Az Európai Unió
Tanácsa

Brüsszel, 2014. november 18.

15585/14

COPS 303
POLMIL 103
CYBER 61
RELEX 934
JAI 880
TELECOM 210
CSC 249
CIS 13
COSI 114

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács
Dátum:	2014. november 17–18.
Előző dok. sz.:	15193/14 + COR 1 COPS 287 POLMIL 97 CYBER 58 RELEX 897 JAI 845 TELECOM 196 CSC 242 CIS 12 COSI 111
Tárgy:	Uniós kibervédelmi szakpolitikai keret

Mellékelten továbbítjuk a delegációknak az uniós kibervédelmi szakpolitikai keretről szóló, a Tanács által 2014. november 18-án elfogadott dokumentumot.

MELLÉKLET

UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET

Háttér és célkitűzések

A kiberteret gyakran a katonai tevékenység ötödik területeként említik, amely éppen olyan alapvető jelentőségű az Európai Unió közös biztonság- és védelempolitikájának (KBVP) végrehajtása szempontjából, mint a szárazföld, a tenger, a légtér vagy a világűr. A KBVP sikeres végrehajtása egyre nagyobb mértékben függ attól, hogy rendelkezésre áll-e biztonságos kibertér és az hozzáférhető-e. Napjainkban szilárd és ellenálló kibervédelmi képességekre van szükség a KBVP-struktúrák, -missziók és -műveletek támogatásához.

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 (EVÜ) együttműködve ki kell dolgozni az uniós kibervédelmi szakpolitikai keretet.

E dokumentum azért íródott, hogy keretül szolgáljon az európai tanácsi és a tanácsi következtetéseknek, valamint az Európai Unió kiberbiztonsági stratégiájában[1] körvonalazott kibervédelmi szempontoknak. A dokumentum meghatározza a KBVP keretébe tartozó kibervédelem kiemelt területeit, továbbá pontosítja a különböző európai szereplők feladatait, ezzel egyidejűleg teljes körűen tiszteletben tartja az uniós szereplők és a tagállamok feladatait és hatásköreit, csakúgy mint az EU intézményi keretét és döntéshozatali autonómiáját. A kiberpolitikai kérdésekkel foglalkozó „elnökség barátai”csoport megállapodást ért el az uniós kiberbiztonsági stratégia végrehajtásának folyamatáról.

[1] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér”, 2013. február 7., valamint az Általános Ügyek Tanácsának 2013. június 25-én elfogadott, kapcsolódó következtetései.

Ez a szakpolitikai keret elsődlegesen a tagállamok által a KBVP céljaira rendelkezésre bocsátott kibervédelmi képességek fejlesztésére, illetve az Európai Külügyi Szolgálat (EKSZ) KBVP szempontból fontos kommunikációs és információs hálózatainak védelmére összpontosít. A képzés területén kiemelt feladatként szerepel a KBVP parancsnoki láncában helyet kapó különböző csoportoknak szánt programok kidolgozása. Annak érdekében, hogy javuljon az EU képessége a KBVP-vel összefüggő, kiberválságok során hozott válaszintézkedések megtételére, továbbá javuljanak a stratégiai döntéshozatali eljárások, valamint megerősödjön az információs infrastruktúra architektúrája, olyan gyakorlatokra van szükség, amelyek megfelelőképpen foglalkoznak a kiberdimenzióval. A kibertér olyan, gyorsan fejlődő szakterület, amelyen a kettős felhasználású képességek alapvetően fontos szerephez jutnak; ennélfogva a kibertérhez kapcsolódó új kihívások kezelése érdekében fejleszteni kell a civil-katonai együttműködést és szorosabb szinergiákat kell létrehozni a tágabb uniós kiberpolitikákkal , ezzel egyidejűleg tiszteletben kell tartani a tagállamok belső szervezeti kereteit és hatásköreit.

