

KÖFOP-2.1.2-VEKOP-15.

„A jó kormányzást megalapozó közszolgálat- fejlesztés”



„INTEGRÁLT VÉDELEM 2018”

**A Nemzeti Közszolgálati Egyetem
Közös Közszolgálati Gyakorlat**

**Nemzetközi és Európai Tanulmányok Kar
részletes és kiegészítő feladatai**
/oktatói példány/

Kaszap Márton
Tongori Zsófia

Nemzeti Közszolgálati Egyetem
– Budapest, 2018 –

TARTALOMJEGYZÉK

1. ELŐZETES KONCEPCIÓ „INTEGRÁLT VÉDELEM” GYAKORLAT	4
1.1. A gyakorlat alapadatai	4
1.2. A gyakorlat elgondolása	5
1.3. A gyakorlat levezetésének célja	6
1.4. A gyakorlat időpontja, valamint a tervezett létszám a NATK részéről	7
1.5. A nemzetközi gyakorlatrész	8
1.6. A gyakorlat kidolgozásának és levezetésének általános rendje	8
2. INDÍTÓ FELADAT ÉS LEVEZETÉSI TERV	9
2.1. Előzmények, fő keretek	9
2.2. A gyakorlat levezetésének mozzanatai	10
3. RÉSZLETES FELADAT	17
4. A NEMZETKÖZI ÉS EURÓPAI TANULMÁNYOK KAR SZERVEZETEIRE VONATKOZÓ FELADATOK IDŐRENDI LEBONTÁSA SZERVEZETEK SZERINT	26
5. A GYAKORLAT HALLGATÓI	33
6. A HALLGATÓK SZERVEZETI BEOSZTÁSA	35
6.1. A Nemzetközi és Európai Tanulmányok Kar hallgatóinak feladata a Nemzeti Közszoigálati Egyetem integrált gyakorló szervezetében (összesen 5 fő)	35
6.2. A Nemzetközi és Európai Tanulmányok Kar hallgatóinak beosztása a NETK karon belül A és B csoportban (összesen 84 fő)	35
6.3. A gyakorlat vezetői és segítők (összesen 9 fő)	38
6.4. Terembeosztás	38
7. A NEMZETKÖZI SZERVEZETEK ÉS A KIBERBIZTONSÁG	41
7.1. A NATO és a kiberbiztonság	41
7.1.1. A NATO kibervédelmi politikája	41
7.1.2. A NATO kibervédelmi képessége	41
7.2. Kiberbiztonság az Európai Unióban	44
7.3. A kibernetikus fenyegetések	44
7.4. A jelenlegi helyzet	46
7.5. Stratégiák	47
7.6. Jogalkotás	47
7.7. Hálózatok és szervezetek	48
7.8. Finanszírozás	48
8. AZ EURÓPA TANÁCS ÉS A KIBERBIZTONSÁG	49
8.1. A Számítástechnikai bűnözésről szóló Egyezmény	49

8.2. Cybercrime Convention Committee	50
8.3. Projektek	51
9. NEMZETKÖZI SZERVEZETEK ÉS A KATASZTRÓFAVÉDELEM	52
9.1. A NATO és a katasztrófavédelem	52
9.1.1. Az Euro-atlanti Katasztrófa Elhárítási Koordinációs Központ (EADRCC).....	52
9.1.2. Támogatás a nemzeti hatóságoknak lakossági katasztrófákban	53
9.1.3. Több nemzetiségű szakértői csoport.....	53
9.1.4. Polgári készenlét.....	53
9.2. Az Európai Unió katasztrófavédelmi és reagáló képességei	54
10. A NEMZETKÖZI JOG ÉS A KIBERBIZTONSÁG	58
11. MINTAANYAGOK AZ ELKÉSZÍTENDŐ JELENTÉSEKHEZ, HÁTTÉRANYAGOKHOZ	61

1. ELŐZETES KONCEPCIÓ „INTEGRÁLT VÉDELEM” GYAKORLAT

1.1. A gyakorlat alapadatai

Előzmények

A Nemzeti Közszerológati Egyetem (NKE) a 2013/2014-es tanévben beindította az új rendszerű képzést, amely az Egyetemi Közös Modult is magába foglalja. A közös modult a közös közszérológati gyakorlat zárja – amely a 2014/2015-ös tanév tavaszi félévében kerülhetett először lebonyolításra. A közszérológat szellemében már 2013-ban - összességében levezetésre került a „VADVÍZ 2013” fantázianeű első válságkezelési gyakorlat, melyet követettek a „VÉGVÁR 2014”, a „VÉGVÁR 2015” a VIHAR 2016.gyakorlatok, tavaly 2017-ban összességében jó értékeléssel - levezetésre került a „VÁNDOR 2017.” tömeges migráció kezelésének modellezése.

A Fenntartói Testület döntése alapján a Nemzeti Közszerológati Egyetem (NKE) 2018. évi Egyetemi Közös Közszerológati Gyakorlatának központi témája egy kibertámadás által okozott veszélyhelyzet következményeinek felszámolása. A gyakorlat neve: Integrált Védelem 2018.

A gyakorlat témaköre

A témakör megválasztásnál fő szempont volt, hogy **mindegyik hivatásrend hallgatói gyakorolni tudják a hivatásrendre jellemző feladataikat** mindegyik hivatásrendnek olyan feladatokat is végre kell hajtaniuk, amelyekkel a gyakorlati életben a szervezetnek szembesülnie kell.

A gyakorlat megvalósításába bevonásra kerülnek a hazai rendészeti, honvédelmi, közigazgatási, a kibervédelemmel foglalkozó állami szervek, illetve az energiaellátással, közlekedéssel, közművek üzemeltetésével foglalkozó gazdálkodó szervezetek szakemberei is. A gyakorlaton részt vesz valamennyi kar és karközi intézet alapképzésben és mesterképzésben tanuló nappali munkarendes végzős hallgatók, a Katasztrófavédelmi Intézet valamennyi nappali szakos és végzős MA levelezős hallgatója, valamint lehetőség szerint az Elektronikus Információ Biztonsági Vezető szakirányú továbbképzés végzős hallgatói.

1. A gyakorlat központi témája egy olyan helyzet modellezése, amikor a nemzetbiztonsági szérológatokról kapott információk alapján felmerült a külső

beavatkozás gyanúja (szervezett informatikai támadás), ami miatt Budapest egyes kerületeiben, Csongrád és Bács-Kiskun megyék bizonyos részein kibertámadással számolhatunk, amelynek következtében az áram szolgáltatás helyenként megszűnik, időszakonként szünetel.

2. A gyakorlat során a kibertámadások következményei miatt kialakuló veszélyhelyzet kezelésére a következmények felszámolásával összefüggő, a különböző hivatásrendek együttműködésében, illetve az érintett külföldi partner szervezetek közreműködésével hozott intézkedések kerülnek modellezésre.
3. A gyakorlat során megvalósul a magas szintű jogszabály-, illetve a központi közigazgatási, illetve rendvédelmi szervek részéről a jogi szervezetszabályozó eszközök megalkotási folyamata, a Kormány és a minisztériumok védelme, a kritikus infrastruktúra elemek működőképesség fenntartására, vagy kiesés esetén annak visszaállítására irányuló tevékenység, a lakosság ellátásának megszervezése, a közreműködő hivatásrendek alaprendeltetésének folyamatos ellátása normál és a veszélyhelyzet, mint különleges jogrend időszakában.
4. Mindezek mellett a Kormány, a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság és munkaszervei, az érintett minisztériumok, a védelmi bizottságok és operatív törzsek, központok, az érintett együttműködők nyomozati, határőrizeti, mentő, kárelhárító, hibaelhárító szervezetei bevonásra kerülnek, üléseznek, intézkedéseket tesznek, beavatkozó tevékenységet, együttműködést szerveznek a kialakult helyzet kezelése érdekében.

1.2. A gyakorlat elgondolása

Az államigazgatási, a rendvédelmi szervek, a honvédség, az önkormányzatok a gazdálkodó szervezetek folyamatosan végzik normál időszaki tevékenységüket. Saját felelősségi körükben intézkedéseket tesznek a nemzetbiztonsági szolgálatok kibertámadásra irányuló feltételezése alapján a veszélyhelyzetek kezelésére vonatkozó terveik pontosítására, felkészülnek a kidolgozott tervek alkalmazására.

Szembeesülnek az előrejelzéseknek megfelelően egyes szolgáltatások kiesésével, az energetikai és infokommunikációs rendszerek működésképtelenségével, a kormányzati, az államigazgatási, önkormányzati munka, a közlekedés, kereskedelem, ipar, egészségügyi ellátás, banki tevékenység, a klasszikus szolgáltatások akadozásával.

A gyakorló hallgatók a kialakult helyzetnek megfelelően szerepköreik szerint elemzik, értékelik a helyzetet, jelentéseket terjesztenek fel, intézkedéseket hoznak, megtervezik az erők- és eszközök veszélyeztető hatásokkal arányos alkalmazását. A szimulált helyzetben a hivatásrendek területi illetékességük szerint szervezeti hierarchiájuknak megfelelően lépcsőzve hajtják végre a kompetenciájukba tartozó feladataikat. A gyakorló hallgatók országos, megyei, járási, települési és kerületi szinten a végrehajtandó feladatok ellátására létrehozott szerv vezetőjeként, kompetens szolgálati személyeként, az aktivizált bizottságok, operatív törzsek tagjaként valamint az együttműködő, közreműködésre kötelezett szervek szakmai vezetőjeként, vagy a tőlük delegált összekötőként tevékenykednek. A hallgatók egy része megfigyelőként lesz jelen az egyes vezetői fórumokon, ahol megadott szempontok alapján értékelik a beosztásokban levő hallgatótársak tevékenységét, arról feljegyzést készítenek. A különböző irányítói szinteken minden mozzanat végén felkészülnek sajtótájékoztató megtartására az illetékes vezetők, vagy kijelölt sajtószóvivők.

1.3.A gyakorlat levezetésének célja

- Az Egyetem különböző karain és szakjain, szakirányain, valamint a nemzetközi partnerintézményeken (az Európai Unió tagországok/elsősorban a V4 es országok társ-egyetemein) tanuló hallgatók szerezzenek jártasságot (a polgári hallgatók ismereteket) a **komplex szakmai problémák integrált operatív törzsekben történő megoldásában**, a hallgatók **gyakorolják a vezetési funkciókat és a törzsmunkát**, a nemzetközi együttműködést, egyes tevékenységeket a **gyakorlatban is valósítsanak meg**.
- A vezetői felkészítés elméleti tananyagának gyakorlatban való alkalmazása, a **vezetői kompetenciák fejlesztése**. A katonai, rendészeti és polgári vezetést támogató korszerű informatikai rendszerek alkalmazásának gyakorlása (*Robotzsaru, Mars, Marathon*), számítógépes adatbázis létrehozása.
- A **nemzetközi partnerintézmények és partner szervezetek** részéről bevonásra kerülő közreműködők – és megfigyelők – a téma és a workshop jellegéből adódó

tapasztalatainak, sajátos eljárásainak összefoglalásából készülő tanulmánymagyar és angol nyelven.

- Az egyetemi képzés és a fegyveres szervek időszerű feladatai és tevékenysége közötti kapcsolat erősítése, a **képzésben új módszerek** alkalmazása. A tapasztalatok kölcsönös hasznosítása, a jóváhagyott tervek, a működő rendszerek és eljárások közös továbbfejlesztése az elméletben és a gyakorlatban.
- Hozzájárulás a **közzolgálat különböző alrendszerének harmonizálásához** és az egységes közzolgálati szemlélet erősítéséhez, a közzolgálati tisztviselők kompetenciafejlesztéséhez.

A nevelési cél:

A hallgatók személyiségének sokoldalú fejlesztése, hazai és nemzetközi szintén is. Az egységes közzolgálati szemléletmód közelítése, a hazai és nemzetközi együttműködés a vezetői munkakörökre jellemző, valóságot megközelítő helyzetekben.

1.4. A gyakorlat időpontja, valamint a tervezett létszám a NATK részéről

- 2017. április 23-án (*felkészülés*) 8 tanóra (08.00-16.00) és április 24-én (*végrehajtás*) 8 tanóra (08.00-16.00).
- A gyakorlaton részt vesz az egyetemi alapképzésben résztvevő teljes végzős hallgatói állomány. E mellett a meghívott és bevont, külföldi partneregyetemek hallgatói csoportjai, akik a hivatásrendjüknek megfelelő beosztásokban (törzsekben, összekötői szerepkörben, külföldi partnerként, stb), illetve megfigyelőként tevékenykednek. Részt vesznek még a gyakorlaton a HHK és az RTK egyes mesterképzésben részt vevő végzős tanulócsoportjai.
- A Nemzetközi és Európa Tanulmányok kar állományából **89 fő hallgató és 8 fő** oktató vesz részt. A NETK hallgatóinak nagy része a **Ludovika épületben, az I., II., III., és IV. előadóban** végzik munkájukat, illetve a Kormányban, KKB-ban (Katasztrófavédelmi Koordinációs Tárcaközi Bizottság) és a Központi Sajtóban összesen 5 NETK-es hallgató tevékenykedik az **Oktatási épületben**.

1.5. A nemzetközi gyakorlatrész

A kibertámadás következtében kialakult helyzet megoldásában és közvetlen kezelésében a Külgazdasági és Külügyminisztérium feladatai korlátozottak, csakúgy, mint a kibertámadás miatt bekövetkezett áramszolgáltatási hiányosságok orvoslásában. A KKM a vizsgált időszakban ezért arra koncentrál, hogy a magyar kormány álláspontját képviselje és védelmezze a nemzetközi porondon, elsősorban a nemzetközi szervezetekben, információkat gyűjtsön az események trendjeiről, volumenéről, esetleges távlatairól, majd ennek kapcsán stratégiai szintű javaslatokkal támogassa a kormányzati döntés-előkészítő és döntéshozó tevékenységet, koordinálva az ebben esetlegesen szerepet kapó aktorok tevékenységét. Ennek kapcsán a KKM elemzéseket, háttéranyagokat készít, a nemzetközi találkozókra pedig igyekszik elérni, hogy az agenda, illetve a megszülető döntések a magyar kormány álláspontját tükrözzék. Ennek kapcsán fontos a szövetségesek keresése a nemzetközi szereplők között, az aktorok meggyőzése a magyar álláspont helyességéről. Annak érdekében, hogy a gyakorlat életszerű legyen, és valódi konfrontációkra, probléma-megoldásra, vitákra kerülhessen sor, szükséges a különféle külföldi és nemzetközi szereplők megjelenítése, így nemzetközi szervezetek (NATO, Európai Unió, EBESZ, Európa Tanács), illetve egyes érintett szomszédos országok felvonultatása.

1.6. A gyakorlat kidolgozásának és levezetésének általános rendje

- A gyakorlat kidolgozása a karokon **egységes elvek és követelmények** szerint történik –ezeket a gyakorlat vezetősége határozza meg.
- A kidolgozását - az **oktatási rektorhelyettes koordinációja** mellett - a kari dékánok, intézet igazgatók által kijelölt **munkacsoportok hajtják végre.**
- A résztvevő hallgatói állomány részére **felkészítő foglalkozások kerülnek levezetése,** melynek tárgya **a gyakorlat főbb mozzanatai és a tevékenység rendje.**
- A gyakorlat „**Alapfeladat**”-át ami a gyakorlat minden résztvevője számára azonos, az ORH vezetésével, az **Egyetemi Kidolgozó Csoport** alkotja meg, a karok/intézetek képviseletével.
- A „**Részletes Feladat**”-ot a karok, intézetek dolgozzák ki. Az Egyetemi Kidolgozó csoport - az abba delegált kari/intézet képviselő révén - biztosítja, hogy az a többi karéval összhangban legyen.
- „**Kiegészítő feladat**”-ot a gyakorlólhelyek jövőendő vezetői, döntnökei készítik el, kidolgozva a gyakorlat levezetésének részleteit.

2. INDÍTÓ FELADAT ÉS LEVEZETÉSI TERV

A gyakorlat nemzetközi részének fő kidolgozói:

NKE-NETK Kaszap Márton
Tongori Zsófia

További hozzájárulók és a gyakorlatvezetők segítői:

Fekete Csanád
Dr. Hárs András
Jakusné Dr. Harnos Éva
Dr. Kozák Kornélia
Dr. Marsai Viktor
Dr. Pásztor Szabolcs
Szabó Mátyás hallgató

A hat hivatásrend (katonai, rendőri, katasztrófavédelmi, vízügyi, önkormányzati, külügyi) feladatrendszeréből adódóan, a gyakorlat egységes szerkezetben kerül levezetésre, melynek **fő elemeit és részleteit az Alap- és Indító Feladat terv tartalmazza.**

Erre épülnek a karok és intézetek által kidolgozott – a saját szervezetre vonatkozó feladatokat **részletesen tartalmazó levezetési tervek, melyet az ORH hagy jóvá.**

2.1. Előzmények, fő keretek

A Nemzeti Közsolgálati Egyetem Nemzetközi és Európai Tanulmányok Karának (a továbbiakban: NKE-NETK) hallgatói (biztonság- és védelempolitika szak BSc II. évfolyam, illetve nemzetközi igazgatás szak BSc II. évfolyam) illeszkedve az általuk hallgatott szakokhoz a Vándor 2017 gyakorlat során a migrációs veszélyhelyzettel kapcsolatos **nemzetközifeladatokat** fogják végrehajtani. Az NKE-NETK részéről 89 fő vesz részt a gyakorlatban. A hallgatók felkészítésére a Közös Közsolgálati Gyakorlat tárgy keretében kerül sor, a felkészítők Dr. Havasi Zoltán r dandártábornok, Kaszap Márton, abban a felosztásban, hogy az alapozó felkészítést Dr. Havasi Zoltán végzi el, a gyakorlatra való közvetlen felkészítő órákat pedig Kaszap Márton és Tongori Zsófia tartják.

