

KÖFOP-2.1.2-VEKOP-15.

„A jó kormányzást megalapozó közszolgálat- fejlesztés”



„INTEGRÁLT VÉDELEM 2018”

**A Nemzeti Közzolgálati Egyetem
Közös Közzolgálati Gyakorlat**

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

Kaszap Márton
Tongori Zsófia

Nemzeti Közzolgálati 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 Közszerológiai Egyetem integrált gyakorló szervezeteiben (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 kiberfenyegetések	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

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 ábrája⁷taxatívmódon 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 Fortinet⁸és 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>