Rada
Evropské unie

Brusel 19. listopadu 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

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	19. listopadu 2018
Příjemce:	Delegace
Předmět:	Politický rámec EU pro kybernetickou obranu (aktualizace z roku 2018)

Delegace naleznou v příloze Politický rámec EU pro kybernetickou obranu (aktualizace z roku 2018) přijatý Radou na jejím 3652. zasedání konaném dne 19. listopadu 2018.

PŘÍLOHA

POLITICKÝ RÁMEC EU PRO KYBERNETICKOU OBRANU

(aktualizovaný v roce 2018)

Oblast působnosti a cíle

Aby byly schopny reagovat na měnící se bezpečnostní výzvy, musejí EU a její členské státy posilovat svou kybernetickou odolnost a rozvíjet robustní schopnosti v oblasti kybernetické bezpečnosti a obrany.

Politický rámec EU pro kybernetickou obranu podporuje rozvoj schopností kybernetické obrany členských států EU i posilování kybernetické ochrany bezpečnostních a obranných infrastruktur EU, aniž by byly dotčeny právní předpisy členských států a EU, a to včetně rozsahu kybernetické obrany, je-li vymezen.

Kyberprostor představuje pátou oblast operací vedle pozemního, námořního, vzdušného a vesmírného prostoru: úspěšné provádění misí a operací EU rostoucí měrou závisí na nepřetržitém přístupu k bezpečnému kyberprostoru, a vyžaduje tudíž robustní a odolné kybernetické operační schopnosti.

Cílem aktualizovaného politického rámce pro kybernetickou obranu je dále rozvíjet politiku EU pro kybernetickou obranu na základě zohlednění relevantního vývoje v rámci jiných souvisejících fór a oblastí politik a se zřetelem k provádění politického rámce pro kybernetickou obranu od roku 2014. Rámec stanoví prioritní oblasti pro kybernetickou obranu a vyjasňuje úlohu jednotlivých evropských aktérů, přičemž plně respektuje povinnosti a pravomoci subjektů Unie a členských států, jakož i institucionální rámec EU a její nezávislost v rozhodování.

Souvislosti

Evropská rada v závěrech o SBOP z prosince roku 2013 vyzvala stejně jako Rada v závěrech o SBOP z listopadu téhož roku k vypracování politického rámce EU pro kybernetickou obranu na základě návrhu vysoké představitelky připraveného ve spolupráci s Evropskou komisí a Evropskou obrannou agenturou (EDA). Politický rámec EU pro kybernetickou obranu přijala Rada dne 18. listopadu 2014[1]; konkrétní výsledky získávané od té doby na základě provádění rámce přispěly k výraznému posílení schopností kybernetické obrany členských států. Členské státy si vyžádaly aktualizaci politického rámce EU pro kybernetickou obranu v rámci výroční zprávy o jeho provádění za rok 2017[2], a to se zřetelem k iniciativám EU v oblasti bezpečnosti a obrany, jako je zejména koordinovaný každoroční přezkum v oblasti obrany (CARD), stálá strukturovaná spolupráce (PESCO), Evropský obranný fond (EDF) a pakt pro civilní SBOP, a s ohledem na revizi plánu rozvoje schopností (CDP) z roku 2018 a na plán rozvoje civilních schopností (CCDP).

Kybernetická bezpečnost představuje prioritu v rámci globální strategie zahraniční a bezpečnostní politiky EU a v rámci úrovně ambicí EU[3]. V globální strategii je zdůrazněno, že je třeba posilovat kapacity s cílem chránit EU a její občany a reagovat na vnější krize. Globální strategie dále zdůrazňuje, že je nutno posilovat EU jakožto bezpečnostní společenství. V této souvislosti by činnosti v oblasti bezpečnosti a obrany měly rovněž posilovat strategickou úlohu EU a její schopnost jednat samostatně, je-li to nezbytné, a ve spolupráci s partnery, kdykoli je to možné. Tyto cíle vyžadují větší spolupráci v oblasti rozvoje schopností a podporu účinnosti a interoperability výsledných civilních a vojenských schopností.

---

1 Dokument Rady 15585/14 ze dne 18. 11. 2014.
2 Dokument Rady 15870/17 ze dne 19. 12. 2017.
3 Závěry Rady o provádění globální strategie EU v oblasti bezpečnosti a obrany ze dne 14. 11. 2016.

Společný soubor návrhů pro účely provádění společného prohlášení, jež ve Varšavě dne 8. prosince 2016[4] podepsali předseda Evropské rady, předseda Evropské komise a generální tajemník Severoatlantické aliance, zahrnuje konkrétní opatření pro rozšíření spolupráce EU a NATO v oblasti kybernetické bezpečnosti a obrany, a to mimo jiné jak v rámci misí a operací, tak i v souvislosti s rozvojem schopností kybernetické obrany a souvisejícího výzkumu a technologií, odborné přípravy a vzdělávání, cvičení a začleňování kybernetických otázek do řízení krizí. Tato spolupráce probíhá při plném zohlednění zásad otevřenosti, transparentnosti, inkluzivity, reciprocity a rozhodovací autonomie EU. Sdílení informací technického rázu v zájmu lepšího předcházení kybernetickým incidentům, jejich odhalování a reakce na ně v EU i v NATO usnadňuje technická dohoda, kterou v únoru roku 2016 podepsala skupina pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU) a složka NATO pro schopnost reakce na počítačové incidenty (NCIRC).

