dr. Gyaraki Réka r. őrnagy: Jogi szabályozás a nemzeti elektronikus adatvagyon, az ezt kezelő információs rendszerek, létfontosságú információs rendszerek és rendszerelemek biztonságáról

A XXI. század globális kihívásai közé tartoznak a kibertérből érkező támadások, amelyek irányulhatnak a nemzeti adatvagyonunk vagy a kritikus információs infrastruktúrák ellen. „ A technológiai fejlődés és az információs igények globalizálódása, az egyre nagyobb intenzitású és egyre veszélyesebb- többek között a kritikus infrastruktúrákat is érintő- fenyegetések megkövetelik a honvédelmi feladatokhoz kapcsolódó kibervédelmi helyzet áttekintését és a szükséges feladatok meghatározását és végrehajtását."[1]

A tanulmányban a honvédelmi feladatokat tekintem át, így a Nemzeti Kibervédelmi Intézet, a Katonai Nemzetbiztonsági Szolgálat valamint a Magyar Honvédség kibertámadásokkal kapcsolatos tevékenységét és a magyarországi jogi szabályozását. A honvédelem feladata a külső támadásokkal szembeni védelem, amely ma már nem kizárólag fegyverrel, hanem a kiberfenyegetéseknek- kiberterrorizmus és kiber hadviselésnek köszönhetően- fegyver nélkül is meg kell, hogy valósuljon.

Kulcsszavak: honvédség, nemzetbiztonság, nemzeti adatvagyon, kritikus információs infrastruktúra, kiberbiztonsági stratégia

In the 21st century attacks from the cyberspace has become a global issue. These attacks can trend towards our national data assets or critical information infrastructures. The technological development and the globalization of information demands, the more and more intense and more dangerous threats – which can affect the critical infrastructures – demand the overview of the situation of cyber protection inside of national defense, the determination and execution of the necessary tasks in this regard.

In this study I will review the tasks of national defense, the work of the National Cyber Security Center, the Military National Security Service and the Hungarian Defense Forces regarding cyber attacks and the Hungarian legal regulations. The task of national defense is to protect from outsider attacks, which nowadays can be performed not only with guns, but thanks to cyber threats – cyber terrorism and cyber warfare – the defense forces have to be able to protect without guns, too.

Key words: Defense forces, national security, national data asset, critical information infrastructure, strategy of cyber security

[1] 60/2013.(IX.30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának Kiadásáról

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Nemzeti vagyonunk részét képező nemzeti elektronikus adatvagyon, az ezt kezelő információs rendszerek, a létfontosságú információs rendszerek és rendszerelemek. biztonsága feltétlen nemzeti érdek az információs társadalmat érő fenyegetések miatt. A hazai jogi szabályozás a kibertér védelmével kapcsolatos társadalmi elvárásoknak tesz eleget, amikor az állam és az állampolgár számára biztosítja az elektronikus információs rendszerben kezelt adatok és információk hármas követelményét (bizalmasság, sérthetetlenség és rendelkezésre állás), valamint rendszerelemei sérthetetlenségének és rendelkezésre állásának zárt, teljes körű, folyamatos és kockázatokkal arányos védelmet.

Az elektronikus információbiztonság 2013. július 1-jén hatályba lépett törvényi szabályozása[2], majd módosításai és a törvényi felhatalmazás alapján kiadott több kormányrendelet igazolják, hogy a kibertérből jelentkező fenyegetések tartalmukban és veszélyességük tekintetében változnak, így a védelemben és a biztonság megteremtésében is újabb stratégiák kidolgozása szükséges, a létező kockázatok kezelésére alkalmazott eszközökkel együtt.

A 2013. évi L. törvény meghatározza a magyar kibertér fogalmát, amelynek nyomán történik a két honvédelmi szervezet, a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat feladatait működését valamint a nemzeti adatvagyon védelmével kapcsolatos feladataikat.

Az Ibtv. valamint a kibertérből érkező fenyegetések miatt ugyanakkor ezen két szervezeten kívül még egy, a Nemzeti Kibervédelmi Intézet egyes tevékenységeit tartom szükségesnek megemlíteni, mint olyan szervezetet, amelyik kiemelkedő feladatot lát el a hazai szervezeteket, vállalatokat, a magánszférát érintő kibertámadások esetén.

A magyar kiberbiztonság szabályozása

A kiberbiztonság szabályozásának szükségessége a kibertérből érkező és megszaporodó fenyegetések és támadások miatt elengedhetetlenné vált. Ezen fenyegetések kezelése, a támadások elhárítása a honvédség feladata is.

„Első" jelentős jogi szabályozás Magyarország Nemzeti Kiberbiztonsági Stratégiája, amelyet a 1139/2013 (III.21) Korm.határozat rögzíti. A Stratégia az Alaptörvényünkkel összhangban Magyarország biztonságának kialakítása a kibertérben. Ahogy a fizikailag meghatározható határaink védelme esetében, úgy a magyar kibertér védelme is kiemelkedően fontos. A Stratégia tartalmazza többek között a nemzeti adatvagyonunk megfelelő védelmét és a létfontosságú rendszerelemek informatikai hálózatának megóvását a támadásokkal szemben.

Fenyegetés, kiberfenyegetés

A fenyegetés (minatio) fogalma: bizonyos hátrányok jogtalan okozásának kilátásba helyezése[3]. Az idegen szavak és kifejezések szótára szerint pedig: „súlyos hátrány kilátásba helyezése, amely alkalmas arra, hogy a megfenyegetettben komoly félelmet keltsen"[4].