Ez a dokumentum körvonalazza a magánszférával a kibervédelmi képességek fejlesztése terén folyó együttműködés megkönnyítésére vonatkozó alapelveket, különös tekintettel a kutatás és technológia (K+T) valamint az európai védelmi technológiai és ipari bázis (EDTIB) megerősítésére. A dokumentum ezen túlmenően biztosítani hivatott az EU és az Észak-atlanti Szerződés Szervezete (NATO) kibervédelmi törekvései közötti összhangot, valamint egyes területek vonatkozásában javaslatokat tesz az említettek közötti együttműködésre.

Végezetül a kibervédelmi célkitűzéseket jobban be kell építeni az uniós válságkezelési mechanizmusokba. A kiberválságok hatásainak kezelése érdekében adott esetben alkalmazni kell az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés[2] vonatkozó rendelkezéseit.

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

Az uniós kibervédelmi szakpolitikai keret prioritásai

1. A KBVP vonatkozású tagállami kibervédelmi képességek fejlesztésének támogatása

A KBVP végrehajtását támogató hálózatok rezilienciájának biztosítása érdekében az EKSZ által irányított KBVP-struktúrák kommunikációs hálózatainak fokozott védelmét, valamint a KBVP-missziók és -műveletek rendelkezésére álló tagállami kibervédelmi képességek fejlesztését egyaránt központi kérdésként kell kezelni. A tagállamoknak, az EKSZ-nek és az EVÜ-nek e tekintetben együtt kell működnie a hatékony kibervédelmi képességek kifejlesztése érdekében.

A kibervédelmi képességek és technológiák fejlesztése során foglalkozni kell a képességfejlesztés valamennyi aspektusával, ideértve a doktrínát, a vezetést, a szervezést, a személyzetet, a képzést, a technológiát, az infrastruktúrát, a logisztikát és az interoperabilitást.

A KBVP-missziókat és -műveleteket támogató információs infrastruktúrák sebezhető pontjait folyamatosan értékelni kell, és ezzel egyidejűleg biztosítani kell a védelem hatékonyságának közel valós idejű leképezését. Műveleti szempontból a kibervédelmi tevékenységek elsődleges központi kérdésének a KBVP keretében alkalmazott kommunikációs és információs hálózatok működésképességének fenntartását kell tekinteni, kivéve, ha a műveletek vagy missziók megbízatása másként rendelkezik.

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 EVÜ kibervédelmi projektcsoportjának a kibervédelmi képességfejlesztést célzó munkájára építve az EKSZ/EVÜ és a tagállamok a következő intézkedéseket hozzák:

- annak érdekében alkalmazzák a képességfejlesztési tervet és a tagállamok közötti együttműködést megkönnyítő és támogató más eszközöket, 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 keretek között tartása, a dinamikus helyreállítási képességek, a megosztottadat-tárolás és az adattartalékok tekintetében;
- támogatják a kibervédelemmel kapcsolatos jelenlegi és jövőbeli katonai műveletek céljából indított összevonási és megosztási programokat (például a forenzikus tudományok, az interoperabilitás fejlesztése és a normák meghatározása terén);
- a meglévő uniós szintű tapasztalatokat hasznosítva kidolgozzák a kiberbiztonságnak és -bizalomnak a tagállamok által elérendő minimális szintjét meghatározó szabvány célkitűzéseket és előírásokat;
- megkönnyítik a tagállamok közötti cseréket a nemzeti kiberbiztonsági doktrínák, képzési programok és gyakorlatok, illetve a kibervédelmet középpontba helyező munkaerő-felvételi, állományban tartási és tartalékos-programok tekintetében;
- önkéntes alapon javítják az együttműködést a tagállami katonai CERT-ek között, az incidensek megelőzésének és kezelésének javítása érdekében;
- mérlegelik a kibervédelmi képzés fejlesztésének lehetőségét, figyelembe véve az uniós harccsoporti minősítést.
- A tagállamok segítséget kérhetnek az ENISA-tól, amennyiben kibervédelmi képességeik fejlesztéséhez polgári hálózat- és információbiztonsági szakértelem szükséges.

