Az Európai Unió
Tanácsa

Brüsszel, 2018. november 19.
(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

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2018. november 19.
Címzett:	a delegációk
Tárgy:	Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat)

Mellékelten továbbítjuk a delegációknak az uniós kibervédelmi szakpolitikai keretet (2018. évi naprakésszé tett változat), amelyet a Tanács a 2018. november 19-i 3652. ülésén fogadott el.

MELLÉKLET

UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET

(2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT)

Hatály és célkitűzések

Az EU-nak és tagállamainak meg kell erősíteniük a kiberrezilienciájukat és megbízható kiberbiztonsági és -védelmi képességeket kell kialakítaniuk, hogy meg tudjanak felelni a változó biztonsági kihívásoknak.

Az uniós kibervédelmi szakpolitikai keret támogatja az uniós tagállamok kibervédelmi képességeinek fejlesztését, valamint az EU biztonsági és védelmi infrastruktúrája kibervédelmének megerősítését, a tagállamok nemzeti jogszabályai és az uniós jogszabályok sérelme nélkül, ideértve a kibervédelem hatályát is, amennyiben az az említett jogszabályokban meghatározásra kerül.

A kibertér az ötödik műveleti terület a szárazföld, a tenger, a légtér és a világűr mellett: az uniós missziók és műveletek végrehajtásának sikere egyre nagyobb mértékben függ a biztonságos kibertérhez való zavartalan hozzáféréstől, ezért szilárd és ellenálló kiberműveleti képességeket igényel.

A naprakésszé tett uniós kibervédelmi szakpolitikai keret célja az EU kibervédelmi politikájának továbbfejlesztése az egyéb releváns fórumokon és szakpolitikai területeken bekövetkezett lényeges fejlemények, valamint az uniós kibervédelmi szakpolitikai keret végrehajtása során 2014 óta nyert tapasztalatok figyelembevételével. Az uniós kibervédelmi szakpolitikai keret meghatározza a kibervédelem kiemelt területeit, továbbá pontosítja a különböző európai szereplők feladatait, ezzel egyidejűleg teljeskörűen tiszteletben tartja az uniós szereplők és a tagállamok feladatait és hatásköreit, csakúgy mint az EU intézményi keretét és döntéshozatali autonómiáját.

Háttér

A KBVP-ről szóló, 2013. decemberi európai tanácsi következtetésekben és a KBVP-ről szóló, 2013. novemberi tanácsi következtetésekben egyaránt feladatként szerepelt, hogy a főképviselő javaslata alapján, az Európai Bizottsággal és az Európai Védelmi Ügynökséggel (EDA) együttműködve ki kell dolgozni az uniós kibervédelmi szakpolitikai keretet. A Tanács 2014. november 18-án elfogadta az uniós kibervédelmi szakpolitikai keretet[1], és az annak végrehajtása során azóta elért konkrét eredmények hozzájárultak a tagállamok kibervédelmi képességeinek jelentős fokozásához. Az uniós kibervédelmi szakpolitikai keret végrehajtásáról szóló 2017. évi éves jelentés[2] részeként, figyelembe véve a biztonság és védelem területét érintő uniós kezdeményezéseket – nevezetesen a koordinált éves védelmi szemlét (CARD), az állandó strukturált együttműködést (PESCO), az Európai Védelmi Alapot (EDF) és a polgári KBVP területére vonatkozó paktumot –, valamint a képességfejlesztési terv és a polgári képességfejlesztési terv 2018. évi felülvizsgálatát, a tagállamok szükségesnek ítélték az uniós kibervédelmi szakpolitikai keret naprakésszé tételét.

A kiberbiztonság prioritást élvez az EU kül- és biztonságpolitikára vonatkozó globális stratégiájában és az uniós ambíciószinten belül[3]. A globális stratégia hangsúlyozza, hogy fokozni kell az EU és az uniós polgárok védelmével és a külső válságokra való reagálással kapcsolatos kapacitásokat, továbbá hogy meg kell erősíteni az EU-t mint biztonsági közösséget. Ezzel összefüggésben a biztonsági és védelmi erőfeszítések várhatóan növelni fogják az Unió stratégiai szerepét és arra vonatkozó kapacitását is, hogy amikor és ahol szükséges, önállóan, illetve ahol csak lehet, partnerekkel együttműködve tudjon fellépni. E célok elérése szélesebb körű együttműködést igényel a képességfejlesztés területén, előmozdítva az annak eredményeként létrejövő polgári és katonai képességek hatékonyságát és interoperabilitását.

---

1 15585/14 tanácsi dokumentum, 2014. november 18.
2 15870/17 tanácsi dokumentum, 2017. december 19.
3 A Tanács következtetései az EU kül- és biztonságpolitikára vonatkozó globális stratégiájának a biztonság és a védelem területén történő végrehajtásáról, 2016. november 14.

Az Európai Tanács elnöke, az Európai Bizottság elnöke és az Észak-atlanti Szerződés Szervezetének főtitkára által 2016. július 8-án Varsóban aláírt együttes nyilatkozat végrehajtásával kapcsolatos közös javaslatok[4] között szerepelnek az EU–NATO együttműködésnek a kiberbiztonság és -védelem területére történő kiterjesztésére vonatkozó konkrét intézkedések, többek között a missziók és műveletek összefüggésében, továbbá a kibervédelmi képességek fejlesztésével, a kutatással és technológiával, az oktatással, képzéssel és gyakorlatokkal, valamint a kiberszempontoknak a válságkezelési mechanizmusokba való beillesztésével kapcsolatban. Ezen együttműködés során maradéktalanul tiszteletben kell tartani a nyitottság, az átláthatóság, az inkluzivitás és a kölcsönösség elvét, valamint az EU döntéshozatali autonómiáját. Az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) és a NATO kiberbiztonsági eseményeket kezelő képessége (NCIRC) által 2016 februárjában aláírt technikai megállapodás elősegíti a technikai információk cseréjét annak érdekében, hogy mindkét szervezetnél javítani lehessen a kiberbiztonsági események megelőzését, felderítését és az azokra való reagálást.