A kar hallgatói annak érdekében, hogy teljes létszámban bevonásra kerülhessenek a gyakorlatba, és annak kétnapos időtartama alatt megfelelő leterheltség mellett, lehetőleg minél kevesebb „üresjáráttal” dolgozhassanak, **alapvetően három nagy csoportba osztva végzik tevékenységüket.** Az első csoportban a NETK részéről biztosított ún. integrált szereplők kapnak helyet, és összesen 5 fővel képviseltetik magukat a Kormányban (mint külügyminiszter), a KKB-ben, és a Központi sajtóban. A második csoportban a KKM különböző főosztályai, melynek tagjai azt modellezzik, hogy milyen feladatokat kell elvégezniük a KKM munkatársainak, ezzel együtt a magyar diplomáciának. A harmadik csoportban dolgozó hallgatók pedig az egyes érintett országok külügyi apparátusát modellezzik.

Tekintettel a hallgatói létszámra, az elvégzendő gyakorlat jellegére, illetve a KKM-ben végzett előzetes konzultációkra, az NKE-NETK az általa szimulált szereplők **duplikálását támogatja.** Figyelembe véve a KKM stratégiai szerepét, illetve feladatkörét, ez azt fogja jelenteni, hogy az NKE-NETK szimulációja teljes egészében duplikációra kerül, sőt a külgazdasági és külügyminiszteri posztot három személy is betölti majd (1. és 2. KKM, illetve a kormányban). Tekintettel a gyakorlat során végrehajtandó magas szintű találkozókra, illetve a szűk csillagászati időtartamra, az események hitelessége miatt egyértelműen ez a legkedvezőbb megoldás.

2.2. A gyakorlat levezetésének mozzanatai

1. nap (2018-04-23, 8.00-16.00):

0. mozzanat (9.00-13.00)

A 0. mozzanat tartalma, hogy a közigazgatási szervek normál időszakos működésben végzik alaprendeltetésüknek megfelelő általános feladataikat. Az országban nincs különleges jogrend kihirdetve, a honvédelmi, rendvédelmi és vízügyi igazgatási szervek alapvetően hivatali munkarendben, jóváhagyott munkaterveik alapján, illetve a mindennapokra előírt váltásos szolgálati rendben tevékenykednek, látják el ügyeleti és készenléti szolgálataikat.

A nemzetbiztonsági szolgálatok felderítői munkájuk eredményeképpen jelzést adnak egy várható, az elektromos rendszer elleni kibertámadásról az érintett kormányzati szerveknek. A nemzetbiztonsági szolgálatok jelentése, az alárendeltek felterjesztései alapján a

belügyminiszter, a honvédelmi miniszter, a külgazdasági és külügyminiszter illetve a miniszterelnökséget vezető miniszter elrendeli a veszélyelhárítási és műveleti tervek, adatbázisok, kapacitások, ügyrendek pontosítását, amelyekről jelentések kerülnek bekérésre, felkészülve az esetleges áramkimaradásokból adódó, a kritikus infrastruktúra elemek működésében és a lakosság ellátásában keletkező zavarokra.

1. mozzanat (13.00-16.00)

Az 1. mozzanat tartalma, hogy a várható kibertámadás és várható hatásai miatt a belügyminiszter elrendeli a KKB összehívását, aktivizálják annak operatív és tudományos munkaszerveit, a KKB ülésére részvételre felkérlik Magyarország Kiberkoordinátorát. Aktivizálják a BM OKF **Létfontosságú** Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő **Központját** (LRLIBEK), a Nemzeti Kibervédelmi Intézetet, a különböző szintű operatív törzseket, megerősítik az ügyeleti szolgálatokat, kezdeményezik a védelmi bizottságok összeülését a Fővárosban, Csongrád és Bács-Kiskun megyében.

Az előrejelzésnek megfelelően elkezdenek akadózni a szolgáltatások (részleges áramkimaradások) Budapest IV., V., és XIII. kerületeiben, Csongrád megyében Szeged, Rőske, Kiszombor, Bács-Kiskun megye Kecskemét, Bácsalmás, Kiskunhalas térségében, majd bekövetkezik a feltételezett kibertámadás hatására a teljes áramkimaradás, az áramszolgáltatás megszűnése a felsorolt közigazgatási egységek területén.

Budapest IV. kerületében nem működnek a fővárosi ivóvízbázis kútjai, a szennyvíz átemelés és tisztítás, a közlekedési és vasúti jelzőlámpák, számos üzem termelése és az alapvető szolgáltatások leállnak a kerületben.

Csongrád és Bács-Kiskun megyékben a megyeszékhelyeken szűnt meg az elektromos áram szolgáltatás - gondot okozva a közlekedésben, az ivóvíz ellátásban, a hivatalok és a kórházak működésében. Mindenhol sok a közlekedési baleset.

A Budapest XIII. Népfürdő utcában lévő Duna Arénában a számítástechnikai vezérlő rendszer elleni támadás miatt robbanás következik be, nagymennyiségű sósav szabadul ki, a sósavgőzt a szél a Teve utcai ORFK székház, valamint az V. kerület irányába fújja, a lakosságot 1,5 km sugarú körben ki kell telepíteni és fel kell készülni a Parlament kiürítésére.

Az áramkimaradás miatti súlyos zavarokról, a bekövetkezett eseményekről az érintett szervek jelentéseket terjesztenek fel. A jelentéseket a KKB Nemzeti Veszélyhelyzet Kezelési Központ illetve a Nemzeti Kibervédelmi Intézet összesíti.

A kiberbiztonságért felelős rendvédelmi szervek elkezdik a kiberbiztonsági incidens kivizsgálását, koordinált módon tárják fel és osztják meg egymás között az információkat, szükség esetén a piaci és a nemzetközi szereplőkkel is.

A kialakult súlyos helyzetben a KKB összeül, javaslatot tesz a Kormánynak a veszélyhelyzet kihirdetésére.

A Kormány kihirdeti a veszélyhelyzetet. A külügyi szervek tájékoztatják az EU illetékes szerveit és a szomszédos országokat a veszélyhelyzet kihirdetéséről, a kialakult helyzetről, annak lehetséges határon átnyúló hatásairól.

Az érintett településeken a katasztrófavédelem kijelölt tisztjei a polgármesterektől átveszik a katasztrófavédelmi feladatok irányítását.

A hírek hatására a szerbiai határszakasz túloldaláról a migránsok fokozott mozgolódásáról érkeznek felderítési jelentések. Az áram nélkül maradt településrészekben, kerületekben fokozott rendőri jelenlét szükséges a köz-és vagyonbiztonság érdekében.

2. nap (2018-04-24, 8.00-16.00):

2. mozzanat (8.00-10.00)

A 2. mozzanat tartalma, hogy az elektromos ellátó rendszereket ért kibertámadás miatti veszélyhelyzetben a Duna Arénában bekövetkezett vegyi baleset miatt a Kormány működését a Nemzeti Közzolgálati Egyetemre átköltöztetve kell biztosítani. Meg kell tervezni a minisztériumok, a Nagy Ignác utcai Bv. létesítmény és a Teve utcai ORFK székház kiürítését, vagy lehetőség esetén elzárkóztatását is.

A Duna budapesti szakaszán hajózási tilalom kerül bevezetésre.

Az áramkimaradások és a magyar közszolgálati és civil interneten tapasztalható zavarok miatt a hivatalok folyamatos működése érdekében gondoskodni kell szünetmentes tápegységekről, áramforrás aggregátorokról és az informatikai üzemmenet-folytonossági tervek életbe léptetéséről, a Kat. 47. § (4) pont szerinti szerződési kötelezettségek elrendeléséről.

Esetenként kisebb lakossági zavargások, a sötétség leple alatti üzletfeltörések következnek be, de a rendvédelmi szervek fenntartják a közrendet, közbiztonságot.

Fel kell mérni a kialakult közlekedési, oktatási, egészségügyi, pénzügyi és más intézményműködési helyzetet, a lakossági igényeket, meg kell szervezni a lakosság fogyasztási cikkekkel, ivóvízzel való ellátását, egészségügyi biztosítását és a pénzforgalom fenntartását.

Meg kell szervezni továbbá az őrzés-védelmi feladatokat a kormányzati munkavégzés biztosításához, és a zavaros körülmények közötti esetleges terrortámadások kivédésére a kiemelt objektumok tekintetében.

[IDŐUGRÁS 5 nap]

3. mozzanat (10.00-13.00)

A 3. mozzanat tartalma, hogy számos operatív feladatot hajtanak végre a gyakorlók.

A kibertámadásnak kitett fővárosi kerületekben és a megyeszékhelyeken, településeken "semmi nincs, semmi nem működik" állapot alakult ki az ötödik napra az áramszolgáltatás megszűnése miatt. Nem működik a bankrendszer, a közlekedés, az egészségügy, a víz (ivó- és szenny-) ellátás, illetve az oktatás.

Kibertámadás következtében Kecskeméten a Mercedes-Benz Manufacturing Hungary Kft. Gyár festő műhelyében robbanás és tűz keletkezik, a veszélyes anyagnak minősülő festékek és hígítók mérgező égéstermékai betérítik az üzemet és a szél azokat az útbaeső városrész, a katonai repülőtér és a repülő kórház felé viszi.

Szegeden a HUNGUEST Hotel Forrás Gyógy- és Wellness Szálloda 2. emeletén súlyos tűz üt ki, a szálloda wellness részlegében az uszoda gépészet ismeretlen okú meghibásodása miatt

klór szabadul ki, az az érintett városrészek felett a Bv. Szegedi Fegyház és Börtön valamint a Csongrád Megyei Rendőr-főkapitányság épülete felé terjed.

Valamennyi áramkimaradással érintett településen, kerületben a szükségvilágító eszközök szakszerűtlen használata miatt sok tüzeset, a közlekedési lámpák működésképtelensége miatt számos közúti és néhány kisebb vasúti baleset következik be.

A KKB javaslatára a Kormány az Európai Bizottság Humanitárius Segélyek és Polgári Védelmi Főigazgatóságához fordul nagy mennyiségű áramfejlesztő soron kívüli biztosítására katasztrófasegélyként.

A lakosság ellátására a települési, kerületi, munkahelyi és területi köteles polgári védelmi szervezetek alkalmazási készenlétbe helyezésére a belügyminiszter intézkedik, úgyszintén bevonásra kerülnek a Magyar Honvédség logisztikai egységei, valamint a karitatív és önkéntes mentőszervezetek.

Bácsalmás és Kiskunhalas térségében az áramszünetről értesülve migránsok jelentős tömege igyekszik átkelni illegálisan a magyar határon, nagyon sok helyen megrongálva az ideiglenes biztonsági határzárat (kerítést).

A működő szerb távközlési rendszereken keresztül számos fénykép és beszámoló kerül fel a közösségi médiába, amelyek egyrészt a magyar szervek tehetetlenségéről szóló narratívát erősítik a nemzetközi sajtóban, másrészt pontosan bemutatják a magyar védelmi erők elhelyezkedését, ami növeli a terrorveszélyt. A kibervédelmi szervek intézkednek a migránsoktól elkobzott informatikai eszközök tartalmának elemzésére, szakmai figyelmeztetéseket adnak a határ védelmét ellátó katonák, rendőrök megelőző elektronika védelmi szabályainak foganatosítására, az esetleges, drónok alkalmazásával elkövethető terror támadás kivédésére.

Az áramkimaradás okozta zavart kihasználva a Csongrád megyei határátkelőkön a vámelőírások megsértésével akar számos kamion ki és belépni.

A fővárosi, az érintett megyei és helyi védelmi bizottságok üléseznek, határozatokat hoznak a helyzet kezelésére.

[IDŐUGRÁS újabb 5 nap]

[VIP vendégek látogatása - bemutató]

A kiberbiztonsággal foglalkozó szervek, az informatikai biztonsági szakemberekkel szakaszosan állítják helyre az információs rendszerek működését, az áramellátás hiányából adódott más ágazati működési és rendszerszervezési problémákat.

A védelmi bizottságok, önkormányzatok, a katasztrófavédelem erői a honvédség és rendőrség, a vízügyi igazgatási szervek és más szolgáltatók közreműködésével folyamatosan irányítják és biztosítják az ideiglenes ellátást, a helyreállítás megszervezését.

A KKB összeül, a javuló helyzetről a jelentéseket tudomásul veszi, javaslatot tesz a Kormánynak a veszélyhelyzet megszüntetésére, a Kormányzat visszaköltöztetésére.

4. mozzanat (13.00-14.30):

A gyakorlat utolsó mozzanatának tartalma, hogy az informatikai rendszerek kijavítása, kibervédetségük megerősítése, megszervezése után intézkedés történik a Kormány és Minisztériumok, valamint más kitelepített intézmények visszaköltöztetésére.

Megszervezik a Kormányzat, a minisztériumok, országos hatáskörű szervek, a lakosság alapellátás biztosítását, megtörténik a normál állapot /eredeti helyzet visszaállítása.

[IDŐUGRÁS]

A kormány megszünteti a veszélyhelyzetet, a kormányzati, védelemigazgatási, honvédelmi, rendvédelmi, vízügyi igazgatási szervek, a visszatérnek normál állapotú működési rendjükhöz.

A katasztrófavédelem területi szerveihez bevonulnak a településeken a katasztrófavédelmi tevékenységek irányítását a veszélyhelyzet időszakában átvevő tisztek.

A KKB, a védelmi bizottságok, az események kezelésében részt vett szervezetek összegző jelentéseket készítenek és terjesztenek fel az elvégzett műveletekről, tevékenységekről, a felhasznált anyagokról, eszközökről, pénzösszegekről a jóváhagyott jelentési rendnek megfelelően.

3. RÉSZLETES FELADAT

A Nemzetközi és Európai Tanulmányok Kar szervezeteire vonatkozó közlések valamint egyéb karok bennünket érintő közlései

Idő		Kitől	Kinek	A közlés tartalma	Módja	A gyakorlók tevékenysége
Csill.	Műv.					
0. Mozzanat: 2018.04.23. 09.00-13.00 A közigazgatási szervek általános feladatainak végzése.						
2018. 04. 23 09.16		ACS	Belügyminiszter	A belügyminiszter minisztériumi kabinetülésen megtárgyalja a Nemzetbiztonsági Szolgálatoktól kapott jelentést, a várható kibertámadásról tájékoztatót küld az érintett miniszterekhez, a központi közigazgatási szervekhez (HM. KÜKÜM, MEVM, ORFK, BM OKF, Nemz. Kibervéd. Int.) a kibertámadás elhárításában feladattal bíró vezetőknek.	interneten, írásban	Az érintett miniszterek, országos hatáskörű érintett vezetők fogadják a Belügyminiszter által megküldött nemzetbiztonsági tájékoztatót a várható kibertámadásról.
2018. 04. 23. 9.16		KKM Kabinet	Mindenki a KKM-ben	A KKM lásson hozzá a kiberbiztonsággal kapcsolatos magyar álláspont összefoglalásához, amelyben érintse a nk-i jog szabályait is.	interneten, írásban	KKM Kabinet és KKM Sajtó: a magyar kibervédelmi álláspont összefoglalása 10.30-ig. KKM Főosztályok: a nk-i jog tanulmányozása a kiberbiztonsággal kapcsolatban 10.30-ig.
2018. 04. 23. 9.17		KKM Európai Bilaterális Főosztály, KKM Közép-Európa Főosztály	Minden külföldi külügyminisztérium	A KKM vegye fel a kapcsolatot a külföldi külügyminisztériumokkal, hogy információt kapjon a kiberbiztonság helyi nemzeti szabályozásával kapcsolatban. Továbbá arra is kíváncsiak, hogy látnak-e bármilyen szokatlan vagy rendellenes jelet, amely alátámaszthatja a Magyarország elleni kibertámadást. Ők mit észlelnek saját számítógépes rendszereiken?		A külföldi külügyminisztériumok elkészítik a jelentéseket a kiberbiztonsággal kapcsolatos álláspontjukról 10.30-ig, és átküldik a KKM-nek. Jelzik, hogy tapasztaltak-e bármilyen rendellenességet saját országaikban.
2018. 04. 23. 9.17		KKM BPNSZEU	Minden nk-i szervezet	A KKM vegye fel a kapcsolatot a kiberbiztonságban érintett nk-i szervezetekkel (NATO, Európai Bizottság, EBESZ, Európa Tanács, ENSZ) tanácsért a kibertámadás kezelésével kapcsolatban		A nk-i szervezetek rövid jelentést küldenek, hogy a kiberbiztonság területén mi a feladatuk és kompetenciájuk 10.30-ig.