[2] 2013.évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
[3] www.kislexikon.hu
[4] Bakos Ferenc: Idegen szavak és kifejezések szótára (Akadémia Kiadó Budapest2002,)

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

A kibertérből származó fenyegetések:

- Vírusok
- Kémszoftverek
- Spam vagy kéretlen levelek
- Keyloggerek
- Kéretlen reklám programok
- Botnetek
- Trójai vírusok
- Adathalászat
- Túlterheléses vagy elosztott túlterheléses támadás (DoS vagy DdoS támadás)
- Férgek
- Kevert fenyegetések

Ezek a felsorolt fenyegetések célja lehet többek között adatszerzés, pénzszerzés valamint a másik fél/felek számítógépes hálózatainak működésképtelenné tétele. Ezek akár külön-külön vagy egyben is alkalmasak arra, hogy a megtámadott országban félelmet keltsenek és az alkotmányos rend megváltoztatását megkíséreljék vele.

Ahogy Kovács László mk.ezredes rámutatott, a kiberhadviselés célpontjai lehetnek akár a szembenálló fél információs rendszerei (ilyenek a katonai-, közigazgatási- és nemzetbiztonsági rendszerek), akár a kritikus információs infrastruktúrák (energiaellátás, ipari irányítás, kommuikáció, közlekedés stb..)[5]

Szükséges még egy fogalom tisztázása, ez pedig a kibertér fogalma, mivel

A 60/2013. (IX. 30.) HM utasítás külön kitér az információs fenyegetésekre valamint utal a korábban bekövetkezett eseményekre, mint a 2007-es Észtországot érő orosz kibertámadás, amelyet követően a világ gondolkodása a háborús konfliktusok helyszínéről. Az utasítás már nyíltan kimondja, hogy az iráni urándúsítót ért vírustámadás kiberháborúként értelmezhető[6].

„A fenyegetett célok változnak, egyre szélesebb körû szolgáltatások veszélyeztethetõk. A támadó célja info- kommunikációs eszközök alkalmazásával a vezetési és irányítási rendszerek feletti irányítás megszerzése, a táma- dott fél erõinek lekötése, reagáló képességének felmérése, a nemzeti kritikus infrastruktúrák, a nemzeti adatvagyon veszélyeztetése vagy a katonai mûveletek, katonai erõ hatékony alkalmazásának blokkolása, befolyásolása. ..... A támadás forrása lehet hacker tevékenység, szervezett bűnözés, ideológiai vagy politikai szélsõség, kormányzati támogatással rendelkezõ agresszió[7]."

[5] Prof. Dr. Kovács László mk. Ezredes Ludovika Szabadegyetem előadása 2015. március 24.-én
[6] Stuxnet vírus: 2010-ben az iráni Bushehr erőműben urándúsítója elleni számítógép-vírussal fertőzött támadás, amelynek következtében az urándúsítóban üzemzavar illetve leállás következett be.
[7] 60/2013 (IX.30.) HM utasítás

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Nemzeti Kibervédelmi Intézet (NKI)

Az Ibtv. 2015. évi módosításának eredményeként 2015. október 1-jén megalakult a Nemzeti Kibervédelmi Intézet- a Nemzetbiztonsági Szakszolgálat keretei között-, amelyen belül három szakmai szervezeti terület került elkülönítésre a tevékenységüknek megfelelően:

- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterület (a Kormányzati Eseménykezelő Központ, azaz a GovCERT);
- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);
- a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási-, és sérülékenység vizsgálati (GovCERT) szakterület.[8]

A három terület mellett az NKI feladata még többek között a honvédelmi és a kritikus információs infrastruktúrák védelme is.

Az NKI - Kormányzati Eseménykezelő Központ incidenskezelési terület feladata:

- Biztonsági események kezelése
- Fenyegetésmenedzsment
- Ügyeleti szolgálat
- Elemzés/értékelés
- Kibervédelmi gyakorlat
- Képzés, tudatosítás
- Felelősök kijelölésének támogatása
- Sérülékenységvizsgálat
- Biztonságiesemény-kezelés kapcsán együttműködés a NISZ-szel, illetve a digitális szolgáltatókkal
- Rendszeres vezetői tájékoztatás
- Biztonságirányítás és sérülékenység vizsgálat,
- biztonsági események kivizsgálása,
- EMIR / FAIR rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása

A GovCERT alapvető feladata az állami és önkormányzati szervek informatikai biztonsági támogatása,
- amely egyrészt preventív jellegű, (értve ezalatt a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követését és a sérülékenység menedzsmentet),
- másrészt pedig reaktív jellegű, a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően - a kezelésük koordinációjára irányul.

a) A sérülékenység menedzsment során GovCERT információkat gyűjt a szoftver-sérülékenységekről és káros szoftverekről, megvizsgálják azok relevanciáját az állami IT

[8] forrás: NKI

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

rendszerek tekintetében és általános körben vagy célzottan tájékoztatják a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében ezen rendszereket üzemeltetőket.

b) Az incidenskezelési tevékenység során a GovCERT 24 órás ügyeletet működtet, ahol folyamatosan fogadja az IT rendszereket érő incidensek bejelentéseit, és megteszi az alapvető intézkedéseket (incidens nyilvántartásba vétele, bejelentő visszatájékoztatása, alapvető információk azonosítása, stb.). A bejelentett incidens felszámolása során a következő lépés a jogosultsággal és/vagy képességgel rendelkező szerv/személy tájékoztatása a teendőkről, szükség esetén kapcsolattartás a bejelentővel, valamint az érintett incidens felszámolásának nyomon követése (incidens-koordináció). Amennyiben szükséges, az incidensre utaló jelek alapján a GovCERT összegyűjti az incidens felderítéséhez szükséges információkat (pl. naplóadatok) és ezek elemzésével megkísérlik rekonstruálni az incidens kiváltó okait, egyúttal javaslatot tesznek a hasonló incidensek megelőzését vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekre.