Emlékeztetni kell arra, hogy a kibervédelmi szakpolitika e dokumentumban meghatározott céljaihoz számos uniós politika hozzájárul, és arra, hogy az uniós kibervédelmi szakpolitikai keret figyelembe veszi a polgári területre vonatkozó releváns jogszabályokat, szakpolitikákat és technológiai támogatást is. 2016 júliusában például az Európai Parlament és a Tanács elfogadta a hálózat- és információbiztonsági irányelvet[5], amely javítani fogja a tagállamok általános felkészültségét a kiberfenyegetésekkel szemben, és fokozni fogja az egész Unióra kiterjedő együttműködést. Az említett irányelv a belső piac működésének javítása érdekében intézkedéseket állapít meg a hálózati és információs rendszerek Unión belüli egységesen magas szintű biztonságának megvalósítása céljából. Az irányelv átültetésének határideje 2018. május 9. volt.

---

4 A Tanács következtetései az Európai Tanács elnöke, az Európai Bizottság elnöke és az Észak-atlanti Szerződés Szervezete főtitkára együttes nyilatkozatának végrehajtásáról (2016. december 6., 15283/16; 2017. december 5., 14802/17).

5 Az Európai Parlament és a Tanács 2016. július 6-i (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

Az uniós kiberbiztonsági jogszabályra irányuló 2017. szeptemberi bizottsági javaslat új megbízatást tartalmaz az uniós kiberbiztonsági ügynökség (ENISA) számára, valamint előirányozza egy uniós szintű kiberbiztonsági tanúsítási keretrendszer létrehozását. A tanúsítási keretrendszernek, amint életbe lép, elő kell mozdítania az ikt-folyamatokra, -termékekre és -szolgáltatásokra vonatkozó szigorú szabványok érvényesülését, versenyelőny forrásává kell válnia, és hozzá kell járulnia a fogyasztók és a beszerzők bizalmának növeléséhez. A Bizottság 2017 szeptemberében újabb lépést tett az EU nagy léptékű, határokon átnyúló kiberbiztonsági eseményekre való felkészültségének javítása érdekében („tervezet”), és most az európai kiberbiztonsági válsághelyzeti együttműködési keret kialakításán dolgozik a tagállamokkal és más intézményekkel, szervekkel és hivatalokkal együtt, kidolgozva az összes releváns szereplőre, folyamatra és eljárásra vonatkozó gyakorlati szabályokat és dokumentációt, a már meglévő uniós válság- és katasztrófakezelési mechanizmusokkal – elsősorban az uniós politikai szintű integrált válságelhárítási mechanizmussal – összefüggésben.

A Tanács az Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről szóló, 2016. novemberi következtetéseiben felvázolta az EU stratégiai autonómiájának növelésére vonatkozó közös célkitűzést, és arra az EU kül- és biztonságpolitikára vonatkozó globális stratégiájáról szóló, 2016. novemberi következtetéseiben is hivatkozik, többek között a kibertér vonatkozásában. Az Európai Tanács 2018 júniusában megerősítette ezt a célkitűzést, továbbá hangsúlyozta, hogy meg kell erősíteni az EU-n kívülről érkező kiberbiztonsági fenyegetésekkel szembeni védelmi képességeket.

A Tanács 2017-ben elfogadta a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét (az úgynevezett „kiberdiplomáciai eszköztárat”)[6]. A keret a várakozások szerint ösztönözni fogja az együttműködést, elő fogja segíteni a fenyegetések csökkentését, valamint hosszú távon hatással lesz a potenciális támadók magatartására. A keret a rossz szándékú kibertevékenységek megelőzése és az azokra való reagálás érdekében a közös kül- és biztonságpolitikai intézkedésekre támaszkodik, ideértve a korlátozó intézkedéseket is. A rossz szándékú kibertevékenységek elkövetőit felelősségre kell vonni a cselekményeikért, az uniós tagállamokat pedig ösztönözni kell a rossz szándékú kibertevékenységekkel kapcsolatos reagálási képességeik koordinált módon, a kiberdiplomáciai eszköztárral összhangban történő továbbfejlesztésére. Az államok nem végezhetnek, illetve tudatosan nem támogathatnak olyan információs és kommunikációs technológiai tevékenységeket, amelyek ellentétesek a nemzetközi jog szerinti kötelezettségeikkel, és nem engedélyezhetik, hogy területükön, a tudomásukkal az információs és kommunikációs technológiákat felhasználó és a nemzetközi joggal ellentétes, rossz szándékú tevékenységek folyjanak.

A Bizottság és a főképviselő/alelnök 2017 szeptemberében a kiberbiztonságról szóló közös közleményt[7] terjesztett elő, amely célul tűzte ki a fenyegetések folyamatosan változó természetéből eredő kockázatok mérséklését. A közös közlemény az intézkedések egyik fő területeként jelöli meg a kibervédelmet, az uniós kibervédelmi szakpolitikai keretet pedig a kibervédelem konkrét végrehajtásának egyik pilléreként[8].

A Tanács a kiberbiztonsággal foglalkozó, 2017. novemberi következtetéseiben megállapította, hogy a kiberbiztonság és -védelem egyre jobban összefonódik, és felszólította a tagállamokat a kibervédelmi együttműködés fokozására, többek között ösztönözve a kiberbiztonsági eseményeket elhárító, polgári és katonai területen tevékenykedő közösségek közötti együttműködést. Hangsúlyozta továbbá, hogy egy különösen súlyos kiberbiztonsági esemény vagy válság elegendő alapot szolgáltathat a tagállamoknak arra, hogy az uniós szolidaritási klauzulára és/vagy a kölcsönös segítségnyújtást előíró rendelkezésre hivatkozzanak.

---

6 A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”), 9916/17, 2017. június 7.

7 Közös közlemény az Európai Parlamentnek és a Tanácsnak: „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” (JOIN (2017) 450 final)).

8 A Tanács következtetései az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről (2017. november 20., 14435/17).

2017. december 11-én megkezdődött az állandó strukturált együttműködés (PESCO). Ezt az ambiciózus, kötelező erővel bíró, inkluzív együttműködési keretet 25 tagállam hozta létre, kötelezettséget vállalva arra, hogy fokozzák a kibervédelem területén folytatott együttműködésre és a kapcsolódó PESCO-projektekre irányuló erőfeszítéseiket. A PESCO-ban részt vevő tagállamok által 2017-ben előirányzott első PESCO-projektek között szerepel két kibervédelmmel kapcsolatos projekt is, „Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén”, illetve „A kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform” címmel. A tervek között további PESCO-projektek is szerepelnek. A PESCO elősegíti a kibervédelmi képességek fejlesztését, ezáltal erősíti a részt vevő tagállamok közötti együttműködést, és növeli az interoperabilitást.