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04. 23. 9.20		ET Titkárság	Minden ET Külgymisztérium	Az ET egy nk-i konferenciát szervez a kiberbűnözés általános problémaköréről.		Minden külgymisztérium összegyűjti a kiberbűnözéssel kapcsolatos saját tagállami álláspontját. Ismertetik, hogy aláírták-e/ ratifikálták-e a Budapesti Konvenciót? Miért igen, miért nem?
2018.04.23. 9.25		ACS	Csongrád megyei KVI ügyelet	Segélyhívások vétele Az M5 autópálya 170 kilométerszelvényében, nem messze a határátkelőtől, a Belgrád felé vezető oldalon egy spanyol rendszámú mikrobusz eddig tisztázatlan körülmények között felborult. A járműben 9 fő utazott, közülük 1 fő a helyszínen életét vesztette, 2 személy súlyosan, 2 fő könnyen sérült, 4 fő feltehető migráns azonban gyalogosan futva elhagyta a helyszínt. A roncsot kikerülve egy arra haladó klórt szállító tartálykocsi is a gyors irányváltás miatt félig felborult, a klór szivárog.	interneten írásban	tűzoltó erők helyszínre küldése, - Mentőszolgálat, rendőrség helyszínre irányítása, - műszaki mentés elvégzése, - tolmács helyszínre rendelése, - nemzetiség tisztázása, - megfelelő külképviselet értesítése. - jelentés elkészítése, fe0lterjesztése - MKI OpTö működés elrendelése
2018. 04. 23. 9.30		KKM Európai Bilaterális Főosztály	Spanyol Külgymisztérium	Tájékoztatás a felborult spanyol teherautóról. A hozzá szükséges információk beszerzése a Katasztrófavédelem munkatársaitól.		
2018. 04. 23. 10.15		KKM Kabinet	KKM Mindenki	Kezdjék meg a külföldi és a nk-i tapasztalatok elemzését, amint beérkeznek a KKM-be.		A külföldi jelentések főosztályok szerinti elemzése, és számba vétele. Azokból 1 oldalas összefoglaló jelentés írása a KKM Kabinetnek.
2018. 04. 23. 10.30		ET Titkárság	Minden ET Külgymisztérium	Az ET nk-i vitanapot és konferenciát szervez a kiberbűnözés nk-i szabályozásáról Strasbourgban.	szóban	A konferenciára meghívják az USA és Oroszország delegációját is. Az USA elmondja miért csatlakozott a Kiberbűnözés Elleni Konvencióhoz, annak ellenére, hogy nem tagja az ET-nek. Oroszország pedig azt, hogy

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

						miért nem csatlakozott, ha mégis tagja az ET-nek. Ezek után minden ország – köztük Magyarország is – ismerteti az álláspontját. Szóbeli vita 12.00-ig
2018. 04. 23. 12.00		ET Titkárság	Minden ET Külügyminisztériumok	Jelentések készítése a korábbi találkozóról.	írásban	1 oldalas jelentés a találkozóról
2018. 04. 23. 12.00-13.00	Ebédszünet					
1. Mozzanat: 2018. 04. 23. 13.00-16.00 A kibertámadás, a részleges, majd teljes áramkimaradások bekövetkezése, a veszélyhelyzet kihirdetése						
2018. 04. 23. 13.00		Bolgár Küm	Minden EU KÜM	Minden ország kezdje meg a felkészülést az EU ülésre.		A soros elnök Bulgária kezdeményez egy rendkívüli COREPER II ülést Brüsszelben a Magyar-országon kialakuló helyzetről. Napirenden lesz mind a külügyi mind a bel-és igazságügyi vonatkozás.
2018. 04. 23. 13.00		Észt Külügyminisztérium	KKM Kabinet, NATO Nemzetközi Főtitkárság	A 2007-es észtországi kibertámadás tapasztalataira támaszkodva Észtország javasolja a NATO Kiberbiztonsági Bizottságának összehívását.		
2018. 04. 23. 13.05		NATO NT	Minden NATO KÜM	Minden ország kompetens szakértője kezdje meg a felkészülést a NATO Biztonsági Bizottságának ülésére.		
2018. 04. 23. 13.00.	2018. 03.25.	ACS		A várható kibertámadás és annak bekövetkező hatásai miatt a Belügyminiszter elrendeli a KKB összehívását, az NVK, a TT, a BM OKF LRLIBEK, a Nemzeti Kibervédelmi A KKB ülésen részvételre felkéri Magyarország Kiberkoordinátorát, Intézetaktivizálását.	interneten, írásban	A KKB összeül, megtárgyalja a nemzetbiztonsági szolgálatok jelentését, Intézkedés a munkaszervek, operatív törzsek aktivizálására, az ügyletek megerősítésére, az Kezdeményezik az FVB, Csongrád és Bács-Kiskun MVB összeülésétáramszolgáltatás várható kiesése miatti események kezelésére.

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04. 23. 13.05		KKM	Minden KÜM és nk-i szervezet	Tájékoztatás a kormányülésről.		
2018. 04. 23. 13.10		Minden KÜM és nk-i szervezet	KKM	Ország specifikus segítség felajánlása.		Minden külügyminisztérium számba veszi, hogyan tud segíteni Magyarországon. Összefoglaló elküldése 14.00-ig
2018. 04. 23. 13.35		ACS	Csongrád MKI, Bács-Kiskun MKI	<i>Csongrád és Bács-Kiskun megyékben a megyeszékhelyeken megszűnt az elektromos áram szolgáltatás - gondot okozva a közlekedésben, az ivóvíz ellátásban, a hivatalok és a kórházak működésében. Mindenhol sok a közlekedési baleset.</i>	interneten, írásban,	<i>Jelentések vétele, elöljárók, társszervek tájékoztatása, okozott hatások, károk számbavétele, közlekedési balesetekhez tűzoltóságok riasztása, műszaki mentések elvégzése.</i>
2018. 04. 23. 13.36		KKM Kabinet	Szerb Külügymin, Horvát Külügymin, Román Külügymin	Információgyűjtés az NKI és a katasztrófavédelem munkatársaitól. Utána a környező országok tájékoztatása.	interneten, írásban	
2018. 04. 23. 14.00		Bolgár Küm	Minden EU KÜM	COREPER II ülés Brüsszelben (az EU-hoz akkreditált nagykövetek részvételével)	interneten, írásban	szóbeli vita 15.15-ig. Az ülést Bulgária vezeti. Figyelembe kell venni, hogy a kérdés több EU-s szakpolitikai témát is lefed (külügy, bel- és igazságügy), amelyekben eltérő EU-s kompetenciák vannak.
2018. 04. 23. 14.00		NATO Nk-i Titkárság	Minden NATO KÜM	NATO Kibervédelmi Bizottsága (Cyber Defence Committee) ülést tart Brüsszelben a magyarországi kibertámadásról.		szóbeli vita 15.15-ig.
2018. 04. 23. 14.00		ACS	FKI	<i>A Budapest XIII. Népfürdő utca 36. alatt lévő Duna Arénában a számítástechnikai vezérlő rendszer elleni támadás miatt robbanás következik be, nagymennyiségű sósav (250 kg) A lakosságot 1,5 km sugarú körben ki kell telepíteni. Fel kell készülni a Parlament kiürítésére. A sósavgőzt a szél a Teve utcai ORFK székház, valamint az V. kerület irányába fújja. szabadul ki. A</i>		<i>- tűzoltó erők, Mentőszolgálat, rendőrség helyszínre irányítása,</i>

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

				<i>lakosságot 1,5 km sugarú körben ki kell telepíteni. Fel kell készülni a Parlament kiürítésére.</i>		
2018. 04. 23. 14.05		KKM Kabinet	Szomszédos országok és V4	Tájékoztatás a katasztrófavédelem munkatársainál. Utána a környező országok tájékoztatása a helyzetről.	interneten, írásban	
2018. 04. 23. 15.00		ACS	KKB elnöke	<i>A kialakult súlyos helyzetben a KKB összeül, javaslatot tesz a Kormánynak a veszélyhelyzet kihirdetésére.</i>	interneten, írásban	- KKB összeül, előterjesztést készít a Kormány számára a veszélyhelyzet kihirdetésére
2018. 04. 23. 15.15		KKM Kabinet	KKM Sajtó	A sajtóosztály készüljön fel egy rövid nk-i sajtótájékoztatóra, amely 15.45-től lesz megtartva magyar és angol nyelven.		A Sajtóosztály felkészül egy nk-i sajtótájékoztatóra 15.45-től, amely magyar és angol nyelven lesz megtartva. Témák: KKB ülése, EU ülés és NATO ülése.
2018. 04. 23. 15.30		ACS	Kormány	<i>A Kormány ülésén megtárgyalja, elfogadja a KKB javaslatát, kihirdeti a veszélyhelyzetet</i>		- a Kormány rendkívüli ülést tart, megtárgyalja a KKB javaslatát, kihirdeti a veszélyhelyzetet
2018. 04. 23. 15.35		KKM Kabinet	Minden KÜM, nk-i szervezet	Tájékoztatás a kormányülésről.		írásbeli tájékoztatás
2018. 04. 23. 15.37		Minden KÜM, nk-i szervezet	KKM	Kérdéseket tesznek fel, hogyan befolyásolja ez a magyar belpolitika működését? Hogyan érinti ez Magyarország nk-i kapcsolatait és kötelezettségeit.		Minden külügyminisztérium számba veszi, hogyan tud segíteni Magyarországon. Rövid felajánlás írása és elküldése.
2018. 04. 23. 15.45	2018. 04. 05.	ACS	Országos szint. BM OKF	<i>A Belügyminisztérium sajtófőnöke bejelentette, hogy az országos hatáskörű közigazgatási szervek sajtó tájékoztatója a Belügyminisztériumban megkezdődött.</i>	interneten, írásban	Sajtótájékoztató megtartása magyar és angol nyelven. A sajtótájékoztató egyenes adásban zajlik, a gyakorlók nyomon követhetik.

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04. 23. 15.45		KKM Sajtó	Minden Külügyminisztérium, nk-i szervezet	A KKM nemzetközi sajtótájékoztatót tart		A Sajtó Főosztály magyarul és angolul tartja a sajtó-tájékoztatót. Témák: KKB ülése, EU ülés és NATO ülése.
2. Mozzanat: 2018.04.24. 08.00-10.00 A kormányzati működés biztosítása, a lakosság ellátásához szükséges igények felmérése						
2018. 04. 24. 08.05		ACS	BM OKF	<i>A BM OKF intézkedik a vízügyi közlekedési hatósággal együttműködve a hajózási tilalom bevezetésére a Dunán</i>	<i>interneten, írásban</i>	<i>-BM OKF RSOE intézkedik a tilalom közlésére a Dunán közlekedő hajók felé</i>
2018. 04. 24. 08.07		KKM Közép-Európa	Szomszédos országok és V4	Tájékoztatás a Dunán kialakult helyzetről.		
2018. 04. 24. 08.10		Szomszédos országok és V4	KKM Közép-Európa	Kérdéseket tesznek fel, hogyan befolyásolja ez a kétoldalú kereskedelmet?	telefon, internet, írásban	
2018. 04. 24. 08.15		Orosz KÜM	EBESZ Titkárság	Oroszország kezdeményezi az EBESZ Állandó Tanácsának összehívását.		Az Orosz KÜM megpróbálja a kérdést a NATO helyett az EBESZ színterére terelni.
2018. 04. 24. 8.25		USA KÜM	Minden NATO KÜM, NATO Nk-i Titkárság	Az USA kezdeményez egy rendkívüli NATO észak-atlanti tanácsi ülést.		Az USA megpróbál válaszolni azon orosz kezdeményezésre, hogy az ügyet az EBESZ tárgyalja. Párhuzamosan kezdeményez egy rendkívüli NATO találkozót.
2018. 04. 23. 8.30		NATO Nemzetközi Titkárság	Minden NATO Külügyminisztérium	Minden ország kezdje meg a felkészülést az NATO ülésre.		Minden külügyminisztérium kidolgozza a tárgyalási álláspontjait és a háttéranyagát..
2018. 04. 24. 9.45		EBESZ Titkárság	Minden KÜM	EBESZ Állandó Tanácsa (Permanent Council) ülést tart		szóbeli vita 11.15-ig.
2018. 04. 23. 9.45		NATO Nemzetközi Főtitkárság	Minden NATO Külügyminisztérium	NATO Észak-atlanti Tanácsának ülése Brüsszelben a magyarországi kibertámadásról.	szóban	szóbeli vita 11.15-ig.

3. Mozzanat: 2018. 04. 24. 10.00-13.00 A szolgáltatások szünetelése, - „semmi nincs, semmi sem működik”, ideiglenes ellátás, helyreállítás megszervezése						
2018. 04. 24. 10.00	2018. 04.10.	ACS	minden csoport	Nem működik a bankrendszer, a közlekedés, az egészségügy, az ivó-és szennyvízellátás, illetve az oktatás a kibertámadásnak kitett fővárosi kerületekben a Csongrád és Bács-Kiskun megyei megyeszékhelyeken, említett településeiken.		A tájékoztató helyzetjelentés vétele, Operatív feladatok végrehajtása
2018. 04. 24. 10.02		KKM BPNSZEU	ENSZ, EB, NKI, LRLIBEK	A bankrendszer, közlekedés, eü és ivóvízellátás akadozása miatt az nk-i szakosított intézmények és ügynökségek értesítése, és segítség kérése. Ehhez a KKM kapcsolatba lép a az NKI és LRLIBEK munkatársaival is.		Az ENSZ és EB összeszedi az érintett szakosított szervezetek és ügynökségek listáját, illetve azt, hogy mit tudnak segíteni a magyar kormánynak. Jelentések küldése 11.00-ig.
2018. 04. 24. 10.05	5 nappal később (időugrás)	ACS	Bács-Kiskun MKI	Kibertámadás következtében Kecskeméten a Mercedes autó gyár festőműhelyében robbanás és tűz keletkezik, a veszélyes anyagnak minősülő festékek és hígítók mérgező égéstermékei betérítik az üzemet és a szél azokat az útbaeső városrész, a katonai repülőtér és a repülő kórház felé viszi.		tűzoltó erők/KML helyszínre rendelése, -tűzoltás, műszaki mentés végrehajtása, -Mentőszolgálat, rendőrség helyszínre irányítása, -kapcsolatfelvétel a telephely szerint illetékes szakemberekkel, (KVT életbe léptetése),-az érintett lakosság tájékoztatása, -kimenekítés -javaslat a HVB, MVB összehívására
2018. 04. 24. 10.06		KKM Európai Bilaterális Főosztály	Német KÜM, EB, ENSZ	Tájékoztatás a Mercedes gyár helyzetéről. Az autógyártással kapcsolatos nk-i intézmények megkeresése és tájékoztatása.		
2018. 04. 24. 10.10		ACS	Csongrád MKI	Szegeden a HUNGUEST Hotel Forrás Gyógy- és Wellness Szálloda 2. emeletén súlyos tűz üt ki, a szálloda wellness részlegében az uszoda gépészet ismeretlen okú meghibásodása miatt klór szabadul ki, az az érintett városrészek felett a Bv.		tűzoltó erők/KML helyszínre rendelése, -tűzoltás, műszaki mentés végrehajtása, -Mentőszolgálat, rendőrség helyszínre irányítása,

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

				Szegedi Fegyház és Börtön valamint a Csongrád Megyei Rendőr-főkapitányság épülete felé terjed.		-kapcsolatfelvétel a szálloda illetékes szakembereivel, -az érintett lakosság tájékoztatása, -kimenekítés -javaslat a HVB, MVB összehívására
2018. 04. 24. 10.12		KKM Közép-Európa	Szerb Külügymin, Román Külügymin	Tájékoztatás a Hunguest hotel helyzetéről.		
2018. 04. 24. 10.30		ACS	Kormány	A KKB javaslatára a Kormány az Európai Bizottság Humanitárius Segélyek és Polgári Védelmi Főigazgatóságához fordul nagy mennyiségű áramfejlesztő soron kívüli biztosítására katasztrófasegélyként	interneten, írásban	A katasztrófasegély kérésének dokumentumának elkészítése a BM OKF-en a Kormány nevében, megküldése az EU illetékes szervéhez.
2018. 04. 24. 10.32		KKM Kabinet	Bolgár KÜM	A KKM kezdeményezi a soros EU-elnök Bulgáriánál, hogy segítse koordinálni az EU-tagállamoktól érkező rendkívüli katasztrófavédelmi felajánlásokat.		
2018. 04. 23. 11.30		NATO Nemzetközi Főtitkárság	Minden NATO Külügyminisztérium	Minden ország kezdje meg a jelentések írását a NATO ülésről.	írásban	0.5 oldal 12.00-ig
2018. 04. 24. 11.30		EBESZ Titkárság	Minden Küm	Minden ország kezdje meg a jelentések írását az EBESZ ülésről.		0.5 oldal 12.00-ig
2018. 04. 23. 11.30		KKM Kabinet	KKM Sajtó	A sajtóosztály készüljön fel egy nk-i sajtótájékoztatóra, amely 13.00-tól lesz megtartva magyar és angol nyelven.		A korábbi NATO és EBESZ ülések valamint egyéb fejlemények taglalása.
2018. 04. 23. 12.00-13.00	Ebédszünet					
4. Mozzanat: 2018. 04. 24. 13.00-14.30 A normál állapot, eredeti helyzet visszaállítása						
2018. 04. 23. 13.00		KKM Sajtó	Minden Külügyminisztérium, nk-i szervezet	A KKM nemzetközi sajtótájékoztatót tart		A Sajtó Főosztály magyarul és angolul tartja a sajtó-tájékoztatót. A külföldi külügyminisztériumok testesítik meg a nk-i sajtó munkatársait, akik kérdéseket tesznek fel. A kérdések és válaszok már csak magyarul hangoznak el.

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04. 24. 13.50		ACS	Kormány tagjai	A Kormány ülése, a KKB javaslatának elfogadása a veszélyhelyzet megszüntetéséről. A veszélyhelyzet megszüntetése.	interneten, írásban	A kormány ülésének összehívása, a KKB előterjesztésének megtárgyalása, elfogadása. A veszélyhelyzet megszüntetése – Korm. rendelet kihirdetése.
2018. 04. 23. 13.50		KKM Kabinet	Minden Külügyminisztérium, nk-i szervezet	Tájékoztatás a kormányülésről.	írásban	
2018. 04. 24. 14.30	2018. 04.30.	ACS	Összes Csoportnak	Gyakorlat vége	Interneten, írásban	Okmányok zárása, irattározása, informatikai eszközök, rádiók kikapcsolása, leadása az NKE anyagfelelőseinek leltár szerint.