Je třeba mít na paměti, že k plnění cílů politiky kybernetické obrany vymezených v tomto dokumentu přispívá několik politik EU a že tento rámec zohledňuje rovněž příslušnou regulační, politickou a technologickou podporu v civilní oblasti. Například v červenci roku 2016 Evropský parlament a Rada přijaly směrnici o bezpečnosti sítí a informací[5], kterou bude navýšena celková připravenost členských států na boj proti kybernetickým hrozbám a posílena spolupráce napříč EU. Touto směrnicí se stanoví opatření pro dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů v rámci Unie s cílem zlepšit fungování vnitřního trhu. Lhůta pro provedení směrnice uplynula dne 9. května 2018.

---

[4] Závěry Rady o provádění společného prohlášení předsedy Evropské rady, předsedy Evropské komise a generálního tajemníka Severoatlantické aliance (6. prosince 2016, dokument 15283/16; 5. prosince 2017, dokument 14802/17).

[5] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

Návrh aktu EU o kybernetické bezpečnosti ze září roku 2017 zahrnuje nový mandát pro agenturu Evropské unie pro kybernetickou bezpečnost (neboli agenturu ENISA) a zřízení rámce pro certifikaci na úrovni celé EU. Jakmile začne být tento certifikační rámec uplatňován, měl by podporovat vysoké standardy pro procesy, produkty a služby v oblasti informačních a komunikačních technologií a sloužit jako zdroj konkurenční výhody a rovněž větší jistoty na straně spotřebitelů a zadavatelů zakázek. Rovněž v září roku 2017 učinila Komise další krok směřující k tomu, aby byla EU připravena na případy přeshraničních incidentů velkého rozsahu v oblasti kybernetické bezpečnosti ("Blue Print"), a v současné době spolupracuje s členskými státy a dalšími institucemi, agenturami a subjekty na vývoji evropské spolupráce pro případ kybernetické bezpečnostní krize, přičemž jsou zaváděna praktická operační ustanovení a dokumentace pro všechny relevantní aktéry, procesy a postupy v kontextu stávajících mechanismů EU pro zvládání krizí a katastrof, zejména opatření pro integrovanou politickou reakci na krize.

V závěrech Rady o posílení evropské kybernetické odolnosti z listopadu roku 2016 byl vymezen společný cíl, jímž je přispívat ke strategické samostatnosti EU, jak je uvedeno v závěrech Rady z listopadu roku 2016 o globální strategii zahraniční a bezpečnostní politiky Evropské unie, a to rovněž v oblasti kyberprostoru. Evropská rada tento cíl opětovně potvrdila v červnu roku 2018 s tím, že také vyzdvihla potřebu posilovat schopnosti zaměřené na boj proti hrozbám v oblasti kybernetické bezpečnosti, jež mají původ mimo EU.

V roce 2017 Rada přijala rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru v podobě souboru nástrojů pro diplomacii v oblasti kybernetiky[6]. Rámec by měl podpořit spolupráci, usnadňovat zmírňování hrozeb a dlouhodobě ovlivňovat chování potenciálních agresorů. K předcházení nepřátelským činnostem v kyberprostoru a k boji proti nim využívá rámec opatření SZBP včetně omezujících opatření. Pachatelé nepřátelských činností v kyberprostoru musejí být za své činy hnáni k odpovědnosti a členské státy EU se vybízejí, aby dále rozvíjely své schopnosti reakce na nepřátelské činnosti v kyberprostoru, a to koordinovaným způsobem v souladu se souborem nástrojů pro diplomacii v oblasti kybernetiky. Státy by neměly provádět nebo vědomě podporovat činnosti v oblasti informačních a komunikačních technologií, jež jsou v rozporu s jejich závazky podle mezinárodního práva, a neměly by vědomě umožňovat, aby jejich území bylo využíváno k páchání mezinárodních protiprávních činů za využití informačních a komunikačních technologií.

V září roku 2017 Komise a vysoká představitelka, místopředsedkyně Komise předložily společné sdělení[7] o kybernetických otázkách, jehož cílem je omezit rizika plynoucí z nových hrozeb. Kybernetická obrana je v něm zahrnuta jako jedna z hlavních oblastí činnosti a politický rámec pro kybernetickou obranu představuje jeden z pilířů jeho konkrétního provádění[8].

Ve svých závěrech z listopadu roku 2017 o kybernetických otázkách Rada uznala, že se prohlubuje propojenost kybernetické bezpečnosti a obrany, a vyzvala k intenzivnější spolupráci v oblasti kybernetické obrany, mimo jiné k podpoře spolupráce mezi civilními a vojenskými pracovníky činnými na poli reakce na incidenty. Rovněž v těchto závěrech zdůraznila, že by mimořádně závažný kybernetický incident nebo krize mohly danému členskému státu zavdat dostatečný důvod k uplatnění doložky solidarity EU nebo doložky o vzájemné pomoci.

---

6 Závěry Rady o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“), dokument 9916/17, 7. června 2017.

7 Společné sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU (13. září 2017, (JOIN (2017) 450 final)).

8 Závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU (20. listopadu 2017, dokument 14435/17).

Dne 11. prosince 2017 byla zahájena stálá strukturovaná spolupráce (PESCO). Tento ambiciózní, závazný a inkluzivní rámec spolupráce zřízený mezi 25 členskými státy obsahuje závazek, podle něhož má být zvýšeno úsilí ve spolupráci na kybernetické obraně, jakož i na souvisejících projektech PESCO. První soubor projektů PESCO, jejž členské státy účastnící se stálé strukturované spolupráce identifikovaly v roce 2017, zahrnuje dva projekty týkající se kybernetické obrany: „Týmy rychlé kybernetické reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti“ a „Platforma pro sdílení informací o kybernetických hrozbách a reakci na incidenty“. S dalšími soubory projektů PESCO se počítá do budoucna. PESCO bude rozvíjet schopnosti kybernetické obrany, a posilovat tak spolupráci mezi zúčastněnými členskými státy a zvyšovat interoperabilitu.

V aktualizovaném plánu EU pro rozvoj schopností (CDP), jejž schválil Řídící výbor EDA v červnu roku 2018, byla kybernetická obrana identifikována jako jeden z klíčových prvků, přičemž bylo uznáno, že je zapotřebí obranných kybernetických operací v jakémkoli operačním kontextu, založených na sofistikované aktuální i prediktivní informovanosti o situaci v kyberprostoru, včetně schopnosti kombinovat velké objemy údajů a zpravodajských informací z mnoha zdrojů na podporu urychleného rozhodování a posílené automatizace procesu shromažďování údajů, analýzy a asistence při rozhodování. Plán rozvoje schopností na rok 2018 identifikuje priority pro schopnosti kybernetické obrany v následujících oblastech: spolupráce a synergie s relevantními aktéry napříč oblastmi kybernetické obrany a kybernetické bezpečnosti; činnosti v oblasti výzkumu a technologií kybernetické obrany; rámce pro inženýrství systémů pro kybernetické operace; vzdělávání, odbornou přípravu, cvičení a hodnocení (ETEE); řešení výzev pro kybernetickou obranu ve vzduchu, vesmíru, na moři a na souši.

Kromě toho vyšlo v posledních několika letech jednoznačně najevo, že předcházení konfliktům, spolupráce a stabilizace v kyberprostoru musí být úkolem mezinárodního společenství. EU v úzké spolupráci s dalšími mezinárodními organizacemi, zejména s OSN, OBSE a regionálním fórem ASEAN, prosazuje strategický rámec pro předcházení konfliktům, spolupráci a stabilitu v kyberprostoru, jenž zahrnuje i) uplatňování mezinárodního práva v kyberprostoru, zejména Charty OSN v celém jejím rozsahu; ii) dodržování univerzálních nezávazných norem, pravidel a zásad odpovědného chování států; iii) vypracování a provádění regionálních opatření pro budování důvěry. Politický rámec pro kybernetickou obranu by měl podporovat i tyto činnosti.

Priority

V aktualizovaném politickém rámci pro kybernetickou obranu bylo vymezeno šest prioritních oblastí. Politický rámec je zaměřen zejména na rozvoj schopností kybernetické obrany a na ochranu komunikačních a informačních sítí používaných v rámci SBOP EU. Další prioritní oblasti zahrnují: odbornou přípravu a cvičení, výzkum a technologie, spolupráci civilní a vojenské oblasti a mezinárodní spolupráci. Pokud jde o odbornou přípravu, důraz je kladen na posílení odborné přípravy, již členské státy uskutečňují v oblasti kybernetické obrany, a odborné přípravy zaměřené na kybernetickou informovanost v linii velení v rámci SBOP. S cílem zlepšit schopnost EU reagovat na kybernetické a hybridní krizové situace, a zdokonalit za tímto účelem rozhodovací postupy a dostupnost informací je navíc třeba náležitým způsobem zohledňovat kybernetický rozměr při cvičeních. Kyberprostor je rychle se vyvíjející oblastí, a v civilní i ve vojenské oblasti je proto nutno podporovat nový technologický vývoj. Pro zajištění soudržné reakce na kybernetické hrozby má spolupráce civilní a vojenské oblasti v kybernetických otázkách klíčový význam. V neposlední řadě by pak pro posilování kybernetické bezpečnosti v EU i mimo ni, jakož i pro účely prosazování zásad a hodnot EU mohla být prospěšná intenzivnější spolupráce s mezinárodními partnery.

Tento rámec vymezuje návrhy a možnosti koordinace mezi relevantními orgány, institucemi a jinými subjekty EU. Rovněž bere zřetel na významnou úlohu, již na poli vývoje technologií pro kybernetickou bezpečnost a kybernetickou obranu plní soukromý sektor.

Kromě toho pak politický rámec pro kybernetickou obranu podporuje začlenění kybernetické obrany do mechanismů Unie určených pro řízení krizí, a to v případech, kdy mohou být v zájmu řešení účinků kybernetické krize použitelná příslušná ustanovení Smlouvy o EU a Smlouvy o fungování EU[9].

1. Podpora rozvoje schopností členských států v oblasti kybernetické obrany

Rozvoj schopností a technologií v oblasti kybernetické obrany by měl obnášet všechny aspekty rozvoje schopností, včetně doktríny, vedení, organizace, pracovníků, odborné přípravy, průmyslu, technologií, infrastruktury, logistiky a interoperability. Za tímto účelem by v zájmu zajištění účinné schopnosti kybernetické obrany měly členské státy zvýšit své úsilí. ESVČ, Komise a EDA by měly spolupracovat a uvedené úsilí podporovat.

Je zapotřebí průběžné hodnocení slabin informačních infrastruktur, které podporují mise a operace SBOP, jakož i sledování účinnosti ochrany v téměř reálném čase. Z operačního hlediska bude jednou z hlavních oblastí zájmu činností v oblasti kybernetické obrany zachování dostupnosti, integrity a důvěrnosti komunikačních a informačních sítí SBOP, nebude-li v mandátu operace nebo mise stanoveno jinak. ESVČ bude kromě toho ve spolupráci s členskými státy dále začleňovat kybernetické schopnosti do misí a operací SBOP.

Pachatelé nepřátelských činností v kyberprostoru musejí být za své činy hnáni k odpovědnosti. Je důležité, aby členské státy EU v zájmu reakce na nepřátelské činnosti v kyberprostoru spolupracovaly za podpory ze strany ESVČ. Na podporu takové společné reakce byl vypracován soubor nástrojů pro diplomacii v oblasti kybernetiky. ESVČ a EDA budou na základě souboru nástrojů pro diplomacii v oblasti kybernetiky pořádat pravidelná cvičení, v jejichž rámci budou moci členské státy EU provádět nácvik této reakce.

[9] Článek 222 SFEU a čl. 42 odst. 7 SEU s náležitým zohledněním článku 17 SEU.

Existující vymezení rozsahu kybernetické obrany ve vnitrostátních právních předpisech členských států i v právních předpisech EU je široké a nejednotné, a je tudíž třeba vypracovat jeho společné souhrnné pojetí.

Jelikož vojenské operace SBOP využívají pro účely velení, řízení, spojení a komunikačních a informačních systémů infrastrukturu poskytnutou členskými státy, je při plánování požadavků na informační infrastrukturu, které souvisejí s kybernetickou obranou, zapotřebí určitá míra strategické konvergence.

V návaznosti na činnost týmu EDA, který pracuje na projektu z oblasti kybernetické obrany zaměřeném na rozvoj schopností kybernetické obrany, EDA a členské státy:

- budou využívat plánu rozvoje schopností a jiných nástrojů, které usnadňují a podporují spolupráci mezi členskými státy, například koordinovaného každoročního přezkumu v oblasti obrany, a to s cílem zvýšit míru konvergence při plánování požadavků členských států v oblasti kybernetické obrany na strategické úrovni, zejména pokud jde o monitorování, získávání poznatků o situaci, prevenci, odhalování a ochranu, sdílení informací, schopnosti forenzní analýzy a analýzy škodlivého softwaru, vyvozená poučení, omezení škod, schopnosti dynamického obnovení, distribuované ukládání dat a zálohování dat;
- podpoří stávající i budoucí projekty sdružování a sdílení určené pro vojenské operace a související s kybernetickou obranou (např. v oblasti forenzních věd, rozvoje interoperability či stanovování norem)
- s využitím stávajících celounijních zkušeností vypracují standardní soubor cílů a požadavků, přičemž vymezí minimální úroveň kybernetické bezpečnosti a důvěry, jíž mají členské státy dosáhnout.

ESVČ a EDA:

- usnadní výměnu informací mezi členskými státy ohledně vnitrostátních doktrín a programů pro nábor a udržení pracovníků a pro záložní jednotky zaměřených na kybernetickou obranu.

EDA:

- provede studii rozsahu vojenských požadavků na kybernetickou obranu zakotvených ve vnitrostátních právních předpisech jednotlivých členských států, jakož i osvědčených postupů. Hlavním účelem této studie bude vypracování podnikové architektury kybernetické obrany, zahrnující rozsah, funkce a požadavky, jež v dané oblasti uplatňují členské státy na základě vnitrostátních a unijních právních předpisů.

Členské státy na dobrovolném základě:

- zlepší spolupráci mezi svými vojenskými skupinami pro reakci na počítačové hrozby (CERT) s cílem zlepšit předcházení incidentům a jejich řešení;
- využijí stálé strukturované spolupráce k dalšímu posílení spolupráce v oblasti kybernetické obrany, a to včetně nových projektů;
- budou ke společnému rozvoji schopností kybernetické obrany využívat Evropský obranný fond;
- vypracují společné pojetí uplatňování doložky o vzájemné pomoci v kybernetické oblasti, při současném zachování její flexibility;
- vypracují základní požadavky kybernetické obrany na informační infrastrukturu;
- v případech, kdy zlepšování schopností v oblasti kybernetické obrany závisí na civilních odborných poznatcích v oblasti bezpečnosti sítí a informací, budou využívat odborné poznatky ENISA, orgánů členských států sdružených ve skupině pro spolupráci v oblasti bezpečnosti sítí a případně dalších subjektů na úrovni EU, které na poli civilní kybernetické bezpečnosti disponují odborností.

Členské státy, ESVČ / Vojenský štáb EU, EBOŠ a EDA:

- s ohledem na certifikaci bojových skupin EU zváží přípravu odborné přípravy zaměřené na kybernetickou obranu.

Komise ve spolupráci s členskými státy:

- zváží začlenění kybernetické obrany do pracovních programů Evropského programu rozvoje obranného průmyslu a Evropského obranného fondu.

2. Posílení ochrany komunikačních a informačních systémů SBOP používaných subjekty EU

Aniž je dotčena úloha skupiny pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU) jako ústřední struktury všech orgánů, institucí a jiných subjektů EU určené ke koordinaci reakce na kybernetické incidenty, vypracuje ESVČ v rámci příslušných pravidel týkajících se rozpočtu Unie vhodnou a autonomní koncepci bezpečnostních otázek a otázek ochrany sítě a vybuduje vlastní schopnost v oblasti bezpečnosti informačních technologií. Jejím cílem bude zvýšit odolnost sítí ESVČ používaných v rámci SBOP s důrazem na prevenci, odhalování, reakci na incidenty, získávání poznatků o situaci, výměnu informací a mechanismy včasného varování.

Ochranu komunikačních a informačních systémů ESVČ a rozvoj schopností v oblasti bezpečnosti informačních technologií zajišťuje generální ředitelství ESVČ pro rozpočet a administrativu (BA). Další vyčleněné zdroje a podporu poskytnou také Vojenský štáb Evropské unie (EUMS), ředitelství pro řešení krizí a krizové plánování (CMPD) a útvar schopnosti civilního plánování a provádění (CPCC). Tato schopnost v oblasti bezpečnosti informačních technologií se bude vztahovat na systémy podléhající utajení i na systémy, které utajení nepodléhají, a bude nedílnou součástí stávajících provozních jednotek.

Rovněž je třeba zjednodušit bezpečnostní pravidla pro informační systémy poskytované během provádění misí a operací SBOP různými institucionálními subjekty EU. V této souvislosti by s cílem zvýšit odolnost sítí používaných v rámci SBOP mohla být zvážena možnost zavést jednotnou linii velení.

V zájmu lepší koordinace a posílené ochrany a odolnosti komunikačních a informačních systémů a sítí používaných v rámci SBOP byla v roce 2017 zřízena interní rada ESVČ pro správu kybernetických záležitostí pod vedením generálního tajemníka ESVČ.

ESVČ / BA:

- posílí na základě stávajících technických schopností a postupů schopnost ESVČ zabezpečit informační technologie s důrazem na prevenci, odhalování, reakci na incidenty, získávání poznatků o situaci, výměnu informací a mechanismus včasného varování. Rovněž bude dále rozvinuta strategie spolupráce se skupinou CERT-EU a existujícími schopnostmi EU v oblasti kybernetické bezpečnosti.

ESVČ / BA společně s EUMS, útvarem schopnosti vojenského plánování a vedení (MPCC), CMPD a CPCC:

- v oblasti zabezpečení informačních technologií vypracují soudržnou politiku a pokyny, přičemž zohlední mimo jiné technické požadavky na kybernetickou obranu v rámci SBOP pro účely struktur, misí a operací a stávající rámce spolupráce EU a její politiky s cílem dosáhnout konvergence, pokud jde o pravidla, politiky a organizaci.

ESVČ / společná zpravodajsko-analytická složka (SIAC):

- za využití stávajících struktur posílí schopnost posuzování kybernetických hrozeb a zpravodajské schopnosti s cílem identifikovat nová kybernetická rizika a poskytovat pravidelná posouzení rizik na základě strategického posouzení hrozeb a informací o incidentech v téměř reálném čase koordinovaných mezi příslušnými strukturami EU a zpřístupňovanými s různým stupněm utajení.

ESVČ/SIAC a CERT-EU:

- budou podporovat sdílení informací o kybernetických hrozbách v reálném čase mezi členskými státy a příslušnými subjekty EU. Příslušné vnitrostátní a evropské orgány za tímto účelem vypracují mechanismy pro sdílení informací a opatření pro budování důvěry, a to na základě dobrovolného přístupu, který bude vycházet ze stávající spolupráce.

EEAS/EUMS a MPCC:

- pro účely vojenských misí a operací SBOP budou dále rozvíjet koncepci kybernetické obrany a začlení ji do strategického plánování;
- ve spolupráci s operačním vedením vypracují standardní kybernetický operační postup na obecně použitelné operační úrovni.

EEAS/CPCC a CMPD:

- pro účely civilních misí SBOP budou dále rozvíjet koncepci kybernetické obrany a začleňovat ji do strategického plánování;
- budou posilovat schopnosti civilních misí SBOP v oblasti kybernetické obrany, využívat za tímto účelem existující infrastrukturu a prosazovat standardizaci a harmonizaci technologií, jež jsou v rámci misí a operací SBOP používány, přičemž v relevantních případech využijí odborných poznatků CERT-EU, ENISA a EDA;
- v průběhu posilování civilní SBOP budou dále zkoumat, jak mohou civilní mise SBOP podpořit hostitelské země v oblasti kybernetické bezpečnosti.

ESVČ:

- bude dále rozvíjet společné požadavky pro účely vojenských i civilních misí a operací SBOP;
- s využitím stávajících celounijních zkušeností posílí koordinaci kybernetické obrany v zájmu plnění cílů souvisejících s ochranou sítí, které používají institucionální subjekty EU podporující SBOP;
- s ohledem na měnící se situaci, pokud jde o hrozby, bude v konzultaci s členskými státy a jinými orgány EU provádět pravidelný přezkum požadavků na zdroje a dalších příslušných politických rozhodnutí.

3. Podpora civilně-vojenské spolupráce

Kyberprostor je rychle se vyvíjející oblastí: v civilní i ve vojenské oblasti je proto nutno technologický vývoj posilovat bezpečnostními systémy. V rámci možností by měla být naplánována koordinace mezi civilní a vojenskou oblastí v případech, kdy jsou obdobné technologické poznatky zdrojem řešení pro civilní i vojenské použití. V jiných případech jsou vojenské schopnosti a zbraňové systémy natolik specifické, že pro sdílení s civilními technologiemi neexistuje prostor. Aniž jsou dotčeny vnitřní uspořádání a právní předpisy členských států, využití civilně-vojenské spolupráce v oblasti kybernetiky lze zvážit mimo jiné pro výměnu osvědčených postupů, výměnu informací a mechanismy včasného varování, reakce na incidenty, posuzování rizik a zvyšování informovanosti, jakož i pro odbornou přípravu a cvičení.

Zlepšení civilní kybernetické bezpečnosti je důležitým faktorem, který přispívá k celkové odolnosti v oblasti bezpečnosti sítí a informací. Směrnice o bezpečnosti sítí a informací zvyšuje připravenost na vnitrostátní úrovni a posiluje spolupráci mezi členskými státy na úrovni Unie, a to na strategické i operační úrovni. Do této spolupráce jsou zapojeny vnitrostátní orgány dohlížející na politiky v oblasti kybernetické bezpečnosti i vnitrostátní skupiny CERT a skupina CERT-EU. Spolupráce mezi civilními a vojenskými skupinami CERT by měla být posilována při řádném zohlednění uvedeného vývoje. Cílem nového evropského aktu o kybernetické bezpečnosti je posílit evropskou odolnost vůči kybernetickým útokům a poskytnout rámec pro certifikaci produktů a služeb v oblasti kybernetické bezpečnosti, díky němuž vzroste důvěra v digitální civilní sféru.

EDA, ENISA, Evropské centrum pro boj proti kyberkriminalitě (EC3) a CERT-EU jsou společně s dalšími příslušnými orgány a agenturami EU vybízeny k tomu, aby v rámci svých příslušných mandátů a aniž by docházelo k překrývání s pravomocemi členských států, dále prohlubovaly svou spolupráci v následujících oblastech, k čemuž jsou rovněž vyzývány členské státy:

- vypracování společných profilů kompetencí v oblasti kybernetické bezpečnosti a obrany na základě osvědčených mezinárodních postupů a certifikace používané orgány, institucemi a jinými subjekty EU, přičemž se zohlední rovněž certifikační normy soukromého sektoru;
- přispění k dalšímu rozvoji a přizpůsobení organizačních a technických norem veřejného sektoru v oblasti kybernetické bezpečnosti a obrany za účelem použití v odvětví obrany a bezpečnosti. V případě potřeby se naváže na probíhající práci agentur ENISA a EDA;
- zavádění či další rozvoj pracovních mechanismů a ujednání pro účely výměny osvědčených postupů, zejména v oblasti vzdělávání, odborné přípravy a cvičení, jakož i v oblasti výzkumu a technologií a v dalších oblastech zajišťujících součinnost mezi civilní a vojenskou oblastí;
- vycházet ze stávajících zkušeností EU v oblasti předcházení kyberkriminalitě a jejího vyšetřování a schopností ve sféře forenzních věd a jejich lepšího uplatňování při rozvoji schopností kybernetické obrany;

Členské státy budou na dobrovolném základě:

- posilovat spolupráci civilních a vojenských skupin CERT napříč různými členskými státy.

ESVČ, Komise a členské státy:

- začlení kybernetickou obranu do postupů EU pro zvládání krizí a katastrof (prostřednictvím procesu v rámci plánu).

4. Výzkum a technologie

Poskytovatelé služeb v oblasti infrastruktury a informačních a komunikačních technologií (IKT) pro civilní a obranné účely se v důsledku společných požadavků týkajících se technologií a operačních schopností potýkají v oblasti kybernetické bezpečnosti s podobnými problémy. Společné potřeby v oblasti výzkumu a technologií a společné požadavky na systémy jsou odhadovány předem v zájmu zlepšení interoperability systémů v dlouhodobém horizontu a snížení nákladů na vývoj řešení. Aby bylo možné čelit stále rostoucímu počtu hrozeb a zranitelných míst, je nezbytné dosáhnout úspor z rozsahu. To by pak mělo usnadnit, aby byl v Evropě zachován konkurenceschopný průmysl zaměřený na kybernetickou obranu a zajištěn jeho růst.

Rozvoj schopností kybernetické obrany má důležitý rozměr v oblasti výzkumu a technologií. V rámci výzkumného programu v oblasti kybernetické obrany (CDRA) poskytla agentura EDA solidní základ pro stanovení priorit pro budoucí financování výzkumu a technologií v kontextu mezivládního rámce. Následný strategický plán výzkumu vypracovaný příslušnými ad hoc pracovními skupinami EDA zajišťuje fakticky podložené vymezení priorit, pokud jde o kybernetické technologie nezbytné pro vojenské účely, přičemž určuje příležitosti pro činnosti a investice v oblasti dvojího užití, pokud jde o vnitrostátní, nadnárodní či Evropskou unií financovaná opatření.

Pro zmírnění hrozeb a omezení zranitelných míst má zásadní význam rozvoj technologických kapacit v Evropě. Hlavní hybnou silou technologií a inovací souvisejících s kybernetickou obranou bude i nadále průmysl. Mezi oblasti, jimiž je třeba se zabývat, patří mimo jiné kryptografie, zabezpečené vestavěné systémy, odhalování škodlivého softwaru, simulační a vizualizační techniky, ochrana sítí a komunikačních systémů a technologie pro identifikaci a autentizaci. Je rovněž důležité zasazovat se o konkurenceschopný evropský průmyslový dodavatelský řetězec v oblasti kybernetické bezpečnosti tím, že se podpoří zapojení malých a středních podniků.

Zajištění toho, aby byla Evropa schopna udržet krok s mezinárodní konkurencí, pokud jde o technologické schopnosti v kybernetické oblasti, rovněž závisí na naší schopnosti podporovat průlomové inovace prostřednictvím vnitrostátních i unijních nástrojů, jako je Evropská rada pro inovace.

Pro usnadnění civilně-vojenské spolupráce při rozvoji schopností kybernetické obrany a pro posílení evropské technologické a průmyslové základny obrany[10], jakož i ve snaze přispět ke strategické samostatnosti EU rovněž v oblasti kyberprostoru, je-li to nezbytné, a ve spolupráci s partnery, kdykoli je to možné,

budou agentura EDA, Komise a členské státy:

- usilovat o součinnost úsilí v oblasti výzkumu a technologií vynakládaného ve vojenském odvětví s civilními programy pro výzkum a vývoj, zejména programy souvisejícími s průlomovými inovacemi, a při provádění přípravné akce zaměřené na obranný výzkum zohlední rozměr kybernetické bezpečnosti a obrany;
- sdílet plány výzkumu v oblasti kybernetické bezpečnosti (například strategický plán výzkumu v oblasti kybernetické bezpečnosti vypracovaný Evropskou obrannou agenturou), jakož i výsledné plány a opatření; za tímto účelem bude v úzké spolupráci s Komisí a členskými státy vypracován meziodvětvový výzkumný program v oblasti kybernetické obrany;
- přispívat k lepšímu začlenění rozměru kybernetické bezpečnosti a kybernetické obrany do programů, které mají rozměr dvojího užití v oblasti bezpečnosti a obrany, jako je například projekt pro výzkum uspořádání letového provozu jednotného evropského nebe (SESAR).

[10] Sdělení s názvem „Směrem ke konkurenceschopnějšímu a účinnějšímu odvětví obrany a bezpečnosti“, dokument COM (2013) 542.

Komise:

- zváží vytvoření Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost se sítí národních koordinačních center za účelem podpory technologických a průmyslových kapacit v oblasti kybernetické bezpečnosti a zvýšení konkurenceschopnosti průmyslu Unie v odvětví kybernetické bezpečnosti, a to při zajištění doplňkovosti a zamezení zdvojování úsilí v rámci sítě center kompetencí pro kybernetickou bezpečnost a s dalšími agenturami EU; centrum by mělo mimo jiné posílit spolupráci mezi oblastí civilních a obranných technologií a jejich využití, a to v úzké spolupráci a při zajištění plné doplňkovosti s EDA v oblasti kybernetické obrany;
- bude podporovat rozvoj průmyslových ekosystémů a inovačních seskupení zahrnujících celý hodnotový řetězec v oblasti bezpečnosti prostřednictvím využití akademických znalostí a inovací a průmyslové výroby v malých a středních podnicích.

Komise ve spolupráci s členskými státy:

- zohlední otázky kybernetické obrany ve výzvách v rámci přípravné akce zaměřené na obranný výzkum;
- zohlední kybernetickou obranu v rámci témat, k nimž vyzývá Evropský obranný fond;
- podpoří soudržnost politik EU s cílem zajistit, aby politické a technické aspekty kybernetické ochrany EU zůstaly v popředí technologických inovací a byly harmonizovány v celé EU (schopnost provádět analýzy a posuzování kybernetických hrozeb, iniciativy zaměřené na „bezpečnost již od fáze návrhu“, řízení závislosti pro přístup k technologiím atd.).

5. Zlepšení možností vzdělávání, odborné přípravy a cvičení

Má-li se zvýšit připravenost, pokud jde o řešení kybernetických hrozeb, a vytvořit společná kultura kybernetické obrany v rámci celé EU, z níž budou mít prospěch i mise a operace EU, je nutné zlepšit a posílit možnosti odborné přípravy v oblasti kybernetické obrany. Je zásadně důležité, aby rozpočty na vzdělávání a odbornou přípravu byly využívány účinně a aby se zároveň zajistila co nejvyšší kvalita. Klíčový význam bude mít sdružování a sdílení vzdělávání a odborné přípravy v oblasti kybernetické obrany na evropské úrovni.

Evropská bezpečnostní a obranná škola (EBOŠ), ESVČ, EDA, Komise a členské státy:

- na základě analýzy potřeb odborné přípravy v oblasti kybernetické obrany provedené agenturou EDA a zkušeností získaných v rámci odborné přípravy EBOŠ zaměřené na kybernetickou bezpečnost zavedou odbornou přípravu a vzdělávání v oblasti SBOP, které budou určeny různým cílovým skupinám, včetně ESVČ, personálu misí a operací SBOP a úředníků členských států, což by mělo rovněž řešit problémy související s udržením kvalifikovaného personálu v krátkodobém, střednědobém a dlouhodobějším horizontu;
- navrhnou navázání dialogu o kybernetické obraně zaměřeného na normy a certifikaci odborné přípravy s členskými státy, orgány EU, třetími zeměmi a dalšími mezinárodními organizacemi, jakož i soukromým sektorem;
- budou spolupracovat s poskytovateli odborné přípravy z evropského soukromého sektoru, jakož i s akademickými institucemi s cílem zlepšit kompetence a dovednosti personálu působícího v operacích a misích SBOP.

EBOŠ:

- bude dále rozvíjet platformu pro vzdělávání, odbornou přípravu, hodnocení a cvičení v kybernetické oblasti, která byla zřízena v jejím rámci (dále jen „kybernetická platforma“).
- zajistí součinnost s programy odborné přípravy jiných zúčastněných subjektů, jako jsou agentura ENISA, Europol, CEPOL a středisko excelence NATO pro spolupráci při kybernetické obraně;
- prozkoumá možnost společných programů odborné přípravy v oblasti kybernetické obrany organizovaných EBOŠ a NATO, které by byly přístupné všem členským státům EU, s cílem podpořit společnou kulturu kybernetické obrany.

Komise:

- posoudí možnosti, jak v rámci členských států posílit příležitosti k odborné přípravě a vzdělávání, které určila kybernetická platforma.

EDA:

- ve spolupráci s EBOŠ vypracuje další kurzy EDA za účelem splnění požadavků členských států na vzdělávání, odbornou přípravu a cvičení v oblasti kybernetické obrany;
- podpoří kybernetickou platformu, mimo jiné prostřednictvím postupného začleňování modulů vzdělávání, odborné přípravy, hodnocení a cvičení v kybernetické oblasti, vypracovaných v rámci Evropské obranné agentury.

ESVČ a členské státy:

- budou sledovat zavedené certifikační mechanismy EBOŠ pro programy odborné přípravy, a to v úzké spolupráci s příslušnými útvary orgánů, institucí a jiných subjektů EU na základě stávajících norem a znalostí; zváží možnost vytvoření specifických kybernetických modulů v rámci iniciativy vojenský Erasmus;

Je třeba zlepšit příležitosti, pokud jde o cvičení vojenských i civilních aktérů SBOP v oblasti kybernetické obrany. Společná cvičení slouží jako nástroj pro rozvoj společných znalostí a pochopení kybernetické obrany. Umožní se tak silám jednotlivých států zlepšit připravenost na působení v rámci mnohonárodního prostředí. Provádění společných cvičení v oblasti kybernetické obrany přispěje rovněž k budování interoperability a důvěry.

ESVČ, EDA, CERT-EU a členské státy se zaměří na podporu prvků kybernetické obrany v rámci SBOP a dalších cvičení:

- začlenění rozměru kybernetické obrany do stávajících scénářů cvičení pro účely cvičení *MILEX* a *Multi Layer*;
- pravidelné pořádání strategických/politických cvičení, jako byl *CYBRID 2017*, v koordinaci s paralelním a koordinovaným cvičením vedeným EU (PACE) a technicko-operačních cvičení, jako je *DEFNET*;
- případný rozvoj specializovaného cvičení v oblasti kybernetické obrany v rámci EU SBOP a prozkoumání možnosti koordinace s celoevropskými kybernetickými cvičeními, jako je cvičení *CyberEurope*, pořádané agenturou ENISA;
- pokračující účast na dalších mezinárodních cvičeních v oblasti kybernetické obrany, jako je *Locked Shields*;
- přizvání příslušných mezinárodních partnerů, jako je NATO, k účasti na cvičeních, a to v souladu s rámcem EU v oblasti politiky cvičení;
- pořádání pravidelných cvičení na základě souboru nástrojů pro diplomacii v oblasti kybernetiky, v jejichž rámci mohou členské státy EU provádět nácvik reakce na nepřátelské činnosti v kyberprostoru.

6. Posílení spolupráce s příslušnými mezinárodními partnery

V rámci mezinárodní spolupráce je třeba zajistit dialog s mezinárodními partnery, zejména s NATO a dalšími mezinárodními organizacemi, s cílem přispět k rozvoji účinných schopností kybernetické obrany. Je třeba usilovat o větší zapojení do práce vykonávané v rámci Organizace pro bezpečnost a spolupráci v Evropě (OBSE) a Organizace spojených národů (OSN) za účelem předložení strategického rámce pro předcházení konfliktům, pro spolupráci a stabilitu v kyberprostoru.

V EU existuje politická vůle více spolupracovat s NATO v oblasti kybernetické obrany s cílem vyvinout robustní a odolné schopnosti kybernetické obrany v souladu s požadavky stanovenými ve společném prohlášení podepsaném předsedou Evropské rady, předsedou Evropské komise a generálním tajemníkem Severoatlantické aliance dne 8. července 2016 ve Varšavě. Pravidelné vzájemné konzultace mezi zaměstnanci, vzájemné informování, jakož i případná setkání mezi Politicko-vojenskou skupinou a příslušnými výbory NATO napomohou zabránit zbytečnému zdvojování činnosti a zajistí soudržnost a doplňkovost úsilí v souladu s výše uvedeným rámcem.

ESVČ a EDA budou společně s členskými státy dále rozvíjet spolupráci mezi EU a NATO v oblasti kybernetické obrany, a to s patřičným ohledem na institucionální rámec a rozhodovací samostatnost zmíněných organizací:

- posílení činností probíhajících v rámci provádění společného prohlášení předsedy Evropské rady, předsedy Evropské komise a generálního tajemníka Severoatlantické aliance;
- výměna osvědčených postupů v oblasti řešení krizí, jakož i kybernetické obrany v rámci vojenských a civilních misí a operací;
- úsilí o soudržnost při vypracovávání požadavků na schopnosti kybernetické obrany, pokud se překrývají, zejména v souvislosti s dlouhodobým rozvojem schopností kybernetické obrany;
- další využití rámce EDA pro spolupráci se střediskem excelence NATO pro spolupráci při kybernetické obraně, který by měl sloužit jako počáteční platforma pro posílenou spolupráci na mnohonárodních projektech v oblasti kybernetické obrany, a to na základě patřičného hodnocení.

EBOŠ, ESVČ a EDA:

- posílí spolupráci týkající se koncepcí pro odbornou přípravu, vzdělávání a cvičení v oblasti kybernetické obrany;
- zajistí reciproční účast personálu na cvičeních v souladu s dohodnutým rámcem.

CERT-EU:

- bude dále využívat technické ujednání mezi CERT-EU a složkou NATO pro schopnost reakce na počítačové incidenty (NCIRC) za účelem zlepšení poznatků o situaci, sdílení informací, mechanismů včasného varování a předjímání hrozeb, jež by mohly mít dopad na obě organizace.

Pokud jde o další mezinárodní organizace a relevantní mezinárodní partnery EU, budou ESVČ a členské státy v případě potřeby:

- sledovat strategický vývoj a v otázkách kybernetické obrany vést konzultace s mezinárodními partnery (mezinárodními organizacemi a třetími zeměmi);
- zkoumat možnosti spolupráce v otázkách kybernetické obrany, mimo jiné i s třetími zeměmi, jež se účastní misí a operací SBOP;
- v rámci příslušných mezinárodních organizací, zejména OSN, OBSE a regionálního fóra ASEAN prosazovat uplatňování stávajícího mezinárodního práva v kyberprostoru, zejména Charty OSN v celém jejím rozsahu, vypracování a provádění univerzálních nezávazných norem odpovědného chování států, jakož i regionálních opatření k budování důvěry mezi státy za účelem zvýšení transparentnosti a snížení rizika nepochopení chování států.

Komise a ESVČ:

- podpoří ve vhodných případech budování kybernetických schopností partnerů EU prostřednictvím pozměněného nástroje přispívajícího ke stabilitě a míru.

Navazující činnosti

V návaznosti na koordinaci ze strany ESVČ, pokud jde o provádění politického rámce pro kybernetickou obranu, by ESVČ/EDA/Komise měly předložit Politicko-vojenské skupině, za účasti členů Horizontální pracovní skupiny pro otázky týkající se kybernetiky, a Politickému a bezpečnostnímu výboru výroční zprávu o pokroku zahrnující šest výše uvedených oblastí s cílem posoudit provádění zmíněného rámce. Každých šest měsíců budou rovněž poskytnuty ústní informace.

Je nezbytné, aby v závislosti na vývoji kybernetických hrozeb byly určeny nové požadavky na kybernetickou obranu a tyto následně začleněny do politického rámce pro kybernetickou obranu. Příští revize tohoto rámce by měla být předložena nejpozději v polovině roku 2022, a to v úzké konzultaci s členskými státy.