Az EDA irányítóbizottsága által 2018 júniusában jóváhagyott, naprakésszé tett uniós képességfejlesztési terv kulcsfontosságú elemként jelöli meg a kibervédelmet, és megállapítja, hogy minden művelettel összefüggésben szükség lehet defenzív kiberműveletekre, amelyeknek alapos, a kibertér aktuális és jövőbeli helyzetére vonatkozó helyzetismereten kell alapulniuk, ideértve az arra vonatkozó képességet is, hogy számos forrásból származó, nagy mennyiségű adatot és hírszerzési információt tudjunk összevetni a gyors döntéshozatal érdekében, továbbá ideértve az adatgyűjtési, -elemzési és döntéstámogatási folyamat fokozott automatizálását is. A 2018. évi képességfejlesztési terv a következő területeken határoz meg a kibervédelmi képességekre vonatkozó prioritásokat: együttműködés és szinergiák az érintett szereplőkkel a kibervédelem és a kiberbiztonság teljes területén; kibervédelmi kutatási és technológiai tevékenységek; kiberműveletekre vonatkozó rendszertervezési keretek; oktatás, képzés, gyakorlatok és értékelés; valamint kibervédelmi kihívások kezelése a légtérben, a világűrben, a tengeren és a szárazföldön.

Végezetül, az elmúlt néhány évben egyértelművé vált, hogy a nemzetközi közösségnek együtt kell működnie, és a konfliktusok megelőzésére és a kibertér stabilitásának erősítésére kell törekednie. Az EU más nemzetközi szervezetekkel, elsősorban az ENSZ-szel, az EBESZ-szel és az ASEAN regionális fórummal együtt, elő kíván mozdítani egy olyan, a konfliktusmegelőzésre, az együttműködésre és a kibertér stabilitásának erősítésére vonatkozó stratégiai keretet, amely magában foglalja a következőket: i. a nemzetközi jognak és különösen az ENSZ Alapokmányának teljes körű alkalmazása a kibertérben; ii. a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó egyetemes, nem kötelező erejű normák, szabályok és elvek tiszteletben tartása; iii. regionális bizalomépítő intézkedések kidolgozása és végrehajtása. Ezt a törekvést az uniós kibervédelmi szakpolitikai keretnek is támogatnia kell.

Prioritások

A naprakésszé tett uniós kibervédelmi szakpolitikai keret hat prioritási területet határoz meg. A szakpolitikai keret legelső sorban a kibervédelmi képességek fejlesztésére, valamint az EU KBVP-vel kapcsolatos kommunikációs és információs hálózatainak védelmére összpontosít. További prioritási területek: képzés és gyakorlatok, kutatás és technológia, polgári-katonai együttműködés, valamint a nemzetközi együttműködés. A képzés területén külön hangsúlyt kell fektetni a tagállamok kibervédelmi képzéseinek, valamint a KBVP parancsnoki lánca kibertudatossággal kapcsolatos képzéseinek fejlesztésére. Fontos továbbá, hogy a gyakorlatok keretében megfelelő figyelmet kapjon a kiberdimenzió, annak érdekében, hogy a döntéshozatali eljárások javítása, valamint az információk rendelkezésre állásának fokozása révén javuljon az EU kiber- és hibrid válságokra való reagálási képessége. A kibertér gyorsan fejlődő terület, ezért támogatni kell az új technológiai fejlesztéseket a polgári és a katonai területen egyaránt. A kiberfenyegetésekre való koherens reagálás biztosítása szempontjából alapvető fontossággal bír a kiberkérdésekkel kapcsolatos polgári-katonai együttműködés. Végül, de nem utolsósorban, a nemzetközi partnerekkel való együttműködés fokozása segítheti az EU-n belüli és kívüli kiberbiztonság növelését, valamint az uniós elvek és értékek előmozdítását.

Az uniós kibervédelmi szakpolitikai keret az érintett uniós intézmények, szervek és hivatalok közötti koordinációra vonatkozó javaslatokat és lehetőségeket vázol fel. Felhívja továbbá a figyelmet arra, hogy a magánszektornak jelentős szerepet kell kapnia a kiberbiztonsági és kibervédelmi technológiák fejlesztése terén.

Az uniós kibervédelmi szakpolitikai keret emellett továbbra is támogatja a kibervédelmi vonatkozásoknak az uniós válságkezelési mechanizmusokba való beillesztését, amennyiben a kiberválságok hatásainak kezelésére alkalmazandóak lehetnek az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés vonatkozó rendelkezései[9].

1. A tagállami kibervédelmi képességek fejlesztésének támogatása

A kibervédelmi képességek és technológiák fejlesztése során foglalkozni kell a képességfejlesztés valamennyi aspektusával, ideértve a doktrínát, a vezetést, a szervezést, a személyzetet, a képzést, az ipart, a technológiát, az infrastruktúrát, a logisztikát és az interoperabilitást. A tagállamoknak e célból fokozniuk kell a hatékony kibervédelmi képességek megteremtésére irányuló erőfeszítéseiket. Az EKSZ-nek, a Bizottságnak és az EDA-nak együtt kell működnie ezen erőfeszítések támogatása érdekében.

A KBVP-missziókat és -műveleteket támogató információs infrastruktúrák gyenge pontjait folyamatosan értékelni kell, és ezzel egyidejűleg biztosítani kell a védelem hatékonyságának közel valós idejű leképezését. Műveleti szempontból a kibervédelmi tevékenységek egyik legfontosabb területének a KBVP-vel kapcsolatos kommunikációs és információs hálózatok működőképességének, sértetlenségének és titkosságának megóvását kell tekinteni, kivéve, ha a műveletek vagy missziók megbízatása másként rendelkezik. Ezenkívül az EKSZ-nek – a tagállamokkal együttműködve – még inkább integrálnia kell a kiberképességeket a KBVP-missziókba és -műveletekbe.

A rossz szándékú kibertevékenységek elkövetőit felelősségre kell vonni a cselekményeikért. Fontos, hogy az uniós tagállamok az EKSZ támogatásával fokozzák a rossz szándékú kibertevékenységekre való reagálással kapcsolatos kölcsönös együttműködésüket. A kiberdiplomáciai eszköztár létrehozásának célja az említett reagálással kapcsolatos kölcsönös együttműködés elősegítése. Az EKSZ és az EDA a kiberdiplomáciai eszköztár alapján rendszeres gyakorlatokat fog szervezni, amelyek keretében a tagállamok gyakorolhatják e tevékenységet.

---

[9] Az EUMSZ 222. cikke és az EUSZ 42. cikkének (7) bekezdése, az EUSZ 17. cikkének megfelelő figyelembevételével.