4. A NEMZETKÖZI ÉS EURÓPAI TANULMÁNYOK KAR SZERVEZETEIRE VONATKOZÓ FELADATOK IDŐRENDI LEBONTÁSA SZERVEZETEK SZERINT

Idő		KKM Minisz- teri Kabinet	KKM Sajtó Főosz- tály	KKM Európai Bilaterális Főosztály	KKM Közép- Európa Főosztály	KKM Biztonság- politikai, Nk-i szerve- zetek és EU Főosz- tályok	Szerb Külügy- minisz- térium	Román Külügy- minisz- térium	Bolgár Külügy- minisz- térium	Horvát Külügy- minisz- térium	Osztrák Külügy- minisz- térium	Lengyel Külügy- minisz- térium	Szlovák Külügy- minisz- térium	Cseh Külügy- minisz- térium	Német Külügy- minisz- térium
Csill.	Műv														
0. Mozzanat: 2018.04.23. 09.00-13.00 A közigazgatási szervek általános feladatainak végzése.															
2018. 04.23. 9.16		KKM Kabinet és KKM Sajtó: a magyar kibervédelmi álláspont összefoglalása 10.30-ig. KKM Főosztályok: a nk-i jog tanulmányozása a kiberbiztonsággal kapcsolatban 10.30-ig.						A külföldi külügyminisztériumok elkészítik a jelentéseket a kiberbiztonsággal kapcsolatos álláspontjukról 10.30-ig, és átküldik a KKM-nek. Jelzik, hogy tapasztaltak-e bármilyen rendellenességet saját országaikban.							
2018. 04.23. 9.20		Minden külügyminisztérium összegyűjti a kiberbűnözéssel kapcsolatos saját tagállami álláspontját az ET ülésre. Ismertetik, hogy aláírták-e/ ratifikálták-e a Budapesti Konvenciót? Miért igen, miért nem?													
2018. 04.24. 10.30		ET nk-i konfere ncia	A külföldi jelentések főosztályok szerinti elemzése, és számba vétele. Azokból 2 oldalas összefoglaló jelentés írása a KKM Kabinetnek.					ET nk-i konferencia							
ülés után		Jelentések írása az ET nk-i konferenciájáról az ET Titkárságnak.													
2018. 04.23. 12.00- 13.00		Ebédszünet													
1. Mozzanat: 2018. 04. 23. 13.00-16.00 A kibertámadás, a részleges, majd teljes áramkimaradások bekövetkezése, a veszélyhelyzet kihirdetése															
2018. 04.23. 13.00		Felké- szülés az EU ülésére.	Jelentés írása az országos kataszt- rófavé- delmi helyzet	Jelentés írása az új német kormány és Magyar- ország kapcsola-	Jelentés írása a V4 biztonság politikai és gazdasági hatásairól	Felkészü- lés az EU ülésére.	Jelentés írása az EBESZ felada- táról, műkö- déséről	Felkészülés az EU ülésre.							

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04.23. 13.05		Felkészülés a NATO ülésére.	állapotáról	tárol		Felkészül és a NATO ülésére.	ill. kibebiztonsági érintettségről.	Felkészülés a NATO ülésére.	Jelentés írása Ausztriának a migráns válsággal kapcsolatos álláspontjáról.	Felkészülés a NATO ülésére.
2018. 04.23. 14.00		NATO ülés	Nk-i sajtótájékoztatóra való felkészülés	Jelentés írása a Brexit hatásáról Magyarország tekintetében.	Jelentés írása az osztrák migránspolitika alakulásáról és Magyarország kapcsolatairól	Jelentés írása Magyarország Keleti nyitáspolitikájáról		NATO ülés		NATO ülés
2018. 04.23. 14.00		EU találkozó						EU találkozó		
2018. 04. 23. 15.15		Jelentés készítése a NATO és EU találkozókról a KKM-nek 16.00-ig								
2018. 04.23. 15.45		A KKM nemzetközi sajtótájékoztatót tart. Témák: KKB ülése, EU ülés és NATO ülése.								
2. Mozzanat: 2018.04.24. 08.00-10.00 A kormányzati működés biztosítása, a lakosság ellátásához szükséges igények felmérése										
2018. 04.24. 08.17		Felkészülés az EBESZ ülésére.								
2018. 04.24. 08.30		Felkészülés a NATO ülésére.	Jelentés írása az országos katasztrófavédelmi helyzet állapotáról	Jelentés írása a tegnapi EU és NATO találkozók tagállami álláspontjairól	Jelentés írása a tegnapi EU és NATO találkozók tagállami álláspontjairól	Felkészülés a NATO ülésére.	Jelentés írása a migráns-válság szerbiai kezeléséről a KKM-nek	Felkészülés a NATO ülésére.	Jelentés írása az új osztrák kormány V4 politikájáról a KKM-nek	Felkészülés a NATO ülésére.

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04.23. 9.45		EBESZ találkozó	Nk-i sajtótájékoztatóra való felkészülés	Jelentés írása a székely autonómia-törekvés és más európai országok regionális törekvéseinek összehasonlításáról	Jelentés írása a magyar-lengyel kapcsolatokról	Összefoglaló jelentés írása a tegnapi EU és NATO találkozóról	EBESZ találkozó			
2018. 04.24. 9.45		NATO ülés					Jelentés írása a migráns-válság szerbiai kezeléséről a KKM-nek	NATO ülés	Jelentés írása az új osztrák kormány V4 politikájáról a KKM-nek	NATO ülés
3. Mozzanat: 2018. 04. 24. 10.00-13.00 A szolgáltatások szünetelése, - „semmi nincs, semmi sem működik”, ideiglenes ellátás, helyreállítás megszervezése										
2018. 04.24. 11.00		Jelentések készítése az EBESZ és NATO találkozókról.								
2018. 04.23. 12.00-13.00	Ebédszünet									
4. Mozzanat: 2018. 04. 24. 13.00-14.30 A normál állapot, eredeti helyzet visszaállítása										
2018. 04.23. 13.00		A KKM nemzetközi sajtótájékoztatót tart. A Sajtó Főosztály magyarul és angolul tartja a sajtótájékoztatót. A külföldi külügyminisztériumok testesítik meg a nk-i sajtó munkatársait, akik kérdéseket tesznek fel. A kérdések és válaszok már csak magyarul hangoznak el.								

Idő		Francia Külügy- minisz- térium	Brit Külügy- minisz- térium	Svéd Külügy- minisz- térium	Spanyol Külügy- minisz- térium	Észt Külügy- minisz- térium	Orosz Külügy- minisz- térium	USA Külügy- minisz- térium	Ukrán Külügy- minisz- térium	EU Bizottság	NATO Nemzet- közi Titkárság	EBESZ Titkárság	Európa Tanács Titkárság	ENSZ Titkárság
Csill.	Műv									Orosz csapat csinálja	Ukrán csapat csinálja	Szerb csapat csinálja	USA csapat csinálja	Ukrán csapat csinálja
0. Mozzanat: 2018.04.23. 09.00-13.00 A közigazgatási szervek általános feladatainak végzése.														
2018. 04.23. 9.16		A külföldi külügyminisztériumok elkészítik a jelentéseket a kiberbiztonsággal kapcsolatos álláspontjukról 10.30-ig, és átküldik a KKM-nek. Jelzik, hogy tapasztaltak-e bármilyen rendellenességet saját országaikban.								Jelentések írása az adott nk-i szervezet érintettségéről a kiberbiztonsággal kapcsolatban 14.00-ig..				
2018. 04.23. 9.20		Minden külügyminisztérium összegyűjti a kiberbűnözéssel kapcsolatos saját tagállami álláspontját az ET ülésre. Ismertetik, hogy aláírták-e/ ratifikálták-e a Budapesti Konvenciót? Miért igen, miért nem?												
2018. 04.24. 10.30		ET nk-i konferencia												
ülés után		Jelentések írása az ET nk-i konferenciájáról az ET Titkárságnak.												
2018. 04.23. 12.00- 13.00		Ebédszünet												
1. Mozzanat: 2018. 04. 23. 13.00-16.00 A kibertámadás, a részleges, majd teljes áramkimaradások bekövetkezése, a veszélyhelyzet kihirdetése														
2018. 04.23. 13.00		Felkészülés az EU ülésre.					Jelentés írása Oroszország kiber- és média-befolyásáról napjainkban.	Jelentés írása az amerikai hadsereg kibervédelmi helyzetéről	Jelentés írása az orosz-ukrán kapcsolatokról	Jelentés írása Oroszország kiber- és médiabefolyásáról napjainkban.	Jelentés írása az orosz-ukrán kapcsolatokról	Jelentés írása az EBESZ feladatáról, működéséről ill. kiberbiztonsági érintettségéről.	Jelentés írása az amerikai hadsereg kibervédelmi helyzetéről	Jelentés írása az orosz-ukrán kapcsolatokról

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04.23. 13.05		Felkészülés a NATO ülésére.	Jelentés írása Svéd-ország nk-i	Felkészülés a NATO ülésére.		Felké- szülés a NATO ülésére.			Felké- szülés a NATO ülésére.			Felkészülés a NATO ülésére.
2018. 04.23. 14.00		NATO ülés	semleges- ségéről a kiberbiz- tonsággal összefüg- gésben.	NATO ülés		NATO ülés			NATO ülés		NATO ülésen már részt vesz	NATO ülésen már részt vesz
2018. 04.23. 14.00		EU találkozó			Jelentés írása az orosz- amerikai kapcsolatokról Trump megválasztása után	Jelentés írása az EU- ukrán kapcso- latokról		EU találkozó	Jelentés írása az EU- ukrán kapcso- latokról	Jelentés írása a Ny- Balkán EU bővíté- séről	Jelentés írása az orosz- amerikai kapcso- latokról Trump megválasz- tása után	Jelentés írása az EU-ukrán kapcsola- tokról
2018. 04.23. 15.15		Jelentés készítése a NATO és EU találkozókról a KKM-nek 16.00-ig										
2018. 04.23. 15.45		A KKM nemzetközi sajtótájékoztatót tart. Témák: KKB ülése, EU ülés és NATO ülése.										
2. Mozzanat: 2018.04.24. 08.00-10.00 A kormányzati működés biztosítása, a lakosság ellátásához szükséges igények felmérése												
2018. 04.24. 08.17		Felkészülés az EBESZ ülésére.										

INTEGRÁLT VÉDELEM 2018 - GYAKORLAT

2018. 04.24. 08.30		Felkészülés a NATO ülésére.	Jelentés írása Svédország migráns politikájáról a KKM-nek	Felkészülés a NATO ülésére.	Jelentés írása Paks 2 előrehaladásáról a KKM-nek	Felkészülés a NATO ülésére.	Jelentés írása Paks 2 előrehaladásáról a KKM-nek	Felkészülés a NATO ülésére.	Jelentés írása a migráns válság szerbiai kezeléséről a KKM-nek	Felkészülés a NATO ülésére.	Jelentés írása az ET feladatáról, működéséről ill. kiberbiztonsági érintettségéről
2018. 04.23. 9.45		EBESZ találkozó									
2018. 04.24. 9.45		NATO ülés	Jelentés írása Svédország migráns politikájáról a KKM-nek	NATO ülés	Az EB jelentést ír a magyar kormány, hogy milyen EU-s intézményeket, ügynökségeket stb. kell tájékoztatni, ha komoly fennakadások vannak a bankrendszer, a közlekedés, az egészségügy, az ivó- és szennyvízellátás, illetve az oktatás területén.	NATO ülés	Az EB jelentést ír a magyar kormány, hogy milyen EU-s intézményeket, ügynökségeket stb. kell tájékoztatni, ha komoly fennakadások vannak a bankrendszer, a közlekedés, az egészségügy, az ivó- és szennyvízellátás, illetve az oktatás területén.	NATO ülés	Jelentés írása a migráns válság szerbiai kezeléséről a KKM-nek	Jelentés írása az amerikai-magyar kereskedelmi kapcsolatokról	Az ENSZ jelentést ír a magyar kormány, hogy milyen ENSZ-es szakosított intézményeket, ügynökségeket stb. kell tájékoztatni, ha komoly fennakadások vannak a bankrendszer, a közlekedés, az egészségügy, az ivó- és szennyvízellátás, illetve az oktatás területén.

3. Mozzanat: 2018. 04. 24. 10.00-13.00 A szolgáltatások szünetelése, - „semmi nincs, semmi sem működik”, ideiglenes ellátás, helyreállítás megszervezése		
2018. 04.24. 11.00		Jelentések készítése az EBESZ és NATO találkozóról.
2018. 04.23. 12.00- 13.00		Ebédszünet
4. Mozzanat: 2018. 04. 24. 13.00-14.30 A normál állapot, eredeti helyzet visszaállítása		
2018. 04.23. 13.00		A KKM nemzetközi sajtótájékoztatót tart. A Sajtó Főosztály magyarul és angolul tartja a sajtótájékoztatót. A külföldi külügyminisztériumok testesítik meg a nk-i sajtó munkatársait, akik kérdéseket tesznek fel. A kérdések és válaszok már csak magyarul hangoznak el.

5. A GYAKORLAT HALLGATÓI

Vezetéknév	Keresztnév	Neptun kód	Képzés
Ackermann	Vilmos	GOSCFR	nemzetközi igazgatási
Adámy	Réka	D7QHGD	nemzetközi igazgatási
Anti	Renáta	H5OU3H	nemzetközi igazgatási
Badar	Fanni	TC34UF	nemzetközi igazgatási
Bálint	Sára Réka	ABGAJJ	nemzetközi igazgatási
Bánfalvi	Eszter	SOHNX0	nemzetközi biztonság- és védelempolitikai
Bíró	Máté	YSV9GM	nemzetközi biztonság- és védelempolitikai
Bodó	Norbert	GC3NZI	nemzetközi igazgatási
Bognár	Adrienn	D5X5B4	nemzetközi igazgatási
Borsányi	András	HO21OI	nemzetközi biztonság- és védelempolitikai
Budai	Nóra	EZDW21	nemzetközi igazgatási
Csató	Eszter	V7J4CZ	nemzetközi igazgatási
Csepregi	Katalin	Q2GXJK	nemzetközi biztonság- és védelempolitikai
Csillag	Eszter	TSGMEY	nemzetközi igazgatási
Csonka	Attila Endre	HIJ4ZB	nemzetközi igazgatási
Csrepka	Márton	W47NJ8	nemzetközi igazgatási
Dancsok	Petra	WVQ13D	nemzetközi igazgatási
Dankó	Mihály	RLLR77	nemzetközi biztonság- és védelempolitikai
Dobos	István	JNPWR4	nemzetközi biztonság- és védelempolitikai
Doma	Ádám	JNKRKI	nemzetközi biztonság- és védelempolitikai
Fehér	Fruzsina	K3SPC7	nemzetközi biztonság- és védelempolitikai
Fejes	Blanka	ZE5SR4	nemzetközi igazgatási
Fekécs	Gergely	ML58Z4	nemzetközi biztonság- és védelempolitikai
Felde	András Bence	GEL4P6	nemzetközi biztonság- és védelempolitikai
Ferenczi	Péter	YW48ZY	nemzetközi igazgatási
Fodor	Márk Jozipovics	TIUW60	nemzetközi biztonság- és védelempolitikai
Fórizs	Gabriella	IWSCHC	nemzetközi igazgatási
Fülöp	Adriána	IO6OAV	nemzetközi igazgatási
Fülöp	Erik	YW8JA3	nemzetközi biztonság- és védelempolitikai
Gál	Zoltán	I5HX1J	nemzetközi igazgatási
Gál	Máté	KH7DVY	nemzetközi biztonság- és védelempolitikai
Garádi	Áron	YRDXGA	nemzetközi biztonság- és védelempolitikai
Hajdu	Dorina	HR1K1X	nemzetközi biztonság- és védelempolitikai
Halász	Bence	I3CED2	nemzetközi igazgatási
Hegedűs	Eszter	ILNXJ4	nemzetközi igazgatási
Hollósi	Jázmin	EHWTBM	nemzetközi biztonság- és védelempolitikai
Horváth	Ármin	YTPZR5	nemzetközi biztonság- és védelempolitikai
Juhász	Zsófia	KS0FBH	nemzetközi igazgatási
Katona	Martina Vivien	BV3JRK	nemzetközi igazgatási
Kerekes	Kristóf Miklós	MELGAM	nemzetközi igazgatási
Kis	Anna	I6I48J	nemzetközi igazgatási
Kiss	Beatrix	MSXBOS	nemzetközi biztonság- és védelempolitikai
Komonyi	Arnold	L5DEP9	nemzetközi biztonság- és védelempolitikai
Kovács	András Bence	QCVY7I	nemzetközi biztonság- és védelempolitikai
Kovács	Viktória	VSV8OL	nemzetközi biztonság- és védelempolitikai
Kovács	Gergely	KH8LJF	nemzetközi igazgatási
Krizsán	Bence	DAPV9C	nemzetközi biztonság- és védelempolitikai
Laczó	Levente	U1LHJ0	nemzetközi igazgatási
Lénárt	Tamás	V38MU6	nemzetközi biztonság- és védelempolitikai
Lombos	Dorottya	BL1AS4	nemzetközi igazgatási
Loós	Viktória	W0KK0V	nemzetközi igazgatási
Márkus	Dóra	FM6PH5	nemzetközi igazgatási
Marton	Ádám	F37CY1	nemzetközi biztonság- és védelempolitikai
Matusik	András Valter	ZMMQKH	nemzetközi igazgatási
Mészáros	Tamás	JSBNCZ	nemzetközi biztonság- és védelempolitikai

Murányi	Eszter	IT536O	nemzetközi igazgatási
Nagy	Barnabás	IT4TZG	nemzetközi igazgatási
Németh	István	O6OS81	nemzetközi igazgatási
Nyárádi	Fanni	D3VVP5	nemzetközi igazgatási
Oravecz	Ákos	XKJO35	nemzetközi biztonság- és védelempolitikai
Orémusz	Bertalan	IJ5G6C	Nemzetközi biztonság- és védelempolitikai BSc
Pálinkás	Julianna	XC0S6C	nemzetközi biztonság- és védelempolitikai
Pálinkás	Petra	WAUJB4	nemzetközi biztonság- és védelempolitikai
Paulik	Dénes	ANCMQE	nemzetközi biztonság- és védelempolitikai
Petróczki	Márk,	YJ8KZU	nemzetközi biztonság- és védelempolitikai
Petrovác	Eszter	QCXN7K	nemzetközi igazgatási
Polgár	Judit Dalma	S0QNW7	nemzetközi igazgatási
Poszavec	Tamás	HRVC7B	nemzetközi biztonság- és védelempolitikai
Rozgonyi	Attila	O2E1VQ	nemzetközi biztonság- és védelempolitikai
Sallai	Fruzsina	JO42Y2	nemzetközi biztonság- és védelempolitikai
Sánta	György	HLPEJ3	nemzetközi biztonság- és védelempolitikai
Sásdi	Árpád	W2MMC2	nemzetközi igazgatási
Schultheisz	Máté	V51C3C	nemzetközi igazgatási
Szabados	Boglárka	X5DTYI	nemzetközi igazgatási
Szabó	Orsolya Réka	HGMSHL	nemzetközi biztonság- és védelempolitikai
Szántó	Viola	AT2KMX	nemzetközi igazgatási
Szekeres	Ákos	URRXZE	nemzetközi igazgatási
Szűcs	Evelin	W0LM0Q	nemzetközi igazgatási
Tományi	Enikő	FQQRJZ	nemzetközi igazgatási
Tóth	Hajnalka Judit	F20VLO	nemzetközi biztonság- és védelempolitikai
Tóth	Klaudia	DL63X5	nemzetközi igazgatási
Varga	Benjámín	FK1TE5	nemzetközi biztonság- és védelempolitikai
Varga	Dóra	VHWPBZ	nemzetközi igazgatási
Varga	Olivér	FSVSJB	nemzetközi biztonság- és védelempolitikai
Vladár	Veronika Fanni	MUJW88	nemzetközi igazgatási
Yousif	Zaki Ádil	YDQKD5	nemzetközi igazgatási