Az NKI- Nemzeti Elektronikus Információbiztonsági Hatóság hatósági tevékenysége:

- Ügyfelek és rendszerek nyilvántartása
- Biztonsági osztályba és szintbe sorolás ellenőrzése
- Követelmények teljesülésének ellenőrzése (jogszabályi követelmények és eljárási szabályok teljesítése megtörtént-e)
- Sérülékenység vizsgálat elrendelése
- Javaslat létfontosságú rendszer kijelölésére
- Javaslat információbiztonsági felügyelő kirendelésére
- Engedélyezések/hozzájárulások
- Az Unió tagállamaiban történő elektronikus információs rendszer üzemeltetés tekintetében engedélyezési eljárás lefolytatása

A Nemzeti Elektronikus Információbiztonsági Hatóság az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. Amennyiben az ellenőrzött szervezet a hatósággal nem működik együtt, azaz az Ibtv. szerint a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a hatóság köteles felszólítani a – követelmények és az eljárási szabályok - teljesítésre,melynek elmaradása esetén bírság szabható ki, annak ismételhető volta mellett. Kivételt képeznek a költségvetési szervek, esetükben - a hatóság felszólítását követő teljesítési kötelezettség elmulasztása esetén– a hatóság kezdeményezheti információbiztonsági felügyelő kirendelését.
A hatóság ellenőrző funkciója erőteljes támogató funkcióval is bír, ugyanis jogosult a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában véleményezni és ellenőrizni az információbiztonsági követelmények megtartását. Az információtechnológiai fejlesztések elektronikus információbiztonsága szempontjából kiemelt fontosságú, hogy a vonatkozó előírások a rendszerek teljes életciklusa alatt következetesen és maradéktalanul megvalósításra kerüljenek és a fejlesztések eredményeként önmagukban is teljes, továbbá a meglévő rendszerekhez funkcionálisan és biztonsági aspektusból is harmonikusan és költséghatékonyan illeszkedő rendszerelemek, rendszerek épüljenek ki.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

Sérülékenységvizsgálat

A sérülékenységvizsgálat célja az esetleges biztonsági események bekövetkeztét megelőzően az elektronikus információs rendszer gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása. A sérülékenységvizsgálat végrehajtása során a vizsgálat alá vont elektronikus információs rendszerben felkutatásra kerül - többek között - a potenciális szoftverhibák~~at~~, gyenge jelszavak~~at~~, hibás beállítások~~at~~, amelyeket a támadó kihasználhat, és ezeken keresztül kárt okozni a rendszerben. Ez a tevékenység együtt jár azzal, hogy a vizsgálatot végzők pontos, mélyreható ismeretekkel rendelkeznek az adott elektronikus rendszerről. Egyes rendszerek esetén az ismeret ezen foka, a sérülékenységvizsgálat által feltárt információk jellege, nemzetbiztonsági szempontú megközelítést kíván. Az Ibtv. éppen emiatt rendelkezik arról, hogy a zárt célú elektronikus információs rendszerek, az állami és önkormányzati szervek létfontosságú rendszerelemeinek elektronikus információs rendszerei, valamint a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek vonatkozásában kizárólag a GovCERT végezheti a sérülékenységvizsgálatot, kivéve a honvédelmi célú elektornikus információs rendszereket, valamint a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit. A fenti körbe nem tartozó állami rendszerek esetében pedig lehetővé teszi magas szintű szakmai és biztonsági elvárásoknak megfelelő gazdálkodó szervek számára a sérülékenységvizsgálat lefolytatását.
A sérülékenységvizsgálat eredményeként előálló vizsgálati jelentésben a GovCERT minden esetben javaslatot tesz az azonosított sérülékenységek kijavítására is.

Biztonságirányítás

Míg az NKI egyes szakterületei kívülről támogatják az állami és önkormányzati szerveket abban, hogy saját rendszereik védelmét ellássák, és ennek keretében kialakítsák saját ún. információbiztonsági irányítási rendszerüket (röviden: biztonságirányítási rendszer), addig a biztonságirányítási szakterület ezt a feladatot tevőlegesen is végzi – részint az NKI biztonsági felügyeletére bízott, kiemelt kormányzati rendszerek esetében, részint pedig szakmai támogatást nyújtva a hatósági szakterület részére.

Kiberbiztonság fejlesztése a tudatosság növelésével:

A kibervédelem legolcsóbb és leghatékonyabb módja a biztonságtudatos használat. A hazai állami elektronikus biztonsági rendszerek vonatkozásában a teljes körű biztonsági szint eléréshez, a kielégítőnek tekinthető kiberbiztonság megteremtéséhez nem elegendő az optimálisnak tekinthető szervezetrendszer kialakítása, új technológia bevezetése és alkalmazása. Amennyiben az anyagi erőforrások nem biztosítják a már meglévő és biztonságilag hiányos rendszereknek az Ibtv.-ben meghatározott, a biztonsági szint emelését előíró folyamatokat, nem lehet a kibervédelem sikerességéről beszélni. illetve azt elvárni.