A tagállamok nemzeti jogszabályai és az uniós jogszabályok tágan értelmezve és különbözőképpen határozzák meg a kibervédelem hatályát – amennyiben tartalmaznak erre vonatkozó meghatározást –, ezért ki kell dolgozni a kibervédelem hatályának közös, átfogó értelmezését.

Mivel a KBVP katonai műveletei a tagállamok által biztosított vezetés, irányítás, hírközlés és informatika (C4) infrastruktúrájára épülnek, az információs infrastruktúrák kibervédelmi előírásainak megtervezésekor szükség van bizonyos mértékű stratégiai konvergenciára.

Az EDA kibervédelmi projektcsoportjának a kibervédelmi képességfejlesztést célzó munkájára építve az EDA és a tagállamok:

- annak érdekében alkalmazzák a képességfejlesztési tervet és a tagállamok közötti együttműködést megkönnyítő és támogató más eszközöket, például a CARD-ot, hogy stratégiai szinten növekedjen a tagállamok kibervédelmi követelményeinek megtervezésében a konvergencia mértéke, különösen a monitoring, a helyzetismeret, a megelőzés, a felderítés és a védelem, az információmegosztás, a rosszindulatú számítógépes programok elemzésére vonatkozó és a forenzikus képesség, a tanulságok, a károk mérséklése, a dinamikus helyreállítási képességek, a megosztottadat-tárolás és az adattartalékok tekintetében;
- támogatják a kibervédelemmel kapcsolatos, jelenlegi és jövőbeli katonai műveletek céljából indított erőforrás-összevonási és -megosztási projekteket (például a forenzikus tudományok, az interoperabilitás fejlesztése és a normák meghatározása terén);
- a meglévő uniós szintű tapasztalatokat hasznosítva kidolgozzák a kiberbiztonságnak és a bizalomnak a tagállamok által elérendő minimális szintjét meghatározó közös célkitűzéseket és előírásokat.

Az EKSZ és az EDA:

- megkönnyítik a tagállamok közötti cseréket a nemzeti kiberbiztonsági doktrínák, illetve a kibervédelmet középpontba helyező munkaerő-felvételi, állományban tartási és tartalékos programok tekintetében.

Az EDA:

- tanulmányozza a kibervédelmi katonai előírásoknak a tagállamok nemzeti jogszabályaiban és legjobb gyakorlataiban meghatározott hatályát. E tanulmányok fő célja a kibervédelem szervezeti architektúrájának kidolgozása, amelynek magában kell foglalnia az ezen a területen a tagállamok által alkalmazott hatályt, funkciókat és követelményeket a nemzeti és az uniós jogszabályok alapján.

A tagállamok önkéntes alapon:

- a biztonsági események megelőzésének és kezelésének javítása érdekében fokozzák az együttműködést a katonai hálózatbiztonsági vészhelyzeteket elhárító csoportjaik között;
- a kibervédelem területén folytatott együttműködés további javítása érdekében igénybe veszik a PESCO kínálta lehetőségeket, ideértve az új projekteket is.
- a kibervédelmi képességek közös fejlesztése érdekében igénybe veszik az Európai Védelmi Alap kínálta lehetőségeket;
- közös álláspontot dolgoznak ki a kölcsönös segítségnyújtást előíró rendelkezésnek a kibervédelem területén való alkalmazására vonatkozóan, megőrizve annak rugalmasságát;
- kidolgozzák az információs infrastruktúrák kibervédelmére vonatkozó alapvető követelményeket;
- olyan mértékben, amennyiben a kibervédelmi képességek javítása támaszkodik a polgári hálózat- és információbiztonsági szakértelemre, hasznosítják az ENISA, a Kiberbiztonsági Együttműködési Csoport keretében együttműködő tagállami hatóságok, valamint a polgári kiberbiztonsági tapasztalatokkal rendelkező, egyéb uniós szervezetek szakértelmét.

A tagállamok, az EKSZ/az Európai Unió Katonai Törzse, az EBVF és az EDA:

- mérlegelik a kibervédelmi képzés fejlesztésének lehetőségét, figyelembe véve az uniós harccsoporti minősítést.

A Bizottság, a tagállamokkal együttműködve:

- beépíti a kibervédelmet az európai védelmi ipari fejlesztési program és az Európai Védelmi Alap munkaprogramjaiba.

2. Az uniós szervek által a KBVP keretében használt kommunikációs és információs rendszerek védelmének növelése

Azon szerep sérelme nélkül, amelyet az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) az összes uniós intézmény, szerv és hivatal központi uniós kiberincidens-kezelési koordinációs struktúrájaként tölt be, illetve az uniós költségvetésre vonatkozó releváns szabályok keretében az EKSZ kidolgozza a biztonsági és hálózatvédelmi kérdések megfelelő és autonóm értelmezését, továbbá fejleszti saját információtechnológiai biztonsági kapacitását. Célja a KBVP keretében használt EKSZ-hálózatok rezilienciájának javítása, középpontba helyezve a megelőzést, a felderítést, az incidenskezelést, a helyzetismeretet, az információcserét és a korai előrejelző mechanizmusokat.

Az EKSZ kommunikációs és információs rendszereinek védelme és információtechnológiai biztonsági kapacitásának fejlesztése az EKSZ költségvetési és adminisztrációs főigazgatóságának irányítása alatt folyik. További célzott erőforrásokat és támogatást biztosít az Európai Unió Katonai Törzse (EUKT), a Válságkezelési és Tervezési Igazgatóság (CMPD), valamint a Polgári Tervezési és Végrehajtási Szolgálat (CPCC). Ez az információtechnológiai biztonsági kapacitás mind a minősített, mind a nem minősített rendszerekre kiterjed majd, és a meglévő operatív egységek szerves része lesz.

Emellett a KBVP-missziók és -műveletek végrehajtása során a különböző uniós intézményi szereplők által rendelkezésre bocsátott információs rendszerekre vonatkozó biztonsági szabályokat is észszerűsíteni kell. Ezzel összefüggésben mérlegelni lehetne azt a lehetőséget, hogy a KBVP keretében használt hálózatok rezilienciájának javítása érdekében egységes parancsnoki lánc jöjjön létre.

A KBVP keretében használt kommunikációs és információs rendszerek és hálózatok jobb koordinációja és fokozottabb védelme érdekében 2017-ben létrejött az EKSZ főtitkára által vezetett kiberirányítási testület.