6. A HALLGATÓK SZERVEZETI BEOSZTÁSA

6.1. A Nemzetközi és Európai Tanulmányok Kar hallgatóinak feladata a NemzetiKözzszolgálati Egyetem integrált gyakorló szervezeteiben (összesen 5 fő)

Végrehajtási szintek és szervezetek:

I/1. Kormány, Katasztrófavédelmi Koordinációs Tárcaközi Bizottság (KKB)

Összetétele	Funkció	Létszám
Külgazdasági és külügyminiszter	KKM	Varga Olivér
A KKM 1. szakértője	A miniszter segítője	Dankó Mihály
A KKM 2. szakértője	A miniszter segítője	Kovács Marcell

Központi Sajtó

Összetétele	Funkció	Létszám
KKM összekötő 1.	A KKM képviselte a Kp-i Sajtóban	Kiss Beatrix
KKM összekötő 2.	A KKM képviselte a Kp-i Sajtóban	Szabó Orsolya Réka

6.2. A Nemzetközi és Európai Tanulmányok Kar hallgatóinak beosztása a NETK karon belül A és B csoportban (összesen 84 fő)

Magyarország Külgazdasági és Külügyminisztériuma

KKM Külügyminiszter/akkreditált nagykövet/külügyi szakértő (1-1 fő)

KKM Miniszteri Kabinet (2-2 fő)

A	B
Ferenczi Péter	Bánfalvi Eszter
Murányi Eszter	Csonka Attila Endre
Nagy Barnabás	Yousif Zaki Ádil

KKM Sajtó Főosztály

KKM Biztonságpolitikai, Nk-i szervezetek és EU Főosztályok

A	B
Anti Renáta	Juhász Zsófia
Fejes Blanka	Szűcs Evelin
Varsányi Áron	Kiss Péter Botond

KKM Európai Bilaterális Főosztály

A	B
Polgár Judit Dalma	Bodó Norbert
Fülöp Adriána	Gál Máté

KKM Közép-Európa Főosztály

A	B
Szántó Viola	Hollósi Jázmin
Németh István	Tóth Klaudia

Szerb Külügyminisztérium/EBESZ Titkárság

A	B
Csillag Eszter	Doma Ádám
Rozgonyi Attila	Sánta György

Román Külügyminisztérium

A	B
Csrepka Márton Bertalan	Sásdi Árpád
Orémusz Bertalan	Varga Dóra

Bolgár Külügyminisztérium/a Tanács soros elnöksége (COREPER II)

A	B
Loós Viktória	Lénárt Tamás
Oravecz Ákos	Komonyi Arnold

Horvát Külügyminisztérium

A	B
Dobos István	Garádi Áron
Mészáros Tamás	Kovács András Bence

Osztrák Külügyminisztérium

A
Lombos Dorottya
Paulik Dénes

Lengyel Külügyminisztérium

A	B
Adámy Réka	Kovács Viktória
Halász Bence	Petrovác Eszter

Szlovák Külügyminisztérium

A	B
Kovács Gergely	Matusik András Valter
Szekeres Ákos	Schultheisz Máté

Cseh Külügyminisztérium

A	B
Badar Fanni	Csató Eszter
Budai Nóra	Hegedűs Eszter

Német Külügyminisztérium

A	B
Ackermann Vilmos	Bognár Adrienn
Borsányi András	Márkus Dóra

Francia Külügyminisztérium

A	B
Pálincás Petra	Hajdu Dorina
Tóth Hajnalka Judit	Pálincás Julianna

Brit Külügyminisztérium

A	B
Katona Martina Vivien	Bálint Sára Réka
Vladár Veronika Fanni	Dancsok Petra

Svéd Külügyminisztérium

B
Felde András Bence
Poszaveczi Tamás

Spanyol Külügyminisztérium

A	B
Fehér Fruzsina	Csepregi Katalin
Tományi Enikő	Fórizs Gabriella

Észt Külügyminisztérium

A	B
Marton Ádám	Gál Zoltán
Laczó Levente	Horváth Ármin

Orosz Külügyminisztérium/Európai Bizottság

A	B
Fekécs Gergely	Nyárádi Fanni
Fülöp Erik	Szabados Boglárka

USA Külügyminisztérium/Európa Tanács Titkársága

A	B
Kerekes Kristóf Miklós	Bíró Máté
Sallai Fruzsina	Kis Anna

Ukrán Külügyminisztérium/NATO Nk-i Titkárság & ENSZ Titkárság

A	B
Fodor Márk Jozsipovics	Krizsán Bence
Varga Benjámin	Petróczki Márk

6.3. A gyakorlat vezetői és segítők (összesen 9 fő)

Megfigyelő	Gyakorló szervezet		Megjegyzés
	Neve	Helye	
Kaszap Márton	NKE-NETK		főkidolgozó
Tongori Zsófia.	NKE-NETK		főkidolgozó
Dr. Pásztor Szabolcs	NKE-NEKT		segítő
Dr. Marsai Viktor	NKE-NEKT		segítő
Jakusné Dr. Harnos Éva	NKE-NETK		segítő
Dr. Kozák Kornélia	NKE-NETK		segítő
Hárs András	NKE-NETK		segítő
Fekete Csanád	NKE-NETK		segítő
Szabó Mátyás	NKE-NETK		segítő

6.4. Terembeosztás

6.4. Terembeosztás

KKM 'A' 10 fő – Ludovika Campus Kollégium „A” terem

KKM 'B' 10 fő – Ludovika Campus Kollégium „B” terem

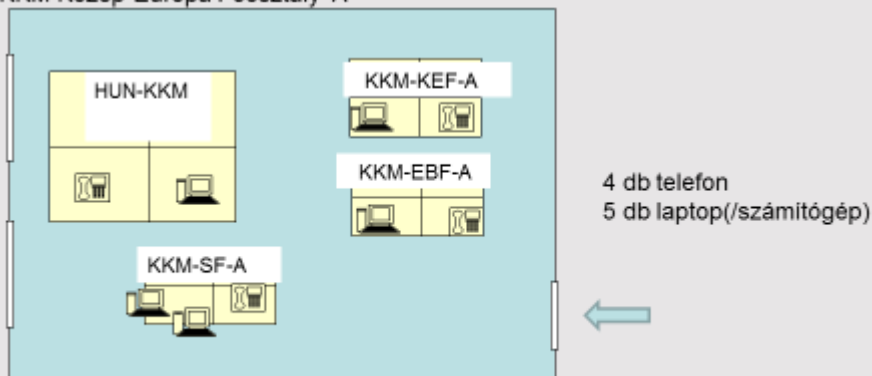
Egyéb Külügyminisztériumok 'A' 32 fő – Ludovika Campus Kollégium„C” terem

Egyéb Külügyminisztériumok 'B' 32 fő – Ludovika Campus Kollégium„D” terem

LUDOVIKA CAMPUS –KOLLÉGIUM

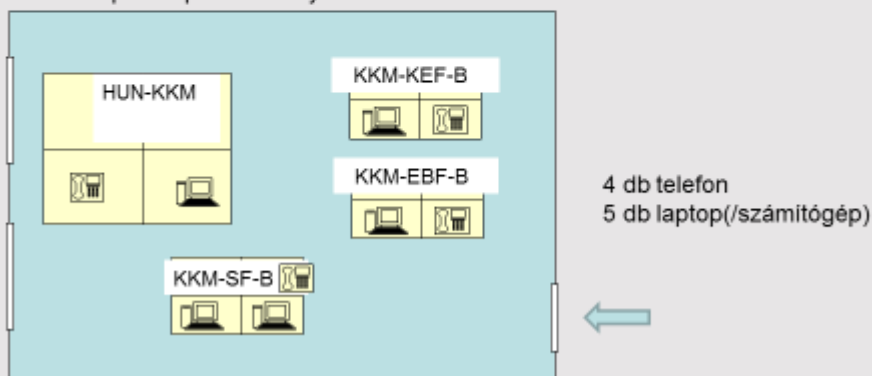
Ludovika Campus Kollégium A. terem Magyarország Külgazdasági és Külügyminisztériuma + EU szervezetek 'A' (10 fő)

- Magyarország Külgazdasági és Külügyminisztériuma A (HUN-KKM-A)
- KKM Sajtó Főosztály, KKM Biztonságpolitikai, Nk-i szervezetek és EU Főosztályok 'A'
- KKM Európai Bilaterális Főosztály 'A'
- KKM Közép-Európa Főosztály 'A'



Ludovika Campus Kollégium B. terem Magyarország Külgazdasági és Külügyminisztériuma + EU szervezetek 'B' (10 fő)

- Magyarország Külgazdasági és Külügyminisztériuma A (HUN-KKM-B)
- KKM Sajtó Főosztály, KKM Biztonságpolitikai, Nk-i szervezetek és EU Főosztályok 'B'
- KKM Európai Bilaterális Főosztály 'B',
- KKM Közép-Európa Főosztály 'B'



Ludovika Campus Kollégium C. terem

Egyéb Országok Külgazdasági és Külügyminisztériumai 'A, (32 fő)

Németország Külügyminisztériuma A
 Lengyelország Külügyminisztériuma A
 Osztrák Külügyminisztérium A
 Horvátország Külügyminisztériuma A
 Szerbia Külügyminisztériuma A
 Román Külügyminisztérium A
 Bolgár Külügyminisztérium A
 Szlovák Külügyminisztérium A
 Spanyol Külügyminisztérium A

Francia Külügyminisztérium A
 Észt Külügyminisztérium A
 Orosz Külügyminisztérium/Európai Bizottság A
 USA Külügyminisztérium/Európa Tanács Titkársága A
 Ukrajna Külügyminisztérium/NATO & ENSZ 'A'

GER-KUM 2 fő	CRA-KUM 2 fő	BUL-KUM 2 fő	AUT-KUM 2 fő
POL-KUM 2 fő	SRB-KUM 2 fő	SVK-KUM 2 fő	CZE-KUM 2 fő
GER-KUM 2 fő	FRA-KUM 2 fő	GBR-KUM 2 fő	ESP-KUM 2 fő
EST-KUM 2 fő	RUS-KUM 2 fő	USA-KUM 2 fő	UKR-KUM 2 fő

8 db telefon
16 db laptop/számítógép)

Ludovika Campus Kollégium D. terem

Egyéb Országok Külgazdasági és Külügyminisztériumai ,B, (32 fő)

Németország Külügyminisztériuma B
 Lengyelország Külügyminisztériuma B
 Osztrák Külügyminisztérium B
 Horvátország Külügyminisztériuma B
 Szerbia Külügyminisztériuma B
 Román Külügyminisztérium B
 Bolgár Külügyminisztérium B
 Szlovák Külügyminisztérium B
 Spanyol Külügyminisztérium B
 Cseh Külügyminisztérium B
 Brit Külügyminisztérium B

Francia Külügyminisztérium B
 Észt Külügyminisztérium B
 Orosz Külügyminisztérium/Európai Bizottság B
 USA Külügyminisztérium/Európa Tanács Titkársága B
 Ukrajna Külügyminisztérium/NATO & ENSZ B

GER-KUM 2 fő	CRA-KUM 2 fő	BUL-KUM 2 fő	AUT-KUM 2 fő
POL-KUM 2 fő	SRB-KUM 2 fő	SVK-KUM 2 fő	CZE-KUM 2 fő
GER-KUM 2 fő	FRA-KUM 2 fő	GBR-KUM 2 fő	ESP-KUM 2 fő
EST-KUM 2 fő	RUS-KUM 2 fő	USA-KUM 2 fő	UKR-KUM 2 fő

8 db telefon
16 db laptop(/számítógép)

7. A NEMZETKÖZI SZERVEZETEK ÉS A KIBERBIZTONSÁG

7.1. A NATO és a kiberbiztonság

Az egyre elterjedtebb kibertámadásokat mind az állami, mind a nem-állami cselekvők használhatják katonai célokra. A kibertámadások a hibrid hadviselés részeivé váltak. A NATO és szövetségesei erős és ellenálló kibervédelmet hoztak létre, hogy megvédjék hálózataikat és működésüket a kibertámadásoktól, és teljesítsék fő feladataikat a kollektív védelem, a válságkezelés és a kooperatív biztonság terén. A kibervédelem területén a NATO együttműködik az Európai Unióval, az Egyesült Nemzetek Szervezetével, valamint az Európai Biztonsági és Együttműködési Szervezettel.

7.1.1. A NATO kibervédelmi politikája

A 2014. évi walesi csúcstalálkozón a NATO szövetségesek elfogadták azt az akciótervet, amely kimondja, hogy a kibervédelem része a szövetség alapfeladatának, a kollektív védelemnek; megállapítja, hogy a nemzetközi jogot érvényesnek kell tekinteni a kibertérben, és sürgeti a NATO együttműködését az iparral. A legfőbb célkitűzés a Szövetség tulajdonában lévő és általa működtetett kommunikációs rendszerek védelme. A NATO kibervédelmi politikája foglalkozik a koordinált kibervédelmi kormányzással, és a szövetségeseknek nyújtandó segítség összehangolásával (beleértve a lakossági vészhelyzetre vonatkozó tervezést).

A 2016. évi varsói csúcstalálkozón a szövetségesek megállapodtak, hogy erősítik a nemzeti infrastruktúrák és hálózatok kibervédelmét. Megerősítették a NATO védelmi jellegét, ugyanakkor, mivel manapság a legtöbb konfliktus és válság a kibertérben is megjelenik, a kibertér olyan műveleti területként ismerték el, amelyen a szövetségnek ugyanolyan hatékonyan meg kell védenie magát, mint a szárazföldön, a levegőben és a tengereken.

7.1.2. A NATO kibervédelmi képessége

A NATO Számítógépes Incidens Reagáló Központja (NATO Computer Incident Response Capability: NCIRC) a Szövetséges Erők Európai Főparancsnokságán (SHAPE), Monsban, Belgiumban működik. Folyamatos kibervédelmi támogatást nyújt a Szövetség

létesítményeinek. A nemzeti kibervédelmi képességek erősítése részévé vált a NATO védelmi tervezési folyamatának. Az NCIRC Koordinációs Központ felel a NATO központban és a tagországokban a kibervédelmi tevékenységek összehangolásáért.

A 2012. évi chicagói csúcstalálkozón a Szövetségesek megerősítették elkötelezettségüket, hogy növeljék a Szövetség kibervédelmét az által, hogy az összes NATO hálózatot központi védelem alá helyezik, és számos korszerűsítést hajtanak végre az NCIRC-ben. 2012 júliusában a NATO szervezeti reformjának a részeként ott hozták létre a NATO Kommunikációs és Informatikai Ügynökségét (NATO Communications and Information Agency: NCIA).

A NATO Kommunikációs és Informatikai Ügynöksége (NCIA) a Monsban, Belgiumban található NCIRC Technikai Központja révén felelős a technikai kiberbiztonságért az egész NATO-ban. Kulcsszerepe van a kibertámadásokra adott válaszlépésekben. Ez a központ jelenti a támadásokat és terjeszti az ezekre vonatkozó információt a rendszergazdáknak, a biztonsági felelősöknek és a felhasználóknak.

A NATO Kibervédelmi Kiválósági Központja (NATO Cooperative Cyber Defence Centre of Excellence: CCD CoE) Tallinnban, Észtországban működik. NATO-akkreditált szakértői központ, amely kibervédelmi oktatással, konzultációval, elemzéssel, kutatással és fejlesztéssel foglalkozik, de egyelőre nem része a NATO vezetési struktúrájának.

A kibervédelmet integrálták a NATO Intelligens Védelem (Smart Defence) programjába, melynek lényege, hogy az országok együttműködnek olyan képességek fejlesztésében és beszerzésében, amelyekre egyedül nem rendelkeznének megfelelő anyagi eszközökkel. A kibervédelem esetében ez a következőkre vonatkozik: a Kártevő Információ Megosztó Platform (Malware Information Sharing Platform: MISP), az Intelligens Védelem Többnemzetiségű Kibervédelmi Képességfejlesztési Program (Smart Defence Multinational Cyber Defence Capability Development: MN CD2) és a Többnemzetiségű Kibervédelmi Oktató és Kiképző Program (Multinational Cyber Defence Education and Training: MN CD E&T).

Az Észak-atlanti Tanács (NAC) gyakorol felügyeletet a kibervédelemmel kapcsolatos válságkezelés fölött. Ezt a testületet tájékoztatják a fontosabb incidensekről és

kibertámadásokról. A Tanácsnak alárendelt Kibervédelmi Bizottság (Cyber Defence Committee) a tagállamok tevékenységét felügyeli kibervédelmi területen. A NATO Kibervédelmi Irányító Testülete (Cyber Defence Management Board: CDMB) felelős a gyakorlatban a kibervédelem összehangolásáért a polgári és a katonai testületek között. A NATO Konzultációs, Vezetési és Ellenőrző Bizottsága (NATO Consultation, Control and Command: NC3 Board) felelős a kibervédelem technikai megvalósításáért.