A védelemre ~~á~~lló pénzügyi források korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett alakítható ki a megfelelő szinten. Az NKI önmagában nem képes biztosítani a magyar kibertér védelmét, azonban szakmai tudásával hozzájárul ahhoz, hogy az egyes elektronikus információs rendszerek üzemeltetői megszerezzék és alkalmazzák a rendszereik védelméhez szükséges ismereteket. Ez a tevékenység a tudatosítás, mely számos formában megjelenhet, mint például szakmai anyagok

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

és útmutatók készítése, közvetlenül kifejtett oktatási vagy képzési tevékenység, a kiberbiztonság hangsúlyának növelése a médiában stb.
A tudatosító tevékenység számos réteget céloz, ezek közt elsősorban kell említeni a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését, és tőlük várható el a védelmi intézkedések működtetése), és a felhasználókat, akiket meg kell tanítani az internet és az információs technológiák biztonságos használatára, saját és a rájuk bízott adatok felelős és szakszerű kezelésére.

A nemzeti adatvagyon védelméről szóló 2010. évi CLVII. törvény alapján nemzeti adatvagyonnak minősül a „közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége."[9]
A Fehér Könyv tanulmányában a fogalmi megközelítés alapján külön veszi a közszférát és a magánszférát, amellyel bár szükséges lenne foglalkozni, de a törvény mégsem teszi ezt meg.
Az állami szférával kapcsolatban megkülönbözteti az állami szervek és vállalatok, valamint az önkormányzati szervek és vállalatok révén létrejövő adatokat, így a különböző nyilvántartásokat, jogi- és szervezeti normákat, gyűjteményeket...stb.[10]

2. A Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat feladatai a nemzeti adatvagyon és kritikus információs infrastruktúrák védelme esetében
Az információs társadalom egyes elemei közül a honvédelmi ágazatot érintő szabályozást tekintettem át. A honvédelmi célú elektronikus információs rendszerre vonatkozó szabályok legalább hét jogszabályban (törvény és kormányrendelet) fogalmazódtak meg és módosításra is kerültek. Az ágazati jogalkalmazók feladata tehát nem egyszerű, nem csak a keletkezett joganyag száma miatt, hanem a jogszabályok a hatáskör gyakorlójának jogosultsága vagy kötelezettsége tekintetében a rendelkezések összevetése és értelmezése miatt is.

A honvédelmi célú elektronikus információs rendszer fogalmát[11] kormányrendelet határozza meg (a rendelet alkalmazásában), az Ibtv.[12] felhatalmazása alapján. Megállapíthatóan ez az információs rendszer összetett, mivel a honvédelemért felelős miniszter vezetése, irányítása alatt álló szervek zárt célú elektronikus információs rendszereit, valamint egyéb – funkciója, rendeltetése, feladatellátása szerint – nyílt elektronikus információs rendszereit jelenti. A kétinformációs rendszer összessége támogatja ágazat-specifikus módon a honvédelmi ágazaton belüli és ágazatok közötti működést.

A honvédelmi ágazatban is, a zárt célú elektronikus információs rendszer, a rendeltetése szerint elkülönült információs rendszer, amely információs feladatok ellátását biztosítja, és kizárólagosan specifikus igények kielégítését szolgálja az e célra létrehozott szervezet útján és

[9] 2010. évi CLVII. törvény 1.§ 1.) pontja
[10] Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér Könyvhöz (Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete Budapest, 2016. július p.19.)
[11] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 1.§ 2.

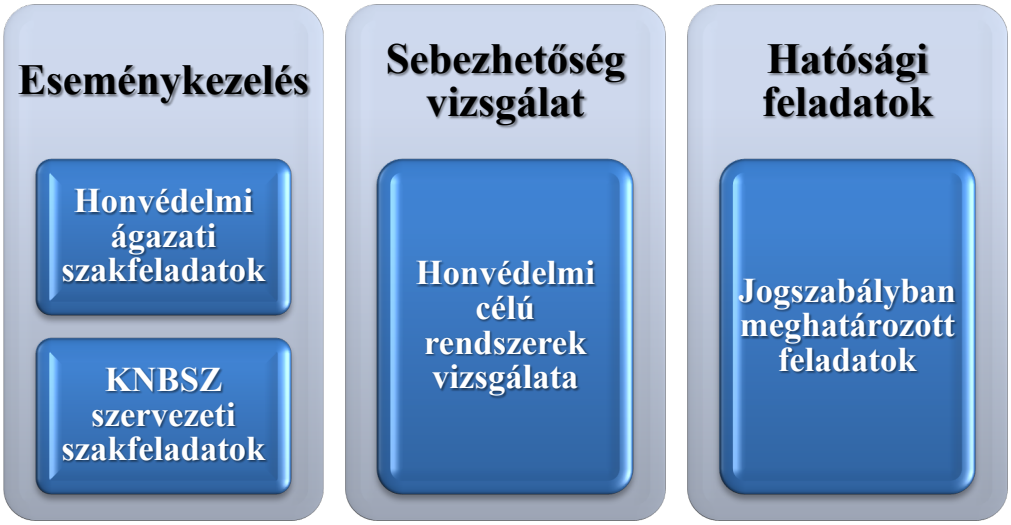
[12] 2013.évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1.§ 47.
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