Az EKSZ/a KÖLTSÉGVETÉSI ÉS ADMINISZTRÁCIÓS FŐIGAZGATÓSÁG:

- megerősíti az EKSZ keretében rendelkezésre álló információtechnológiai biztonsági kapacitást a meglévő műszaki képességek és eljárások alapján, középpontba helyezve a megelőzést, a felderítést, az incidenskezelést, a helyzetismeretet, az információcserét és a korai előrejelző mechanizmust. Ki kell dolgozni, illetve tovább kell fejleszteni a CERT-EU-val és a meglévő uniós kibervédelmi képességekkel való együttműködésre vonatkozó stratégiát.

Az EKSZ/a KÖLTSÉGVETÉSI ÉS ADMINISZTRÁCIÓS FŐIGAZGATÓSÁG az EUKT-val, az MPCC-vel, a CMPD-vel és a CPCC-vel közösen:

- koherens információtechnológiai biztonsági politikát és iránymutatásokat dolgoz ki, figyelembe véve a struktúrák, missziók és műveletek vonatkozásában a KBVP keretében fennálló kibervédelmi műszaki követelményeket, szem előtt tartva az Unión belül meglévő együttműködési kereteket és szakpolitikákat annak érdekében, hogy a szabályok, a politikák és a szervezés tekintetében konvergencia valósuljon meg.

Az EKSZ/az egységes információelemzési kapacitás (SIAC):

- a meglévő struktúrákra építve megerősíti a számítógépes veszélyforrásokkal kapcsolatos értékelő és felderítő kapacitást, hogy lehetséges legyen az új kiberkockázatok azonosítása és rendszeres kockázatelemzések készítése a stratégiai fenyegetések elemzése és az incidensekre vonatkozó, az érintett uniós struktúrák között koordinált, a különböző minősítési szintek szerint hozzáférhető, közel valós idejű információknak az alapján.

Az EKSZ/a SIAC és a CERT-EU:

- előmozdítja a számítógépes veszélyforrásokkal kapcsolatos, a tagállamok és az érintett uniós szervek közötti valós idejű információcserét. Ennek érdekében a meglévő együttműködésre épülő önkéntes alapú megközelítést alkalmazva az érintett nemzeti és európai hatóságok közötti információmegosztási mechanizmusokat és bizalomépítő intézkedéseket kell kidolgozni.

Az EKSZ/az EUKT és az MPCC:

- továbbfejleszti a KBVP keretében folyó katonai missziók és műveletek vonatkozásában a kibervédelmi koncepciót, és beépíti azt a stratégiai szintű tervezésbe;
- a műveleti parancsnokságokkal együttműködve kidolgozza a kibertérre alkalmazandó általános operatív szintű eljárási standardokat.

Az EKSZ/a CPCC és a CMPD:

- továbbfejleszti a KBVP keretében folyó polgári missziók vonatkozásában az egységesített kibervédelmi koncepciót, és beépíti azt a stratégiai szintű tervezésbe;
- a meglévő infrastruktúrára építve, illetve a KBVP-misszióknál és -műveleteknél használt technológiák standardizálásának és harmonizációjának előmozdításával megerősíti a polgári KBVP-missziók kibervédelmi képességeit, kihasználva adott esetben a CERT-EU, az ENISA és az EDA révén rendelkezésre álló szakértelmet;
- a polgári KBVP megerősítése érdekében tovább vizsgálja, hogy a polgári KBVP-missziók miként támogathatják a fogadó nemzeteket kiberbiztonság terén.

Az EKSZ:

- továbbfejleszti a katonai és polgári KBVP-missziókra és -műveletekre vonatkozó közös követelményeket;
- a meglévő uniós szintű tapasztalatokat hasznosítva megszilárdítja a kibervédelem koordinálását az uniós intézmények által használt, a KBVP-t támogató hálózatok védelmére vonatkozó célkitűzések elérése érdekében;
- a változó fenyegetettségi helyzet alapján rendszeresen felülvizsgálja az erőforrásokra vonatkozó követelményeket és más vonatkozó szakpolitikai döntéseket, és eközben konzultál a tagállamokkal és más uniós intézményekkel.

3. A polgári–katonai együttműködés előmozdítása

A kibertér gyorsan változik: a biztonsági rendszereknek a polgári és a katonai területen is támogatniuk kell a technológiai fejlődést. Amennyire lehetséges, elő kell irányozni a polgári és a katonai terület közötti együttműködést az olyan esetekben, amikor a hasonló technológiai fejlesztések a polgári és katonai alkalmazásokhoz is megoldásokat kínálnak. Más esetekben a katonai képességek és a fegyverrendszerek annyira specifikusak, hogy nincs lehetőség a polgári technológiák használatára. A tagállamok belső szervezeti kereteinek és jogszabályainak sérelme nélkül a kiberterületen folyó polgári–katonai együttműködés fontólóra vehető többek közt az alábbiak megvalósításához: a legjobb gyakorlatok cseréje, az információcsere és a korai előrejelző mechanizmusok, az incidenskezelési kockázatelemzések, a figyelemfelkeltés, valamint a képzések és a gyakorlatok.

A polgári vonatkozású kiberbiztonság javítása a hálózat- és információbiztonság általános rezilienciájának biztosításához hozzájáruló egyik fontos tényező. A hálózat- és információbiztonságról (NIS) szóló irányelv célja a nemzeti szintű kiberbiztonsági felkészültség növelése és az uniós szintű – mind stratégiai, mind pedig operatív – együttműködés megerősítése a tagállamok között. Az együttműködésben részt vesznek mind a kiberbiztonsági politikákat felügyelő nemzeti hatóságok, mind pedig a hálózatbiztonsági vészhelyzeteket elhárító nemzeti szintű csoportok (CERT-ek) és a CERT-EU. E fejleményekre figyelemmel meg kell erősíteni a polgári és a katonai CERT-ek közötti együttműködést. Az új uniós kiberbiztonsági jogszabály célja, hogy javítsa Európának a kibertámadásokkal szembeni rezilienciáját, továbbá létrehozza a termékek és szolgáltatások kiberbiztonsági tanúsítási rendszerét, és ezzel növelje a polgári digitális szféra bizalmát.

Arra ösztönözzük az EDA-t, Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA), a Számítástechnikai Bűnözés Elleni Európai Központot (EC3) és a CERT-EU-t és a többi érintett uniós szervet és hivatalt – saját hatáskörükön belül, és a tagállami hatáskörökkel való átfedések nélkül –, valamint a tagállamokat, hogy fokozzák együttműködésüket az alábbi területeken:

- dolgozzanak ki közös kiberbiztonsági és védelmi kompetenciaprofilokat a legjobb nemzetközi gyakorlatok és az uniós intézményekben, szervekben és hivatalokban használt minősítés alapján, figyelembe véve továbbá a magánszférában alkalmazott minősítési előírásokat is;
- vegyenek részt a közszférában alkalmazott kiberbiztonsági és védelmi szervezeti és technikai normák továbbfejlesztésében és kiigazításában a védelmi és biztonsági ágazatban való felhasználás céljából. Adott esetben építsenek az ENISA és az EDA folyamatban lévő munkájára;
- dolgozzák ki, illetve fejlesszék tovább azokat a munkafolyamatokat és eljárásokat, amelyek lehetővé teszik különösen az oktatással, a képzéssel és a gyakorlatokkal, a kutatással és a technológiával, továbbá más, polgári–katonai szinergiákat rejtő területekkel kapcsolatos legjobb gyakorlatok cseréjét;
- használják fel a kiberbűnözés megelőzése és az ilyen bűncselekmények kinyomozása, valamint a forenzikus képességek területén rendelkezésre álló uniós tapasztalatokat, és még jobban aknázzák ki azokat a kibervédelmi képességek fejlesztése során.

A tagállamok önkéntes alapon:

- megerősítik a tagállamok polgári és a katonai CERT-jei közötti együttműködést.

Az EKSZ, a Bizottság és a tagállamok:

- beépítik a kibervédelmet az uniós válság- és katasztrófakezelési eljárásokba (a tervezet kidolgozásának folyamata során).

4. Kutatás és technológia

Mivel a technológiákkal és operatív képességekkel kapcsolatos követelményeik megegyeznek, az infrastruktúrák, valamint az informatikai és kommunikációs (ikt) szolgáltatások üzemeltetői hasonló kiberbiztonsági kihívásokkal szembesülnek függetlenül attól, hogy polgári vagy katonai céllal végzik-e az üzemeltetést. A közös k+t igények és a rendszerekkel kapcsolatos közös követelmények a várakozások szerint hosszú távon javítani fogják a rendszerek interoperabilitását, továbbá csökkenteni fogják a megoldások kifejlesztésének költségeit. A folyamatosan növekvő számú fenyegetést és az egyre több gyenge pontot akkor lehet sikeresen kezelni, ha megvalósítjuk a méretgazdaságosságot. Ez pedig várhatóan megkönnyíti majd az európai kibervédelmi ipar versenyképességének megőrzését és fokozását.

A kibervédelmi képességek fejlesztésének kérdése jelentős kutatási és technológiai fejlesztési (k+t) dimenzióval rendelkezik. A kibervédelmi kutatási menetrend (CDRA) keretében az EDA szilárd alapot biztosított a jövőbeli k+t kiadások prioritási sorrendjének a kormányközi keretben történő megállapításához. Az EDA *ad hoc* munkacsoportjában kidolgozott újabb stratégiai kutatási menetrend kutatási eredményekre alapozva határozza meg a katonai szempontból szükséges kibertechnológiák prioritási sorrendjét, ugyanakkor arra is rámutat, hogy mely törekvések és befektetések esetében van lehetőség kettős felhasználásra, akár nemzeti, akár nemzetközi, akár uniós finanszírozású összefüggésben.

Alapvetően fontos, hogy a fenyegetések és a gyenge pontok csökkentése érdekében kiépítsük a technológiai kapacitásokat Európában. A jövőben is az ipar lesz a kibervédelemmel kapcsolatos technológiák és innováció elsődleges mozgatórugója. A kriptográfia, a biztonságos beágyazott rendszerek, a rosszindulatú szoftverek felderítése, a szimulációs és vizualizációs technikák, a hálózati és kommunikációs rendszerek védelme, az azonosítási és hitelesítési technológia azon területek közé tartozik, amelyekkel foglalkozni kell. A kis- és középvállalatok (kkv-k) bevonásával elő kell mozdítani, hogy létrejöjjön Európában egy versenyképes ipari kiberbiztonsági ellátási lánc.

Ahhoz, hogy a kibertechnológiai képességek terén Európa képes legyen lépést tartani a nemzetközi versenytársakkal, az is fontos, hogy nemzeti és uniós eszközökkel – így például az Európai Innovációs Tanács segítségével – fel tudjuk lendíteni az áttörést hozó innovációt.

A kibervédelmi képességfejlesztés terén folytatott polgári–katonai együttműködés elősegítése, az európai védelmi technológiai és ipari bázis megerősítése[10] és annak érdekében, hogy hozzájáruljon ahhoz, hogy az EU stratégiailag autonóm legyen a kibertér vonatkozásában is, ha és amikor szükséges, és lehetőség szerint a partnerekkel együttműködve**,**

Az EDA, a Bizottság és a tagállamok:

- törekszenek a szinergiákra a katonai k+t programok, valamint a polgári – különösen az áttörést hozó innovációkkal kapcsolatos – kutatási és fejlesztési programok között, és figyelembe veszik a kiberbiztonsági és -védelmi dimenziót a kutatásokhoz kapcsolódó előkészítő intézkedések végrehajtása során;
- megosztják egymással kiberbiztonsági kutatási menetrendjüket (pl. az Európai Védelmi Ügynökség stratégiai kutatási menetrendje) és az ezekhez tartozó ütemterveket és intézkedéseket; ebből a célból a Bizottsággal és a tagállamokkal szorosan együttműködve ki fogják dolgozni az ágazatokon átívelő kibervédelmi kutatási menetrendet;
- részt vesznek az arra irányuló törekvésekben, hogy a kiberbiztonság és a kibervédelem dimenziója még jobban beépüljön azokba a programokba, amelyek a kettős felhasználással összefüggő biztonsági és védelmi dimenzióval rendelkeznek, mint pl. az „Egységes európai égbolt” légiforgalmi szolgáltatási kutatási program (SESAR).

[10] Közlemény: „Úton egy versenyképesebb és hatékonyabb védelmi és biztonsági ágazat felé”, COM (2013) 542.

A Bizottság:

- megvizsgálja az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózata létrehozásának lehetőségét azzal a céllal, hogy támogassák a kiberbiztonsági technológiai és ipari képességeket, és növeljék az uniós kiberbiztonsági ipar versenyképességét, és eközben ne legyenek átfedések a kiberbiztonsági kompetenciaközpontok hálózatán belül, sem pedig más uniós hivatalok feladataival. A kompetenciaközpontnak többek között az lenne a feladata, hogy javítsa a polgári és a védelmi technológiák és alkalmazások közötti koordinációt, szorosan együttműködve az Európai Védelmi Ügynökséggel, és teljes mértékben kiegészítve annak a kibervédelem területén végzett tevékenységét;
- a tudományos ismeretekre, a kkv-k innovációs tevékenységére és az ipari termelésre építve támogatja a teljes biztonsági értékláncot lefedő ipari ökoszisztémák és innovációs klaszterek kialakítását.

A Bizottság a tagállamokkal együttműködve:

- a védelmi célú kutatásra irányuló előkészítő intézkedések pályázati felhívásaiban figyelembe veszi a kibervédelmi kérdéseket;
- az Európai Védelmi Alap pályázati felhívásaiban szereplő témák között figyelembe veszi a kibervédelmet;
- támogatja az uniós szakpolitikák közötti koherencia megteremtését, mivel ezzel biztosítható, hogy az uniós kibervédelem politikai és technikai szempontjai folyamatosan kiemelt figyelmet kapjanak a technológiai innováció során és az EU egész területén megvalósuljon harmonizációjuk (számítógépes fenyegetések elemzésére és értékelésére vonatkozó képesség, beépített biztonsági megoldásokra irányuló kezdeményezések, dependenciakezelés a technológiákhoz való hozzáférés érdekében stb.).

5. A képzési, oktatási és gyakorlati lehetőségek javítása

A kiberfenyegetésekre való felkészültség javítása és a közös uniós kibervédelmi kultúra kidolgozása érdekében, továbbá az uniós missziók és műveletek támogatása céljából javítani és bővíteni kell a kibervédelmi képzések lehetőségének tárházát. Alapvető fontosságú, hogy az oktatási és képzési forrásokat hatékonyan, ugyanakkor a lehető legjobb minőséget nyújtva használjuk fel. Kulcsfontosságú lesz a kibervédelemmel kapcsolatos oktatás és képzés uniós szintű összevonása és megosztása.

Az Európai Biztonsági és Védelmi Főiskola (EBVF), az EKSZ, az EDA, a Bizottság és a tagállamok:

- az EDA-nak a kibervédelemmel kapcsolatos képzési szükségletekről készített elemzése, valamint az EBVF által nyújtott kiberbiztonsági képzéssel kapcsolatos tapasztalatok alapján KBVP témájú képzést és oktatást dolgoznak ki többféle célközönség, köztük az EKSZ, a KBVP-missziók és -műveletek személyzete, illetve a tagállamok tisztviselői számára, hogy ezzel rövid, közép- és hosszú távon kezelni lehessen a képzett szakemberek megtartásával kapcsolatos nehézségeket;
- javasolják képzési szabványokkal és képesítésekkel kapcsolatos kibervédelmi párbeszéd megkezdését a tagállamokkal, az uniós intézményekkel, harmadik országokkal és egyéb nemzetközi szervezetekkel, valamint a magánszektor képviselőivel;
- együttműködésre lépnek az európai magánszektorbeli képzésszolgáltatókkal és felsőoktatási intézményekkel, a KBVP-műveletek és -missziók személyzete kompetenciáinak és készségeinek fejlesztése céljából.

Az EBVF:

- továbbfejleszti az EBVF keretében létrehozott kiberbiztonsági oktatási, képzési, értékelési és gyakorlati fórumot (kiberbiztonsági ETEE-fórum);
- szinergiákat alakít ki más érdekelt felek – pl. az ENISA, az Europol, az Európai Rendőrakadémia (CEPOL) és a NATO Kibervédelmi Kiválósági Együttműködési Központjának – képzési programjaival;
- megvizsgálja az EBVF–NATO közös kibervédelmi képzési programok lehetőségét, melyek valamennyi uniós tagállam számára nyitva állnának a közös kibervédelmi kultúra előmozdítása érdekében.

A Bizottság:

- megvizsgálja, hogy milyen lehetőségek vannak a kiberbiztonsági ETEE-fórum által meghatározott tagállami képzési és oktatási lehetőségek fejlesztésére.

Az EDA:

- az EBVF-fel közösen továbbfejleszti a kurzusait, hogy azok megfeleljenek a tagállamok követelményeinek a kibervédelmi oktatás, képzés és gyakorlat szempontjából;
- támogatja a kiberbiztonsági ETEE-fórumot többek között azzal, hogy fokozatosan beépíti az EDA keretében kidolgozott kibervédelmi oktatási, képzési, értékelési és gyakorlati modulokat.

Az EKSZ és a tagállamok:

- a képzési programok akkreditálására az EBVF jelenlegi akkreditációs mechanizmusait fogják alkalmazni, az uniós intézmények, szervek és hivatalok releváns szolgálataival szoros együttműködésben, továbbá a meglévő normák és ismeretek alapján; fontolóra fogják venni kiberspecifikus modulok létrehozását a Katonai Erasmus kezdeményezés keretében.

Több lehetőséget kell biztosítani a KBVP katonai és polgári szereplőinek arra, hogy kibervédelmi gyakorlatokban vegyenek részt. A közös gyakorlatok jó eszközt jelentenek a kibervédelemmel kapcsolatos közös tudás és ismeretek elmélyítésére, és lehetővé teszik a nemzeti erők számára, hogy jobban felkészüljenek arra, ha többnemzetiségű környezetben kell működniük. A közös kibervédelmi gyakorlatok növelik továbbá az interoperabilitást és a bizalmat.

Arra összpontosítva, hogy a KBVP-hez kapcsolódó és egyéb gyakorlatok során nagyobb hangsúlyt kapjanak a kibervédelmi elemek, az EKSZ, az EDA, a CERT-EU és a tagállamok:

- beépítik a kibervédelem dimenzióját a *MILEX* és a *MULTILAYER* programok keretében folytatott gyakorlatok forgatókönyveibe;
- rendszeresen szerveznek olyan stratégiai/politikai gyakorlatokat, mint az EU által vezetett párhuzamos és koordinált gyakorlattal (PACE) összehangolva lefolytatott *CYBRID 2017*, és olyan technikai-operatív gyakorlatokat, mint a *DEFNET*;
- adott esetben külön erre a célra kidolgoznak egy, a KBVP-hez tartozó uniós kibervédelmi gyakorlatot, és megvizsgálják a páneurópai kibervédelmi gyakorlatokkal, például az ENISA által szervezett *CyberEurope* gyakorlattal való koordináció lehetőségét;
- a jövőben is részt vesznek más olyan nemzetközi kibervédelmi gyakorlatokban, mint pl. a *Locked Shields*;
- a gyakorlatokra vonatkozó uniós szakpolitikai kerettel összhangban meghívják a gyakorlatokra a releváns nemzetközi partnereket, pl. a NATO-t;
- a kiberdiplomáciai eszköztár alapján rendszeres gyakorlatokat szerveznek, amelyekben a tagállamok gyakorolhatják a rosszindulatú kibertevékenységekre való válaszadást.

6. A releváns nemzetközi partnerekkel folytatott együttműködés elmélyítése

A nemzetközi együttműködés keretében biztosítani kell a nemzetközi partnerekkel, különösen a NATO-val és egyéb nemzetközi szervezetekkel folytatott párbeszédet, annak érdekében, hogy hatékonyabb kibervédelmi képességeket lehessen létrehozni. Erőteljesebb részvételre kell törekedni az Európai Biztonsági és Együttműködési Szervezet (EBESZ) és az Egyesült Nemzetek Szervezete (ENSZ) keretében folyó munkában, hogy megvalósuljon a kibertérben való konfliktusmegelőzés, együttműködés és stabilitás stratégiai kerete.

Az EU-ban megvan a politikai szándék arra, hogy továbbra is együttműködjünk a NATO-val a kibervédelem területén úgy, hogy stabil és ellenálló kibervédelmi képességeket alakítunk ki az Európai Tanács elnöke, az Európai Bizottság elnöke és az Észak-atlanti Szerződés Szervezetének főtitkára által 2016. július 8-án Varsóban aláírt együttes nyilatkozatban előírtaknak megfelelően. Célszerű rendszeres személyzeti szintű konzultációkat, más érintett szerveknek szóló tájékoztatókat és esetleg találkozókat tartani a katonapolitikai kérdésekkel foglalkozó csoport és a releváns NATO-bizottságok tagjai között, mivel ez hozzájárul a szükségtelen átfedések elkerüléséhez és biztosítja az erőfeszítések koherenciáját és egymást kiegészítő jellegét, a fent említett kerettel összhangban.

Az EKSZ és az EDA a tagállamokkal közösen – kellőképpen igazodva az intézményi kerethez és tiszteletben tartva az egyes szervezetek döntéshozatali autonómiáját – az alábbiak révén kibővíti az EU és a NATO közötti kibervédelmi együttműködést:

- fokozzák az Európai Tanács elnöke, az Európai Bizottság elnöke és az Észak-atlanti Szerződés Szervezete főtitkára együttes nyilatkozatának végrehajtásának keretében folyó tevékenységeket;
- kicserélik egymással a válságkezeléssel, valamint a katonai és polgári missziókkal és műveletekkel kapcsolatos legjobb gyakorlatokat;
- különösen a kibervédelmi képességek hosszú távú fejlesztése tekintetében törekszenek a koherenciára a kibervédelmi képességekre vonatkozó követelmények kidolgozása során, amennyiben azok átfedik egymást;
- – megfelelő értékelések alapján – fokozottabban kihasználják az EDA és a NATO Kibervédelmi Kiválósági Együttműködési Központja közötti együttműködési keretet, amely a nemzetközi kibervédelmi projektekben való megerősített együttműködés kiindulási pontja.

Az EBVF, az EKSZ és az EDA:

- elmélyíti a kibervédelmi képzéssel és oktatással, valamint gyakorlatokkal kapcsolatos elvek kidolgozása terén folytatott együttműködést;
- biztosítja személyzetük kölcsönös részvételét az elfogadott keret szerinti gyakorlatokban.

A CERT-EU:

- fokozottabban kiaknázza a CERT-EU és a NCIRC (a NATO számítógép-incidenskezelő képessége) közötti technikai megállapodást a helyzetismeret, az információmegosztás és a korai előrejelző mechanizmusok javítása érdekében, illetve azért, hogy elébe lehessen menni a mindkét szervezetet érintő esetleges fenyegetéseknek.

Az egyéb nemzetközi szervezetek és az EU releváns nemzetközi partnerei tekintetében az EKSZ és a tagállamok adott esetben:

- követik a stratégiai fejleményeket és kibervédelmi kérdésekben konzultációkat folytatnak a nemzetközi partnerekkel (nemzetközi szervezetekkel és harmadik országokkal);
- megvizsgálják, hogy a kibervédelmi kérdések terén milyen együttműködési lehetőségek nyílnak, többek között a KBVP-missziókban és -műveletekben részt vevő harmadik országokkal;
- az érintett nemzetközi szervezetekben – főleg az ENSZ-ben, az EBESZ-ben és az ASEAN regionális fórumon – előmozdítják a hatályos nemzetközi jog, különösen az ENSZ Alapokmányának teljes egészében való alkalmazását a kibertérben, a felelős állami magatartásra vonatkozó egyetemes, nem kötelező normák kidolgozását és bevezetését, valamint az államok közötti regionális bizalomépítő intézkedéseket, amelyekkel növelhető az átláthatóság és csökkenthetők az állami magatartással kapcsolatos téves nézetek.

A Bizottság és az EKSZ:

- adott esetben a stabilitás és a béke elősegítését szolgáló módosított eszköz segítségével támogatja az uniós partnerek kiberképesség-építését.

Követő intézkedések

Az EKSZ-nek/az EDA-nak/a Bizottságnak a kibervédelmi szakpolitikai keretnek az EKSZ által koordinált végrehajtása során elért eredményekről a fenti hat területre kiterjedő éves jelentést kell benyújtania a katonapolitikai kérdésekkel foglalkozó csoport számára – amelynek ülésén a kiberkérdésekkel foglalkozó horizontális munkacsoport tagjai is részt vesznek –, valamint a Politikai és Biztonsági Bizottság számára, hogy értékelhessék a kibervédelmi szakpolitikai keret végrehajtását. Ezenfelül félévente szóban is be kell számolniuk.

Mivel egyre több kiberbiztonsági fenyegetéssel kell szembenéznünk, alapvetően fontos, hogy meghatározzuk a kibervédelemmel kapcsolatos új követelményeket, és azokat aztán beépítsük a kibervédelmi szakpolitikai keretbe. A kibervédelmi szakpolitikai keret következő felülvizsgálatára 2022 közpéig fog sor kerülni, a tagállamokkal szoros egyeztetésben.