A NATO Ipari Kibervédelmi Partnerségi programjában (NATO Industry Cyber Partnership: NICP) a Szövetségesek az iparral erősítik az együttműködésüket. A már létező struktúrákra építve bevonják a Nemzeti Számítástechnikai Reagáló Csoportokat és az ipar képviselőit a kibervédelemmel kapcsolatos információk megosztásába, az oktatásba és a kiképzésbe.

2016. február 16-án a NATO és az EU technikai megállapodást kötött a kibervédelemről, hogy elősegítse a kibertámadások megelőzését és kivédését mindkét szervezetben. Ez a technikai megállapodás az NCIRC és az EU Számítástechnikai Vészhelyzeti Reagáló Csoportja között (Computer Emergency Response Team: CERT-EU) keretet nyújt az információcseréhez és a legjobb gyakorlatok cseréjéhez a két reagáló csoport között.

2017. november 8-án a NATO védelmi miniszterei elvi megállapodást kötöttek az új Kiberművelési Központ létrehozásáról, amely a NATO korszerűsített vezetési struktúrájának része lesz. Ez megerősíti a NATO kibervédelmét, és elősegíti annak a NATO tervezési és művelési rendszerébe való integrálását. A miniszterek arról is döntöttek, hogy a nemzeti kiberműveleteket fel lehet ajánlani NATO missziókba és -műveletekbe. E felajánlások fölött a Szövetségesek tulajdonjogot gyakorolnak, csakúgy, mint ahogyan a tulajdonukat képezik a NATO missziókban használt harckocsik, hajók és repülőgépek.

2017. december 5-én a NATO és az EU miniszterei megállapodtak, hogy számos területen erősítik az együttműködést a két szervezet között, beleértve a kiberbiztonságot és kibervédelmet. A további együttműködés egyik területe a kiberfenyegetések elemzése és a vészhelyzeti reagáló csoportok közötti együttműködés, a másik pedig a jó gyakorlatokról szóló információcsere a válságkezelés informatikai vetületéről.¹

¹https://www.nato.int/cps/en/natohq/topics_78170.htm

7.2. Kiberbiztonság az Európai Unióban

Áttekintés

Az utóbbi évtizedekben az információs technológia térhódítása, valamint a technikai eszközök és szoftverek exponenciális ütemű gyorsulása és kapacitásnövekedése révén egy olyan bonyolult és komplex fejlődési folyamat zajlik a globális kibertérben, melyet nemhogy a jog, de még a védelmi mechanizmusok fejlődése sem bír követni. Bár az Európai Unióban jelenleg is célként szerepel az egységes kibertér létrehozása² és az EU kibervédelmi stratégiával³ is rendelkezik, egyelőre a kibervédelem jelenleg nincsen közösségi szinten szabályozva az Európai Unióban, holott számos tendencia indokolja az utóbbi időben a magasabb szintű együttműködést.

Mindazonáltal az uniós döntéshozók észlelték a problémát és az utóbbi években a kiberbiztonság kérdésköre – bár nem a legmagasabb prioritású – EU-ügy lett. Az Európai Unió Hálózat- és Információbiztonsági Ügynökség⁴(továbbiakban: ENISA) 2016-os jelentése⁵ részletesen bemutatja a kiberfenyegetések különböző típusait, melyek nemcsak a magánszemélyeket, de a közszférát is fenyegetik. Az Európai Unió fő eszközei közé tartoznak a stratégiák, a jogalkotás, a hálózatok és szervezetek, valamint a pénzügyi támogatások.

Milyen társadalomtörténeti és aktuális szociális háttere van a kiberfenyegetések fejlődésének? Hogyan képes a kibervédelem e folyamatokkal szemben a lépést tartani? Milyen típusú kiberfenyegetésekkel kell az Európai Uniónak, a tagállamoknak, a köz- és magánszférának, valamint a személyes felhasználóknak szembenézni? Hol és milyen szinten létezik és működik a kibervédelem az EU-ban? Milyen fejlődési irányok, perspektívák alkalmasak a helyzet kezelésére?

7.3. A kiberfenyegetések

Társadalmi háttér

A kiberfenyegetések gyakorlatilag egyidősek az elektromosságon alapuló kommunikációs eszközök (morze, telefonok, rádió) megjelenésével. Az információtechnológia az 1990-es évektől robbanásszerű fejlődésnek indult, egyúttal a gazdaság, oktatás, kutatás és az innováció

²<https://ec.europa.eu/digital-single-market/en/cyber-security>

³http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

⁴<https://www.enisa.europa.eu/>

⁵https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport

legfőbb motorjává is vált. Mindezekkel párhuzamosan az IT-eszközök és szolgáltatások a civil szférában is széleskörűen elterjedtek.

Az európai IT-infrastruktúra többszintű és komplex, viszonylag magas szintű adatforgalommal, megszámlálhatatlan magánfelhasználóval. De a magánfelhasználók mellett az államok, intézmények, szervezetek és vállalatok is megjelennek, így az IT-infrastruktúra nagy szerepet tölt be a menedzsment, adminisztráció, adattárolás révén is. A kibertér sokrétű felhasználói köre miatt is válnak ezek az IT folyamatok egyre gyakrabban kiberbűncselekmények célpontjává.

Ami a magánfelhasználókat illeti, az európaiak 80,2 %-a használja napi szinten az internetet,⁶ ami jóval meghaladja a globális átlagot (51,7 %). A hozzáférhetőség és a felhasználói kör sokrétűsége mellett, a tagállamok különböző jogrendszerei és a szabályozási gyakorlat nagy eltérései is veszélyfaktort jelentenek, hiszen a kibertérben zajló folyamatok átnyúlnak az országhatárokon, ez pedig nemzetközi együttműködést igényel, ami Európa esetében sokkal nehezebb, mint például az Egyesült Államok számára.

Mindemellett a kibertevékenységek és a legkomolyabb fenyegetések globális jellegéből fakadóan, nem fenntartható és működőképes minden tagállam számára egy külön kibervédelmi stratégia és rendszer, úgy hogy az egyúttal képes legyen felvenni a versenyt a legkockázatosabb és legnagyobb horderejű kiberfenyegetésekkel szemben is. Bár az egyes kibervédelmi rendszerek információ kényes, nemzetbiztonsági jelentőségű adatok, ezek megosztása, közösségi szinten történő racionalizálás nélkül és a tudatosság megteremtése nélkül a hatékony és gyors reakcióra képes védelem nem működtethető.

A fenyegetések

Az ENISA jelentésében rangsorolja a kiberfenyegetések 15 leggyakoribb típusát. Ezek közül a leggyakoribb típusok *malware-támadások* (Malware attacks), *web alapú támadások* (Web based attacks) és a *web applikációs támadások* (web application attack), de elterjednek számítanak a *szolgáltatásmegtagadással járó támadások* (Denial service), az *adathalászat* (Phishing), a *levélszemét* (Spam) és a *zsarolóvírusok* (Ransomware) is. Nemcsak a fenyegetések különböző típusai, de az elkövetők terén tapasztalható differenciáltság is

⁶<http://www.internetworldstats.com/stats.htm>

complex védelmet tesz szükségessé. Az ENISA ábrája⁷ taxatív módon sorolja fel az elkövetők típusait: *kiberbűnözők* (cybercriminals), *“bennfentesek”* (insiders), *államok* (nation states), *vállalatok* (corporations), *hacktivisták* (hacktivists), az ún. *“cyberfighters”* (cyberfighters), *kiberterroristák* (cyberterrorists) és *hackerek* (script kiddies). Világosan megmutatkozik tehát, hogy vállalatok és államok nem csak az elszenvedők között vannak jelen, hanem eszközként használják is ezeket a folyamatokat. A jövőben valószínűleg a kibertámadások válnak majd az elsődleges háborús eszközökké.

Végül, de nem utolsó sorban a fenyegetések mennyisége is nehezítheti a védelmet. A kiberbűncselekmények növekedése globális trenddé vált. A valós idejű megfigyelő rendszerek Európa helyzetére is rávilágítanak a globális kibertérben. A Fortinet⁸ és a Norse Corp.⁹ is azt mutatják, hogy az Egyesült Államok területe a legnagyobb elszenvedő és kezdeményező is egyben. A második legaktívabb terület Kelet-Ázsia. Annak ellenére, hogy Európa nem tartozik a legaktívabb területek közé, inkább elszenvedőjének számít az egyre agresszívabb támadásoknak.

7.4. A jelenlegi helyzet

Bár a kibervédelem jelenleg nem közösségi szakpolitika az Európai Unióban, az európai kiberterek biztonságát különböző mélységben több szakpolitika érinti, mint a közös kül- és biztonságpolitika, vagy a bel- és igazságügyi együttműködés. Az Unió most már több mint 10 éve fogott hozzá az önálló kibervédelem megteremtéséhez, az első intézkedések 2001.09.11-i terrortámadásokra is adott reakciók voltak. Az Európai Unió alapvetően négy féle módon képes hozzájárulni a kibervédelem fejlesztéséhez:

- a) stratégiák kidolgozásával,
- b) a jogalkotás révén,
- c) hálózatok és szervezetek működtetésével,
- d) és finanszírozással.

⁷ Threat Landscape Report 2016 (ENISA). 73. p. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport

⁸ <https://threatmap.fortiguard.com/>

⁹ <http://map.norsecorp.com/>

E folyamat sorána döntéshozóknak kényesen kell egyensúlyozni a szabad és nyílt internet megtartása, a túlszabályozás és a biztonság kérdéseinek háromszögben.

7.5. Stratégiák

Az Európai Unió stratégiái öt vagy több évre határoznak meg célokat és kereteket a programok és akciótervek végrehajtásához. Az első tízéves biztonsági stratégia 2003-ban, szó szerint még nem tartalmazta a kiberbiztonságot, azonban a 2016-ban megszületett második stratégia¹⁰ kiemelt kérdéskörként kezelte.

Az első stratégia, amely konkrétan és átfogóan a kibervédelemmel foglalkozott, 2013-ban megszületett meg Az Európai Unió Kiberbiztonsági Stratégiája: Egy Nyílt, Biztonságos és Megbízható Kibertér címmel.¹¹ Ennek fő pontjai és céljai a reziliencia erősítése, a kiberbűnözés leküzdése, a kibervédelmi politika létrehozása, ipari és technológiai szféra, valamint az erőforrásaik bevonása egy egységes Európai Kibertér létrehozásához.

A kiberbiztonság közvetetten az Európai Biztonsági Agendában (2015-2020)¹² is megjelenik, melyet a CEPOL¹³ dolgozott ki. Az Agenda célul tűzte ki a csalás, a hamisítás, illetve a gyermekek szexuális kihasználásának leküzdését, illetve a kiberkapacitás növelését.

A harmadik legfontosabb dokumentum a Digitális Belső Piac Stratégia,¹⁴ mely az Európai Kibertér egységesítésén keresztül kíván hozzájárulni a kutatási és innovációs kiválósághoz, illetve a magánszektor bevonásának támogatásához. A DBPS egy erős gazdasági aspektussal is bír, ami a megfelelő finanszírozásra való törekvésben nyilvánul meg.

7.6. Jogalkotás

Ami a jogalkotást illeti, az Európai Unió rendes eljárás keretében másodlagos jogforrásokat alkot a kiberbiztonságra vonatkozóan. Ezek közül a legfontosabb Az információs rendszerek elleni támadásokról szóló direktíva (NIS direktíva),¹⁵ mely három területre fókuszál. Az első *a tagállamok felkészültsége*, amit a nemzeti intézményrendszeren keresztül kíván ösztönözni,

¹⁰ https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

¹¹ https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

¹² https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

¹³ Az európai Unió Bűnüldözési Képzési Ügynöksége. <https://www.cepol.europa.eu/>

¹⁴ <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>

¹⁵ <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

a második a tagállamok közötti együttműködést célozza, a harmadik pedig a „Biztonság Kultúrájának” megteremtése, mely szabályokban, kontrollmechanizmusokban és az együttműködésben nyilvánul meg.

7.7. Hálózatok és szervezetek

Európában a kiberbiztonságot érintő szervezeti fejlesztések a 1990-es években indultak meg, melyek eredetileg nemzeti szinten jöttek létre. A következő lépést az Európai Közösségek, majd az Európai Unió tagállamai közötti együttműködés és ezek mentén létrejövő hálózatok jelentették. Az ENISA vezető szerepet tölt be a CERT-ek (Computer Emergency Response Team)¹⁶ támogatásában, melyeket minden egyes tagállamban létre kell hozni. Mindemellett az ügynökség adatgyűjtéssel és adatelemzéssel, valamint kockázatelemzéssel is foglalkozik.

Közvetetten az Europolnak (the European Police Office)¹⁷ is van szerepe az európai kibervédelemben, mégpedig a szervezeti keretei között működő EC³ (Europol's Cybercrime Centre)¹⁸ révén, mely a nyomozó hatóság irányába képez egy összekötő kapcsot. A EC³ fő szerepe a koordináció, a szakértői munka, a tréningek szervezése, kapacitásbővítés, valamint a rendészeti és nem-rendészeti emberi erőforrások és módszerek közti kooperáció és szinergia megteremtése. A központok emellett technikai és digitális támogatást is nyújtanak.

7.8. Finanszírozás

Az Európai Unió hozzájárulásai 2007-től érték el a legmagasabb szintet és a kutatás-fejlesztésre, az innovációra, az infrastrukturális fejlesztésekre, valamint kiberbűnözés elleni projektekre koncentráltak. Kutatás-fejlesztésre az EU 334 millió eurót fizetett ki 2007 és 2013 között, amely a kiberbiztonságra koncentrált. A második periódusban 2014 és 2016 között az EU 160 millió eurót fektetett be. A jelenlegi szakaszban pedig összesen 450 millió euro került elkülönítésre a *Horizon 2020 Programra*, mely a digitális biztonságot, a bűnözés és a terrorizmus leküzdését célozza.

Az EU finanszírozás másik meghatározó lába az infrastrukturális fejlesztés célozza. Az Európai Strukturális és Befektetési Alap 400 millió eurót határozott meg allokációs keretként.

¹⁶ A Magyarországon működő CERT (Kormányzati Eseménykezelő Központ) weboldala. <http://www.cert-hungary.hu>

¹⁷ Az Európai Rendőrségi Hivatal weboldala. <https://www.europol.europa.eu>

¹⁸ <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

A keret a pénzügyi biztonság, az adatvédelem, az interoperabilitás, elektronikus azonosítás mellett, számos digitális fejlesztést célzó projektre lehívható. A *Digital Service Infrastructures*¹⁹ és a *Connecting Europe Facility*²⁰ programokat is érdemes megemlíteni, melyek a határon átnyúló együttműködést támogatják, egyúttal hozzájárulnak a Digitális Belső Piac kiépítéséhez. Végül, de nem utolsósorban az Europol programjai is 15 millió euros támogatásban részesültek, így a jelenlegi ciklusban a finanszírozások és keretek összértéke meghaladja az 1 milliárd eurót.

8. AZ EURÓPA TANÁCS ÉS A KIBERBIZTONSÁG

8.1. A Számítástechnikai bűnözésről szóló Egyezmény

Az Európa Tanács 2001. nov. 23-án fogadta el Budapesten a Számítástechnikai bűnözésről szóló Egyezményt, mely az ebben a tárgykörben született első nemzetközi szerződés. Jelenleg 55 ország tag, további 15 ország ratifikálta, vagy meghívták a csatlakozásra. Nigériát 2017. július 10-én hívták meg az Egyezményhez való csatlakozásra. Az Egyezmény három fő területre terjed ki: a számítógépes bűncselekmények anyagi jogi és eljárásjogi szabályainak harmonizációjára, valamint a nemzetközi együttműködésre. Az Egyezmény Első Része az értelmező rendelkezéseket tartalmazza. Az 1. Cikkben meghatározza az egyes anyagi jogi tényállásokban, illetőleg az eljárásjogi rendelkezések esetében használt kifejezések pontos tartalmát, többek között az „számítástechnikai rendszer”, illetve „számítástechnikai adat” fogalmát is.

Az Egyezmény Második Rész I. Fejezete büntető anyagi jogi rendelkezéseket tartalmaz és meghatározza a nemzeti szinten meghozandó jogalkotási intézkedéseket, illetve azokat a cselekményeket, amelyeket a szerződő államoknak bűncselekménnyé kell nyilvánítani. A 2. Cikk büntetőjogi szankció alkalmazását követeli meg a számítástechnikai rendszerbe történő jogosulatlan és szándékos belépéssel szemben. Az Egyezmény 3. Cikke büntetni rendeli a számítástechnikai rendszerben tárolt vagy annak útján továbbított számítástechnikai adatok jogosulatlan kifürkészését, míg az Egyezmény 4. Cikke az adatok jogosulatlan törlését, megváltoztatását szankcionálja. Az 5. Cikk a számítástechnikai rendszer működésének jogosulatlan akadályozását nyilvánítja bűncselekménnyé. A 6. Cikk önálló, sui generis

¹⁹ <https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facility-cef-digital-service-infrastructures>

²⁰ <https://ec.europa.eu/inea/en/connecting-europe-facility>

bűncselekményként rendeli büntetni a nemzeti jogokban a számítástechnikai eszközökkel történő visszaélést. Az Egyezmény 7. és 8. Cikke a számítógéppel kapcsolatos bűncselekményeket, így a számítógéppel kapcsolatos hamisítást és csalást tartalmazza. Az Egyezmény 9. Cikkében önálló tényállásként szabályozza a gyermek-pornográfiával kapcsolatos, számítástechnikai rendszer útján megvalósuló cselekményeket. A 10. Cikk a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmény tartalmát írja le. Az Egyezmény 11. Cikke büntetendővé nyilvánítja a felsorolt cselekmények kísérletét és a bűnrészességet is. A 12. Cikke a jogi személyek felelősségére vonatkozóan tartalmaz rendelkezéseket.

Az Egyezmény Második Rész II. Fejezete a számítástechnikai bűncselekmények alapján indult nyomozásra és büntetőeljárásra vonatkozó szabályokat tartalmazza. Az Egyezmény többek között a tárolt számítástechnikai adat gyors megőrzésével, a közlésre kötelezéssel, illetve a tárolt számítástechnikai adat átvizsgálásával és lefoglalásával is foglalkozik.