működése által. Ez utóbbiak a honvédelmi miniszter vezetése, irányítása alá tartozó szervek és a tulajdonosi joggyakorlása alatt álló gazdasági társaságok használatában lévő zárt célú elektronikus információs rendszereket jelentik, amilyenek – többek között – a honvédelmi célú közigazgatási döntés-előkészítő és vezetés-irányítási rendszerek, a honvédelmi stacioner és tábori, nemzetközi műveleteket, valamint gyakorlatokat támogató műveleti vezetési rendszerek, a katonai nemzetbiztonsági területen titkos információgyűjtést, illetve titkos adatszerzést támogató rendszerek stb.

A zárt célú elektronikus információs rendszerek egyszerűsítetten a következőkben tagolandók (a titkos információgyűjtést ettől elkülönítve):

- a Magyar Honvédségnél üzemelő MH Kormányzati Célú Elkülönült Hálózat (katonai és közigazgatási szakfeladatok), amely a honvédelmi szervezetek központi szolgáltatásait látja el - mellette rengeteg helyi rendszer üzemel; valamint a KNBSZ[13] elkülönült hálózata;
- a védelmi igazgatási szakfeladatokat szolgáló rendszer;
- a HM tulajdonú gazdasági társaságok saját rendszerei.

Az említett szakfeladatokat integráltan a következő ábra szemlélteti (mint ágazati és a KNBSZ szervezeti feladatok ellátása). Az első pillér - eseménykezelés (ágazati és KNBSZ saját), a második pillér sérülékenység vizsgálat (honvédelmi célú elektronikus információs rendszereknél), a harmadik pillér – elektronikus információbiztonsági felügyeleti és hatósági feladatok ágazati szinten:



A honvédelmi elektronikus információs rendszerekkel összefüggésben szükséges kiemelni KNBSZ nemzetbiztonsági feladatai közül a kibertér biztonságára vonatkozókat, úgy mint az információk gyűjtését a honvédelmi érdeket veszélyeztető kiber-tevékenységről és szervezetekről, valamint a honvédelemért felelős miniszter által vezetett minisztérium, a

[13] Katonai Nemzetbiztonsági Szolgálat

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

Honvéd Vezérkar információvédelmi tervező munkájához szükséges adatok biztosítását[14]. Ezen feladatai ellátása során a KNBSZ elemzi és értékeli a működési területén felderített, a nemzetbiztonság katonai elemeit érintő információkat, azokról folyamatosan tájékoztatja a honvédelemért felelős minisztert, a minisztérium feladat- és hatáskörrel rendelkező vezetőit, a Magyar Honvédség feladat- és hatáskörrel rendelkező parancsnokait, vezetőit, a vezérkari főnököt, valamint a főparancsnokot[15].

A honvédelmi ágazatnál (EU terminológiával: szektornál) a kibertér védelmét – zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátását, továbbá a honvédelmi célú elektronikus információs rendszerek biztonságának felügyeletét – kizárólagosan a KNBSZ látja el (a KNBSZ főigazgatója a nevesített, mint Kormány által kijelölt hatóság[16]). Tehát az ágazatspecifikusságra tekintettel a kibervédelemben a szervezet a jogosult és kötelezett – a korábban már összetett jelzővel illetett elektronikus információs rendszerek vonatkozásában, így a kormányrendelet azonos jogszabályhelyeket jelölt meg a feladatellátásában.

A honvédelmi ágazati eseménykezelésben együttműködés van (következő ábra szemlélteti), az azonosított szereplők mellett az Alkotmányvédelmi Hivatal, a KKM és a nemzeti koordinációs feladatokat végző nemzeti kiberkoordinátor említendő még. Az eseménykezelési együttműködés egyben a honvédelmi ágazat nemzeti és nemzetközi szervezetekkel való kapcsolati rendszerét is megmutatja. A KNBSZ szakmai felkészültsége biztosíték adott kibervédelmi területű művelet (pl. egy kód elemzése) vagy stratégia szintű feladat megoldásához szükséges közös kormányzati szintű együttműködéshez (pl. munkacsoportban egy folyamat kidolgozása, jogszabály előkészítése).

A KNBSZ, mint kijelölt hatóság elektronikus információbiztonsági felügyeleti feladatait a felsorolás mutatja be:

- ellenőrzés, intézkedés, visszaellenőrzés;
- biztonsági esemény kivizsgálás elrendelés;
- tudatosság növelése;
- kockázatelemzés;
- kibervédelmi gyakorlatok;
- kapcsolattartás;
- nyilvántartás;
- sérülékenységvizsgálat elrendelése.

Kiegészítés a felsoroláshoz a teljesség igénye nélkül:
A kibervédelmi gyakorlatok kettős feladatot jelentenek: az eseménykezelő központ és funkciói végzik a gyakorlati feladatokat, az esetleges kapcsolattartási és egyéb feladatok (pl. együttműködési szerződés) a hatósági feladatok közé tartozik.

A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események (tehát az elektronikus biztonsági rendszerben változást vagy ismeretlen helyzetet előidéző, nem kívánt

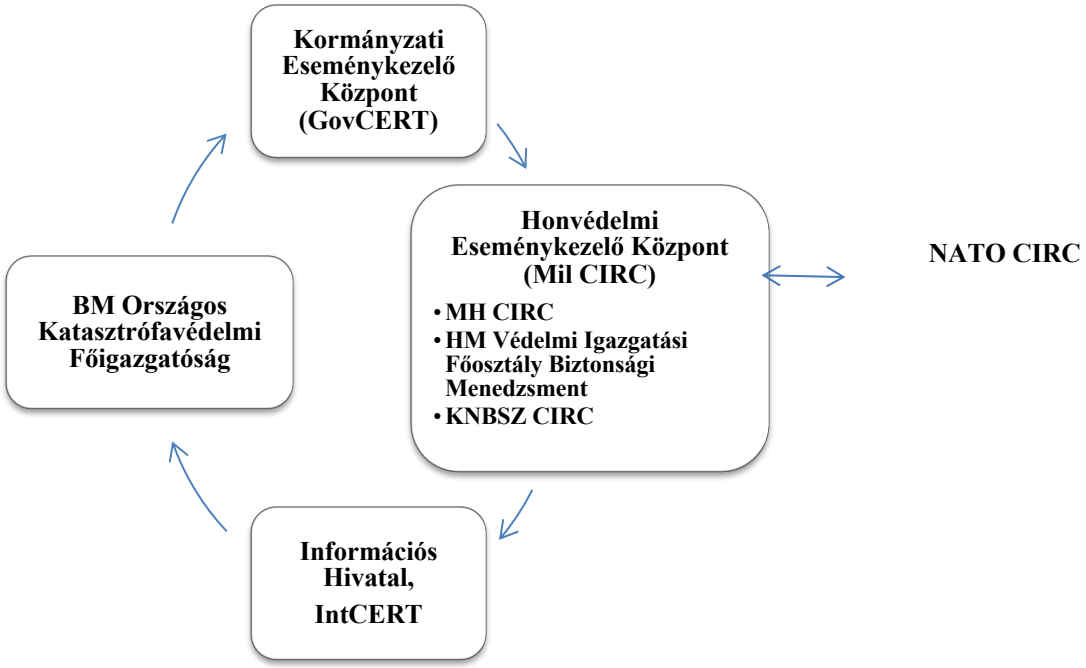
[14] 1995.évi CXXV. törvény a nemzetbiztonsági szolgálatokról 6.§ g)
[15] 1995.évi CXXV. törvény a nemzetbiztonsági szolgálatokról 7.§ (1)
[16] 187/2015 (VII.13.) Korm. rendelet 15. § (2) bekezdés

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

vagy nem várt egyedi esemény vagy eseménysorozat stb.), és fenyegetések kezelése a KNBSZ feladata[17], és a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő – a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – eseménykezelő központokkal együtt látja el. A hétköznapokban használt „kibertámadás" kifejezés (valamint a kiberháború, kiberhadviselés megfogalmazások) hazánkban nem eléggé kiforrott, a teljes elemzés, a bizonyítottság és egyéb kritériumok még nem biztosítják a szakterület teljes megértését, nincs egyetértett terminológia sem. A gyakorlatban inkább a „célzott támadási kísérlet" kifejezés célszerűnek és szakszerűnek.

A magyar eseménykezelés folyamatában a kommunikációs protokoll egyszerű: GovCERT központú, ami azt jelenti, hogy az eseményeket (nemzetközi szakkifejezéssel: incidenseket) a GovCERT felé kell bejelenteni, aki továbbítja a szükséges információkat az összes érintett szervezet felé, rögzíti az esetet, szükség esetén közvetlen együttműködést ajánl fel.

A honvédelmi ágazati **<u>eseménykezelési együttműködést</u>** a következő nagybani ábra szemlélteti:



A feladat egyszerűen bemutatva a fent említett funkciók integrált alkalmazásával reaktív és preventív részekre bontható:

– reaktív feladatok: az érzékelt vagy bejelentett (saját hálózatoknál megjelenő) incidensek alapján a szükséges védelem biztosítása érdekében az eseménykezelő rendszernek támogatnia kell az üzemeltető szervezetek tevékenységét (technikai tanácsadás, azonnali segítségnyújtás, külső kapcsolati rendszeren belül segítség keresése, kódok és események technikai analizálása - megoldáskeresés), illetve más szervezetnél bekövetkezett eseményekről történt értesítés kapcsán ugyanezt végezni (a „más kárán tanul az okos" elv

[17] 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

alapján). Milyen technikai feladatok elvégzése szükséges? Az erre adható válasz szerint eset függően történik a technikai eszköz kiválasztása. Így tűzfal vagy egyéb mechanizmus beállításának változtatása, ideiglenes vagy végleges konfiguráció változtatás, javítócsomag vagy kiegészítő program alkalmazása, hardver-szoftver elem szeparálása és technikai elemzése….

– preventív feladatok: sérülékenységvizsgálat, ahol a honvédelmi célú rendszerek biztonsági réseit kell felkutatni és ajánlatot tenni a hiányosság felszámolására; illetve felügyeleti feladatok, ahol a szabályozás, ellenőrzés (megfelelőség tanúsítás), hiányosságok felszámolása érdekében szükséges feladatszabás történik.

Amennyiben a fenti tevékenységek során jogszabályt sértő információ kerül elő (pl. incidenst okozó rosszindulatú szoftver elemzése során azonosított nevek, cselekmények, elérhetőségi vagy egyéb, azonosítást akár csak közvetetten is támogató adatok), a KNBSZ honvédelmi ágazati szakterületének feladata az illetékes szervezet értesítése, a kinyert adatok átadása.

A honvédelmi szektorra vonatkozó, a globális kibertérből érkező biztonsági események és fenyegetések közül kiemelést érdemel - az Alaptörvény 15. cikk (3) bekezdésében és a Htv.[18]81.§ (1) bekezdés b) pontjában kapott felhatalmazás alapján - a kormány rendelete[19], amely a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszerben meghatározott feladatokat, eljárási rendet, a közreműködők kötelezettségeit szabályozza. A kormányrendeletben összefoglaltan szabályozásra került a NATO válságkezelési rendszerrel összehangolt nemzeti válságkezelési rendszer, melyben az érintett szervezetek szakfeladatait és az együttműködési feladatokat azonosították (Nemzeti Intézkedés Gyűjtemény – NIGY), a terrorfokozatok elrendelése esetén a közigazgatási szervezetek részéről az adott helyzetnek megfelelő készenléti szintjük és kapacitásaik szabályozása (így a KNBSZ honvédelmi ágazati szakterületének feladatellátása a kibervédelemben), valamint a honvédelmi ágazatnál is a létfontosságú infrastruktúra védelem kibervédelmi szegmensei miatt.

A kibertámadások nemzeti szintű nyilvántartása nem ismert, így támadó országokról az megalapozott bizonyíték nélkül tényt állítani nem lehet, csupán vélelmekről vagy véleményekről van szó, melyeket a média felkap, terjeszt. A legjobb példa a Stuxnet, melyet média hivatkozások alapján éveken keresztül USA és Izrael számlájára írt, egyértelmű bizonyíték nélkül. Az amerikai elnökválasztás megelőző téma volt pl., hogy Obama elnök sajtóhírek szerint orosz forrású támadásokat sejt az amerikai elnökválasztási kampány befolyásolásaként, de csak közvetett bizonyítékok állnak rendelkezésre.
Általánosságban megállapítható, hogy hazánk is a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, és ezeken a rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese; azaz a globális kibertér tekintetében érintett, azonos vagy hasonló trendek érvényesülnek, mint az európai régióban. Tény azonban, hogy az internethasználattal, a felhasználók nagy száma miatt is nő az eseménykezelésekben is résztvevő, valamint az elektronikus információs rendszereket alkalmazó szervezetekkel szembeni fokozott elvárás (nagyobb kihívásnak kell eleget tenni a szervezeteknek).

[18] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

[19] 278/2011. (XII. 20.) Korm. rendelet a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

A KNBSZ részéről[20] megfogalmazott vélemény (vélelmezhetően további kibervédelmi szereplők egyetértésével), hogy az Ibtv. és végrehajtására megjelent kormányrendeletek által megfogalmazott elektronikus információbiztonsági követelményrendszer, egy új szakmai kultúra megalapozásának tekinthető. A kibervédelem jogi szabályozásának hatékonysága, működőképessége nemzeti szinten 8-10 év múlva lesz azonosítható, amennyiben a szükséges markerek („bizonyítékok") gyűjtése és elemzése megtörténik. Kiegészítő szempont, hogy az amerikai alapú szabályozás honosítása adja a szabályozás alapját, ami rámutat, hogy egy szabályozási elem átvétele mennyire hatékony a környezeti szabályozó elemek átvétele nélkül. A végrehajtáshoz szükséges erőforrások biztosítása az alkalmazó szervezetek erőforrásainak függvénye, így a nemzeti, egységes védelmi rendszer szintje e szerint megítélendő majd a jövőben.

Megfogalmazásra került néhány, kifejezetten a jogi szabályozásra vonatkozóan gyakorlati szempontú vizsgálati érdekesség is:

- hogyan kell jó szabályzatot írni (folyamatokat meghatározni) egy közigazgatási szervezetnél;
- a kockázatelemzés szempontjai úgy, hogy azok szervezetek között is értelmezhetők legyenek;
- a biztonsági osztályra vonatkozó egyedi megfogalmazási lehetőségek mennyire támogatják-befolyásolják a nemzeti infrastruktúrák kialakulását;
- a minősített elektronikus adatkezelés és az Ibtv. kapcsolata.

A Magyar Honvédség kibervédelemmel kapcsolatos feladatai

A honvédség feladata leginkább hazánk területének, függetlenségének, szuverenitásának, alkotmányos rendjének megőrzése a külső és/vagy belső támadásokkal szemben fegyverrel vagy fegyver nélkül.
A tanulmány elején említett fenyegetések ma már a kibertérből is érkezhetnek, éppen ezért a NATO 5.cikkelye a fegyveres támadásokra vonatkozóan 2016. június 15.-én kiegészült az alábbiakkal:
„ az interneten elkövetett támadások is katonai agressziónak számítanak" ami azt jelenti, hogy a NATO nemcsak akkor lép fel a tagállamai védelmének érdekében, ha azt fegyveres támadás éri, hanem akkor is, amikor kibertérből érkező fenyegetés történik.

A honvédelem nemzeti ügy[21]. A honvédség részére a honvédelmi miniszter a 60/2013 (IX.30.) HM Utasítás alapján[22] a következő általános célkitűzéseket határozza meg:
- katonai kritikus információs infrastruktúrák elleni támadás elhárítása;
- katonai kritikus információs infrastruktúrák sebezhetõségének csökkentése;
- katonai kritikus információs infrastruktúrák sérüléseinek helyreállításához szükséges idõk csökkentése;
- honvédelmi célú feladatvégrehajtás szempontjából a kritikus információs infrastruktúrák védelmének biztositása kapcsán az ágazati együttmûködési feladatok végzése, részvétel a nemzeti kritikus infrastruktúra védelmi programokban és feladatokban, a katonai kritikus

[20] Dr. Kassai Károly ezredes KNBSZ
[21] 2011. évi CXIII. törvény a Honvédelem alapjairól szóló törvény
[22] *a 60/2013. (IX. 30.) HM utasításhoz* A Magyar Honvédség Kibervédelmi szakmai koncepciója

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

információs infrastruktúra védelem továbbfejlesztése a honvédelmi kritikus információs infrastruktúra védelem irányába.

Magyarország (is) rendelkezik katonai stratégiával[23], amelyben a kiberteret új kihívásként és potenciális veszélyforrásként jellemzi és amelyben Magyarország számára is fenyegetést jelentenek a megnövekedett számú számítógépes támadások, emiatt szükségesnek érzik a háború fogalmának újraértelmezését. Továbbá globális kihívásként értékeli, hogy ennek köszönhetően a kibertérből érkező fenyegetésekre adott válaszreakció és döntéshozatali idő megrövidül a korábbiakhoz képest.
Álláspontom szerint az egyre jobban megszaporodó kibertámadások miatt a honvédség feladatai szélesedtek, hiszen nemcsak a határaink védelmében, a szövetséges fegyveres erők támogatásában szükséges a részvételük, hanem a digitális kihívás következtében és annak hatásaként

Kitérő: büntetőjogi szabályozás a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény

A 2012. évi C. törvény 267.§-a szabályozza a nemzeti adatvagyont sértő jogellenes cselekményt. A törvény büntetni rendeli a nemzeti adatvagyon körébe tartozó adat hozzáférhetetlenné tételét, amennyiben azt az adat kezelője számára teszi hozzáférhetetlenné. Ugyanakkor – mivel ez egy szubszidiárius tényállás- így annak elkövetése csak akkor valósul meg, ha az elkövetési magatartás nem valósít meg másik bűncselekményt. Azaz, amennyiben az elkövetése kifejezetten a kiberterrorizmus, vagy kiberhadviselés- jellegével történik meg, úgy abban az esetben az annál súlyosabban minősülő deliktum miatt indul eljárás.

Az Európai Unió Kiberbiztonsági Stratégiája

Az Európai Unió kiberbiztonságának megteremtését sürgető stratégiájába fogalmazta meg azt az 5 prioritást, amelynek egyes elemei honvédelmi feladatnak minősíthető:

- a kibertámadásokkal szembeni ellenálló képesség elérése
- a számítástechnikai bűnözés drasztikus csökkentése
- a kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése
- összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió alapértékeinek támogatására.

A felsoroltakból a tanulmány szempontjából a KBVP feladatok ellátását emelem ki egy rövid gondolat erejéig, mivel ebben fejezi ki az Unió szándékát arra vonatkozóan, hogy fejlesszék a tagállamok a kommunikációs és információs rendszerek védelmére irányuló képességét. Ezek a fejlesztések a civil és a katonai módszerek közötti együttműködésre kell, hogy irányuljanak, amire történő törekvés hazánkban is a jogi szabályozás tekintetében megindult, ugyanakkor a már többször említett Ibtv. és annak végrehajtási rendeletét továbbá a KI-re vonatkozó törvényt leszámítva, nem foglalkoznak érdemben a jogalkotók.

A nemzeti adatvagyon védelmével kapcsolatban az Unió Stratégiája külön nem tér ki.

De amennyiben a Fehér Könyv tanulmányában foglaltakat elemzem, akkor látható, hogy a nemzeti adatvagyont csak és kizárólag, szigorúan értelmezve állami- illetve önkormányzati

[23] 1656/2012 (XII.20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

szervezetek és vállalatok kezelhetnek, míg a magánszférához tartozó vállalatok, egyetemek, magánszemélyek által kezelt adatok- amíg nem kerülnek a közszférába- addig a törvény szerint nem nemzeti adatvagyon és nem minősül védelembe?! Miközben a magánszektorhoz tartozó vállalatok információs rendszerein keresztül ugyanúgy és sokszor ugyanazokat az adatokat kezelik.

Összegezve a honvédelmi elektronikus információs rendszerekkel, a feladatokkal és a kijelölt hatósággal kapcsolatos jogi szabályozásról leírtakat, a szakma részéről alkotott véleményt és megtett javaslatot, megállapítható, hogy a jogalkotóknak figyelemmel kell kísérni továbbra is az ágazat elektronikus információbiztonságára vonatkozó és a kiberteret érintő változásokat követő követelmények jogi kereteinek karbantartását.

Bibliográfiai hivatkozások jegyzéke:

1. 60/2013.(IX.30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának Kiadásáról
2. 1995.évi CXXV. törvény a nemzetbiztonsági szolgálatokról
3. 2013.évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
4. Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér Könyvhöz (Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete
5. 1656/2012 (XII.20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról
6. 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről
7. 278/2011. (XII. 20.) Korm. rendelet a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről
8. 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”