo v delovnih programih evropskega programa za razvoj obrambne industrije oziroma Evropskega obrambnega sklada.

2. Izboljšanje zaščite komunikacijskih in informacijskih sistemov SVOP, ki jih uporabljajo subjekti EU

ESZD bo v okviru ustreznih pravil glede proračuna Unije brez poseganja v vlogo skupine za odzivanje na računalniške grožnje za institucije, organe in agencije EU (CERT-EU) kot osrednje strukture EU za usklajevanje odzivanja na kibernetske incidente za vse institucije, organe in agencije Unije oblikovala ustrezno in avtonomno razumevanje varnostnih vprašanj in vprašanj obrambe omrežja ter razvila lastno sposobnost za zagotavljanje informacijske varnosti. Prizadevala si bo za izboljšanje zanesljivosti svojih omrežij SVOP, pri tem pa se osredotočila na preprečevanje, odkrivanje, odzivanje na incidente, poznavanje razmer, izmenjavo informacij in mehanizme zgodnjega opozarjanja.

Za zaščito komunikacijskih in informacijskih sistemov ESZD ter razvoj sposobnosti za zagotavljanje informacijske varnosti skrbi generalni direktorat ESZD za proračun in upravo. Dodatna namenska sredstva in podporo bodo zagotavljali še Vojaški štab Evropske unije (VŠEU), direktorat za krizno upravljanje in načrtovanje (CMPD) ter civilna zmogljivost za načrtovanje in izvajanje operacij (CPCC). Sposobnost za zagotavljanje informacijske varnosti bo zajemala tako tajne sisteme kot tiste, ki niso tajni, in bo sestavni del obstoječih operativnih subjektov.

Prav tako je treba posodobiti varnostna pravila za informacijske sisteme, ki jih zagotavljajo različni institucionalni akterji EU med izvajanjem misij in operacij v okviru SVOP. V tej zvezi bi lahko razmislili o enotni liniji poveljevanja, da bi izboljšali zanesljivost omrežij, ki se uporabljajo za SVOP.

Za boljše usklajevanje ter okrepitev zaščite in odpornosti komunikacijskih in informacijskih sistemov in omrežij SVOP je bil leta 2017 ustanovljen notranji odbor ESZD za kibernetsko upravljanje, ki deluje pod okriljem generalne sekretarke ESZD.

ESZD/generalni direktorat za proračun in upravo bo:

- na podlagi obstoječih tehničnih zmogljivosti in postopkov izboljšal zmogljivosti za zagotavljanje informacijske varnosti znotraj ESZD, pri tem pa se osredotočil na preprečevanje, odkrivanje, odzivanje na incidente, poznavanje razmer, izmenjavo informacij in mehanizme zgodnjega opozarjanja. Dodatno bo okrepljena strategija sodelovanja s CERT-EU in obstoječimi zmogljivostmi EU za kibernetsko varnost.

ESZD/generalni direktorat za proračun in upravo bo skupaj z VŠEU, vojaško zmogljivostjo za načrtovanje in izvajanje (MPCC), CMPD in CPCC:

- razvil skladno politiko in smernice za informacijsko varnost, pri tem pa upošteval tudi tehnične zahteve za kibernetsko obrambo za strukture, misije in operacije v okviru SVOP ter obstoječe okvire in politike sodelovanja znotraj EU z namenom zbližanja pravil, politik in organizacije.

ESZD/Enotna zmogljivost za analizo obveščevalnih podatkov (SIAC) bo:

- na podlagi obstoječih struktur okrepila zmogljivosti za oceno kibernetske ogroženosti in obveščevalne zmogljivosti za prepoznavanje novih kibernetskih tveganj ter izvajala redne ocene tveganj na podlagi strateške ocene ogroženosti in informacij o incidentih v skoraj realnem času, ki bi se uskladile med ustreznimi strukturami EU in bile dane na voljo pod različnimi stopnjami tajnosti.

ESZD/SIAC in skupina CERT-EU bosta:

- spodbujali izmenjavo informacij o kibernetski ogroženosti v realnem času med državami članicami in ustreznimi subjekti EU. V ta namen bodo oblikovani mehanizmi za izmenjavo informacij in ukrepi za krepitev zaupanja med ustreznimi nacionalnimi in evropskimi organi, in sicer na prostovoljni osnovi na podlagi obstoječega sodelovanja.