A III. Fejezet a joghatóságra vonatkozó rendelkezéseket tartalmaz, melyben az Egyezmény a Szerződő Felek számára előírja a joghatósági kérdések rendezését, illetve az erre vonatkozó jogalkotási aktusok megalkotását.

Az Egyezmény Harmadik Része a nemzetközi együttműködésre vonatkozóan tartalmaz rendelkezéseket, így a nemzetközi együttműködésre, a kiadatásra, a jogsegélyre.

Az Egyezmény Negyedik Része tartalmazza a Záró rendelkezéseket, mely foglalkozik többek között az Egyezményhez való csatlakozás kérdésével. Emellett szabályozza az Egyezményhez fűzött fenntartásokat, az Egyezmény módosítását, a Felek közötti egyeztetést, stb.

8.2. Cybercrime Convention Committee

A Bizottság az Egyezményben részes államok képviselőjét látja el. Az Egyezmény 46. Cikke értelmében az egyeztetések célja az Egyezmény hatékony alkalmazása és átültetése, az információk cseréje, illetve egyéb jövőbeni kiegészítések, módosítások megfontolása.

Cybercrime Programme Office

A Bukarestben található Iroda feladata a Szerződő államok közötti együttműködés segítése.

Az Iroda feladata többek között:

- jogalkotási folyamatok megerősítése a számítástechnikai bűnüldözés területén, figyelemmel az emberi jogokra és az adatvédelemre;
- bírák, ügyészek képzése;
- speciális részlegek létrehozása, az ügynökségek közötti együttműködés fejlesztése;
- gyermekek védelme az internetes szexuális erőszakkal szemben;
- a nemzetközi együttműködés eredményességének, hatékonyságának növelése.

8.3. Projektek

GLACY (2013-2016)

Az Európai Unióval közös program, melynek célja, hogy elősegítse a Budapesti Egyezmény átültetését.

Területek:

- döntéshozatal
- jogharmonizáció
- jogi továbbképzések
- nemzetközi együttműködés
- információcsere, stb.

GLACY+ (2016-2020)

Az Európai Unióval közös program, melynek célja, hogy kiterjessze a GLACY-projekt tapasztalatait Afrika, Ázsia és a Karib-térség bizonyos országaira és növelje a nemzetközi együttműködés hatékonyságát.

Cybercrime@Octopus (2014-2019)

Az Európa Tanács projektje, melynek célja a Budapesti Egyezmény átültetésének elősegítése, valamint az adatvédelem és egyéb jogi biztosítékok erősítése.

9. NEMZETKÖZI SZERVEZETEK ÉS A KATASZTRÓFAVÉDELEM

9.1. A NATO és a katasztrófavédelem

9.1.1. Az Euro-atlanti Katasztrófa Elhárítási Koordinációs Központ (EADRCC)

Az Euro-atlanti Katasztrófa Elhárítási Koordinációs Központ (Euro-Atlantic Disaster Response Coordination Centre: EADRCC) a NATO fő polgári védelmi szervezete az euro-atlanti térségben. Folyamatosan működik, és tagja mind a 29 tagállam, valamint az összes partner ország. Természeti és ember okozta katasztrófák következményeivel kapcsolatos információs központként szolgál mind a segélykérések, mind a segélyfelajánlások összehangolásában.

Az EADRCC az összes feladatát az ENSZ Humanitárius Ügyi Hivatalával (UN OCHA) együttműködésben látja el, amely elsődleges szerepet játszik a nemzetközi katasztrófa elhárító műveletekben. Az EADRCC feladata a regionális koordináció, az ENSZ tevékenységének támogatása és kiegészítése. Nemzetközi segítséget igénylő katasztrófa esetén az egyes NATO-tagállamok, illetve partner államok döntésén múlik, hogy segítséget nyújtanak-e az EADRCC-től kapott információk alapján.

Az EADRCC-t az Euro-atlanti Partnerségi Tanács (Euro-Atlantic Partnership Council: EAPC) hozta létre 1998-ban a NATO polgári védelmi tervezési fórumaként, valamint a nemzetközi katasztrófa elhárítás együttműködési szerveként. Kiegészítő komponense az Euro-atlanti Katasztrófa Elhárító Egység, amely ideiglenesen működtethető, többnemzetiségű, polgári és katonai alkotóelemekből álló alakulat. Súlyos természeti vagy ember okozta katasztrófák esetén telepíthető az EAPC tagállamaiba.

Az 1990-es évek végén főleg a koszovói háború menekültjeinek nyújtott segítség koordinálásával foglalkozott. Azóta több, természeti katasztrófákkal kapcsolatos segélykérésre válaszolva működött, de segítséget nyújtott vegyi, biológiai, radiológiai és nukleáris (CBRN) incidensek, köztük terrortámadások esetén is (lásd a részleteket az EADRCC honlapon).

9.1.2. Támogatás a nemzeti hatóságoknak lakossági katasztrófákban

Az EADRCC továbbítja a segélykéréseket a NATO-tagállamoknak és a partnerországoknak, amelyek közlik felajánlásaikat a Központtal és az érintett országgal. A Központ nyilvántartja a felajánlott segítségnyújtást (beleértve a más nemzetközi szervezetektől és –cselekvőktől érkező felajánlásokat); a katasztrófa sújtotta ország által elfogadott segítséget, a szállítási dátumokat, továbbá a még mindig szükséges segítségnyújtást, valamint a helyszínen kialakult helyzetet. Ezeket az információkat helyzetjelentések formájában eljuttatja a NATO- és a partnerországokhoz, és közzéteszi a honlapján (<http://www.nato.int/eadrcc>).

9.1.3. Több nemzetiségű szakértői csoport

Az EADRCC a brüsszeli NATO Központban található. Személyi állományát a NATO-tagállamok és a partnerországok szakértői és a NATO Nemzetközi Törzs tagjai alkotják. Összekötő szerepet tölt be a UN OCHA, a NATO katonai szervei (NMA) és más jelentős nemzetközi szervezetek között. Tényleges katasztrófahelyzetben az EADRCC-t kiegészíthetik további személyi állománnyal, amelyet a NATO-tagállamok vagy a partner országok delegálnak, vagy amelyet a NATO nemzetközi polgári és katonai törzséből irányítanak át. A Központ nemzeti polgári védelmi szakértőkkel is kapcsolatba léphet nagyobb katasztrófa esetén.

9.1.4. Polgári készenlét

A haderő és a katonai felszerelések hatékony szállítása a polgári erőforrásokra és infrastruktúrára épül; ilyen például a vasút, a kikötők, a repülőterek, a nemzeti energia elosztó hálózatok. Ezek mind a külső támadásnak, mind a belső sérülésnek kitettek. A polgári készenlét azt jelenti, hogy az alapvető kormányzati funkciók vészhelyzetben vagy katasztrófahelyzetben is működnek, mind békeidőben, mind válság idején. Ez azt is magában hordozza, hogy a NATO országok polgári szektora képes volna támogatást nyújtani egy NATO katonai műveletnek.

Az Észak-atlanti Szerződés 3. cikkelye alapján minden szövetséges köteles helyreállító képességet kifejleszteni, amely a polgári készenlét és a katonai képességek kombinációja. A Szövetségben elfogadott helyreállítási követelmények hét stratégiai jelentőségű szektort érintenek, amelyek a következők: a kormányzás és a kritikus kormányzati infrastruktúrák

folyamatos működése, az energiaellátás folyamatossága, a lakosság spontán mozgásának kezelése, az élelmiszer- és vízellátás, tömeges sérülések ellátása, a távközlési és kibernetikai hálózatok, és a szállítórendszerek.

A 2016. évi varsói NATO-csúcstalálkozón a tagállamok vezetői elkötelezték magukat a polgári készenlét és a helyreállító képesség erősítése mellett, amely a kollektív védelem alapvető feltétele. A NATO a kelet-ukrajnai konfliktus miatt elfogadott Készenléti Akciótervének (Readiness Action Plan: RAP) fontos kiegészítője a polgári készenlét. A hibrid hadviselés veszélyei elhomályosítják a háború és a békeidő közötti határvonalat, és hatástalanná, sőt elavulttá teszik a rendkívüli helyzetre vonatkozó jogi szabályozást. A mai biztonsági környezetben az ilyen veszélyekkel szembeni ellenállás szükségessé teszi a katonai és a polgári képességek hatékony együttműködését. A Szövetségesek válsághelyzetekre való reagáló képességének javítása érdekében a polgári készenlét elemeit beépítik a NATO hadgyakorlataiba, például a 2018. évi Trident Juncture hadgyakorlatba.²¹

Az EADRCC honlapján útmutató található a segélykéréshez, valamint a segítségnyújtás felajánlásához (Checklist and Non-Binding Guidelines for the Request, Reception and Provision of International Assistance in the Event of a CBRN Incident or Natural Disaster, valamint: EADRCC Assistance Requests Glossary). A szó- és kifejezés gyűjteményt az elmúlt évtizedek dokumentumai alapján állították össze, de nem kötelező érvényű.²²

9.2. Az Európai Unió katasztrófavédelmi és reagáló képességei

Az Európai Unió katasztrófavédelmi és reagáló képességei egészen az 1990-es évekig nyúlnak vissza, jelen kereteiket pedig a 2007-ben aláírt Lisszaboni Szerződés 196. cikke szabályozza. Ennek fő elemei a szolidaritás növelése, illetve a koordináció kiépítése, megerősítése és javítása a tagállamok között. Fontos, hogy bár a **szerződés** „a korábbi alacsony szintű szabályozottság helyett uniós alapjogi szintre emelte a polgári védelmet, ezzel együtt azonban a tagállamok nem adtak át hatásköröket az EU-nak, a polgári védelem továbbra is kizárólagos tagállami hatáskörben van.”²³ 2013 végén a Tanács és a Parlament elfogadta az uniós polgári védelmi Mechanizmusról szóló 1313/2013/EU határozatot. Az EU

²¹https://www.nato.int/cps/en/natohq/topics_117757.htm

²²<https://www.nato.int/eadrcc/docs/glossary.html>

²³Európai Unió rendszere. *BM*

OKF.http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_nemzetkozi_eu (2018.02.05.)

polgári védelmi mechanizmusa elsősorban az emberek, valamint a környezet és a tulajdon védelmére terjed ki, figyelembe véve mindennemű emberi okozta és természeti katasztrófát. Ahogy az OKF hangsúlyozza, „a terrorcselekmények, illetve a nukleáris vagy radiológiai balesetek által okozott katasztrófák esetében az uniós mechanizmus csak a polgári védelem körébe tartozó katasztrófa-felkészültségi és -reagálási intézkedésekre terjedhet ki.”²⁴

Az uniós polgári védelmi mechanizmus a következő elemekből építkezik:

1. Megelőzés és kockázatkezelés: ennek keretében a tagállamok háromévente benyújtják kockázatelemzéseiket, illetve a kockázatok elhárítására, minimalizálására vonatkozó terveiket a Bizottságnak;
2. Veszélyhelyzet-kezelési Koordinációs Központ (Emergency Response Coordination Centre – ERCC). Ez az a szerv, amely a gyakorlatban is megvalósítja a tagállamok, illetve szükség esetén a külső partnerek közti koordinációt. Elődjét, a Megfigyelési és Információs Központot (Monitoring and Information Centre – MIC) 2001-ben hozták létre az EU Polgári Védelmi Mechanizmusának (EU Civil Protection Mechanism) keretében. A szintén 2001-ben megalakított Mechanizmus célja az volt, hogy mélyítse a már meglévő koordináció, és intézményesített formát adjon neki. Mára az EU mind a 28 tagállama, illetve Montenegró, Izland, Norvégia, Macedónia, Szerbia és Törökország csatlakozott a programhoz. Ezen kívül a Koordinációs Központ számos nemzetközi szervezettel tart fenn kapcsolatot a megbízhatóbb és gyorsabb információáramlás érdekében. A Mechanizmus mind a természeti, mind az ember okozta katasztrófák kezelésére kiterjed mind Európában, mind azon kívül. 2017 novemberében – figyelembe véve a különféle veszélyhelyzetek növekvő számát – a Bizottság egy felülvizsgálat mellett döntött, amely napra készebbé teszi a Mechanizmust. Az ERCC a hét minden napján 24 órás felügyeletben látja el feladatát, amelynek köszönhetően percek alatt képes továbbítani a beérkezett kéréseket a tagállamok felé. 2001 óta a Mechanizmus több mint 300 veszélyhelyzetet kísért figyelemmel, és 200 esetben konkrét kéréseket is fogadott. Az EU által telepített szakemberek és segélyszállítmányok olyan válsághelyzetek kezelését segítették elő, mint 2010-ben a haiti földrengés; a 2011-ben a Japánt sújtó szökőár;

²⁴Európai Unió rendszere. *BM*

OKF.http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_nemzetkozi_eu (2018.02.05.)

2013-ban fülöp-szigeteki tájfun; 2014-ben a pusztító áradások a Balkánon, illetve a nyugat-afrikai államokban tomboló ebola-járvány, az ukrajnai háború vagy a 2015-ben az európai migrációs válság.²⁵ 2016-ban a karibi térséget sújtó hurrikánok következményeit enyhítette az EU,²⁶ 2017 őszén pedig az ERCC a tagállami felajánlásoknak köszönhetően a Dél-Európában tomboló erdő- és bozóttüzek megfékezését segítette elő.²⁷

3. Közös Veszélyhelyzeti Kommunikációs és Tájékoztatási Rendszer (Common Emergency Communication and Information System – CECIS). A CECIS egy zárt hálózat, amelyen keresztül a Koordinációs Központ és a tagállamok kapcsolati pontjai – hazánk esetében a BM OKF – kommunikálnak és információt cserélhetnek.
4. Európai Veszélyhelyzet-kezelési Képesség (European Emergency Response Capacity - EERC) vagy közismertebb nevén néven önkéntes eszköztár. 2016 elején ennek keretében hivatalosan is megalakult az ún. Európai Egészségügyi Hadtest, melynek felállítását a nyugat-afrikai ebola-járvány tapasztalatai indokolták. Az EERC létrehozását egy új uniós mechanizmus írja elő, ennek értelmében a tagállamok az EU rendelkezésére bocsátanak önkéntes, ideiglenes és előzetes reagálási képességeket – modulokat, egyéb reagálási képességeket és szakértőket –, amelyek alapján az EU összeállít bizonyos bevethető csoportokat, elősegítendő a tervezhetőséget. A Hadtest több tagállam, a Bizottság, valamint az Egészségügyi Világszervezet (WHO), kooperációjában, tagállami eszközök felajánlásával jött létre. Az Európai Egészségügyi Hadtest elsősorban orvosi csapatokat, egészségügyi és járványügyi felszerelést, labort, illetve különleges szállítási kapacitásokat tartalmaz.
5. Polgári Védelmi Modulok: ahogy az OKF oldala fogalmaz, ezek „egy vagy több tagállam erőforrásaiból állnak és képesek előre meghatározott reagálási feladatok ellátására, rövid idő alatt bevethetőek, meghatározott ideig önellátóak és autonóm

²⁵EU Civil Protection Mechanism. http://ec.europa.eu/echo/what/civil-protection/mechanism_en. (2018. február 5.)

²⁶European Civil Protection helps Haiti overcome hurricane Matthew. http://ec.europa.eu/echo/field-blogs/photos/european-civil-protection-helps-haiti-overcome-hurricane-matthew_en (2018.02.05.)

²⁷Forest fires: EU helps mobilise firefighting planes and satellite mapping for Italy. http://ec.europa.eu/echo/news/forest-fires-eu-helps-mobilise-firefighting-planes-and-satellite-mapping-italy_en (2018.02.05.)

módon működnek, továbbá más modulokkal együttműködtethetők, csakúgy, mint más uniós és nemzetközi szervezetek, különösen az ENSZ reagálási egységeivel.”²⁸

6. Segítség szállítása: mivel a katasztrófhelyzetekben alapvető fontosságú a gyors reagálás, kulcskérdés a segítség odajuttatása. A mechanizmus azt igyekszik elősegíteni, hogy összekapcsolja a szabad szállítási kapacitásokat a felajánlott segítséggel, így az időben a helyszínre érkezhessen.
7. Képzések és gyakorlatok: a mechanizmus keretében rendszeresen sor kerül többlepcsős, angol nyelvű képzések, tréningek tartására, amelyekre a tagállamok kvóta alapján jelentkezhetnek. Ezek mind gyakorlati, mind elméleti elemeket tartalmaznak.²⁹

²⁸Európai Unió rendszere. *BM*

OKF.http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_nemzetkozi_eu (2018.02.05.)

²⁹ Uo.

10. A NEMZETKÖZI JOG ÉS A KIBERBIZTONSÁG

A nemzetközi jog szempontjából a kiberbiztonság gyengén szabályozott területnek tekinthető. Nincs univerzális egyezmény, sem egységes szokásjog, amely rendezné a nemzetközi közösség véleményét a kérdésről. Ennek egyik oka, hogy a kibertámadások és az ezzel összefüggő kiberbiztonság kérdésköre viszonylag új jelenségnek számítanak, amelyekre a jelenleg hatályos dokumentumok elfogadásakor (1945 – ENSZ Alapokmány, 1949 Genfi Egyezmények és azok 1977-es Kiegészítő Jegyzőkönyvei) azok létrehozói még nem is gondolhattak. A szabályozás hiányának másik oka az államok eltérő érdekeiben keresendő, mivel egyrészt valamilyen szinten minden állam érdekelt az online információ-szerzésben, másrészt államok egy meghatározott csoportja befolyásának bővítésére, a nemzetközi közösségen belül számára kedvező változások előidézésére is felhasználja.