2. Az uniós szervek által a KBVP keretében használt kommunikációs hálózatok védelmének növelése

Azon szerep sérelme nélkül, amelyet a CERT-EU az összes uniós intézmény, szervezet és szerv 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 erőforrás-kezelési ügyvezető igazgatóságának 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-műveletek és -missziók végrehajtása során a különböző uniós intézményi szereplők által előírt, információs rendszerekre vonatkozó biztonsági szabályokat is ésszerűsíteni 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 hálózatok védelmének javítása érdekében az ügyvezető igazgatóság, az EUKT, a CMPD és a CPCC az INTCEN-nel együttműködve a következő intézkedéseket hozza:

- 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 a CERT-EU-val és a meglévő uniós kibervédelmi képességekkel való együttműködésre vonatkozó stratégiát, illetve a meglévőket tovább kell fejleszteni;
- 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;
- 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;
- előmozdítja a számítógépes veszélyforrásokkal kapcsolatos, a tagállamok és az érintett uniós szervek közötti információcserét. Ennek érdekében a meglévő együttműködésre épülő önkéntes alapú megközelítést alkalmazva az érintett nemzeti és európai hatóságok között végrehajtandó információmegosztási mechanizmusokat kell kialakítani és bizalomépítő intézkedéseket kell kidolgozni;
- kidolgozza a KBVP keretében folyó katonai műveletek[3] és polgári missziók vonatkozásában az egységesített kibervédelmi koncepciót, és beépíti azt a stratégiai szintű tervezésbe;
- 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 fenyegetéskörnyezetnek megfelelően rendszeresen felülvizsgálja az erőforrásokra vonatkozó követelményeket és más vonatkozó politikai döntéseket, és eközben konzultál az érintett tanácsi munkacsoportokkal és más uniós intézményekkel.

[3] a katonai műveletek esetében az EU vezette katonai műveletekhez készült jelenlegi uniós kibervédelmi koncepciót e politikai keretet figyelembe véve korszerűsíteni kell.

3. A polgári-katonai együttműködésnek, illetve a tágabb uniós kiberpolitikákkal, az érintett uniós intézményekkel és ügynökségekkel, valamint a magánszférával fennálló szinergiáknak az előmozdítása

A kibertér olyan, gyorsan fejlődő szakterület, amelyen a kettős felhasználású képességek alapvetően fontos szerephez jutnak, és ahol ez a keret erősíteni fogja a szinergiát a KBVP és más uniós horizontális politikák, például az űr- és tengerhajózási biztonsági politikák, illetve a stratégiák, például a tengerhajózási biztonsági stratégia és cselekvési terve között. A tagállamok belső szervezeti kereteinek és jogalkotásának sérelme nélkül a kiberterületen folyó katonai-polgári együttműködés javára fog válni a kettős felhasználású képességek fejlesztése, a K+T, a legjobb gyakorlatok cseréje, az információcsere és a korai előrejelző mechanizmusok, az incidenskezelési kockázatelemzések és a figyelemfelkeltés. A képzés és a gyakorlatok terén a közös tevékenységek fokozzák majd az együttműködést és csökkentik a költségeket a különböző szakpolitikai területeken.

Arra ösztönözzük az EVÜ-t, az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA)[4], a Számítástechnikai Bűnözés Elleni Európai Központot (EC3) és más érintett uniós ügynökségeket, valamint a tagállamokat, hogy a KBVP összefüggésében fokozzák az együttműködést a következő területeken:

- közös kiberbiztonsági és védelmi kompetenciaprofilok kidolgozása a legjobb nemzetközi gyakorlatok és az uniós intézményekben használt minősítés alapján, figyelembe véve továbbá a magánszférában alkalmazott minősítési előírásokat is;
- részvétel a közszférában alkalmazott kiberbiztonsági és védelmi szervezeti és technikai normák továbbfejlesztésében és kiigazításában a védelmi és biztonsági ágazatban való felhasználás céljából; adott esetben az ENISA és az EVÜ folyamatban lévő munkájára építve;
- olyan munkamechanizmus kidolgozása, amely lehetővé teszi a gyakorlatokkal, a képzéssel és a polgári-katonai szinergiák esetleges egyéb területeivel kapcsolatosan a legjobb gyakorlatok cseréjét;
- az Unióban rendelkezésre álló, a számítástechnikai bűnözés megelőzésére és a kinyomozására irányuló, valamint a forenzikus képességek formálása és kiterjedt felhasználása a kibervédelmi képességek fejlesztése során;

[4] Az ENISA megbízatásának keretein belül és az ENISA többéves munkatervével összhangban, a tagállami hatáskörökkel való átfedés elkerülése mellett.

A polgári vonatkozású kiberbiztonság javítása a hálózat- és információbiztonság általános ellenálló képességének biztosításához hozzájáruló egyik fontos tényező. A hálózat- és információbiztonságról (NIS) szóló irányelvre irányuló javaslat célja a nemzeti szintű kiberbiztonsági felkészültség növelése és az uniós szintű – mind stratégiai, mind pedig operatív – együttműködés megerősítése a tagállamok között. Az együttműködésbe be kell vonni mind a kiberbiztonsági politikákat felügyelő nemzeti hatóságokat, mind pedig a hálózatbiztonsági vészhelyzeteket elhárító nemzeti szintű csoportokat (CERT-ek) és a CERT-EU-t. A köz-magán NIS platform célja, hogy meghatározza a kiberbiztonság fokozásához hozzájáruló, technológiai szempontból semleges legjobb gyakorlatokat, és intézkedéseket dolgozzon ki biztonságos ikt-megoldások alkalmazásának ösztönzésére.

Kutatás és technológia a magánszektorral és a tudományos élet képviselőivel való együttműködésben

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 sebezhető 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 K+T dimenzióval rendelkezik. A kibervédelmi kutatási menetrend (CDRA) keretében az EVÜ szilárd alapot biztosít a jövőbeli K+T kiadások prioritási sorrendjének megállapításához és a képességek fejlesztéséhez mind nemzeti, mind pedig európai szinten.

Alapvetően fontos, hogy a fenyegetések és a sebezhető pontok csökkentése érdekében erős technológiai kapacitásokat építsünk ki Európában. A jövőben is az ipar lesz a kibervédelemmel kapcsolatos technológiák és innováció elsődleges mozgatórugója. Ezért döntő fontosságú a magánszektorral folytatott szoros együttműködés megőrzése, és – ahol csak lehetséges – szinergiákra kell törekedni a polgári megoldásokkal, szolgáltatásokkal és képességekkel (különösen a következő technológiai területeken: kriptográfia, beágyazott rendszerek, rosszindulatú számítógépes programok felismerése, szimulációs és megjelenítő technikák, hálózati és kommunikációs rendszerek védelme, azonosítás és hitelesítés). Emellett a szilárd európai kibervédelmi ágazat kialakításának a támogatása révén, többek között a kis- és közepes méretű vállalkozások (kkv-k) bevonásával elő kell mozdítani Európában egy megbízható és versenyképes ipari kiberbiztonsági ellátási lánc működését.

Az EVÜ a Bizottság szolgálataival és a tagállamokkal együttműködésben és annak érdekében, hogy a kiberiparra vonatkozó uniós megközelítéssel összhangban előmozdítsa a polgári és katonai együttműködést a kibervédelmi képességek fejlesztése területén és hogy megerősítse az európai védelmi technológiai és ipari bázist[5]:

- szinergiákra törekszik a katonai K+T programok, valamint a polgári kutatási és fejlesztési programok – például a Horizont 2020 – között, és a KBVP vonatkozású kutatásokhoz kapcsolódó előkészítő intézkedések meghatározása során figyelembe veszi a kiberbiztonság és -védelem dimenzióját is;
- elsősorban az európai együttműködési keret alkalmazásával tájékoztatja az uniós intézményeket és ügynökségeket a kiberbiztonsági kutatással kapcsolatos menetrendekről (például a kibervédelmi kutatási menetrendről), valamint az ezek alapján kidolgozott ütemtervekről és intézkedésekről;
- 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;
- 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 Európai Unió egész területén megvalósuljon harmonizációjuk (számítógépes fenyegetések elemzésére és értékelésére vonatkozó képessége, beépített biztonsági megoldásokra irányuló kezdeményezések, önállóságvesztés kezelése a technológiákhoz való hozzáférés tekintetében stb.);
- részt vesz az arra irányuló törekvésekben, hogy a kiberbiztonság és a kibervédelem dimenziója még jobban beépüljön azokba a programokba, amelyek kettős biztonsági és védelmi dimenzióval rendelkeznek (pl. SESAR);
- tevékenyen elősegíti, hogy a polgári kiberbiztonsági ipart érintő szakpolitikák kidolgozása során, melyet nemzeti szinten a tagállamok, uniós szinten pedig a Bizottság végez, szinergiák alakuljanak ki.

[5] „Úton egy versenyképesebb és hatékonyabb védelmi és biztonsági ágazat felé” című közlemény, COM (2013) 542.

4. A képzési, oktatási és gyakorlati lehetőségek javítása

Képzés és oktatás

Ahhoz, hogy a KBVP parancsnoki láncának valamennyi szintjén – többek között a missziók és a műveletek során – közös kibervédelmi kultúrát tudjunk létrehozni, javítani kell a kibervédelemmel kapcsolatos képzési lehetőségeket. Tekintettel arra, hogy napjainkban egyre szűkülnek a védelmi kiadások, 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 EKSZ a KBVP-vel kapcsolatos oktatás területén a következő prioritásokat állapítja meg, és az EVÜ-vel, az Európai Biztonsági és Védelmi Főiskolával (EBVF) és a tagállamokkal közösen:

- az EVÜ-nek a kibervédelemmel kapcsolatos képzési szükségletekről készített elemzése, valamint az EBVF által nyújtott kiberbiztonsági képzéssel kapcsolatos tapasztalatok alapján KBVP témájú képzést és oktatást dolgoz ki több célközönség, köztük az EKSZ, a KBVP-missziók és -műveletek résztvevői, illetve a tagállamok tisztviselői számára;
- javasolja képzési szabványokkal és képesítésekkel kapcsolatos kibervédelmi párbeszéd megkezdését a tagállamokkal, az uniós intézményekkel, harmadik országokkal és egyéb nemzetközi szervezetekkel, valamint a magánszektor képviselőivel;
- az EVÜ által elvégzett megvalósíthatósági értékelés alapján megvizsgálja, hogy lehetséges és indokolt-e kibervédelmi képzési létesítmény felállítása a KBVP keretein belül;
- további EVÜ-képzéseket dolgoz ki azzal a céllal, hogy kielégítse a KBVP keretében a kibervédelmi képzéssel kapcsolatos szükségleteket;
- a képzési programok akkreditálására az EBVF jelenlegi akkreditációs mechanizmusait fogja alkalmazni, az uniós intézmények releváns szolgálataival szoros együttműködésben és a meglévő normák és ismeretek alapján; fontolóra fogja venni kiberspecifikus modulok létrehozását a Katonai Erasmus-kezdeményezés keretében;
- szinergiákat valósít meg más érdekelt felek, például az ENISA, az Europol, a számítástechnikai bűnözéssel foglalkozó európai képzési és oktatási csoport (ECTEG) és az Európai Rendőrakadémia (CEPOL) képzési programjaival;
- megvizsgálja az EBVF és a NATO Védelmi Kollégium keretén belül nyújtandó közös kibervédelmi képzési programok lehetőségét, melyek valamennyi uniós tagállam számára nyitva állnak és céljuk a közös kibervédelmi kultúra előmozdítása;
- együttműködésre lép az európai magánszektorban működő képzésszolgáltatókkal és oktatási intézményekkel, a KBVP-műveletek és -missziók résztvevőinek kompetenciái és készségei fejlesztése céljából.

Gyakorlatok

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 az interoperabilitást és a bizalmat.

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

- beépítik a kibervédelem dimenzióját a MILEX és a MULTILAYER programok keretében folytatott gyakorlatok forgatókönyveibe;
- adott esetben külön erre a célra kidolgoznak egy, a KBVP-hez tartozó uniós kibervédelmi gyakorlatot, és megvizsgálják a páneurópai kibervédelmi gyakorlatokkal, mint például az ENISA által szervezett *CyberEurope* gyakorlattal való koordináció lehetőségét;
- fontolóra veszik a más nemzetközi kibervédelmi gyakorlatokban történő részvétel lehetőségét;
- amikor az EU elkészül a KBVP-hez tartozó kibervédelmi gyakorlat kidolgozásával, a gyakorlatokkal kapcsolatos uniós politikával összhangban bevonja a releváns nemzetközi partnereket, például az EBESZ-t és a NATO-t.

5. A 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.

Az Uniónak politikai szándéka, hogy elmélyítse a NATO-val a kibervédelem területén annak érdekében folytatott együttműködést, hogy e szakpolitikai kereten belül létrejöjjenek a szükséges, megbízható és ellenálló kibervédelmi képességek. Célszerű rendszeres konzultációkat, 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 NATO-val folytatott együttműködés meglévő keretrendszerével összhangban.

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

- a válságkezeléssel, valamint a katonai műveletekkel és polgári missziókkal kapcsolatos bevált gyakorlatok cseréje;
- koherencia megvalósítása a kibervédelmi képességekre vonatkozó, átfedésben lévő követelmények kidolgozása során, különösen a hosszú távra szóló kibervédelmi képességek fejlesztése tekintetében;
- a kibervédelmi képzéssel és oktatással, valamint gyakorlatokkal kapcsolatos elvek kidolgozása terén folytatott együttműködés elmélyítése;
- az EVÜ és a NATO Kibervédelmi Kiválósági Együttműködési Központja közötti kapcsolattartási megállapodásban rejlő lehetőségek fokozottabb kihasználása – megfelelő értékelések alapján – a nemzetközi kibervédelmi projektekben való megerősített együttműködés kiindulási platformjaként;
- a CERT-EU, a releváns uniós kibervédelmi szervek valamint a NCIRC (a NATO számítógép-incidenskezelő képessége) közötti együttműködés megerősítése 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 az EVÜ – a tagállamokkal közösen – adott esetben:

- követi a nemzetközi partnereknél (nemzetközi szervezeteknél és harmadik országokban) a stratégiai fejleményeket, és konzultációkat folytat velük kibervédelmi kérdésekben;
- megvizsgálja, hogy a kibervédelmi kérdések terén milyen együttműködési lehetőségek nyílnak, többek között a KBVP-missziókban és -műveletekben részt vevő harmadik országokkal;
- továbbra is támogatja bizalomépítő intézkedések kidolgozását a kiberbiztonság területén, az egyes államok között az átláthatóság növelése és a félreértések kockázatának csökkentése érdekében, mégpedig az e területre vonatkozó nemzetközi normák folyamatban lévő kidolgozásának előmozdítása révén.

Nyomon követés

Félévente jelentést kell benyújtani a katonapolitikai kérdésekkel foglalkozó csoportnak, a Politikai és Biztonsági Bizottságnak és a Tanács egyéb releváns munkacsoportjainak a fent körvonalazott öt területen elért előrehaladásról, hogy az említett csoportok értékelni tudják a szakpolitikai keret végrehajtásában elért eredményeket. Mivel egyre több kiberbiztonsági fenyegetéssel kell szembenéznünk, alapvetően fontos, hogy meghatározzuk a kibervédelemmel kapcsolatos új követelményeket, és azokat aztán beépítsük a kibervédelmi szakpolitikai keretbe.