ESZD/VŠEU in MPCC bosta:

- dodatno razvila koncept kibernetske obrambe za vojaške misije in operacije v okviru SVOP ter ga vključila v načrtovanje na strateški ravni;
- v sodelovanju z operativnimi štabi razvila generični standardni postopek na operativni ravni na področju kibernetske obrambe.

ESZD/CPCC in CMPD bosta:

- dodatno razvili koncept kibernetske obrambe za civilne misije v okviru SVOP ter ga vključili v strateško načrtovanje;
- okrepili zmogljivosti kibernetske obrambe civilnih misij v okviru SVOP, in sicer na podlagi obstoječe infrastrukture ter ob spodbujanju standardizacije in harmonizacije tehnologije, ki se uporablja v misijah in operacijah SVOP, pri tem pa se po potrebi oprli na strokovno znanje skupine CERT-EU ter agencij ENISA in EDA;
- v procesu krepitve civilnih vidikov SVOP nadalje preučili možnost, da bi s civilnimi misijami v okviru SVOP zagotovili podporo državam gostiteljicam na področju kibernetske varnosti.

ESZD bo:

- poskrbela za nadaljnji razvoj skupnih zahtev za vojaške in civilne misije in operacije v okviru SVOP;
- okrepila usklajevanje na področju kibernetske obrambe z namenom izvajanja ciljev, povezanih z zaščito omrežij, ki jih uporabljajo institucionalni akterji EU, ki podpirajo SVOP, ter se pri tem oprla na izkušnje iz celotne EU;
- ob posvetovanju z državami članicami in drugimi institucijami EU redno pregledovala potrebe po virih in druge pomembne politične odločitve na podlagi spreminjajočih se razmer ogroženosti.

3. Spodbujanje civilno-vojaškega sodelovanja

Kibernetski prostor je hitro razvijajoče se področje: tehnološki razvoj je treba okrepiti z varnostnimi sistemi na civilnem in vojaškem področju. Predvideti bi bilo treba čim večje usklajevanje med civilno in vojaško domeno v primerih, ko podoben tehnološki razvoj ponuja rešitve za civilno in vojaško uporabo. V drugih primerih so vojaške zmogljivosti in orožni sistemi tako specifični, da ni možnosti za izmenjavo s civilnimi tehnologijami. Brez poseganja v notranjo organizacijo in zakonodajo držav članic bi lahko o civilno-vojaškem sodelovanju na kibernetskem področju razmislili med drugim pri izmenjavi najboljših praks in informacij, mehanizmih zgodnjega opozarjanja, ocenjevanju tveganja pri odzivanju na incidente in ozaveščanju ter pri izvajanju usposabljanja in vaj.

Izboljšanje civilne kibernetske varnosti je pomemben dejavnik, ki prispeva k splošni trdnosti omrežne in informacijske varnosti. Direktiva o varnosti omrežij in informacij povečuje pripravljenost na nacionalni ravni ter krepi strateško in operativno sodelovanje med državami članicami na ravni Unije. To sodelovanje vključuje tako nacionalne organe, pristojne za politike kibernetske varnosti, kot nacionalne skupine CERT in skupino CERT-EU. Sodelovanje med civilnimi in vojaškimi skupinami CERT bi bilo treba okrepiti z upoštevanjem teh sprememb. Novi evropski akt o kibernetski varnosti je namenjen izboljšanju evropske odpornosti na kibernetske napade in zagotovitvi okvira certificiranja za kibernetsko varnost za izdelke in storitve, s čimer bi se povečalo zaupanje v civilnem digitalnem okolju.

EDA, Agencija Evropske unije za varnost omrežij in informacij (ENISA), Evropski center za boj proti kibernetski kriminaliteti (EC3) in skupina CERT-EU, skupaj z drugimi ustreznimi telesi in agencijami EU v okviru svojih pooblastil in brez prekrivanja s pristojnostmi držav članic, ter države članice, naj še okrepijo svoje sodelovanje na naslednjih področjih:

- razvoj skupnih profilov usposobljenosti za področje kibernetske varnosti in obrambe na podlagi najboljših mednarodnih praks in certificiranja, ki se uporablja v institucijah, organih in agencijah EU, pri čemer se upoštevajo tudi standardi zasebnega sektorja za certificiranje;
- prispevajo k nadaljnjemu razvoju organizacijskih in tehničnih standardov javnega sektorja za kibernetsko varnost in obrambo ter njihovi prilagoditvi za uporabo v obrambnem in varnostnem sektorju, po potrebi ob opiranju na tekoče delo agencij ENISA in EDA;
- vzpostavijo ali nadaljnje razvijejo mehanizme in ureditve za izmenjavo najboljše prakse, zlasti glede izobraževanja, usposabljanja in vaj ter na področjih raziskav, tehnologije in drugih področjih za zagotavljanje civilno-vojaških sinergij;
- uporabijo pridobljene izkušnje EU na področju preprečevanja in preiskovanja kibernetske kriminalitete ter zmogljivosti kibernetske forenzike, te pa v večji meri upoštevajo pri razvoju zmogljivosti kibernetske obrambe.

Države članice bodo prostovoljno:

- okrepile sodelovanje med civilnimi in vojaškimi skupinami CERT med državami članicami.

ESZD, Komisija in države članice bodo:

- kibernetsko obrambo vključevale v postopke EU za obvladovanje kriz in nesreč (proces „načrta“).

4. Raziskave in tehnologija

Upravitelji infrastrukture in storitev IKT za civilne in obrambne namene se zaradi skupne tehnologije in zahtev glede operativne zmogljivosti soočajo s podobnimi izzivi na področju kibernetske varnosti. Skupne potrebe na področju raziskav in tehnologije ter skupne sistemske zahteve naj bi dolgoročno izboljšale interoperabilnost sistemov ter zmanjšale stroške razvoja rešitev. Nujno je doseči ekonomijo obsega, da bi se lahko soočili z naraščajočim številom groženj in šibkih točk. To bi moralo posledično omogočiti ohranitev in rast konkurenčne industrije kibernetske varnosti v Evropi.

Raziskave in tehnologija so pomembna razsežnost razvoja zmogljivosti kibernetske obrambe. EDA je v okviru raziskovalnega programa za kibernetsko obrambo zagotovila trdno podlago za prednostno razvrstitev prihodnjega financiranja na področju raziskav in tehnologije v medvladnem okviru. Nadaljnji strateški raziskovalni program, ki so ga razvile zadevne ad hoc delovne skupine EDA zagotavlja na podlagi informacij temelječo prednostno razvrstitev kibernetskih tehnologij, potrebnih za vojaško rabo, pri čemer se opredelijo možnosti za dvojno rabo in naložbe, financirane na nacionalni, večnacionalni ali evropski ravni.

Za ublažitev groženj in šibkih točk je nujen razvoj tehnoloških zmogljivosti v Evropi. Industrija bo še naprej glavna gonilna sila tehnologij in inovacij, povezanih s kibernetsko obrambo. Kriptografija, varni vgrajeni sistemi, odkrivanje zlonamerne programske opreme, tehnike simulacije in vizualizacije, zaščita omrežij in komunikacijskih sistemov ter tehnologije za identifikacijo in avtentikacijo so med področji, ki jih je treba obravnavati. Pomembno je tudi spodbuditi konkurenčno evropsko industrijsko dobavno verigo za kibernetsko varnost s podpiranjem vključevanja malih in srednjih podjetij (MSP).

Ali bo Evropa lahko v koraku z mednarodnimi tekmeci, kar zadeva kibernetske tehnološke zmogljivosti, je odvisno tudi od naše sposobnosti, da prek instrumentov na nacionalni in na EU ravni, kot je evropski svet za inovacije, spodbujamo prelomne inovacije.

Da bi olajšali civilno-vojaško sodelovanje pri razvoju zmogljivosti kibernetske obrambe, okrepili tehnološko in industrijsko bazo evropske obrambe[10] in prispevali k strateški avtonomiji EU tudi v kibernetskem prostoru, če in kadar je to potrebno ter s partnerji, kadar je to mogoče,

bodo EDA, Komisija in države članice:

- skušale doseči sinergije med prizadevanji na področju raziskav in tehnologije v vojaškem sektorju ter civilnimi raziskovalnimi in razvojnimi programi, zlasti tistimi, ki so povezani s prelomnimi inovacijami, ter pri izvajanju pripravljalnih ukrepov o raziskavah na področju obrambe upoštevale razsežnost kibernetske varnosti in obrambe;
- izmenjevale programe raziskav na področju kibernetske varnosti (kot je strateški program raziskav za kibernetsko varnost Evropske obrambne agencije) ter iz tega izhajajoče časovne načrte in ukrepe. V ta namen bo v tesnem sodelovanju s Komisijo in državami članicami razvit medsektorski program raziskav na področju kibernetske obrambe;
- prispevale k boljšemu vključevanja vidikov kibernetske varnosti in kibernetske obrambe v programe z razsežnostjo dvojne rabe na varnostnem in obrambnem področju, kot je program za raziskave o upravljanju zračnega prometa enotnega evropskega neba (SESAR).

[10] Sporočilo „Za konkurenčnejši in učinkovitejši obrambni in varnostni sektor“, COM (2013) 542.

Komisija bo:

- razmislila o ustanovitvi evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost z mrežo nacionalnih koordinacijskih centrov, da bi tako podprli tehnološke in industrijske zmogljivosti na področju kibernetske varnosti in povečali konkurenčnost industrije za kibernetsko varnost v Uniji, zagotovili komplementarnost in se izognili podvajanju v okviru mreže strokovnih centrov za kibernetsko varnost in z drugimi agencijami EU. Center bi moral med drugim okrepiti sodelovanje med civilnimi in obrambnimi tehnologijami in aplikacijami, in sicer v tesnem sodelovanju in popolnem dopolnjevanju z Evropsko obrambno agencijo na področju kibernetske obrambe;
- podpirala oblikovanje industrijskih ekosistemov in inovacijskih grozdov v okviru celotne verige dodane vrednosti na področju varnosti z opiranjem na akademsko znanje, inovacije MSP in industrijsko proizvodnjo;

Komisija bo v sodelovanju z državami članicami:

- v razpisih pripravljalnih ukrepov o raziskavah na področju obrambe upoštevala vprašanja kibernetske obrambe;
- v okviru področij iz evropskega obrambnega sklada upoštevala kibernetsko obrambo;
- podpirala usklajenost politik EU za zagotovitev, da bodo politični in tehnični vidiki kibernetske zaščite EU še naprej v ospredju tehnoloških inovacij in usklajeni po vsej EU (zmogljivost za analiziranje in ocenjevanje kibernetskih groženj, pobude za „vgrajeno varnost“, obvladovanje odvisnosti v zvezi z dostopom do tehnologije itd.);

5. Izboljšanje možnosti za izobraževanje, usposabljanje in vaje

Da bi se povečala pripravljenost za obvladovanje kibernetskih groženj in vzpostavila skupna kultura kibernetske obrambe v vsej EU, ki bo koristila tudi misijam in operacijam EU, je treba izboljšati in razširiti možnosti za usposabljanje na področju kibernetske obrambe. Bistveno je, da se proračuni za izobraževanje in usposabljanje uporabijo učinkovito, hkrati pa se zagotovi čim boljša kakovost. Združevanje in souporaba zmogljivosti za izobraževanje in usposabljanje na področju kibernetske obrambe na evropski ravni bosta ključnega pomena.

Evropska akademija za varnost in obrambo (EAVO), ESZD, EDA, Komisija in države članice bodo:

- na podlagi analize EDA glede potreb po usposabljanju na področju kibernetske obrambe in izkušenj, pridobljenih pri usposabljanju o kibernetski varnosti v okviru EAVO, vzpostavile usposabljanje in izobraževanje v okviru SVOP za različne ciljne skupine, tudi ESZD, osebje misij in operacij v okviru SVOP ter uradnike držav članic, pri čemer bi bilo treba obravnavati tudi vprašanje zadržanja usposobljenega osebja v kratkoročnem, srednjeročnem in dolgoročnem obdobju;
- predlagale vzpostavitev dialoga na področju kibernetske obrambe o standardih usposabljanja in certificiranja z državami članicami, institucijami EU, tretjimi državami in drugimi mednarodnimi organizacijami, pa tudi zasebnim sektorjem;
- sodelovale z evropskimi ponudniki usposabljanja iz zasebnega sektorja in akademskimi ustanovami, da bi se izboljšale kompetence in strokovno znanje osebja, ki sodeluje v misijah in operacijah v okviru SVOP.

EAVO bo:

- nadalje razvijala svojo platformo za kibernetsko izobraževanje, usposabljanje, ocenjevanje in kibernetske vaje;
- ustvarila sinergije s programi usposabljanja drugih deležnikov, kot so ENISA, Europol, Evropska policijska akademija (CEPOL) in Natov Center odličnosti za sodelovanje pri kibernetski obrambi;
- preučila možnost skupnih programov usposabljanja EAVO in Nata na področju kibernetske obrambe, pri katerih bi lahko sodelovale vse države članice EU, da bi se spodbudila skupna kultura kibernetske obrambe.

Komisija bo:

- ocenila, ali je mogoče razširiti možnosti za usposabljanje in izobraževanje v državah članicah, identificiranih v okviru platforme za kibernetsko izobraževanje, usposabljanje, ocenjevanje in kibernetske vaje.

EDA bo:

- v sodelovanju z EAVO pripravila nadaljnje tečaje EDA, da bi lahko zadostila potrebam držav članic po izobraževanja, usposabljanju in vajah na področju kibernetske obrambe;
- podpirala platformo za kibernetsko izobraževanje, usposabljanje, ocenjevanje in kibernetske vaje, med drugim s postopnim vključevanjem modulov kibernetskega izobraževanja, usposabljanja, ocenjevanja in vaj, razvitih v okviru EDA.

ESZD in države članice bodo:

- v tesnem sodelovanju z zadevnimi službami institucij, organov in agencij EU ter na podlagi obstoječih standardov in znanja uporabljale uveljavljene mehanizme EAVO za certificiranje programov usposabljanja; preučile možnost vzpostavitve posebnih modulov za kibernetsko področje v okviru pobude za vojaški Erasmus.

Izboljšati je treba možnosti, da se vojaški in civilni akterji v okviru SVOP udeležujejo vaj na področju kibernetske obrambe. S skupnimi vajami se oblikuje skupno znanje in razumevanje kibernetske obrambe. To bo nacionalnim silam omogočilo, da bodo bolje pripravljene na delovanje v večnacionalnem okolju. Izvajanje skupnih vaj na področju kibernetske obrambe bo okrepilo tudi interoperabilnost in zaupanje.

ESZD, EDA, skupina CERT-EU in države članice se bodo osredotočile na spodbujanje elementov kibernetske obrambe med vajami v okviru SVOP in drugimi vajami ter bodo:

- vključevale razsežnost kibernetske obrambe v obstoječe scenarije v okviru *MILEX* in *MULTILAYER*;
- redno organizirale strateške/politične vaje, kot je *CYBRID 2017*, in sicer v koordinaciji z vzporedno in usklajeno vajo EU (PACE) ter tehnično-operativnimi vajami, kot je *DEFNET*;
- po potrebi pripravile namensko vajo EU v okviru SVOP na področju kibernetske obrambe in preučile morebitno koordinacijo z vseevropskimi kibernetskimi vajami, kot je *CyberEurope*, ki jo organizira ENISA;
- še naprej sodelovale v drugih večnacionalnih vajah na področju kibernetske obrambe, kot je *Locked Shields*;
- k sodelovanju na vajah pritegnile zadevne mednarodne partnerje, kot je Nato, v skladu z okvirom EU za politiko urjenja;
- organizirale redne vaje na podlagi zbirke orodij za kibernetsko diplomacijo, v okviru katerih bodo države članice lahko vadile svoj odziv na zlonamerne kibernetske dejavnosti.

6. Okrepitev sodelovanja z zadevnimi mednarodnimi partnerji

V okviru mednarodnega sodelovanja je treba zagotoviti dialog z mednarodnimi partnerji, zlasti Natom in drugimi mednarodnimi organizacijami, da bi prispevali k razvoju učinkovitih zmogljivosti kibernetske obrambe. Zavzemati bi se bilo treba za še večje usklajevanje z delom, ki se opravlja v okviru Organizacije za varnost in sodelovanje v Evropi (OVSE) in Združenih narodov (ZN), da bi pripravili strateški okvir za preprečevanje konfliktov, sodelovanje in stabilnost v kibernetskem prostoru.

V EU obstaja politična volja za nadaljnje sodelovanje z Natom na področju kibernetske obrambe z namenom oblikovanja zanesljivih in odpornih zmogljivosti za kibernetsko obrambo, kot je zapisano v Skupni izjavi predsednika Evropskega sveta, predsednika Evropske komisije in generalnega sekretarja Organizacije Severnoatlantske pogodbe z dne 8. julija 2016 iz Varšave. Redna posvetovanja na ravni osebja, vzajemno poročanje ter morebitna srečanja med Skupino za politično-vojaške zadeve in zadevnimi odbori Nata bodo prispevali k temu, da se prepreči nepotrebno podvajanje dela ter zagotovita usklajenost in komplementarnost prizadevanj v skladu z navedenim okvirom.

ESZD in EDA bosta ob ustreznem upoštevanju institucionalnega okvira in avtonomije odločanja EU in Nata skupaj z državami članicami še naprej razvijali sodelovanje na področju kibernetske obrambe med EU in Natom ter bosta:

- okrepili prizadevanja v okviru izvajanja Skupne izjave predsednika Evropskega sveta, predsednika Evropske komisije in generalnega sekretarja Organizacije Severnoatlantske pogodbe;
- izmenjevali najboljše prakse kriznega upravljanja ter kibernetske obrambe v okviru vojaških in civilnih misij in operacij;
- prizadevali si, da bi bile zahteve po zmogljivostih kibernetske obrambe, ki se prekrivajo, medsebojno usklajene, zlasti kar zadeva dolgoročni razvoj zmogljivosti kibernetske obrambe;
- tudi v prihodnje uporabljali okvir za sodelovanje med EDA in Natovim Centrom odličnosti za sodelovanje pri kibernetski obrambi kot izhodiščno platformo za okrepljeno sodelovanje pri večnacionalnih projektih na področju kibernetske obrambe, in sicer na podlagi ustreznih ocen.

EAVO, ESZD in EDA bodo:

- okrepile sodelovanje v zvezi s koncepti usposabljanja in izobraževanja na področju kibernetske obrambe, pa tudi vaj;
- zagotovile vzajemno udeleževanje osebja na vajah v skladu z dogovorjenim okvirom.

Skupina CERT-EU bo:

- dodatno razmislila o tehničnih ureditvah med skupino CERT-EU in ustreznimi organi EU za kibernetsko obrambo ter zmogljivostjo Nata za odzivanje na računalniške incidente (NCIRC), da bi izboljšali poznavanje razmer, izmenjavo informacij in mehanizme zgodnjega opozarjanja ter predvideli grožnje, ki bi lahko vplivale na obe organizaciji.

Kar zadeva druge mednarodne organizacije in zadevne mednarodne partnerje EU, bodo ESZD in države članice po potrebi:

- spremljale strateški razvoj in se glede vprašanj kibernetske obrambe posvetovale z mednarodnimi partnerji (mednarodnimi organizacijami in tretjimi državami);
- preučile možnosti sodelovanja pri vprašanjih kibernetske obrambe, tudi s tretjimi državami, ki sodelujejo pri misijah in operacijah v okviru SVOP;
- v relevantnih mednarodnih organizacijah, zlasti v okviru ZN, OVSE in regionalnega foruma ASEAN, spodbujale uporabo veljavnega mednarodnega prava v kibernetskem prostoru, zlasti vseh določb Ustanovne listine ZN, oblikovanje in izvajanje univerzalnih nezavezujočih norm odgovornega ravnanja držav in regionalnih ukrepov za krepitev zaupanja med državami, da bi se izboljšala preglednost in zmanjšalo tveganje za napačno odzivanje držav.

Komisija in ESZD bosta:

- po potrebi podprli krepitev kibernetskih zmogljivosti za partnerje EU, in sicer prek spremenjenega instrumenta za prispevanje k stabilnosti in miru (IcSP).

Nadaljnji ukrepi

Potem, ko bo ESZD uskladila izvajanje OPKO, bi morale ESZD, agencija EDA in Komisija Skupini za politično-vojaške zadeve s sodelovanjem Horizontalne delovne skupine za kibernetska vprašanja ter Političnemu in varnostnemu odboru predložiti poročilo o napredku, da bi se ocenilo izvajanje OPKO. Vsakih šest mesecev bo zagotovljena tudi ustna predstavitev.

Bistveno je, da se glede na razvoj kibernetskih groženj opredelijo nove zahteve za kibernetsko obrambo, ki bi se nato vključile v okvir politike za kibernetsko obrambo. Naslednji pregled OPKO bi moral biti predložen najpozneje do sredine leta 2022, ob tesnem posvetovanju z državami članicami.