A közelmúltban csupán egyetlen jelentős multilaterális szerződés került elfogadásra, ez a 2001-ben az Európa Tanács égisze alatt elfogadott és 2004. július 1-én hatályba lépett **Convention on Cybercrime**, amelynek hazánk is részese, és amely a „2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről néven vált a magyar jogrend részévé. Az egyezményt jelenleg 56 állam ratifikálta. További fontos forrás a 2013-as **Tallinni Kézikönyv**, amely bár alapos szakértői munka, és a potenciálisan alkalmazható szabályokat taglalja egy kiberkonfliktus esetén, de jogforrási helyzetét tekintve kötelező erővel nem bír.

A kiberjogsértések csoportja három kategóriára osztható: kiberkémkedésre, kiberbűncselekményekre és kibertámadásokra. Nincs éles határvonal az egyes kategóriák között, azonban legfontosabb jellemzőik mentén valamelyest elkülöníthetők egymástól.

A **kiberkémkedés**, akárcsak a hagyományos értelemben vett kémkedés, a nemzetközi jog szürke zónájához tartozik és kevésbé szabályozott. Elkövetőit általában a saját állampolgárságuk szerinti állam védi, azonban a célpont illetve a célponttal szövetséges államok üldözik, méghozzá leggyakrabban titkosszolgálati eszközökkel.

A **kiberbűncselekmények** célja a polgári javak megszerzése, módszere pedig leggyakrabban a gazdaság létesítményei ellen (pl. bankrendszer) indított online művelet. A célpont nem

feltétlenül más államban található, olykor irányulhat saját állama, annak intézményei, polgárai ellen is. Megítélése ettől függetlenül a nemzeti büntetőkódex szerint történik. A nemzetközi jog szerepe az érintett államok között akár a közös felderítés, akár a kiadatás során lehet számottevő. Más megítélés alá esik, ha a bűncselekményeket állami támogatással, állami alkalmazásban álló hackerek követik el. Hasonló eseményre került sor, amikor 2013-ban az Egyesült Államok Kínát vádolta meg azzal, hogy állami háttérrel biztosít kiberbűncselekmények elkövetéséhez. Az ügyből diplomáciai botrány lett, és az Egyesült Államok ellenintézkedések foganatosítását is fontolóra vette.

A **kibertámadás** megítélése azonban már számos kérdést vet fel és több válfajjal rendelkezik, azonban minden kibertámadás esetén közös pont, hogy kizárólag más állam ellen irányul. Végrehajtását tekintve különbséget kell tenni fegyveres konfliktus során, illetve fegyveres konfliktus hiányában elkövetett kibertámadás között. Az előbbire példa a Dél-Osztétia ügyében Grúzia és Oroszország között 2008-ban kirobbant konfliktus, amelynek során az átfogó fegyveres támadás részeként vetettek be számítástechnikai eszközöket. Általánosságban elmondható, hogy amennyiben a támadás katonai célpontok ellen irányul, úgy jogszerűnek minősül. Ilyennek tekinthető például a katonai radar, rakétairányító és egyéb érzékeny elektronikai berendezések zavarása. A jogszerű fegyveres összecsapás során, amely katonai célpont ellen irányul, az abban részt vevő személyek a humanitárius jog szabályai szerint nem büntethetőek, mivel kombattánsnak számítanak: támadhatnak és támadhatók, kiberbűncselekmények elkövetése miatt nem vonhatók felelősségre. A jogszerűség vélelme egészen addig fennáll, amíg a háború szabályait betartják, és nem támadnak polgári célpontokat (így például egy kórház áramellátásának megbénítása már büntetendő cselekménynek minősül). Kérdéses megítélésű, ha polgári személyek hajtanak végre kibertámadást. Ha a kibertámadás fegyveres konfliktus során történik, akkor a hadijog szerint bűncselekményt követnek el. Ez utóbbi kérdéskör túlmutat a fegyveres konfliktusok során alkalmazott joganyagon, mivel a polgári személyek által megvalósított kibertámadás fegyveres konfliktus nélkül is megvalósítható. Az ehhez hasonló cselekmények célja a dezinformáció, álhírek terjesztése, a polgári lakosság véleményének befolyásolása, zavarkeltés a kommunikációs rendszerekben, adatokhoz való hozzáférés, de irányulhat tényleges károkozásra is. Habár nem jár hagyományos fegyverek bevetésével, a nemzetközi jogot számos ponton sértheti: így az állami szuverenitás- és a beavatkozás tilalmának megsértésével. Az ENSZ Alapokmány 51.§-a szerint pedig az **önvédelem joga** alkalmazhatóvá válik: „A jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült

Nemzetek valamelyik tagja ellen irányuló fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát [...]” Vitatható azonban, hogy kibertámadás esetén pusztán az elektronikai eszköz „bevetése” megüti-e az önvédelem alkalmazásának mércéjét. Az elmúlt hetven év szokásjogi jogfejlődése következtében megállapítható, hogy az önvédelem joga csak megkötésekkel hívható fel. A klasszikus nemzetközi jog megköveteli, hogy a támadás állami szereplők részéről érkezzen és tényleges fegyveres támadás történjen. Ezen utóbbi feltételt igyekszik fellazítani az az állam, amely kibertámadás esetén önvédelmi jogára hivatkozik.

Érdemes megvizsgálni a nemzetközi jogi **felelősség** kérdését is, hiszen attól, hogy az ENSZ Alapokmány állami önvédelemről szóló passzusa nem feltétlen alkalmazható, még nem zárja ki, hogy az állam felelős legyen magatartásáért. A nemzetközi jog objektív felelősségi rendszerében ehhez elég a kötelezettségszegés ténye – így például az ENSZ Alapokmány egyes szakaszainak megsértése – és a betudhatóság, amely összeköti a kötelezettségszegő magatartást az állammal. Épp ez utóbbiban áll a bizonyítás nehézsége, hiszen a kibertámadást végrehajtó állam alkalmazásában álló egyének rendkívül ügyesen képesek eltüntetni maguk után a bizonyítékokat. Ha azonban mégis bizonyítást nyer cselekményük betudhatósága az államnak, úgy a kibertámadást elszenvedő állam élhet jóvátétel iránti igényével, vagy választhatja ellenintézkedés megtételét, amellyel igyekszik rákényszeríteni a kibertámadást végrehajtó államot, hogy az okozott sérelmet bírói vagy diplomáciai vitarendezési módszer igénybe vételével orvosolja.

11. MINTAANYAGOK AZ ELKÉSZÍTENDŐ JELENTÉSEKHEZ, HÁTTÉRANYAGOKHOZ

Tárgyalási álláspont minta

A magyar külügyminisztérium álláspontja az az ukrán oktatási törvény módosításáról:

- Ukrajna oktatási törvényének módosításával súlyosan sérti a magyar kisebbség jogait.
- A magyar diplomácia egyik legfontosabb kérdésként tartja napirenden az elfogadott ukrán oktatási törvénymódosítást
- A magyar álláspont szerint az oktatási törvény módosítása súlyosan sérti a magyar kisebbség jogait, érthetetlen hogy egy, az EU-val egyre szorosabb kapcsolatokra törekvő ország ilyen, az európai értékekkel homlokegyenest ellentétes törvényt hozott.
- Elfogadhatatlan, hogy Ukrajnában elvették a jogot a magyaroktól, hogy anyanyelvükön tanulhassanak a középiskolákban és az egyetemeken, csupán az óvodákban és az általános iskolákban hagyták meg ennek lehetőségét.
- Ezen kívül a törvénymódosítás a Kárpátalján működő magyar iskolák jelentős részének működését fenyegeti.
- Az ukrán döntés nemcsak a 150 ezres lélekszámú magyar kisebbség érdekével, az európai értékekkel ellentétes, hanem semmibe veszi Ukrajna nemzetközi kötelezettségvállalásait is.
- Ennek érdekében a magyar kormány minden létező európai fórumon fellép, hogy ez a jogszabály ne léphessen majd életbe.
- A döntés Magyarország irányában különösen barátságtalan, mivel az utóbbi hónapokban többször világossá tette Budapest az ukrán vezetők számára, hogy a módosítás a magyar érdekekkel súlyosan ellentétes, mégis meghozta Kijev.
- Magyarország az elmúlt időszakban számos olyan segítséget nyújtott Ukrajnának, amely elementáris fontosságú volt akár az európai integrációs folyamat, akár Ukrajna szociális vagy biztonsági helyzete szempontjából.
- Magyarország komoly erővel támogatta az ukránok vízummentességét, az első között ratifikálta a társulási megállapodást Ukrajna és az EU között, gázt szállított Ukrajnának Magyarországon keresztül, 600 millió forint értékben nyújtott humanitárius támogatást, 2600 ukrán gyermek üdülését tette lehetővé az utóbbi három évben. (MTI)

Háttér - minta

Az utóbbi években a kibertámadások száma világszerte drámaian megnövekedett. Az egyik legismertebb és legnagyobb károkat okozó támadás a „Petya” néven ismertté vált vírus. 2017 júniusának második felében lényegében egy „világméretű támadás” indult a kibertérben – a BBC szavaival élve – melyben elődeleges Ukrajna kormánya, vállalatai, bankjai voltak érintve, de több támadást észleltek Nagy Britanniában és Dániában is, valamint világszerte érkeztek jelzések cégektől arról, hogy gond van a rendszereikkel.

A brit WPP kreatív ügynökség, az orosz Antonov repülőgépgyár és a Rosneft olajvállalat, valamint a dán Maersk szállítmányozási cég is nehézségekről számolt be. A rotterdami kikötő teher szállító termináljai is az érintettek között voltak. Akárcsak a Mondelez élelmiszeróriás, a DLA Piper globális jogi tanácsadó vagy a francia építőipari vállalat, a St Gobain, valamint a világszerte rengeteg élelmiszeripari márkával jelenlévő Mondelez International egyes telephelyein is technikai gondok keletkeztek.

A támadások földrajzi kiterjedtségére minden biztonsági szereplő kicsit más adatot közölt, ez részben az eltérő felhasználói bázis, részben az eltérő időpillanatban rögzített adatok miatt is lehet. A McAfee által közölt térképen például az Egyesült Államok a legfertőzöttebb, ezzel szemben az ESET és a Kaspersky arról számol be, hogy a detektálások mintegy 75-80 százaléka Ukrajnából érkezett.

Az egyes érintett szereplők között megtalálható a csernobili erőmű állapotát monitorozó rendszer (amely helyett manuális mérésre álltak át), az orosz Rosznyeft kitermelést és finomítást irányító rendszere (már a tartalék rendszerre kapcsolt a cég), az egyik legnagyobb szállítványozó Maersk (amelynek teljes belső IT-ja leállt), a londoni kommunikációs vállalat WPP (amely minden felhasználót a gépek azonnali kikapcsolására szólított fel). A sor hosszan folytatható, az amerikai gyógyszergyártó Merck, a TNT futárszolgálat és az Oreo-gyártó Mondelez is súlyos támadásról számolt be. A legnagyobb károkat azonban az ukrán rendszerek szenvedték el, ott a kijevi reptér, rengeteg kormányzati infrastruktúra, a már említett csernobili rendszer, a helyi áramszolgáltató, sőt, a metró fizetési rendszere is részben vagy egészben leállt.

Elemzések szerint az új kriptovírus több aggasztó újdonságot is hozott, a támadási vektor és az agresszív worm-viselkedés is gondokat okozott a felkészületlen rendszerekben. Vagyis újra

globális káoszt okozott egy kriptovírus - amely ráadásul sokkal aktívabban is terjed, mint a korábban váratlanul megállított WannaCry. A Petya néven emlegetett kártevő eredetileg ukrán célpontok ellen indult, agresszív, számítógépes férgekre jellemző technikákkal azonban rendkívül gyorsan képes terjedni.

A támadás frissebb statisztikájából egyértelműen látszik, hogy Ukrajna, a terjedés kiindulási országa szenvedte el a legtöbb fertőzést ebben a zsarolóvírusos hullámban, mögötte Németország és Lengyelország helyezkedik el. Az ESET kiberbiztonsági cég szerint Magyarország ezekhez az országokhoz képest ugyan jóval kisebb mértékben, de szintén megfertőződött. A támadások mindössze 0,15%-a jelentkezett hazánkban – közölte az ESET. A vállalat szakértői szerint az egészen pontosan PetrWrap néven azonosított, Petya néven ismerté vált zsarolóvírus támadása egészen hasonlít a májusi WannaCry-hullámra, amely akkor több mint 150 ország számítógépes hálózatát fertőzte meg. A mostani támadás azonban sokkal erősebb és agresszívabb az elődjénél.

Az ESET szakértői feltárták a globális vírustámadás forrását. A támadók az M.E.Doc számviteli program frissítéseibe rejtették a fertőző kódot, így a szoftverfrissítésekben álcázva jutottak be számos ukrain vállalkozás hálózatába, köztük több pénzintézetébe is. A globális terjedést több trójai fertőzött M.E.Doc segítségével érték el a támadók.

Szakértők szerint a Petya támadás hasonló volt a 2017 májusában, szintén a fél világon végigsöpört zsarolóvírus, a **WannaCry** támadásához. Ez, a 2017 májusában felbukkant számítógépes vírus, amelynek lényege, hogy a megfertőződött számítógépeken tárolt fájlokat zárolta a vírus és pénzösszeg megfizetéséért cserébe lehet azokat visszakapni. A vírus komoly fennakadásokat okozott többek között Nagy-Britanniában, ahol kórházak számítógépes rendszereit tette elérhetetlenné rövid időn belül, ezáltal megbénítva az adott intézmények működését. E nagyszabású internetes támadás több, mint 230 000 számítógépet fertőzött meg világszerte, összesen 99 országban és 28 nyelven hozott létre zsarolóoldalakat, amelyeken pénz fizetését követeli a fertőzött gépek felhasználóitól. Az Europol nyilatkozata alapján ezen internetes támadás eddig példa nélküli méretű.

Spanyolországban a Telefónica nevű telekommunikációs vállalatot, valamint több nagyobb méretű spanyol vállalatot bénított meg a vírus. Nagy-Britanniában a National Health Service számítógépes rendszerét, Németországban pedig a Deutsche Bahn vasúttársaság, ezen kívül a

FedEx rendszerét érte támadás, többek között. A vírus gyors ütemű terjedését támasztja alá, hogy néhány óra leforgása alatt közel 100 országból jelentettek fertőzéseket. Magyarországon a Telenor távközlési szolgáltató vált érintetté. A WannaCry egyes feltételezések szerint egy észak-koreai tervezésű zsarolóvírus volt, mely 300 ezer számítógépet zárolt 150 országban, a Windows egyik hibáját kihasználva. Bár a hackerek ez alapján nagy bevételre számíthattak volna, végül csak a megzsarolt felhasználók alig egy ezreléke fizethetett, 17 millió forintnyi bitcoin értékben. A WannaCry pusztítását végül egy 22 éves programozó fékezte meg, bár nem minden gépet sikerült helyreállítani a roham után.³⁰

Sajtóanyag - minta

2018. március 19. 12:02

Dr. Mikola István biztonságpolitikai és nemzetközi együttműködésért felelős államtitkár részt vett és felszólalt a 2018. március 14-17. között Bakuban megrendezett VI. Globális Baku Fórum nyugat-balkáni államok jövőjét vizsgáló panelbeszélgetésén.

Az államtitkár hozzászólásában rámutatott, hogy Magyarország elkötelezett a nyugat-balkáni országok euroatlanti integrációjának elősegítésében, valamint az EU és NATO csatlakozásunkkal kapcsolatos tapasztalataink továbbadásában. Nyomatékosította ugyanakkor, hogy Magyarország az Európai Uniónál ambiciózusabb bővítési tervet tart kivitelezhetőnek, így az Európai Bizottság Szerbiát és Montenegrót érintő 2025-ös csatlakozási perspektívája helyett egy közelebbi terminust lát megvalósíthatónak.

Dr. Mikola István kifejtette, hogy Albánia és Macedónia esetében szorgalmazzuk az EU csatlakozási tárgyalások megkezdését 2018 júniusában, valamint megemlítette, hogy Koszovó előtt is nyitva kell hagyni a tagság lehetőségét.

Az államtitkár az EU bővítésén túl hangsúlyozta a NATO integrációs törekvések fontosságát is. Montenegró csatlakozása után sem lassulhat le a nyugat-balkáni bővítési folyamat, hiszen a NATO tagság lehet a régió stabilitásának egyik alappillére, különös tekintettel a régiót érő komplex biztonsági kihívásokra. Felhívta a figyelmet arra, hogy a bővítési folyamat következő lépése egy NATO Tagsági Akcióterv megadása lehet Bosznia és Hercegovina számára.

³⁰https://index.hu/tech/2017/06/27/pusztito_kibertamadas_erte_ukrajnat/https://mno.hu/belfold/vilaghodito-utjara-indult-petya-a-zsarolovirus-2405259http://hvg.hu/tudomany/20170627_kibertamadas_ukrajnaban

Az euroatlanti integráción túl az Államtitkár röviden rámutatott a magyar V4-es elnökség Nyugat-Balkánt érintő prioritásaira, és emlékeztetett arra, hogy a V4+Nyugat-Balkán formáció utolsó budapesti ülésén a V4 országok erős támogatásukról biztosították a balkáni országokat.

A bakui konferencia margóján dr. Mikola István tárgyalást folytatott Mahmud Mammadgulyev azeri külügyminiszter-helyettessel, valamint megnyitotta a Bakui Magyar Nagykövetség és a Bakui Metró közös szervezésében megvalósult Petőfi kiállítást, amely keretében a bakui utazóközönség 12 azeri nyelvre lefordított Petőfi verssel ismerkedhet meg a Memar Ajami 2 metróállomáson, valamint az azeri metró szerelvényeiben.(KKM)

Készült: egy eredeti példányban
Egy példány 66 oldal
Sokszorosítva: 3 példányban
Kidolgozást vezette: Dr. Kovács Gábor r. ddtbk.
Készítette: Kaszap Márton, Tongori Zsófia
Szerkesztette: Dr. habil. Varga János ny. hőr. ezds.
Lektor: Prof. Dr. Padányi József mk. vezérőrnagy

NEMZETI KÖZSZOLGÁLATI EGYETEM



SZÉCHENYI 2020



MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE