Rada
Európskej únie

V Bruseli 19. novembra 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

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	19. novembra 2018
Komu:	Delegácie
Predmet:	Politický rámec EÚ pre kybernetickú obranu (aktualizácia za rok 2018)

Delegáciám v prílohe zasielame Politický rámec EÚ pre kybernetickú obranu (aktualizácia za rok 2018), ktorý Rada prijala na svojom 3 652. zasadnutí 19. novembra 2018.

PRÍLOHA

POLITICKÝ RÁMEC EÚ PRE KYBERNETICKÚ OBRANU

(AKTUALIZÁCIA ZA ROK 2018)

Rozsah pôsobnosti a ciele

S cieľom reagovať na meniace sa bezpečnostné výzvy musí EÚ a jej členské štáty posilniť kybernetickú odolnosť a vybudovať robustné spôsobilosti v oblasti kybernetickej bezpečnosti a obrany.

Politický rámec EÚ pre kybernetickú obranu (CDPF) podporuje budovanie spôsobilostí v oblasti kybernetickej obrany v členských štátoch EÚ, ako aj posilnenie kybernetickej ochrany bezpečnostnej a obrannej infraštruktúry EÚ bez toho, aby boli dotknuté vnútroštátne právne predpisy členských štátov a právne predpisy EÚ, a to aj pokiaľ ide o rozsah pôsobnosti kybernetickej obrany, ak je vymedzený.

Kybernetický priestor je piatou operačnou oblasťou po pozemnom, námornom, vzdušnom a kozmickom priestore: úspešné vykonávanie misií a operácií EÚ čoraz viac závisí od nepretržitého prístupu k bezpečnému kybernetickému priestoru, a preto si vyžaduje robustné a odolné kybernetické operačné spôsobilosti.

Cieľom aktualizovaného CDPF je ďalej rozvíjať politiku EÚ v oblasti kybernetickej obrany tým, že sa zohľadní relevantný vývoj na iných relevantných fórach a v politických oblastiach a vykonávanie CDPF od roku 2014. V CDPF sa identifikujú prioritné oblasti kybernetickej obrany a objasňujú úlohy rôznych európskych aktérov, pričom sa v plnej miere rešpektujú povinnosti a právomoci aktérov a členských štátov Únie, ako aj inštitucionálny rámec EÚ a jej autonómne rozhodovanie.

Kontext

V záveroch Európskej rady o SBOP z decembra 2013 a v záveroch Rady o SBOP z novembra 2013 sa vyzýva na vytvorenie politického rámca EÚ pre kybernetickú bezpečnosť na základe návrhu vysokej predstaviteľky a v spolupráci s Európskou komisiou a Európskou obrannou agentúrou (EDA). Rada prijala politický rámec EÚ pre kybernetickú obranu 18. novembra 2014[1] a odvtedy sa prostredníctvom jeho vykonávania prispieva konkrétnymi výstupmi k výraznému posilneniu obranných spôsobilostí členských štátov v kybernetickej oblasti. Členské štáty vyzvali vo výročnej správe o vykonávaní politického rámca pre kybernetickú obranu za rok 2017[2] na aktualizáciu tohto rámca, berúc do úvahy iniciatívy EÚ v oblasti bezpečnosti a obrany, najmä koordinované výročné preskúmanie v oblasti obrany (CARD), stálu štruktúrovanú spoluprácu (PESCO), Európsky obranný fond (EDF) a ucelený návrh rozvoja civilnej SBOP, ako aj revíziu plánu rozvoja spôsobilostí (CDP) a plánu rozvoja civilných spôsobilostí (CCDP) za rok 2018.

Kybernetická bezpečnosť je prioritou v rámci globálnej stratégia pre zahraničnú a bezpečnostnú politiku EÚ a v rámci úrovne ambícií EÚ[3]. V globálnej stratégii sa zdôrazňuje potreba zvýšiť kapacity na ochranu EÚ a jej občanov a reagovať na vonkajšie krízy. Globálna stratégia zdôrazňuje potrebu posilniť EÚ ako bezpečnostné spoločenstvo. V tejto súvislosti by bezpečnostné a obranné úsilie malo posilniť aj strategickú úlohu EÚ a jej schopnosť konať samostatne, ak je to potrebné, a s partnermi, ak je to možné. Tieto ciele si vyžadujú užšiu spoluprácu v oblasti budovania spôsobilostí na podporu účinnosti a interoperability výsledných civilných a vojenských spôsobilostí.

---

1 15585/14, 18. 11. 2014.
2 15870/17, 19. 12. 2017.
3 Závery Rady o vykonávaní globálnej stratégie EÚ v oblasti bezpečnosti a obrany, 14. 11. 2016.

Spoločný súbor návrhov na účely vykonávania spoločného vyhlásenia, ktoré podpísal predseda Európskej rady, predseda Európskej komisie a generálny tajomník Organizácie Severoatlantickej zmluvy 8. júla 2016 vo Varšave[4], zahŕňa konkrétne opatrenia s cieľom rozšíriť spoluprácu medzi EÚ a NATO v oblasti kybernetickej bezpečnosti a obrany, a to aj v kontexte misií a operácií, ako aj pokiaľ ide o budovanie spôsobilostí kybernetickej obrany, výskum a technológie, vzdelávanie, odbornú prípravu, cvičenia a začlenenie kybernetického aspektu do krízového riadenia. Táto spolupráca sa uskutočňuje v plnom súlade so zásadami otvorenosti, transparentnosti, inkluzívnosti, reciprocity a rozhodovacej autonómie EÚ. Technická dohoda medzi tímom reakcie na núdzové počítačové situácie EÚ (CERT – EU) a tímom pre spôsobilosť reakcie na počítačové incidenty NATO (NCIRC), ktorá bola podpísaná vo februári 2016, uľahčuje výmenu technických informácií v záujme zlepšenia prevencie kybernetických bezpečnostných incidentov, ich odhaľovania a reakcie na ne v oboch organizáciách.

Malo by sa pripomenúť, že viaceré politiky EÚ prispievajú k cieľom politiky v oblasti kybernetickej obrany v zmysle tohto dokumentu a tento rámec berie do úvahy aj príslušnú regulačnú, politickú a technologickú podporu v civilnej oblasti. Napríklad v júli 2016 Európsky parlament a Rada prijali smernicu o bezpečnosti sietí a informačných systémov[5] (NIS), ktorou sa zvýši celková pripravenosť členských štátov na kybernetické hrozby a posilní sa spolupráca v rámci celej EÚ. Touto smernicou sa stanovujú opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci Únie s cieľom zlepšiť fungovanie vnútorného trhu. Termín transpozície smernice bol 9. mája 2018.

---

4 Závery Rady o vykonávaní spoločného vyhlásenia predsedu Európskej rady, predsedu Európskej komisie a generálneho tajomníka Organizácie Severoatlantickej zmluvy (6. decembra 2016, 15283/16; 5. decembra 2017, 14802/17).

5 Smernica (EÚ) 2016/1148 Európskeho parlamentu a Rady zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

Návrh právneho predpisu o kybernetickej bezpečnosti EÚ zo septembra 2017 obsahuje nový mandát agentúry EÚ pre kybernetickú bezpečnosť (ENISA) a zriadenie celoúnijného certifikačného rámca. Certifikačný rámec by mal po zriadení podporovať prísne normy v oblasti procesov, produktov a služieb IKT, byť zdrojom konkurenčnej výhody a zvýšiť dôveru zo strany spotrebiteľov a obstarávateľov. Komisia v septembri 2017 tiež podnikla ďalší krok na prípravu EÚ v prípade rozsiahlych cezhraničných kybernetických incidentov („Blue Print“) a v súčasnosti pracuje s členskými štátmi a inými inštitúciami, agentúrami a orgánmi na vývoji európskej krízovej spolupráce v oblasti kybernetickej bezpečnosti a zavádzaní praktického sfunkčnenia a zdokumentovania všetkých príslušných aktérov, procesov a postupov v rámci existujúcich mechanizmov EÚ v oblasti krízového riadenia a zvládania katastrof, najmä integrovaných dojednaní o politickej reakcii na krízu.

V záveroch Rady o posilňovaní kybernetickej odolnosti Európy z novembra 2016 sa uvádza spoločný cieľ prispievať k strategickej autonómii EÚ, ako sa uvádza v záveroch Rady o Globálnej stratégii pre zahraničnú a bezpečnostnú politiku Európskej únie z novembra 2016, a to aj v kybernetickom priestore. Európska rada potvrdila tento cieľ v júni 2018 a takisto zdôraznila potrebu posilniť spôsobilosti na boj proti kybernetickým hrozbám z krajín mimo EÚ.

Rada v roku 2017 prijala rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor nástrojov kybernetickej diplomacie“)[6]. Očakáva sa, že týmto rámcom sa podporí spolupráca, uľahčí zmierňovanie hrozieb a v dlhodobom horizonte ovplyvní správanie potenciálnych útočníkov. V rámci sa využívajú opatrenia SZBP vrátane reštriktívnych opatrení na predchádzanie škodlivým kybernetickým činnostiam a reakciu na ne. Pôvodcovia škodlivých kybernetických činností aktérov musia byť za svoje činnosti braní na zodpovednosť a členské štáty EÚ sa nabádajú, aby rozvíjali svoju schopnosť reagovať na škodlivé kybernetické činnosti koordinovaným spôsobom a v súlade so súborom nástrojov kybernetickej diplomacie. Štáty by nemali vykonávať alebo vedome podporovať činnosti v oblasti informačných a komunikačných technológií, ktoré sú v rozpore s ich povinnosťami podľa medzinárodného práva, a ani by nemali vedome umožňovať, aby sa ich územie využívalo na páchanie medzinárodných protiprávnych činov prostredníctvom informačných a komunikačných technológií.

Komisia a VP/PK v septembri 2017 predložili spoločné oznámenie[7] o kybernetickej oblasti s cieľom zmierniť riziká vyplývajúce z nových hrozieb. Zahŕňa kybernetickú obranu ako jednu z hlavných oblastí činnosti a CDPF je jedným z pilierov jej konkrétnej realizácie[8].

V záveroch Rady z novembra 2017 o kybernetických otázkach sa uznávajú rastúce prepojenia medzi kybernetickou bezpečnosťou a obranou a vyzýva sa v nich na zintenzívnenie spolupráce v oblasti kybernetickej obrany, a to aj podporovaním spolupráce medzi komunitami civilnej a vojenskej reakcie na incidenty. Zdôrazňuje sa v nich, že obzvlášť závažný kybernetický incident alebo kríza by pre členský štát mohli predstavovať dostatočný dôvod na uplatnenie doložky o solidarite EÚ a/alebo doložky o vzájomnej pomoci.

---

6 Závery Rady o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“), 9916/17, 7. júna 2017

7 Spoločné oznámenie Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ (13. septembra 2017, JOIN (2017) 450 final)).

8 Závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ (20. novembra 2017, 14435/17),

11. decembra 2017 sa začala stála štruktúrovaná spolupráca (PESCO). Tento ambiciózny, záväzný a inkluzívny rámec spolupráce medzi 25 členskými štátmi obsahuje záväzok zvýšiť úsilie pri spolupráci v oblasti kybernetickej obrany, ako aj pri súvisiacich projektoch PESCO. Prvý súbor projektov PESCO, ktoré určili členské štáty zapojené do PESCO v roku 2017, obsahuje dva projekty zamerané na kybernetickú obranu: „Tímy rýchlej kybernetickej reakcie a vzájomná pomoc v oblasti kybernetickej bezpečnosti“ a „Platforma na výmenu informácií v oblasti reakcie na kybernetické hrozby a incidenty“. Ďalšie súbory projektov PESCO sa očakávajú. PESCO bude rozvíjať spôsobilosti v oblasti kybernetickej obrany a tým posilní spoluprácu medzi zúčastnenými členskými štátmi a zvýši interoperabilitu.

V aktualizovanom pláne rozvoja spôsobilostí EÚ (CDP), ktorý schválil riadiaci výbor EDA v júni 2018, je kybernetická obrana označená za kľúčový prvok, pričom sa uznáva potreba kybernetických obranných operácií v každom operačnom kontexte na základe sofistikovaného aktuálneho a prediktívneho situačného povedomia o kybernetickom priestore vrátane schopnosti kombinovať veľké objemy údajov a spravodajských informácií z rôznych zdrojov s cieľom podporiť rýchle rozhodovanie, zvýšenia automatizácie zhromažďovania údajov, analýzy a procesu na podporu rozhodovania. Plán rozvoja spôsobilostí z roku 2018 uvádza priority spôsobilostí v oblasti kybernetickej obrany v týchto oblastiach: spolupráca a synergie s príslušnými aktérmi v oblasti kybernetickej obrany a kybernetickej bezpečnosti; výskumné a technologické činnosti v oblasti kybernetickej obrany; rámce systémového inžinierstva pre kybernetické operácie; vzdelávanie, odborná príprava, cvičenia a hodnotenia (ETEE); riešenie výziev v oblasti kybernetickej obrany vo vzdušnom, v kozmickom, námornom a pozemnom priestore.

Nakoniec, z posledných niekoľko rokov je zrejmé, že je potrebné, aby medzinárodné spoločenstvo predchádzalo konfliktom, spolupracovalo a stabilizovalo kybernetický priestor. EÚ v úzkej spolupráci s inými medzinárodnými organizáciami, najmä s OSN, OBSE a Regionálnym fórom ASEAN-u propaguje strategický rámec na predchádzanie konfliktom a pre spoluprácu a stabilitu v kybernetickom priestore, ktorého súčasťou je i) uplatňovanie medzinárodného práva, a najmä Charty OSN v celom jej rozsahu, v kybernetickom priestore; ii) dodržiavanie univerzálnych nezáväzných noriem, pravidiel a zásady zodpovedného správania sa štátov; iii) vypracúvanie a zavádzanie regionálnych opatrení na budovanie dôvery (CBM). Toto úsilie by mal podporovať aj politický rámec pre kybernetickú obranu.

Priority

V aktualizovanom rámci CDPF bolo vymedzených šesť prioritných oblastí. Hlavným zameraním tohto politického rámca je budovanie spôsobilostí v oblasti kybernetickej obrany, ako aj ochrana komunikačných a informačných sietí SBOP EÚ. Medzi ďalšie prioritné oblasti patrí: odborná príprava a cvičenia, výskum a technológie, civilno-vojenská spolupráca a medzinárodná spolupráca. V oblasti odbornej prípravy sa dôraz kladie na posilňovanie odbornej prípravy členských štátov v oblasti kybernetickej obrany a odbornej prípravy zameranej na zvýšenie povedomia hierarchie velenia SBOP o kybernetických otázkach. Je tiež dôležité, aby sa kybernetický rozmer primerane riešil počas cvičení s cieľom zlepšiť schopnosť EÚ reagovať na kybernetické a hybridné krízy skvalitňovaním postupov rozhodovania a dostupnosti informácií. Kybernetický priestor je rýchlo sa rozvíjajúcou oblasťou a nový technologický vývoj treba podporovať, v civilnej, ako aj vo vojenskej sfére. Civilno-vojenská spolupráca v kybernetickej oblasti je kľúčom k zabezpečeniu koherentnej reakcie na kybernetické hrozby. V neposlednom rade by sa zintenzívnením spolupráce s medzinárodnými partnermi mohla posilniť kybernetická bezpečnosť v EÚ aj mimo nej a mohli by sa ňou propagovať zásady a hodnoty EÚ.

Týmto rámcom sa načrtávajú návrhy a príležitosti na koordináciu medzi príslušnými inštitúciami, orgánmi a agentúrami EÚ. Odzrkadľuje aj dôležitú úlohu súkromného sektora pri rozvoji technológií kybernetickej bezpečnosti a kybernetickej obrany.

Okrem toho sa rámcom CDPF prehlbuje podpora integrácie kybernetickej obrany do mechanizmov krízového riadenia Únie, v rámci ktorého sa na riešenie následkov kybernetickej krízy môžu podľa potreby uplatňovať príslušné ustanovenia Zmluvy o EÚ a Zmluvy o fungovaní EÚ[9].

1. Podpora budovania spôsobilostí členských štátov v oblasti kybernetickej obrany

V rámci rozvoja spôsobilostí a technológií v oblasti kybernetickej obrany by sa mali riešiť všetky aspekty rozvoja spôsobilostí vrátane doktríny, vedenia, organizácie, personálu, odbornej prípravy, priemyslu, technológie, infraštruktúry, logistiky a interoperability. Na dosiahnutie tohto cieľa by členské štáty mali zintenzívniť svoje úsilie o zabezpečenie účinnej spôsobilosti v oblasti kybernetickej obrany. ESVČ, Komisia a EDA by mali spolupracovať a podporovať tieto snahy.

Je potrebné neustále posudzovať slabé stránky informačných infraštruktúr, ktoré podporujú misie a operácie SBOP, ako aj sledovať účinnosť ochrany v takmer reálnom čase. Jedna z hlavných oblastí, ktorým sa pri činnostiach kybernetickej obrany bude z operačného hľadiska venovať pozornosť, bude zachovanie dostupnosti, integrity a dôvernosti komunikačných a informačných sietí SBOP, pokiaľ sa v mandáte operácií alebo misií nestanoví inak. Okrem toho bude ESVČ v spolupráci s členskými štátmi hlbšie integrovať kybernetické spôsobilosti do misií a operácií SBOP.

Pôvodcovia škodlivých kybernetických činností musia byť braní na zodpovednosť za svoje činnosti. Je dôležité, aby členské štáty EÚ s podporou ESVČ rozvíjali vzájomnú spoluprácu s cieľom reagovať na škodlivé kybernetické činnosti. Vyvíja sa súbor nástrojov kybernetickej diplomacie, ktorý má pomôcť dosiahnuť takúto spoločnú reakciu. ESVČ a EDA budú na základe súboru nástrojov kybernetickej diplomacie organizovať v tejto oblasti pravidelné praktické cvičenia pre členské štáty EÚ.

[9] Článok 222 ZFEÚ a článok 42 ods. 7 ZEÚ s náležitým ohľadom na čl. 17 ZEÚ.

Vzhľadom na to, že vo vnútroštátnych právnych predpisoch členských štátov aj v právnych predpisoch EÚ je vymedzenie pojmu kybernetická obrana široké a rozmanité, ak vôbec existuje, je potrebné zhodnúť sa na spoločnom súhrnnom chápaní tohto pojmu.

Keďže vojenské operácie SBOP sa opierajú o infraštruktúru velenia, riadenia, konzultácií a výpočtovej techniky (C4) poskytovanú členskými štátmi, pri plánovaní požiadaviek v oblasti kybernetickej obrany na informačnú infraštruktúru je potrebná určitá miera strategickej konvergencie.

Vychádzajúc z práce tímu EDA pre projekt kybernetickej obrany zameranej na rozvíjanie spôsobilostí v oblasti kybernetickej obrany, EDA a členské štáty:

- budú využívať CDP a iné nástroje, ako napr. CARD, ktoré uľahčujú a podporujú spoluprácu medzi členskými štátmi, s cieľom zvýšiť mieru konvergencie v plánovaní požiadaviek členských štátov v oblasti kybernetickej obrany na strategickej úrovni, najmä pokiaľ ide o monitorovanie, situačné povedomie, prevenciu, odhaľovanie a ochranu, výmenu informácií, spôsobilosti v oblasti forenznej analýzy a analýzy škodlivého softvéru, získané poznatky, zmiernenie škôd, spôsobilosti dynamického obnovenia, distribuované ukladanie údajov a zálohovanie údajov;
- budú podporovať súčasné a budúce projekty súvisiace s kybernetickou obranou v oblasti združovania a spoločného využívania pre vojenské operácie (napr. v oblasti forenznej analýzy, rozvoja interoperability, stanovovania noriem);
- na základe skúseností z celej EÚ vypracujú štandardný súbor cieľov a požiadaviek vymedzujúcich minimálnu úroveň kybernetickej bezpečnosti a dôvery, ktorú majú dosiahnuť členské štáty.

ESVČ a EDA:

- budú uľahčovať výmeny medzi členskými štátmi týkajúce sa národných doktrín v oblasti kybernetickej obrany, ako aj náboru nových pracovníkov zameraného na oblasť kybernetickej obrany, programov ich udržania a vytvárania zoznamov záložníkov.

EDA:

- bude študovať rozdielne rozsahy pôsobnosti vojenských požiadaviek v oblasti kybernetickej obrany vo vnútroštátnych právnych predpisoch a v najlepších postupoch členských štátov; Hlavným cieľom štúdie bude vybudovať podnikovú architektúru pre kybernetickú obranu s cieľom zahrnúť rozsah pôsobnosti, funkcie a požiadavky, ktoré členské štáty používajú v tejto oblasti na základe vnútroštátnych právnych predpisov a právnych predpisov EÚ.

Členské štáty budú na dobrovoľnom základe:

- zlepšovať spoluprácu medzi vojenskými tímami CERT s cieľom zlepšiť prevenciu a riešenie incidentov;
- využívať PESCO na ďalšie posilnenie spolupráce v oblasti kybernetickej obrany vrátane nových projektov;
- využívať Európsky obranný fond s cieľom spoločne rozvíjať spôsobilosti v oblasti kybernetickej obrany;
- budovať spoločné chápanie uplatňovania doložky o vzájomnej pomoci v kybernetickej oblasti pri zachovaní jej flexibility;
- vypracúvať základné požiadavky kladené v oblasti kybernetickej obrany na informačnú infraštruktúru;
- v rozsahu, v akom zlepšenie spôsobilostí v oblasti kybernetickej obrany závisí od civilných odborných znalostí týkajúcich sa sieťovej a informačnej bezpečnosti, využívať odborné znalosti agentúry ENISA, orgánov členských štátov, ktoré sú združené v skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a iných prípadných subjektov na úrovni EÚ s odbornými znalosťami o civilnej kybernetickej bezpečnosti.

Členské štáty, ESVČ/Vojenský štáb EÚ, EABO a EDA:

- budú zvažovať rozvoj odbornej prípravy v oblasti kybernetickej obrany na účely osvedčovania bojových skupín EÚ.

Komisia v spolupráci s členskými štátmi:

- bude zvažovať kybernetickú obranu v pracovných programoch Programu rozvoja európskeho obranného priemyslu a Európskeho obranného fondu.

2. Zlepšenie ochrany komunikačných a informačných systémov SBOP využívaných subjektmi z EÚ

ESVČ v rámci príslušných pravidiel týkajúcich sa rozpočtu Únie dospeje k primeranému a samostatnému chápaniu bezpečnostných záležitostí a záležitostí týkajúcich sa ochrany sietí a vybuduje svoje vlastné kapacity pre bezpečnosť informačných technológií bez toho, aby tým bola dotknutá úloha tímu reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU) ako ústrednej štruktúry EÚ na koordináciu reakcie na kybernetické bezpečnostné incidenty pre všetky inštitúcie, orgány a agentúry Únie. Bude sa snažiť zvýšiť odolnosť sietí ESVČ pre SBOP, pričom sa zameria na prevenciu, odhaľovanie, reakciu na incidenty, situačné povedomie, výmenu informácií a mechanizmy včasného varovania.

Ochrana komunikačných a informačných systémov ESVČ a rozvoj kapacít pre bezpečnosť informačných technológií (IT) sa uskutočňuje pod vedením generálneho riaditeľstva ESVČ pre rozpočet a správu („GR RS“). Ďalšie osobitné zdroje a podporu poskytnú aj Vojenský štáb Európskej únie (EUMS), riaditeľstvo pre krízové riadenie a plánovanie (CMPD) a útvar pre plánovanie a vedenie civilných operácií (CPCC). Táto spôsobilosť v oblasti bezpečnosti IT sa bude vzťahovať na utajované aj neutajované systémy a budú nedeliteľnou súčasťou existujúcich operačných subjektov.

Takisto je potrebné zefektívniť bezpečnostné pravidlá pre informačné systémy poskytované jednotlivými inštitucionálnymi aktérmi EÚ počas realizácie misií a operácií SBOP. V tejto súvislosti by sa mohla zvážiť jednotná hierarchia velenia s cieľom zlepšiť odolnosť sietí využívaných pre SBOP.

Na zlepšenie koordinácie a ochrany a odolnosti komunikačných a informačných systémov a sietí SBOP bol v roku 2017 zriadený interný výbor ESVČ pre správu kybernetických záležitostí, ktorý patrí pod generálneho tajomníka ESVČ.

ESVČ/GR RS:

- posilnia kapacity pre bezpečnosť IT v rámci ESVČ na základe existujúcich technických spôsobilostí a postupov, s dôrazom na prevenciu, odhaľovanie, reakciu na incidenty, situačné povedomie, výmenu informácií a mechanizmy včasného varovania. Ďalej sa posilní stratégia spolupráce s CERT-EU a s existujúcimi spôsobilosťami EÚ v oblasti kybernetickej bezpečnosti.

ESVČ/GR RS spolu s EUMS, MPCC, CMPD a CPCC:

- vypracujú ucelenú bezpečnostnú politiku a usmernenia pre IT, pričom zohľadnia aj technické požiadavky na kybernetickú obranu v kontexte SBOP pre štruktúry, misie a operácie a budú mať zároveň na pamäti existujúce rámce a politiky zamerané na spoluprácu v rámci EÚ s cieľom dosiahnuť zbližovanie pravidiel, politík a organizácie.

ESVČ/jednotná kapacita na analýzu spravodajských informácií (SIAC):

- na základe existujúcich štruktúr posilnia posudzovanie kybernetických hrozieb a budú rozvíjať spravodajské spôsobilosti s cieľom identifikovať nové kybernetické riziká a poskytovať pravidelné posúdenia rizík na základe strategického posúdenia hrozieb a informácie o incidentoch v takmer reálnom čase, ktoré sú koordinované medzi príslušnými štruktúrami EÚ a sprístupnené na rôznych stupňoch utajenia.

ESVČ/SIAC a CERT-EU:

- budú podporovať výmenu informácií o kybernetických hrozbách v reálnom čase medzi členskými štátmi a príslušnými subjektmi EÚ. Na tento účel sa vytvoria mechanizmy výmeny informácií a budovania dôvery medzi príslušnými vnútroštátnymi a európskymi orgánmi prostredníctvom dobrovoľného prístupu, ktorý vychádza z existujúcej spolupráce.

ESVČ/EUMS a MPCC:

- ďalej rozvinú a do plánovania na strategickej úrovni začlenia koncepciu kybernetickej obrany pre vojenské misie a operácie SBOP;
- vypracujú v spolupráci s operačným veliteľstvom všeobecný štandardný operačný postup na operačnej úrovni pre kybernetické záležitosti.

ESVČ/CPCC a CMPD:

- ďalej rozvinú a do strategického plánovania začlenia koncepciu kybernetickej obrany pre civilné misie SBOP;
- posilnia budovanie spôsobilostí v oblasti kybernetickej obrany v rámci civilných misií SBOP v nadväznosti na existujúce infraštruktúry a budú podporovať normalizáciu a harmonizáciu technológií používaných v rámci misií a operácií SBOP za prípadného využitia odborných znalostí tímu CERT-EU a agentúr ENISA a EDA;
- v procese posilňovania civilnej SBOP hlbšie preskúmajú prípadnú podporu hostiteľských krajín v oblasti kybernetickej bezpečnosti prostredníctvom civilných misií SBOP.

ESVČ:

- bude rozvíjať spoločné požiadavky pre vojenské a civilné misie a operácie SBOP;
- zlepší koordináciu kybernetickej obrany s cieľom splniť ciele spojené s ochranou sietí používaných inštitucionálnymi aktérmi EÚ podporujúcimi SBOP na základe existujúcich skúseností z celej EÚ;
- bude na základe meniacich sa hrozieb a po konzultácii s členskými štátmi a inými inštitúciami EÚ pravidelne preskúmavať požiadavky na zdroje a iné príslušné politické rozhodnutia.

3. Podpora civilno-vojenskej spolupráce

Kybernetický priestor je rýchlo sa rozvíjajúcou oblasťou: technologický rozvoj musia posilňovať bezpečnostné systémy vo vojenskej aj v civilnej sfére. V maximálnej možnej miere by sa mala plánovať koordinácia medzi civilnou a vojenskou oblasťou v prípadoch, keď podobný technologický vývoj prinesie riešenia pre civilné a vojenské aplikácie. V ostatných prípadoch sú vojenské spôsobilosti a zbraňové systémy natoľko špecifické, že na ich spoločné využívanie s civilnými technológiami nie je priestor. Bez toho, aby bola dotknutá vnútorná organizácia a právne predpisy členských štátov, možno civilno-vojenskú spoluprácu v kybernetickej oblasti zvažovať okrem iného na účely výmeny najlepších postupov, výmeny informácií a mechanizmov včasného varovania, posúdení rizík v súvislosti s reakciou na incidenty, zvyšovania informovanosti a na účely odbornej prípravy a cvičení.

Zlepšenie civilnej kybernetickej bezpečnosti je dôležitým faktorom, ktorý prispieva k celkovej odolnosti sieťovej a informačnej bezpečnosti. Smernicou NIS sa zvyšuje pripravenosť na národnej úrovni a posilňuje spolupráca na úrovni Únie medzi členskými štátmi, a to na strategickej aj operačnej úrovni. Do tejto spolupráce sa zapájajú vnútroštátne orgány dohliadajúce na politiky v oblasti kybernetickej bezpečnosti, ako aj vnútroštátne tímy CERT a CERT-EU. Spolupráca medzi civilnými a vojenskými jednotkami CERT by sa mala s náležitým prihliadnutím na tento vývoj posilniť. Novým európskym aktom o kybernetickej bezpečnosti sa má zlepšiť odolnosť Európy proti kybernetickým útokom a zriadiť rámec certifikácie kybernetickej bezpečnosti pre produkty a služby, čím sa zvýši dôvera v civilnú digitálnu oblasť.

EDA, Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), Európske centrum boja proti počítačovej kriminalite (EC3) a CERT-EU, spolu s ostatnými príslušnými orgánmi a agentúrami EÚ, v rámci svojich príslušných právomocí a bez prekrývania sa s právomocami členských štátov, ako aj členské štáty samotné sa nabádajú, aby ďalej posilňovali svoju spoluprácu a:

- vytvorili spoločné profily právomocí v oblasti kybernetickej bezpečnosti a obrany na základe medzinárodných najlepších postupov a certifikácie, ktoré používajú inštitúcie, orgány a agentúry EÚ, a zohľadnili pritom aj normy certifikácie v súkromnom sektore;
- prispeli k ďalšiemu rozvoju a prispôsobeniu organizačných a technických noriem v oblasti kybernetickej bezpečnosti a obrany vo verejnom sektore, ktoré sa majú používať v sfére obrany a bezpečnosti. V prípade potreby by mali vychádzať z práce, ktorú vykonávajú ENISA a EDA;
- vytvorili alebo ďalej rozvíjali pracovné mechanizmy a opatrenia na výmenu najlepších postupov, najmä v oblasti vzdelávania, odbornej prípravy a cvičení, ako aj v oblasti výskumu a technológie a v iných oblastiach, v ktorých vznikajú civilno-vojenské synergie;
- využívali existujúce skúsenosti EÚ v oblasti prevencie počítačovej kriminality, ako aj vyšetrovacie a forenzné spôsobilosti a lepšie ich zužitkúvali pri rozvoji spôsobilostí v oblasti kybernetickej obrany.

Členské štáty budú na dobrovoľnom základe:

- posilňovať medzištátnu spoluprácu civilných a vojenských jednotiek CERT jednotlivých členských štátov.

ESVČ, Komisia a členské štáty:

- zahrnú kybernetickú obranu do postupov EÚ na riadenie krízových situácií a zvládanie katastrof (prostredníctvom uvedeného procesu „Blue Print“).

4. Výskum a technológie

Prevádzkovatelia služieb v oblasti infraštruktúry a informačných a komunikačných technológií (IKT) na civilné a obranné účely čelia v dôsledku spoločných požiadaviek na technologické a operačné spôsobilosti podobným výzvam v oblasti kybernetickej bezpečnosti. Očakáva sa, že spoločné potreby v oblasti výskumu a technológií a spoločné požiadavky na systémy zlepšia interoperabilitu systémov z dlhodobého hľadiska a znížia náklady na vývoj riešení. Dosiahnutie úspor z rozsahu je nutnosťou vzhľadom na stále sa zvyšujúci počet hrozieb a zraniteľností. Tým by sa zase malo uľahčiť zachovanie a rast konkurencieschopného priemyslu kybernetickej obrany v Európe.

Rozvoj spôsobilostí v oblasti kybernetickej obrany má dôležitý výskumný a technologický rozmer. EDA v rámci programu výskumu v oblasti kybernetickej obrany (CDRA) poskytla pevný základ pre stanovenie priorít v oblasti budúceho financovania výskumu a technológií v medziach medzivládneho rámca. Následným strategickým výskumným programom vypracovaným v príslušnej *ad hoc* pracovnej skupine EDA sa podloženým spôsobom stanovujú priority, pokiaľ ide o technológie súvisiace s kybernetickou oblasťou potrebné pre armádu, a súčasne určujú možnosti úsilia o technológie s dvojakým použitím a investícií do nich, či už v kontexte vnútroštátneho alebo nadnárodného financovania, alebo financovania na úrovni EÚ.

Zásadný význam pre zmiernenie hrozieb a nedostatkov má vytvorenie technologických kapacít v Európe. Hlavnou hybnou silou pre technológie a inováciu súvisiace s kybernetickou obranou zostane priemysel. Príkladmi oblastí, ktoré je potrebné riešiť, je kryptografia, zabudované systémy, odhaľovanie škodlivého softvéru, simulačné a vizualizačné techniky, ochrana sietí a komunikačných systémov, identifikačné a autentifikačné technológie. Je tiež dôležité rozvíjať konkurencieschopný európsky priemyselný dodávateľský reťazec v oblasti kybernetickej obrany podporou účasti malých a stredných podnikov (MSP).

Zabezpečenie toho, aby Európa bola schopná držať krok s medzinárodnými konkurentmi vo sfére spôsobilostí v oblasti kybernetických technológií, závisí aj od toho, či dokážeme podporovať prelomové inovácie prostredníctvom národných nástrojov, ako aj nástrojov EÚ, akým je Európska rada pre inováciu.

S cieľom uľahčiť civilno-vojenskú spoluprácu pri rozvoji spôsobilostí v oblasti kybernetickej bezpečnosti, posilniť Európsku obrannú technologickú a priemyselnú základňu[10] a prispievať k strategickej autonómii EÚ aj v oblasti kybernetického priestoru, podľa potreby a pokiaľ možno s partnermi,

EDA, Komisia a členské štáty budú:

- vyvíjať snahu o synergie úsilia v oblasti výskumu a technológií vo vojenskom sektore s civilnými programami výskumu a vývoja, najmä pokiaľ ide o prelomové inovácie, a pri vykonávaní prípravnej akcie pre výskum v oblasti obrany zohľadnia rozmer kybernetickej bezpečnosti a obrany;
- zdieľať výskumné programy v oblasti kybernetickej bezpečnosti (napr. strategický výskumný program Európskej obrannej agentúry v oblasti kybernetickej bezpečnosti), ako aj plány a opatrenia, ktoré z nich vyplynú. Na tento účel sa v úzkej spolupráci s Komisiou a členskými štátmi vypracuje medzisektorový výskumný program v oblasti kybernetickej obrany;
- prispievať k zlepšovaniu začleňovania rozmeru kybernetickej bezpečnosti a rozmeru kybernetickej obrany do programov s bezpečnostným a obranným rozmerom s dvojakým využitím, napr. do programu výskumu manažmentu letovej prevádzky jednotného európskeho neba (SESAR).

[10] Oznámenie s názvom „Smerom ku konkurencieschopnejšiemu a efektívnejšiemu odvetviu obrany a bezpečnosti“, COM(2013) 542.

Komisia:

- zváži zriadenie Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti so sieťou národných koordinačných centier na podporu technologických a priemyselných kapacít v oblasti kybernetickej bezpečnosti a s cieľom zvýšiť konkurencieschopnosť európskeho odvetvia kybernetickej bezpečnosti, pričom sa zabezpečí komplementárnosť a predchádza sa duplikácii v rámci siete centier kompetencií v oblasti kybernetickej bezpečnosti a s inými agentúrami EÚ. Centrum by malo okrem iného posilňovať spoluprácu medzi civilnými a obrannými technológiami a aplikáciami v úzkej spolupráci a v plnej komplementárnosti s Európskou obrannou agentúrou v oblasti kybernetickej obrany;
- bude podporovať rozvoj priemyselných ekosystémov a inovačných klasterov pokrývajúcich celý bezpečnostný hodnotový reťazec, pričom sa bude opierať o akademické znalosti, inováciu v MSP a priemyselnú výrobu.

Komisia v spolupráci s členskými štátmi:

- zváži otázky kybernetickej obrany vo výzvach na predkladanie návrhov v rámci prípravnej akcie pre výskum v oblasti obrany;
- zváži kybernetickú obranu v oblastiach výziev na predkladanie návrhov v rámci Európskeho obranného fondu;
- bude podporovať jednotnosť politík EÚ v záujme zabezpečenia toho, aby politické a technické aspekty kybernetickej ochrany EÚ zostali v popredí technologickej inovácie a boli harmonizované v rámci celej EÚ (spôsobilosť v oblasti analýzy a posudzovania kybernetických hrozieb, iniciatívy zaisťovania bezpečnosti už v štádiu návrhu, riadenie závislosti, pokiaľ ide o prístup k technológiám atď.).

5. Zlepšenie možností vzdelávania, odbornej prípravy a cvičení

S cieľom zvýšiť pripravenosť reagovať na kybernetické hrozby a rozvíjať spoločnú kultúru kybernetickej obrany v celej EÚ, ale aj v prospech misií a operácií EÚ je potrebné zlepšiť a rozšíriť možnosti odbornej prípravy v oblasti kybernetickej obrany. Je veľmi dôležité, aby sa rozpočty na vzdelávanie a odbornú prípravu využívali efektívne a zároveň poskytovali čo najvyššiu kvalitu. Kľúčový význam bude mať združovanie a spoločné využívanie vzdelávania a odbornej prípravy v oblasti kybernetickej obrany na európskej úrovni.

Európska akadémia bezpečnosti a obrany (EABO), ESVČ, EDA, Komisia a členské štáty:

- na základe analýzy potrieb odbornej prípravy v oblasti kybernetickej obrany, ktorú uskutočnila EDA, a skúseností EABO z odbornej prípravy v oblasti kybernetickej bezpečnosti zrealizujú odbornú prípravu a vzdelávanie v oblasti SBOP pre rôzne cieľové skupiny vrátane ESVČ, zamestnancov misií a operácií SBOP a úradníkov členských štátov, ktoré budú zamerané aj na otázky udržiavania kvalifikovaných pracovníkov v krátkodobom, strednodobom a dlhodobom horizonte;
- navrhnú nadviazanie dialógu v oblasti kybernetickej obrany o normách odbornej prípravy a osvedčovaní s členskými štátmi, inštitúciami EÚ, tretími krajinami a inými medzinárodnými organizáciami, ako aj so súkromným sektorom;
- budú spolupracovať s poskytovateľmi odbornej prípravy z európskeho súkromného sektora, ako aj s akademickými inštitúciami, s cieľom zvýšiť kompetencie a zručnosti zamestnancov misií a operácií SBOP.

EABO bude:

- rozvíjať platformu pre vzdelávanie, odbornú prípravu, hodnotenie a cvičenia v kybernetickej oblasti zriadenú v EABO;
- dosahovať synergie s programami odbornej prípravy iných zainteresovaných strán, ako sú ENISA, Europol, Európska policajná akadémia (CEPOL) a centrum excelentnosti NATO pre spoluprácu v oblasti kybernetickej obrany;
- skúmať možnosť spoločných programov odbornej prípravy EABO – NATO v oblasti kybernetickej obrany, ktoré by boli otvorené všetkým členským štátom EÚ s cieľom podporovať spoločnú kultúru kybernetickej obrany.

Komisia:

- vyhodnotí možnosti rozšíriť príležitosti na vzdelávanie a odbornú prípravu v členských štátoch, ktoré určí platforma pre vzdelávanie, odbornú prípravu, hodnotenie a cvičenia v kybernetickej oblasti.

EDA:

- vypracuje ďalšie kurzy EDA v spolupráci s EABO s cieľom reagovať na požiadavky členských štátov v oblasti vzdelávania, odbornej prípravy a cvičení týkajúcich sa kybernetickej obrany;
- bude podporovať platformu pre vzdelávanie, odbornú prípravu, hodnotenie a cvičenia v kybernetickej oblasti okrem iného prostredníctvom postupnej integrácie modulov vzdelávania, odbornej prípravy, hodnotenia a cvičení v kybernetickej oblasti vyvinutých v rámci EDA.

ESVČ a členské štáty:

- budú postupovať podľa zavedených certifikačných mechanizmov EABO pre programy odbornej prípravy v úzkej spolupráci s príslušnými útvarmi v inštitúciách, orgánoch a agentúrach EÚ, a to na základe existujúcich noriem a znalostí. Zvážia možnosť vytvorenia osobitných kybernetických modulov v rámci iniciatívy vojenský Erasmus.

Je potrebné zlepšiť príležitosti na cvičenia v oblasti kybernetickej obrany pre vojenských a civilných aktérov SBOP. Spoločné cvičenia slúžia ako nástroj na rozvíjanie spoločných znalostí a chápania kybernetickej obrany. Tým sa vnútroštátnym ozbrojeným silám umožní zlepšiť ich pripravenosť pôsobiť v mnohonárodnom prostredí. Realizáciou spoločných cvičení v oblasti kybernetickej obrany sa bude budovať aj interoperabilita a dôvera.

ESVČ, EDA, CERT-EU a členské štáty sa zamerajú na podporu prvkov kybernetickej obrany v rámci SBOP a iné cvičenia:

- začlenenie rozmeru kybernetickej obrany do existujúcich scenárov pre vojenské cvičenia *MILEX* a *MULTILAYER*;
- pravidelná organizácia strategických/politických cvičení, ako je napr. *CYBRID 2017* v koordinácii s paralelným a koordinovaným cvičením (PACE) pod vedením EÚ, a technicko-operačných cvičení, ako je napr. *DEFNET*;
- prípadná realizácia osobitného cvičenia EÚ SBOP v oblasti kybernetickej obrany a preskúmanie možnej koordinácie s celoeurópskymi kybernetickými cvičeniami, ako napríklad *CyberEurope*, organizované agentúrou ENISA;
- pokračovanie v účasti na iných mnohonárodných cvičeniach v oblasti kybernetickej obrany, ako napríklad *Locked Shields*;
- pozývanie relevantných medzinárodných partnerov, ako sú NATO, na cvičenia v súlade s rámcom politiky EÚ v oblasti cvičení;
- organizácia pravidelných cvičení na základe súboru nástrojov kybernetickej diplomacie, počas ktorých členské štáty EÚ môžu cvičiť reakcie na škodlivé kybernetické činnosti.

6. Posilnenie spolupráce s príslušnými medzinárodnými partnermi

V rámci medzinárodnej spolupráce je potrebné zabezpečiť dialóg s medzinárodnými partnermi, konkrétne s NATO a inými medzinárodnými organizáciami, s cieľom prispieť k rozvoju účinných spôsobilostí v oblasti kybernetickej obrany. Je potrebné usilovať sa o zvýšenú angažovanosť v súvislosti s prácou, ktorá sa vykonáva v rámci Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE) a Organizácie Spojených národov (OSN), s cieľom zriadiť strategický rámec na predchádzanie konfliktom, spoluprácu a stabilitu v kybernetickom priestore.

V EÚ existuje politická vôľa užšie spolupracovať s NATO v oblasti kybernetickej obrany pri budovaní robustných a odolných spôsobilostí kybernetickej obrany, ako sa to vyžaduje v spoločnom vyhlásení, ktoré podpísali predseda Európskej rady, predseda Európskej komisie a generálny tajomník Organizácie Severoatlantickej zmluvy 8. júla 2016 vo Varšave. Pravidelné konzultácie medzi pracovníkmi jednotlivých organizácií, spoločné brífingy a prípadne stretnutia medzi politicko-vojenskou skupinou a príslušnými výbormi NATO pomôžu vyhnúť sa zbytočnej duplikácii a zabezpečia jednotnosť a komplementárnosť úsilia v súlade s uvedeným rámcom.

ESVČ a EDA budú spolu s členskými štátmi rozvíjať spoluprácu v oblasti kybernetickej obrany medzi EÚ a NATO s náležitým ohľadom na inštitucionálny rámec a nezávislosť rozhodovania týchto príslušných organizácií:

- zintenzívnenie prebiehajúcich činností v rámci vykonávania spoločného vyhlásenia predsedu Európskej rady, predsedu Európskej komisie a generálneho tajomníka Organizácie Severoatlantickej zmluvy;
- výmena najlepších postupov v oblasti krízového riadenia, ako aj v oblasti kybernetickej obrany vojenských a civilných misií a operácií;
- práca na jednotnosti výstupov pri vypracúvaní požiadaviek na spôsobilosti v oblasti kybernetickej obrany v prípadoch, keď sa prekrývajú, najmä v rámci dlhodobého rozvoja spôsobilostí v oblasti kybernetickej obrany;
- intenzívnejšie využívanie rámca spolupráce medzi EDA a centrom excelentnosti NATO pre spoluprácu v oblasti kybernetickej obrany ako počiatočnej platformy pre posilnenú spoluprácu na mnohonárodných projektoch v oblasti kybernetickej obrany, a to na základe primeraných posúdení.

EABO, ESVČ a EDA:

- zlepšia spoluprácu na koncepciách pre odbornú prípravu a vzdelávanie, ako aj cvičenia v oblasti kybernetickej obrany;
- zabezpečia recipročnú účasť zamestnancov na cvičeniach v súlade s dohodnutým rámcom.

CERT-EU:

- bude intenzívnejšie využívať svoje technické dohody s NCIRC (tím pre spôsobilosť reakcie na počítačové incidenty NATO) s cieľom zlepšiť situačné povedomie, výmenu informácií, mechanizmy včasného varovania a predvídať hrozby, ktoré by mohli zasiahnuť obe organizácie.

Pokiaľ ide o iné medzinárodné organizácie a príslušných medzinárodných partnerov EÚ, ESVČ a členské štáty podľa potreby:

- sledujú strategický vývoj a uskutočňujú konzultácie o otázkach kybernetickej obrany s medzinárodnými partnermi (medzinárodnými organizáciami a tretími krajinami);
- skúmajú možnosti spolupráce v otázkach kybernetickej obrany, a to aj s tretími krajinami, ktoré sa zúčastňujú na misiách a operáciách SBOP;
- podporujú v príslušných medzinárodných organizáciách, najmä v OSN, OBSE a na Regionálnom fóre ASEAN-u, aby sa v kybernetickom priestore uplatňovalo platné medzinárodné právo, a najmä Charta OSN v celom jej rozsahu, ako aj vypracúvanie a vykonávanie univerzálnych nezáväzných noriem zodpovedného správania sa štátov a regionálnych opatrení na budovanie dôvery (CBM) medzi štátmi s cieľom zvyšovať transparentnosť a znižovať riziko mylného vnímania opatrení, ktoré štáty prijímajú.

Komisia a ESVČ:

- v prípade potreby podporujú budovanie kybernetických spôsobilostí pre partnerov EÚ prostredníctvom zmeneného nástroja na podporu stability a mieru.

Nadväzujúce opatrenia

ESVČ/EDA/Komisia v rámci koordinácie vykonávania CDPF zo strany ESVČ predkladajú politicko-vojenskej skupine s účasťou členov horizontálnej pracovnej skupiny pre kybernetické otázky a Politickému a bezpečnostnému výboru výročnú správu o pokroku, ktorá obsahuje šesť oblastí uvedených vyššie, s cieľom posúdiť vykonávanie CDPF. Každých šesť mesiacov sa podáva aj ústna správa.

Je veľmi dôležité, aby sa – podľa toho, ako sa kybernetické hrozby vyvíjajú – identifikovali nové požiadavky v oblasti kybernetickej obrany a následne sa zahrnuli do CDPF. Najbližšia revízia CDPF by sa mala predložiť najneskôr do polovice roka 2022 v úzkej konzultácii s členskými štátmi.