Magyar Rendészet

A NEMZETI KÖZSZOLGÁLATI EGYETEM RENDÉSZETTUDOMÁNYI SZAKMAI FOLYÓIRATA

XIII. évfolyam, 2013. Különszám

Kiadja a Nemzeti Közszolgálati Egyetem Rendészettudományi Kara
Budapest
ISSN 1586-2895 (nyomtatott)
ISSN 1787-050X (online)

TARTALOM

ELŐSZÓ

Az olvasó figyelmébe

Az informatikai fejlesztések felhasználásával a néhány évtizede még csupán regionális érdekeltségű terrorcselekményeket elkövető csoportok mára globális veszélyforrássá nőtték ki magukat. A terroristák egy része, amint az a tavalyi Terrorizmus és demokrácia a 21. században című konferencia egyik előadásán is elhangzott, a fegyvereit számítógépekre cserélte. A konferencia résztvevői ezen új típusú kihívásokra adandó jogi, felderítési, nyomozási továbbá felszámolási válaszokat járták körül.

A belügyi ágazat fontosnak tartotta, hogy a Kormány 1048/2012 (II.29.) határozata alapján 2012. október 4-5. között sorra kerülő kerülő Budapesti Kibertér Konferencián (BCC2012) való részvételt megelőzően a szaktárca a feladatkörébe tartozó témakörben nemzetközi szakmai-tudományos konferencián vitassa meg a legfontosabb kérdéseket.

2012. szeptember 17-18-n a Duna Palotában lezajlott plenáris ülésen 14, majd a szekciókban mintegy 40 előadó vázolta a kiber bűnözés ellen szükségesnek ítélt lépéseket, és azok várható következményeit szakmai diskurzus keretében. A konferencia nemzetközi jellegét tíz, a témában érintett nemzetközi szervezet vezető képviselőjének előadásán túl, a mintegy húsz európai és tengerentúli partnerszolgálat részvétele biztosította. A két napos rendezvényen összesen mintegy 500 fő vett részt: a belügyi és az igazságügyi terület neves szakemberei, a szakmailag érintett országos hatáskörű szervek munkatársai, a tudományos élet reprezentánsai, valamint kutatók, a kapcsolódó felsőoktatási intézmények, doktori iskolák oktatói és hallgatói.

A rendezvény általános vélemény szerint méltó folytatása volt a 2011. évben Terrorizmus és demokrácia a 21. században című, szintén a Belügyi Tudományos Tanács által szervezett konferenciának, melynek értékei, az elért szakmai-tudományos eredmények hozzáférhetők - többek között - a Magyar Rendészet különszámaként megjelent tanulmánykötetben. A 2012. évi konferencia szakmai tapasztalatai és következtetései a BCC2012 konferencia szakágazati inputjaként szolgálnak.

A Belügyi Tudományos Tanács korlátozott személyi és pénzügyi lehetőségeit számos szervezet támogatása egészítette ki. A program struktúrájának kialakításában elévülhetetlen érdemei voltak a szakmai támogatást nyújtó szervezetek (Alkotmányvédelmi Hivatal, Nemzeti Nyomozó Iroda, Nemzetbiztonsági Szakszolgálat, BM Országos Katasztrófavédelmi Főigazgatóság, Terrorelhárítási Központ, Bevándorlási és Állampolgársági Hivatal, Nemzeti Védelmi Szolgálat, Szervezett Bűnözés Elleni Koordinációs Központ) munkatársainak.

A rendezvény zavartalan és sikeres lebonyolításához nyújtott funkcionális támogatásért köszönet illeti a Belügyminisztérium Európai Együttműködési Főosztálya és Nemzetközi Főosztálya, a Készenléti Rendőrség, a Budapesti Rendőr-főkapitányság munkatársait, valamint a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Stúdiójának munkatársait és hallgatóit.

Dr. Sabjanics István
a Szervezőbizottság vezetője

KONFERENCIA ZÁRÓDOKUMENTUM

„Változó környezet, változó biztonság - Kiberfenyegetések kihívásai napjainkban" című nemzetközi szakmai-tudományos konferencia

A Belügyminisztérium illetve annak Tudományos Tanácsa a Nemzetközi Kibertér Konferencia (Budapest, 2012) rendezvényéhez kapcsolódva 2012. szeptember 17-18-án megszervezte és lebonyolította a „Változó környezet, változó biztonság – Kiberfenyegetések kihívásai napjainkban" című rendezvényt. Komoly előrelépésként könyvelhetjük el, hogy a rendészeti szervek, a nemzetbiztonsági szolgálatok, a hazai és nemzetközi civil szervezetek és a tudományos élet képviselői tudományos igényű, közös gondolkodásának lehettünk részesei.

A résztvevők a kibertér és az Internet használatának összefüggéseit tekintették át különféle témakörökben. Rámutattak arra, hogy mennyire sokrétű, a társadalom és az állam különböző szegmenseiben jelenlévő jelenségről van szó, amelynek feltérképezése, megértése és a káros elemeinek felfedése és hatékony üldözése, a nemzeti érdekek közös konszenzusos érvényre juttatása mellett kell, hogy történjen. A „Kritikus infrastruktúra védelmi kutatások" szekcióban világossá vált, hogy a kiberfenyegetések és az erre adott válaszok még nem alkotnak homogén rendszert. Valamennyi érintettnek – terroristáknak, a szervezett alvilágnak, a védelmi, civil és üzleti élet résztvevőinek – más-más a motivációja, mindegyiknek sajátos nézőpontja, eszközrendszere van. Az információs társadalom informatikai függősége és az ebből fakadó új típusú kihívások nem kezelhetők pusztán technológia kérdésként. E téren különös jelentőséggel bír a civil és üzleti szféra szerepvállalása, amelyek eredményei katalizátorként jelenhetnek meg az állami szereplők tevékenységéhez kapcsolódva. Közös munkánk egyik legfontosabb sarokpontja volt, hogy az új típusú kihívások közé tartozó kiberfenyegetések eredményesebb felfedése, hatásmechanizmusuk megértése és kezelése, az együttműködés továbbfejlesztése az érdekeltek között elindulhasson.

„A civil és üzleti szféra szerepvállalása az informatikai bűnözés ellen folytatott küzdelemben" szekcióban értékes előadások hangzottak el. E szekcióban résztvevő hallgatóság tájékoztatókat hallhatott a jogalkotótól egészen a magán szektort képviselő biztonsági vezetőkig.

A létfontosságú rendszerekkel és létesítményekkel kapcsolatos elkötelezettséget mutatja az idén elfogadott új Nemzeti Biztonsági Stratégia, amely rögzíti azt, hogy hazánk kiemelten kezeli az ország mindennapi életkörülményeinek fenntartásához, a gazdaság és az államszervezet működéséhez szükséges kritikus infrastruktúrák hatékony védelmét. Ismerjük a kapcsolódási pontokat az egyes szakosított infrastruktúrák között, és kockázatelemzési módszereinkkel képesek vagyunk válaszokat adni a kritikus infrastruktúra üzemeltetése során megjelenő kihívásokra. Ugyanakkor a konferencia tapasztalatai világossá tették azt is számunkra, hogy növelve a kormányzati szerepvállalást, közre kell működnünk egy nemzeti kiber biztonsági stratégia kidolgozásában, amelyhez alapul szolgálhatnak a NATO és az Európai Unió vonatkozó stratégiai dokumentumai. A stratégiát egy információbiztonságról szóló jogszabály és annak végrehajtási dokumentumai hasznosan egészíthetnék ki. Továbbá közös elhivatottság szükséges az előzőleg említett szabályozókban előírt kötelezettségek ösz-

szehangolt végrehajtásához is. A konferencia egyik tapasztalata az is, hogy a jogalkotás során támaszkodni kell a tudomány által elért eredményekre. Saját szakterületünk vonatkozásában további szerepünk lesz az egyén és a szervezet tudatosításában és az oktatási, kutatás-fejlesztési lehetőségek támogatásában.

A „Kiberterrorizmus" szekcióban kiváló előadásokat hallhattak a német Szövetségi Bűnügyi Hivatal és az Alkotmányvédelmi Hivatal képviselőitől, melyek gyakorlati példákkal szolgáltak arra nézve, hogy miként lehet sikeresen felvenni a harcot a kiber térben tevékenykedő ellenérdekelt felekkel. A hazai előadók, amellett, hogy bemutatták a technológiai újdonságokat, rámutattak arra a sarkalatos problémára, hogy a technika mesteri szintű ismerete mellett szükséges a megfelelő, tevékenységüket támogató jogszabályi háttér megalkotása. Külön öröm volt, hogy az előadások széles spektrumában, a technikai megoldások taglalása mellett, helyet kapott a leginkább mellőzött „social engineering" elleni védekezési lehetőségeket bemutató prezentáció is.

A szekciókat levezető elnökök, a rendezvényt a tudományos szféra, a szabályozást képviselő állam, a szakmaiság és a biztonságkultúráért való tenni akarás találkozásának nevezték.

A belügyi tárcához kötődő feladatok – a kihívás jellegéből adódóan – akkor lehetnek sikeresen végrehajthatóak, ha a jövőben szakértő partnereink tapasztalataira támaszkodva végezzük munkánkat. Ennek során kiemelten fontos az informatikai, hálózatbiztonsági és komplex információvédelmi tevékenység, a sérülékenység-vizsgálatok tapasztalatainak megosztása, továbbá a hatósági felügyeleti tevékenység során szerzett ismeretek felhasználása.

Mivel manapság multidimenzionális térben dolgozunk, ahol globális kockázatok keletkeznek, olyan közös és konvertálható tudástartalomra van szükség, amely hasznos ismereteket nyújt a kiberfenyegetések kezelésének különböző formáihoz. A pontos ismeretszerzés érdekében a kiberbiztonság okozta problémákat helyi struktúrákra szükséges lebontanunk. Közös fellépésünknek azonban tekintettel kell lenni a rendelkezésre álló eszközök korlátozott mivoltára és az eltérő technológiai színvonalra.

Fontos számunkra, hogy felelősséget vállaljunk a Belügyminisztérium felügyelete alatt működő szervezetek cselekvési irányainak korszerűsítése érdekében, kiküszöbölve az együttműködés esetleges diszfunkcióit.

Mindemellett fontosnak tartottuk azonosítani, tartalommal megtölteni – a társadalom hosszabb távú biztonsági érdekeire tekintettel – a digitális biztonság alappilléreinek összetevőit, azokat a rendészetpolitikai, nemzetbiztonsági kérdéseket, amelyek segítséget nyújthatnak a kiberfenyegetések gyakorlatban történő kezelésére, a veszélytényezők minimalizálására.

A jövőben lehetőséget kell teremtenünk a háttérben meghúzódó bűnös viselkedésformák és kiváltó okaik társadalmi, technológiai, kulturális közegének feltárására, a közös megoldási módozatok kimunkálására. Tovább segítheti törekvéseinket, amennyiben sikerül világosan megfogalmazni a kiber- és hagyományos biztonság közötti kapcsolatokat. Különös felelősségünk a társadalom kiberbűnözéstől mentes közegének megteremtésében rejlik, amelynek eléréséhez a kezeléshez jelenleg szükséges hosszabb időintervallum csökkentése közös érdekünk.

Kötelességünk, hogy saját képességeinkkel járuljunk hozzá a nemzetközi küzdelemben a jövőben meghatározó pozíciót betöltő európai uniós kiber bűnözés elleni központ tevékenységének kialakításához, továbbfejlesztéséhez, valamint a NATO incidenskezelő speciális

képességének fejlesztéséhez. Minderre tekintettel a különböző nemzetközi tapasztalatok, technológiai fejlesztések, bűnügyi és nemzetbiztonsági gyakorlatok, megoldási metódusok megvitatása szükséges a sikeres fellépéshez. Ez feltételez egy folyamatos kormányzati koordinációs tevékenységet nemzeti és nemzetközi viszonylatban is, ami elvezet bennünket az együttműködési fórumok rendszeressé tételéhez, a szakosított intézményekkel való közös munkavégzéshez. A problémakör széleskörű kormányzati érintettsége okán célszerű ágazati munkacsoportokra bontva, koordináltan végezni az egyes speciális részfeladatokat. Így fókuszba helyezhetünk olyan területeket is, mint a kiber kémkedés, a kiberterrorizmus, a kiber bűnözés és a szervezett bűnözés kapcsolata, vagy a kiber hadviselés.

Tudományos rendezvényünkön végzett munkánkkal igyekeztünk hozzájárulni a Budapesten, 2012. október 4-5-én megrendezésre kerülő Nemzetközi Kibertér Konferencia szakmai megalapozásához. Fontos eredménynek tartjuk, hogy tanácskozásunk a problémák azonosításán túl eljutott a lehetséges megoldások feltárásáig. Szűkebb szakterületünk vonatkozásában lehetővé vált az előttünk álló kibervédelmi feladataink azonosítása, a fontosabb kommunikációs, jogalkotási és együttműködési kérdések tisztázása.

FINAL ACT

International professional-scientific Conference on „Changing environment - changing security - Cyber-threat challenges today"

Connected to the Budapest Conference on Cyberspace 2012 the Hungarian Ministry of Interior and its Scientific Council organized and implemented the conference of „Changing environment - changing security" - Cyber-threat challenges today on September 17-18, 2012. It is justly recognized as a major step forward that we could be engaged in the collective thinking process of the law enforcement authorities, the services of national security, the national and international NGOs as well as the representatives of the academia, at a scientific level.

The participants reviewed - from several aspects - the correlations of cyberspace and Internet use. They pointed out that a multi-faceted phenomenon was considered, which exists in the different segments of the society and the state, the exploration and understanding of which, together with the identification and efficient prosecution of its harmful elements must be pursued with the assertion of national interests in consensus. It has become clear in the section on „Critical infrastructure defense research" that the cyber-threats and the responses to them do not yet create a homogeneous system. All of the stakeholders – the terrorists, the organized criminals, the participants of the defense sector, of the civil and business spheres – have different motivation and specific aspects as well as system of instruments. The IT dependence of the information society and the resulting new types of challenges cannot be treated as merely technological questions. The involvement of the civil society and the industry has a particular significance in this domain as its results may act as catalysts for the

operations of the public stakeholders. One of the most important outcomes of our joint work was to launch the increasingly efficient disclosure of cyber-threats, which belong to the challenges of new type, to understand and handle their effect mechanism and to further develop the co-operation among the stakeholders.

Valuable presentations were held in the Section on „The role of civil society and businesses in the fight against cyber-crime". The audience of this Section could listen to briefings from the legislators and the security executives representing the private sector.

The new National Security Strategy adopted this year manifests the commitment to vital systems and facilities and it stipulates that Hungary attaches high priority to the efficient protection of critical infrastructure necessary for sustaining the every day living conditions of the country and for the functioning of the economy and organizations of state. We are aware of the connection points among the various specialized elements of infrastructure and by means of our risk assessment methods we are capable of giving adequate answers to the challenges arising in the course of operating the critical infrastructure. At the same time, the conclusions of the conference have highlighted for us that by strengthening the involvement of the government we must contribute to the elaboration of a national cyber-security strategy with the relevant strategic documents of NATO and the European Union applied as starting points. The strategy could be usefully complemented by a law on the security of information and its implementation documents. Joint dedication is also needed for the harmonized fulfilment of the obligations described in the regulators noted above. A lesson learned from the conference was also that in the course of legislation it is necessary to rely upon the results of science. Regarding our own field of specialisation, we shall have further role in raising the awareness of the individuals and organisations and in supporting the possibilities of education, research and development.

In the section on „Cyber terrorism" excellent presentations could be heard from the representatives of the German Federal Criminal Police Office and the Federal Office for the Protection of the Constitution providing practical examples about the ways of successful action to be taken against the opponents active in the cyber-space. In addition to presenting the technological novelties, the Hungarian speakers highlighted the cardinal problem, that in addition to mastering the technologies it is necessary to create an adequate legal background, which would support hteir operations. It was a particular pleasure that in the wide range of presentations, in addition to elaborating on the technical solutions a presentation was also held on the often neglected subject of introducing the methods of protection against „social engineering".

The chairpersons of the sections defined the event as the meeting of the academia, the state representing the regulation, the professionalism and the will to act in favour of the security culture.

The tasks falling under the scope of the Ministry of Interior – owing to the character of the challenge – can be implemented successfully if we carry on our work in the future capitalising the experience of our professional partners. While doing so, high priority is attached to sharing the experience gained in the fields of the IT security, network security and the complex activities of information protection as well as of the vulnerability assessments and the knowledge acquired in the domain of supervisory activities of the authorities.

As today we act in a multi-dimensional space, where global risks arise, we need such shared and convertible wisdom, which offers useful competences for the various form of handling the cyberthreats. In the interest of acquiring exact knowledge the problems caused by cyber-security must be broken down into local structures. Our joint action, however, must consider the restrictred availability of resources and the difference in the technological standard.

It is important for us that we undertake responsibility for the modernization of the directions of action of the entities operation under the auspices of the Ministry of Interior, striving to eliminate the eventual dysfunctions of the collaboration.

At the same time, we have attached great importance to identifying and filling with contents – in view of the longer term interests of the society – the components of the foundation pillars of digital security, the issues of law enforcement policy and national security, which may help in the practical handling of cyber-threats and minimizing the risk factors.

A possibility must be created in the future for exploring the social, technological and cultural media of the underlying criminal forms of behaviour and the related causes and for the elaboration of the collective methods for the solution. Our efforts might be further assisted if we could clearly define the relations between cyber security and conventional security. We have a particular responsibility for creating the society's medium free from cyber-crime, and it is our joint vested interest to reduce the interval of time required for its achievement.

It is our obligation to pledge our own capabilities as contribution to the establishment and further development of the activities of the European Centre to Combat Cyber Crime, which is to have a key role in this process in the future as well as the promotion of the special NATO capability for handling incidents. In view of all this, the successful action demands the analysis and discussion of various international lessons learned, technological developments, criminal and national security exercises and methods of solution. This assumes a continuous governmental coordination activity, both at the national and international levels, which leads to the regular holding of cooperation fora and the joint work with the specialized agencies. As the scope of problems has a wide-ranging impact on the governments, the various specialized sub-tasks should be performed in coordination, broken down into sectoral working teams. In this way we can focus on such areas as the relations of cyber espionage, cyber terrorism and organized crime or cyber-warfare.

With our work carried out in our scientific conference we have attempted at contributing to the professional foundation of the international Budapest Conference on Cyberspace held on October 4-5, 2012. It is an important achievement that our meeting has gone beyond the identification of problems and reached the stage of exploring the potential solutions. With respect to our closer special domain we have succeeded in defining the cyber-defence tasks facing us as well as in clarifying the main issues of communication, legislation and cooperation.

E SZÁMUNK SZERZŐI

Bencsáth Boldizsár dr., Budapesti Műszaki és Gazdaságtudományi Egyetem, Hálózati Rendszerek és Szolgáltatások Tanszék, CrySyS Adat- és Rendszerbiztonság Laboratórium

Buttyán Levente dr., Budapesti Műszaki és Gazdaságtudományi Egyetem, Hálózati Rendszerek és Szolgáltatások Tanszék, CrySyS Adat- és Rendszerbiztonság Laboratórium

Félegyházi Márk, Budapesti Műszaki és Gazdaságtudományi Egyetem, Hálózati Rendszerek és Szolgáltatások Tanszék, CrySyS Adat- és Rendszerbiztonság Laboratórium

Gyányi Sándor dr., főiskolai tanársegéd, Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, Híradástechnikai Intézet

Hankiss Ágnes dr., EP képviselő, Európai Parlament

Homonnai János dr., legfőbb ügyészségi ügyész, Legfőbb Ügyészség

Horváth Attila dr. habil., alezredes, tanszékvezető egyetemi docens, NKE Hadtudományi és Honvédtisztképző Kar, Katonai Logisztikai Intézet Műveleti Logisztikai Tanszék

Illési Zsolt, főiskolai docens, Dunaújvárosi Főiskola

Károlyi László, biztonsági főigazgató, Magyar Posta Zrt.

Keleti Arthur, IT biztonsági stratéga, T-Systems Magyarország Zrt.

Komjáthy László dr., ny. tű. alezredes PhD., NKE KVI Tűzvédelmi és Mentésirányítási Tanszék, egyetemi adjunktus

Kozák Attila tű. őrnagy, Katasztrófavédelmi Kirendeltség-vezető

Kovács László prof. dr., mk. alezredes, egyetemi tanár, tudományos és nemzetközi dékánhelyettes, NKE Hadtudományi és Honvédtisztképző Kar

Kozlovszky Miklós dr., intézetigazgató, egyetemi docens, Óbudai Egyetem Neumann János Informatikai Kar, Informatikai Rendszerek Intézete

Schubert Tamás dr., Óbudai Egyetem Neumann János Informatikai Kar, Informatikai Rendszerek Intézete

Krasznay Csaba dr., elnökségi tag, Information Systems Audit and Control Association (ISACA)

Krepsz Balázs főhadnagy, osztályvezető, Nemzeti Adó- és Vámhivatal, Bűnügyi Főigazgatóság, Központi Nyomozó Főosztály, Információ-technológiai Osztály

Kuris Zoltán r. százados, biztonsági vezető, Belügyminisztérium

Liflander, Christian-Marc politikai tanácsadó, NATO, Kibervédelmi Szekció (policy advisor, Cyber Defense Section, Emerging Sexurity Challenges Division)

Molnár András dr., oktatási dékánhelyettes, Óbudai Egyetem Neumann János Informatikai Kar

Padányi József prof. dr., mk. dandártábornok, stratégiai és intézményfejlesztési rektorhelyettes, NKE

Pék Gábor, Budapesti Műszaki és Gazdaságtudományi Egyetem, Hálózati Rendszerek és Szolgáltatások Tanszék, CrySyS Adat- és Rendszerbiztonság Laboratórium

Précsényi Zoltán, európai kormányzati kapcsolati manager, Symantec

Suba Ferenc dr., Igazgatótanács alelnöke, Európai Hálózat- és Információbiztonsági Ügynökség (ENISA)

Szabó Endre Győző dr., elnökhelyettes, Nemzeti Adatvédelmi és Információszabadság Hatóság

Szabolcsi Zsolt r. főtörzszászlós, kiemelt főnyomozó, KR Nemzeti Nyomozó Iroda, Csúcstechnológiai Bűnözés Elleni Osztály

Zala Mihály elnök, Nemzeti Biztonsági Felügyelet

STUXNET, DUQU ÉS TÁRSAI – VESZÉLYES CÉLZOTT INTERNETES KÁRTEVŐK

Bencsáth Boldizsár – Buttyán Levente – Félegyházi Márk – Pék Gábor

A világ a Stuxnet 2010-es felfedezésével ismerte fel a célzott informatikai támadások jelentőségét. A Stuxnet volt az első olyan igazán komoly célzott támadás, ahol malware segítségével fizikai berendezés tönkretételét érték el, méghozzá csak a kiválasztott célpontoknál, az Iránban telepített urándúsító berendezéseknél.

A célzott támadások ennél sokkal nagyobb múltra néznek vissza, azonban most ért oda a történelem, hogy egyre több, komoly támadássorozatot leplezzenek le, és értik meg a támadások mibenlétét, módszereit, céljait. A célzott támadások meg is szaporodtak. Laboratóriumunk, a BME CrySyS Adat- és Rendszerbiztonság Laboratóriuma több célzott támadássorozatban használt kártevő programot vizsgált az elmúlt időszakban. Vizsgálataink során jelentős tapasztalatot szereztünk a hasonló ügyek kezelésében, és noha a hasonló kártevők esetében sosem lehet biztosat állítani azok forrásáról, készítéséről, életútjáról, a tapasztalatok segítenek abban is, hogy megértsük, miként működhetnek a hasonló kártevőket előállító szervezetek, szövetségek.

Duqu

A 2010 júniusában felfedezett Stuxnet malware egy új fejezetett nyitott a számítógépes biztonság területén. Először került sor arra a történelemben, hogy egy számítógépes támadás fizikailag tönkre tudta tenni a kritikus infrastruktúra elemeit. A Stuxnet nem volt az első kártékony kód amit ipari rendszerek ellen vetettek be, de az első volt, amelyik világszintű ismertséget is szerzett különleges célja folytán, A Stuxnet az első világszerte ismert számítógépes fegyver. A Stuxnet nem egyedüli mintája a célzott támadásoknak. Köszönhetően a megnövekedett figyelemnek a téma iránt és a megélénkült munkának a malware kutató közösségből, több új célzott támadássorozat is felismerésre került. 2011 októberében laboratóriumunk, a BME CrySyS Adat- és Rendszerbiztonság Laboratóriuma információkat tett közzé a Duqu nevezetű malware felfedezéséről, amely malware megdöbbentő hasonlóságokat mutatott a Stuxnet kártevővel, de teljesen más célt szolgált. A Duqu nem próbált fizikai károkat okozni, hanem információ gyűjtésére volt használható, egyfajta számítógépes kémkedésre. A Duqu felfedezésének érdekessége, hogy egy európai cégnél került megtalálásra, noha a támadássorozat vélhetően összefügg az iráni atomprogrammal kapcsolatos nyugati hírszerzési tevékenységekkel. Laboratóriumunk részletes technikai analízist készített a Duqu malware tárgyában, melyet nyilvánosságra is hoztunk. Később laboratóriumunk vezérletével sikerült kezelni a Duqu fertőzéshez használt ún. „dropper” fájlt is. Ennek a munkának a során derült ki, hogy a támadók egy olyan Windows sérülékenységet használtak ki, amelyikkel gyakorlatilag minden Windows alapú gép támadható lehet több fajta fájl formátum alkalmazásával. A hiba a Windows betűtí-

pus, azaz font kezelését érintette. Fontos azt is megjegyezni, hogy a Duqu esetén (és ennek megfelelően bármely hasonlóan tervezett utódjánál is) lehetséges modulokat betölteni, ami azt jelenti, hogy a felfedezett kártevőn kívül sok más nem felfedezetett modul is létezhet, így az is lehetséges, hogy a kémkedésen túl károkozásra alkalmas moduljai is léteznek.

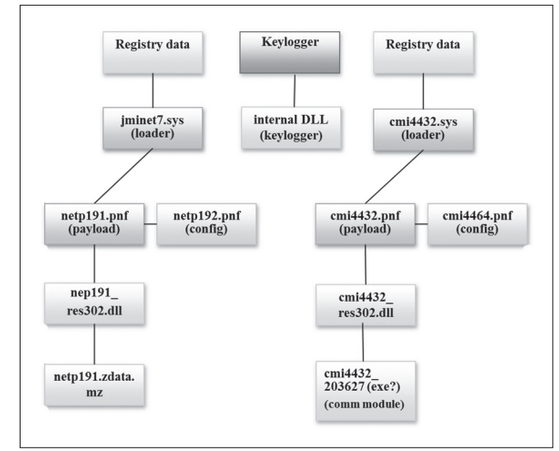
A Duqu felfedezése

A Duqu malware felfedezése az egyik európai áldozat érdeme. Ez a cég észrevette, hogy különös jelenségek történtek számítógépes rendszerében, amelyek arra engednek következtetni, hogy valamilyen súlyosabb számítógépes „betörés" történt. A cég, mint a labor meglévő partnere, felvette a kapcsolatot laboratóriumunkkal is a probléma vizsgálata céljából. A vizsgálat fő célja a probléma kezelése, és a cég helyes, megbízható működésének rendberakása volt, nem volt elsődleges cél sem a támadók sem a támadási eszközök azonosítása. Minden résztvevő kíváncsi volt azonban, hogy mik lehetnek az eszközök, amelyek a betöréshez vezettek, és milyen módon lehet azt kivédeni, hogy esetleg hasonló, vagy ugyanazon támadó ezekkel az eszközökkel újra éljen.

Ennek mentén kapott laboratóriumunk korlátozott felhatalmazást, hogy egyes összegyűjtött ún. forensics anyagokhoz hozzáférést kapjon, és azokban megkereshesse azt, hogy mik lehettek a támadásban érintett kódok. Ez a keresés egyfajta célzott tű a szénakazalban típusú keresés. Sok rendes program, fájl között kell megtalálni, hogy mi is történhet a támadó alkalmazás betöltése közben, de bizonyos indikátorok segítik azt, hogy meg tudjuk mondani, sikerült-e a keresés.

Technikai értelemben már az első napon, és már az érintett cég is tudta, hogy a malware újraindítás után kb. 15 perccel aktivizálódik, és az is felismerésre került, hogy ilyenkor a normálisnál több „lsass.exe" process lásztik a futó processzek listájában (különösképpen vizsgálható a Sysinternals Process Explorer alkalmazásával). Ezt a technikai vizsgálatot folytatva sikerült kideríteni, hogy a malware főbb komponensei cmi4432.sys, a kapcsolódó cmi4432.pnf és cmi4464.pnf, továbbá a jminet7.sys és a hozzá tartozó netp191.pnf és netp192.pnf.

A vizsgálatok során az derült ki, hogy két különböző Duqu verzió került bevetésre, ez a „jmi" és a „cmi" vonalak. Mindkettő esetben egy .sys kernel driver tölti be a belső konfigurációját, majd a registryből szedi ki ez alapján a pontosan specifikációt amelyik egy .pnf fájlra mutat és meghatározza annak dekódolási kulcsát is. A pnf fájl további komponenseket tartalmaz, továbbá egy konfigurációs állományt kezel. Komplex struktúra, melyet részletesen további dokumentumainkban részletezünk. Ami nagyon érdekes, az az, hogy ez a mechanizmus megdöbbentően hasonló a Stuxnet esetéhez, ott gyakorlatilag ugyanez történt meg. Fontos még megjegyezni, hogy a cmi4432.sys kernel driver valódi, jó digitális aláírással rendelkezett, noha a driver program egyértelműen kártékony, a Duqu része. A Duqu felfedezésekor egyetlen híres esetet ismert a közösség hamis digitális aláírást alkalmazó malware-ről, mégpedig a Stuxnet esetét, ahol volt egy aláírt driver fájl (Realtek taiwani gyártótól), és később felmerült egy másik taiwani gyártó által aláírt driver érintettsége, amely cég a Jmicron. Utóbbi esetében nem bizonyított, hogy a Stuxnet malware-hez volt használva az aláírt driver. A Duqu esetében felmerült harmadik hasonló eset (C-Media taiwani gyártó által aláírva) olyan tény volt, amelyik az adott pillanatban önmagában is nagy súlyt jelentett, megmutatta a támadás rendkívüli fontosságát.



1. ábra. A Duqu moduljai

A Duqu technikailag egy kifinomult moduláris malware, amelyik csak a legszükségesebb komponenseket tárolja a merevlemezen. Ha szükséges, képes modulokat letölteni a vezérlő szerverektől (Command and Control Servers, C&C, vagy C2). Két modulról van tudomásunk, de korlátlan számú más modul létezhetett, így nem lehet kategorikusan kijelenteni pl. azt sem, hogy a Duqu nem célzott ipari vezérlőrendszereket (pl. PLC). A két ismert modul egyike egy keylogger, fő célja billentyűzet lenyomások, képernyő állapotok, alkalmazások futásának rögzítése. A másik modul célja fájlok kigyűjtése és összetömörítése, de ez esetben a modult nem ismerjük, viszont ismerjük a fájl formátumot, amit a modul elkészített. Ebből is látható, hogy a vizsgálatok célja főként az, hogy a tevékenység egészét próbáljuk meg megérteni, amire természetesen az egyes technikai részletkérések indítanak, ugyanakkor a nem-technikai háttér információk is nagyon fontos információval látnak el. A laboratórium tevékenységében úgy összegezhetjük ezt, hogy csak kb. 20% technikai feladat volt egy hasonló esetben, és 80%-a a munkának más tevékenység: információ megosztás, munkaszervezés, kapcsolat szakmai szervezetekkel, kormányszervekkel, sajtókapcsolatok stb.

Flame

A Flame malware létezéséről az iráni MAHER CERT 2012. május 27-én adott ki információt (akkor még "Flamer" néven nevezve), majd másnap 2012. május 28-án délután laboratóriumunk a Kaspersky rövid összefoglalójával (Flame malware) párhuzamosan jelentette be eredményeit a malware analíziséről. Röviden összefoglalva a CrySyS Lab 2012. 05. 28-án elsőként közölt egy részletes, kb. 60 oldal terjedelmű dokumentumot egy célzott támadási kampányról, amely főként iráni célpontokat érint, de amelyiknek magyar célpontjai is vannak.

A Flame malware technikai értelemben teljesen más képet mutat, mint a Duqu. A Duqu esetében kifinomult, kicsi, célirányos kódrészletekről beszélhetünk, ahol szinte semmi nincs telepítve a célgépen, a Flame esetében pedig inkább beszélhetünk egy picit szedett-vedett

projektről, ahol mindenféle összevissza, vegyes, esetleg nem is használt kód települ a célgépekre. Ráadásul ebben az esetben a célgépek ezreiről beszélünk, ahova a széles funkcionalitású kód 6-20 MB méretű része települhet.

Ami fontosabb a Flame esetén az az automatikus adatgyűjtési technikák széles skálája. Technikai oldalról megoldható vele információgyűjtés sok nagyon különböző helyzetben, de nagymértékben automatizálva, tehát nem célgépre specifikusan, hanem főként általánosan kiadott parancsok segítségével tömegesen tud adatokat gyűjteni.

A Flame kampány összefüggésben volt a Stuxnet-Duqu kártevőkkel, de ez csak később bizonyosodott be. Egyes rejtjelező kódok azonosak, és egy ún. exploit kódja is azonos a Stuxnet egy régebbi verziója és a Flame-ben használt megoldás között. Ugyanakkor a Stuxnet, Flame kártevők fordításakor többféle fordító verziót használtak a készítők, így valószínű, hogy a kódegyezések annak okai, hogy a készítő csoportok együttműködtek, a verzióeltérések viszont azért lehetségesek, mert az egyes csoportok a más csoportok eredményeit nem forráskód szinten, hanem csak binárisan kapták meg. Tehát az elképzelt kép szerint a fejlesztők több csoportban dolgoztak, és alkalmanként információt cseréltek, de nem teljes mértékben, csak egy bizonyos bináris („API") szinten.

A Flame esetében fontos, hogy az áldozatok száma nagy, mintegy 10 000 áldozatról beszélhetünk, nagy részük Iránban, de kb. 25% Szudánban, és jelentős mennyiségben más országokban is, köztük Magyarországon is 10 fölötti fertőzési esettel.

Flame 0-day trükk

Ami a Duqu esetén a Windows font fájl kezelési sérülékenység volt a fertőzéshez, az a Flame esetében egy még komplexebb probléma volt, nevezetesen hamis tanúsítvány alapú visszaélés a Microsoft Windows Update szolgáltatásával. A támadók ennek a hibának a kiaknázásával tudtak újabb gépeket megfertőzni.

Amikor egy megfertőzött hálózatban egy nem fertőzött számítógép elkezdi a frissítési procedúrát, úgy első körben a helyi hálózatban lekérdezi, hogy mi az ún. proxy szerver (WPAD). A korábban megfertőzött egyik gép ekkor boldogan jelenti, hogy ő az. A nem fertőzött gép ezek után megkérdezi, van-e frissítés a Windows update szolgáltatásához, a támadó fertőzött gép pedig újra boldogan elküldi a speciálisan elkészített támadó csomagokat. A támadó csomagokban speciális, kártékony kód van, ami a Flame malware-t telepíti egy helyi hálózati szerverről, többnyire ugyanarról a szerverről, ahonnan az előbbi hamis WPAD jelzés érkezett.

A fontosabb kérdés, miért fogadja el a Windows a hamis frissítéseket. A valódi frissítések (.cab fájlok), digitálisan alá vannak írva, ezt ellenőrzi a Windows telepítéskor. A támadók kihasználták a Windows Terminal Services Licensing sérülékenységeit: A Microsoft érthetetlen módon a ma már nem biztonságos MD5 hash alapú tanúsítványokat használt a rendszerben, és más gondok miatt végfelhasználóknak kiadott tanúsítványokat kód aláírásra lehetett használni, amit a Windows Update elfogadott. Emellett a támadók egy MD5 hash ütközést is létrehoztak, mert az eredeti tanúsítványt a Windows Vista, Windows 7 rendszerek nem fogadták volna el ún. kritikus X.509 Hydra kiterjesztések miatt. Egy ilyen ütközés létrehozása nehéz, több száz számítógép több nap alatt tud elkészíteni egy ütközést, így gyanús, hogy a támadók vagy óriási támadási kapacitással, vagy olyan tudással rendelkeztek, amelyik az

MD5 ütközés generálását jelentősen redukálni tudja (kriptográfiai tudásban jelentős áttörés birtokában voltak)

Gauss Gödel module

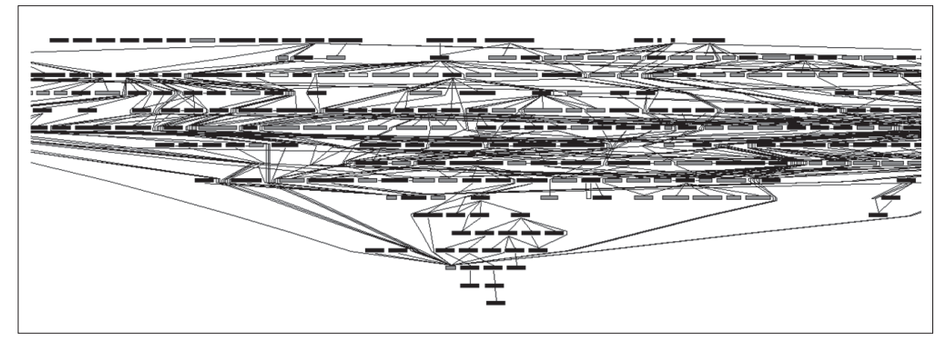
A Flame-hez kapcsolódó Gauss nevű malware-t a Kaspersky Labs analizálta először. Vizsgálatuk szerint a malware nagyon hasonló a Flame-hez, célpontjai azonban elkülönülnek és főként libanoni banki adatokat próbálnak megszerezni vele. Nem pénzt, csak adatokat, és ez újra azt jelzi, hogy állami szereplő van a háttérben, valaki pontosabb adatokat próbál szerezni a libanoni bankügyletekről, amelyek az egész térség aktivitásával összefüggésben lehetnek.

A Gauss malware esetében laborunk még az eredeti riport megjelenésekor egy új szolgáltatást hozott létre: Ismert volt, hogy a malware valamilyen ismeretlen oknál fogva a célberendezéseken egy betűtípust, a „Palida" fontot telepíti. Ha tehát egy gép fertőzött, akkor a font telepítve van rajta. Laboratóriumunk kidolgozott egy kísérleti eljárást arra, hogy egy távoli kliens az erre a célra létrehozott weboldalunk letöltésével meg tudja nézni, hogy a gépén a Palida betűtípus telepítve van-e, vagy sem. Ennek segítségével nagyon kis mértékben sikerül előmozdítanunk a Gauss malware felismerését.

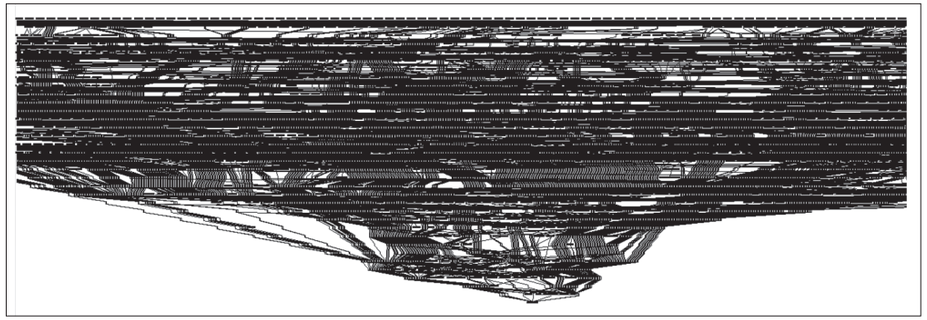
A Gauss malware sokkal érdekesebb specialitása a Gödel modul. Ez olyan rejtjelezett kódot tartalmaz, amely specifikusan csak egy adott célgépen fut le. A Gödel modul úgy dekódolja a kódot, hogy a környezeti változókat (PATH) és egy alkönyvtár listáját (Program Files) használja a dekodoló kulcs elkészítésére. A helyes kulcs csak a célgépen érhető el, és így a malware Gödel moduljának célját máig senki nem ismeri. Laboratóriumunk egy ingyenes eszközt adott ki, amellyel a dekódoláshoz szükséges környezeti változók lehetséges értékeit gyűjtjük önkéntes felhasználóktól.

Analízis

A kódanalízis során az egyik legnagyobb probléma a kód bonyolultsága, kisebb kódokat lehetséges manuálisan teljesen elemezni, nagyobbakat azonban rendkívül nehéz. Az alábbi első példa a duqu keylogger programjának struktúráját mutatja. Mint látható, a kód bonyolult, de még kezelhető méretű.



2. ábra. Duqu Keylogger belső struktúra



3. ábra. Flame browse32 belső struktúra

A Duqu keyloggere bonyolult feladatokat oldott meg illeszkedő bonyolultságú kóddal. Ezzel szemben a Flame Browse32 moduljának kódja túl bonyolult. A kód fő célja a Flame által telepített modulok törlése, azaz az öngyilkosság. Ehhez viszont a feltűnően bonyolult kód feleslegesnek látszik. Vélhetően a kód számos statikusan fordított részt tartalmaz, ezért látszik bonyolultnak az egyébként egyszerű kód.

Malware fejlesztés

A legfontosabb észrevétel a malware fejlesztésről az, hogy a fejlesztők minidig a követelmények alapján legoptimálisabb, és legkevesebb fejlesztést követelő eredményt hozzák létre. A Duqu, Flame, Gauss esetében a fő cél az észrevétlen információszerzés. Ennek megfelelően a szerzők legfontosabb lépése az volt, hogy eredményterméküket (a malware-t) szinte minden antivírus eszköz ellen tesztelték, és csak akkor használták, amikor biztosak voltak abban, hogy az eredményt a megfelelő antivírus termékek nem ismerik fel.

Ennek megfelelően a mai célzott malware nem célozza meg azt, hogy a malware kód analízise bonyolult legyen, ehelyett azt célozza meg, hogy a malware detektálása legyen nehéz. Ha lebukott, akkor már mindegy, jöhet egy újabb verzió

Ez a fejlesztési hozzáállás természetesen felveti azt a kérdést, hogy milyen más malware típusokat fogunk látni a későbbiekben? A választ megadni nehéz, de mintapéldának tegyük fel, hogy lesz olyan támadó amelyik kód segítségével próbál időben pontosan meghatározott támadást elvégezni (pl. robbantás). Egy ilyen malware fejlesztésekor feltehetően a cél nem a detektálhatatlanság lenne, hanem az időszinkronizáció legrobusztusabb módjai, és az, hogy ha bárki detektálja a malware-t, akkor záros időn belül (pl. 1 hét) senki ne tudja megtudni, hogy mi a malware pontos célja.

Detekció

Vajon miért nem tudták felismerni sem a Stuxnet, Duqu, sem a Gauss, Flame malware programokat évekig? Sajnos nem azért, mert detektálhatatlanok voltak. Laboratóriumunk több tesztet elvégzett az említett malware mintákkal és arra jutott, hogy több általános malware detektáló eszköz igen sikeresen tudja jelezni, hogy valami nagy gond van a számítógépes kör-

nyezetben. Tesztjeink során különösképpen a GMER és a XUETR eszközök voltak hatékonyak, és könnyedén jelezték olyan ún. operációs rendszer szintű hookok jelenlétét, amelyek a malware aktivitását jelölik.

Ha tehát az évek során lett volna, vagy esetleg volt olyan rendszergazda, amelyik a fentiekhez hasonló eszközök felhasználásával felismerte volna a gyanús gépeket, és lett volna mögötte egy stáb, cég, amelyik részleteiben is ki tudta volna analizálni a furcsa eredményeket, akkor sokkal hamarabb lebuktak volna ezek a több évig aktív kártevők.

Összegzés

A vizsgálataink tárgyát képező Stuxnet. Duqu, Flame, Gauss malware-ek igen fontos tényezők. Nem azért, mert közvetlen veszélyt jelentenek, hanem azért, mert új helyzetet teremtettek az informatikai támadások területén, és amelyhez alkalmazkodni kell. Rövid tanulmányunkban igyekeztünk bemutatni a legfőbb érdekességeket, de természetesen a részletek iránt érdeklődőknek el kell olvasniuk forrásmunkáinkat is, az adott témákban elérhető riportjainkat, illetve más cégek és kutatószervek kapcsolódó munkáit.

BOTNETEK, A TÚLTERHELÉSES TÁMADÁSOK ESZKÖZEI

Gyányi Sándor

Az informatikai rendszerek működését a meghibásodásokon kívül külső, szándékosan előidézett tényezők is veszélyeztethetik. A nyílt, nyilvános hálózattal összeköttetésben álló rendszerek elérhetők a hálózat – az internet esetében ez gyakorlatilag az egész világot jelenti – összes pontjáról, így a támadók bárhonnan indíthatnak rosszindulatú akciókat. Az informatikai eszközökkel megvalósított támadásokat a könnyebb azonosítás és az ellenük alkalmazható védelem kiválasztása érdekében célszerű valamilyen szempontrendszer szerint kategorizálni. A szakirodalom sokféle osztályozást ismer, az egyik legegyszerűbb, és emellett még jól alkalmazható besorolást Frederick B. Cohen [1] publikálta. Eszerint minden informatikai támadás három kategóriába sorolható:

- Szivárgás (leakage): ennek során a támadó illetéktelen hozzáférésre tesz szert, olyan adatokhoz jut, amikhez nem szabadna.
- Sérülés (corruption): a támadónak sikerül az informatikai rendszerben tárolt adatokat törölnie vagy megváltoztatnia.
- Megtagadás (denial): a megtámadott rendszer működésképtelenné válik.

A támadó szempontjából az első két kategóriába eső akciók kivitelezése rengeteg munka ráfordítást igényel, mindkettő esetében valamilyen hozzáférési jogosultság illetéktelen megszerzése válik szükségessé. Emiatt napjainkban egyre nagyobb jelentőségűek a harmadik csoportba tartozó támadások, amelyek során – általában „nyers erő” használatával túlterhelést okozva - működésképtelenné teszik a célpontot.

Ez egyszerűbb, mint azt először gondolnánk. A számítógépes hálózatok működéséhez a bemenő adatok fogadása és kimenő adatok szolgáltatása is hozzátartozik. Ha az adatok előállítását vagy továbbítását sikerül elviselhetetlenül lassúvá tenni, akkor a felhasználók ezt működésképtelenségnek érzékelik . Jakob Nielsen a „Usability Engineering” [2] című munkájában publikálta a válaszidővel kapcsolatos kutatásainak eredményét. 0,1s vagy rövidebb válaszidő esetén a felhasználó a választ azonnalinak érzékeli, így a rendszernek az eredmény megjelenítésén kívül semmilyen egyéb visszajelzést nem kell produkálnia. Ezt tekinthetjük a normál, üzemszerű állapotnak. 1s alatti válaszidők esetén a felhasználó még nem érzi úgy, hogy a munkáját indokolatlanul megzavarnák, de már érzékeli a rendszer lassulását. A rendszernek még nem szükséges a lassulásról visszajelzést adnia, de a használat kezd kényelmetlenné válni, míg 10s az a határ, amit meghaladva a felhasználó már elkezd egyéb feladatokkal is foglalkozni, vagyis elveszti érdeklődését a rendszerrel szemben. 1-10s közötti válaszidőnél fontos kijelezni a válasz várható időpontját, és így fenntartani az érdeklődést.

Tehát, ha a támadónak sikerül a célpont válaszidejét 10s időtartamnál magasabbra tolni, akkor a felhasználók ezt működésképtelenségnek fogják érzékelni. Az informatikai

támadásoknak létezik egy olyan fajtája, ami kifejezetten ezt a célt próbálja elérni, ezeket összefoglalóan DoS támadásoknak (Denial of Service) nevezzük. A legtöbbször a működésképtelenséget a célpont erőforrásainak túlzott mértékű felhasználásával, túlterhelésével próbálják elérni.

Mivel az ilyen akciók hatásossága a támadó és a célpont erőforrásainak arányán múlik – ha a célpont megfelelő erőforrás többlettel rendelkezik, akkor képes fenntartani a működését terhelt állapotban is – ezért az igazán hatásos túlterheléshez sok hálózati végpontból kell egyidejűleg a kiszolgálóhoz fordulni. Ezt a módszert DDoS-nek (Distributed Denial of Service) nevezzük, és végrehajtásához nagyméretű hálózat – vagy még inkább egymástól független hálózatokban működő számítógépek - birtoklása szükséges. A hatásos csapáshoz szükséges nagyszámú végpont emberi közreműködéssel is hadrendbe állítható, ha sikerül a tulajdonosokat meggyőzni arról, hogy érdemes csatlakozniuk az akcióhoz. Ezt a hacktivizmusnak nevezett módszert régóta használják, az Electronic Disturbance Theater nevű szervezet akciója volt az első a sorban. 1998-ban az aktivisták előre megbeszélt időpontokban, egy speciálisan erre a célra készített alkalmazással összehangoltan kezdtek el keresési műveleteket indítani a Pentagon weboldalán, amely a nagymértékű terhelést nem sokáig bírta [3]. Napjainkban az Anonymous nevű szervezet alkalmazza előszeretettel az ilyen megoldásokat, természetesen kicsit korszerűsítve és automatizálva a módszert. Egy megfelelően kivitelezett akció a hatásossága mellett a résztvevők felelősségre vonását is nehezíti, hiszen mindenki rendeltetésszerűen használja a célpont erőforrásait, csak éppen olyan tömegben, amit az már nem képes kiszolgálni.

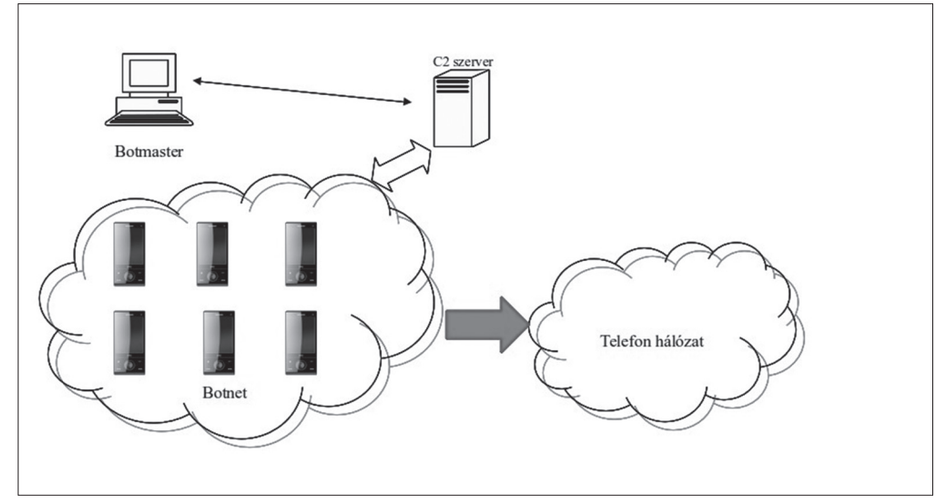
A hacktivizmus mellett automatizált eszközökkel is végrehajtható a célpont túlterhelése. Ehhez a támadónak megfelelő számú hálózati végpontot kell használnia, ekkor viszont már könnyen visszakövethető a tulajdonos. Ennek kivédésére szolgálnak a rosszindulatú programmal megfertőzött számítógépekből kialakított hálózatok. A számítógépes vírusok , férgek és trójai falovak továbbfejlesztése olyan rosszindulatú alkalmazásokat eredményezett, amelyek képesek magukat önállóan terjeszteni, emellett segítségükkel az áldozat számítógépe távolról irányíthatóvá válik. Kedvelt elnevezésük a „robot” szó rövidítéséből adódó „bot”. Természetesen ezek egyenkénti távirányítása nehézkes, ezért központi vezérlés alá helyezve, hálózatba szervezik őket, így biztosítva az összehangolt működést. Az így kialakított botnet 4 fő részből áll:

- Botmaster, vagy botherder: a botnet „tulajdonosa”. Ő adja ki a feladatokat, határozza meg a célpontokat.
- Command & Control (C2) csatorna: a botmaster és a botnet tagok közti kommunikációt biztosítja.
- Drop server: a botnet működése során keletkezett adatok – például a begyűjtött jelszavak – tárolási helye.
- A hálózat tagjai.

Könnyen belátható, hogy a támadás ereje a botnet tagjainak számától, illetve a tagok erőforrásainak méretétől függ. A támadó hálózat erőforrásai egyszerűen növelhetők, csak még több fertőzött számítógépet kell bevonni a hálózatba, míg a célpont saját erőforrásokat csak nehezen tud bővíteni, így az akció „túlélése” szinte lehetetlen.

Új fenyegetést jelent az is, hogy megjelentek a komoly számítási kapacitással rendelkező mobiltelefonok és egyéb elektronikai készülékek. Ezek már az asztali számítógépekkel összemérhető feldolgozási teljesítményt illetve hálózati adatátviteli sebességet képesek produkálni, ráadásul elterjedtségük is rendkívüli. Egyre inkább terjednek az internetre köthető berendezések, amelyek így potenciális célponttá vagy eszközzé válhatnak. Az úgynevezett „okostelefonok” egyre inkább telefonálásra is alkalmas számítógépek, segítségükkel a különböző célú – beszéd és adat - hálózatok átjárhatóvá válhatnak.

Az *1. ábra* egy ilyen botnet szerkezetét mutatja be.



1. ábra. A botnet szerkezete

Az okostelefonokon is az asztali számítógépekéhez hasonló operációs rendszerek működnek, amelyek tartalmazhatnak sérülékenységet. Ezek kihasználásával rosszindulatú alkalmazások is telepíthetők rájuk, de akár készíthető is olyan, hasznos alkalmazásnak tűnő program, amely rosszindulatú kódrészeket is tartalmaz. Ezekkel akár egy botnet is kialakítható, amely a hagyományos botnetekhez képest új típusú fenyegetést jelent. Képzeljünk el egy olyan alkalmazást, amely a központi vezérlő végponttól kapott parancs vétele után a beszédcélú hálózatot használva telefonhívásokat kezdeményez. Ezzel a módszerrel immár nem csak az internetes végpontok működését, hanem bizonyos telefonszámok elérhetőségét is meg lehet akadályozni. Ha ez a megcélzott telefonszám például a segélyhívó szám, akkor a fenyegetés mértéke jóval túllép az internetes weboldalak működésképtelenségéből adódó kényelmetlenségen, és akár emberéleteket is veszélyeztethet.

Bár a szakértők a túlterheléses (DDoS) támadásokat mindig is hajlamosak kevésbé veszélyesnek ítélni, mint az egyéb típusú akciókat, de nem szabad alulbecsülni a veszélyességüket. Az új típusú – elsősorban a mobiltelefonokat érintő – fenyegetések miatt nem az a kérdés, hogy be fog-e következni nagy visszhangot kiváltó ilyen akció, hanem inkább csak az, hogy pontosan mikor?

IRODALOMJEGYZÉK

Civil Disobedience in Cyberspace. Forrás: http://home.clara.net/heureka/gaia/elec-act.htm.
Frederick B. Cohen (1997): *Information system attacks: A preliminary classification scheme.* In: Computers and Security, 16. kötet, 1.
Jakob Nielsen (1993): *Usability Engineering.* San Francisco, Morgan Kaufman. ISBN 0-12-518406-9.

KIBERBIZTONSÁG: AZ EURÓPAI PARLAMENT FELADATAI

Hankiss Ágnes

Engedjék meg, hogy megköszönjem a megtisztelő meghívást és - ha röviden és vázlatosan is - bemutassam Önöknek, hogy a kiberbiztonság vonatkozásában milyen kérdéskörökkel foglalkozik az Európai Parlament.

Mindenekelőtt két olyan állítás fogalmazható meg, amelyben mindenki egyetért, aki így vagy úgy kiberbiztonsággal foglalkozik. Az egyik, hogy a kiberbiztonság, illetve a kiber-fenyegetettség a következő évtizedek egyik legfőbb biztonsági kihívását jelenti. A másik, hogy a kiberbiztonság megvalósítására irányuló erőfeszítések jelenleg elég fragmentáltak, azaz a különböző szereplők hatékony együttműködése még hagy maga után kívánnivalót. Ahogyan az Európai Parlament nézőpontjából látom, a kiberbiztonság területén még komoly problémákat okoz az a fajta párhuzamosság, amely az energiák herdálásával és hasznos információk elsikkadásával járhat. Nem véletlenül ismételgetjük már-már mantraként, hogy milyen fontos a kooperáció, megvalósulását azonban a gyakorlatban számos körülmény nehezíti. Engedjék meg, hogy megemlítsek egy apró példát. Múltkoriban, egyik parlamenti szakbizottságomban vendégül láttuk az Európai Unió Hírszerzési Központjának (Intelligence Center, IntCen) a vezetőjét. Ez a hivatal, bár műveleti felhatalmazással nem rendelkezik, a terrorelhárítási koordinátor hivatala mellett, az Európai Unió egyik legfontosabb értékelő és elemző központja. A találkozón feltettem azt a kérdést, hogyan áll az együttműködés az Intcen és az Unió védelmi - katonai szervei között. Az Intcen vezetője némi tűnődés után azt felelte: „szoktak kérni tőlünk információkat, amit mi megadunk, mi is szoktunk kérni, de még soha nem kaptunk egyet sem".

Az Európai Parlament gyakorlata is a párhuzamosságot tükrözi. A kiberbiztonság kérdésével több szakbizottság is foglalkozik. Ez egyik a Biztonság- és Védelempolitikai albizottság, amelyben magam is dolgozom. A másik az Állampolgári, Jogi, Bel- és Igazságügyi bizottság, amely igen széles területet fog át, emberi és kisebbségi jogoktól a rendvédelemig. Magam ezen belül a szervezett bűnözés és a terrorelhárítás területével foglalkozom. Visszatérő tapasztalatom, hogy miközben a kiberbiztonság témája mind a két szakbizottság agendáján előkelő helyen szerepel valójában alig van átjárás a két bizottság munkája között. Míg a Biztonság - és Védelempolitikai albizottság elsősorban a kiberhadviselés és a nagyobb horderejű kibertámadások veszélyével és elháríthatóságával foglalkozik, a Bel- és Igazságügyi bizottság elsősorban a kiberbűnözés kihívásait tartja napirendjén. Csupán a kritikus infrastruktúrák védelme és a kiberterrorizmus fenyegetése jelent közös nevezőt a két bizottság tevékenysége között.

Ami a kiberhadviselést illeti, ahogyan mások is hangsúlyozták, a kiberhadviselés ma még inkább a jövő rémképe, mint közvetlenül fenyegető valóság. A legsúlyosabb incidens, az észtországi informatikai rendszer megtámadása volt 2007-ben. Az Oroszország és Grúzia közötti konfliktus során komoly támadások érték a grúz kormányzati IT-rendszereket, súlyosan

gyengítve Grúzia védelmi képességeit. Ugyancsak az IT-rendszerek, és rajtuk keresztül a társadalmak, államok sebezhetőséget állította a figyelem fókuszába egy sor olyan kíber-támadás, amely más NATO-országokat ért az elmúlt évtizedben. Az Egyesült Államokat ért egyik támadás alkalmával például 22 kormányhivatal és tucatnyi olyan szerződéses honvédelmi partner is kárt szenvedett, akik védett katonai titkokat őriztek. Ezek az incidensek nyilvánvalóvá tették, hogy a nemzetállamok nem csupán célpontjai lehetnek súlyos kiber-támadásoknak, hanem ugyanakkor maguk is képesek az IT-rendszereken keresztül intézni támadásokat más országok vagy nemzetközi szereplők ellen. A kíbervédelmi képességek fő letéteményese ma a NATO 2008. elejére körvonalazódott a NATO új kíbervédelmi stratégiája, amely lefektette a szövetség kíber-politikájának három alappillérét. Ezek: a biztonság, a szubszidiaritás és a párhuzamosságok kiiktatása. A 2010-es lisszaboni döntés értelmében a kíbervédelem kiépítése folyamatosan és önállóan napirenden lesz a NATO stratégiai célkitűzései között. Az új stratégiai célok kidolgozása mellett a NATO végrehajtja olyan már meglévő struktúrák szükséges megújítását, mint amilyen például a NATO Számítógépes Biztonsági Események Kezelése (CIRC). Fő cél egy továbbfejlesztett „Kíbervédelem 2.0" kialakítása a teljes körű védelem érdekében. Érdemes megemlíteni azt is, hogy a válságövezetekben a NATO olyan „ernyőt" hozott létre, amely a kommunikáció biztonságát hivatott szavatolni.

Több konferencián, amelyen részt vettem, felmerült az a kérdés, hogy a NATO 5. cikkelye, azaz a szolidaritási cikkely, érvényes-e súlyos kibertámadás esetében. Ahogy látom, a NATO vezetőinek egyértelmű álláspontja az, hogy a kibertámadás nem eshet az 5. cikkely érvénye alá, magyarán, ha egy NATO tagországot komoly kibertámadás érne, a NATO katonai erővel nem kelne a védelmére. Ugyanakkor abban mindenki egyetért, hogy a 4. cikkely, amely előírja a közös fellépést és egymást megsegítését, garantálhatja a tagországok védelmét. Kérdés, hogy ennek mennyi a realitása, de az biztosan nem árt, ha van kidolgozott, saját védelmi rendszerünk is.

Ami a kiberkémkedést illeti, három különböző változatát érdemes megemlíteni.

Az egyik, amikor a kiberkémkedés személyes titkok megszerzésére irányul. Az illegális uton megszerzett szenzitív adatok használhatók zsarolásra vagy a kényszerítés és befolyásolás bármilyen más formájára. A másik, azok a többségükben ipari-üzleti kémkedés körébe vágó esetek, amikor cégek akarják megtudni egymás titkait és a piaci versenyben hasznosítani. A harmadik, amely a legközelebb áll a kémkedés hagyományos formáihoz, országok között zajlik. Az igazság az, hogy a dolog természeténél fogva, erről, mi képviselők keveset tudhatunk, de annyit talán érdemes megemlíteni, hogy szakértők szerint az Európai Únió és maga a Parlament is erősen kitett a kémkedés, és ezen belül a kiberkémkedés minden lehető formájának.

A kiberterrorizmust mindenképpen meg kell különböztetni a puszta vandalizmustól. Azt, hogy egy jól képzett hacker belép egy rendszerbe és szándékosan rombol, nem volna értelme terrortámadásnak tekinteni. A kiberterrorizmus meghatározásában, ahogyan a hagyományos terrorizmus definíciójában is, alapkritériumnak kell tekintenünk az ideológiai, politikai vagy vallási célképzetet. Ha az ideológikus töltet hiányzik, kiberterrorizmusról aligha beszélhetünk. Kiberterrorista akciónak az tekinthető, ha a hagyományos terrorizmus információs infrastruktúrákba behatolva és azokat céljaira felhasználva a kritikus infrastruktúrák ellen indít támadást. Az ismert esetek igen különbözőek. Primer változata védett információk megszerzésére irányul. 2003-ban Afganisztánban például találtak egy olyan terrorista kézikönyvet, amiben rengeteg adat az amerikai védelmi minisztérium honlapjáról származott. Donald Rumsfeld védelmi miniszter elrendelte, hogy szűkítsék a honlapot, és szorítkozzanak minimális adatközlésre. Később kiderült, hogy a terrorisztikus szándékú hackkelések a legkülönbözőbb honlapokról szedik össze azokat a részinformációkat, amelyekből azután összerakják a képet. Kétségkívül lehetséges a legkülönbözőbb internetes helyekről leemelni olyan információkat, amelyek önmagukban véve ártalmatlanok, de kiadhatnak egy olyan egészet, amely igen veszélyes tudást adhat illetéktelen kezekbe.

Az Internet számos lehetőséget kínál propagandára és toborzásra is. Újszerű elem, hogy míg korábban propagandisztikus célra olyan filmeket gyártottak, amelyben mondjuk Oszama Bin Laden ül egy széken és egy kamerába monoton szónokol, mára a terroristák is rájöttek arra, hogy a fiatalokat jobban el lehet érni flashmobokkal, tehát műfajt váltottak, és a propagandisztikus üzeneteket szívesen csomagolják modernebb köntösbe, tarka animációkba. Használható az Internet felkészülésre is. Közismert, hogyan lehet szert tenni bombagyártásra alkalmas ismeretekre. Terrorista csoportok az internet segítségével tarthatják egymással a kapcsolatot, egyeztethetik stratégiai terveiket és egy-egy terrorista akció konkrét lépéseit. Az internetről letölthető és viszonylag könnyen kezelhető titkosító programok segítségével biztosíthatják, hogy kommunikációikhoz illetéktelenek ne férjenek hozzá. A titkosítás ismert megoldása az is, hogy a titkos információkat beépítik látszólag közömbös és ártalmatlan tartalmakba, például kódolt szövegrészekbe, képekbe vagy hangfájlok háttérzajába. Újszerű trend, hogy azokat a részleteket, amelyekből az üzenet összerakható, egymástól távol eső, közömbös és ártalmatlan tartalmakba rejtik.

A kibertér a terrorfinanszírozás szempontjából is kiaknázható. Csalás, bankkártya-feltörés és adománygyűjtés sajátos formáit dolgozták már ki. Például a Hezbollah, mint ismert, külön oldalt tart fenn, ahol különböző bújtatott csatornákon keresztül adományokat gyűjtenek. Az Európai Bizottság most dolgozik a terrorfinanszírozással kapcsolatos jelentésen, amely várhatóan jövőre kerül az Európai Parlament szakbizottsága elé. A kiberterrorizmus elméletileg lehetőséget nyújthat erőszakos támadás végrehatására is. A legnagyobb fenyegetést a kritikus infrastruktúrák, illetve a kritikus informatikai infrastruktúrák megtámadása jelenti.

Az Európai Parlamentben nemrégen készült erről jelentés, amelynek véleménykészítője voltam a szakbizottságom részéről. Engedjék meg, hogy idő híján csupán egy-két szempontot említsek meg, amelyet a véleménytervezetembe bevettem. Az egyik az interdiszciplináris megközelítés szükségessége. A védelem fontos területe a jogharmonizáció, az oktatás, különböző képzési tréningek, a gyengébben teljesítő tagországok felzárkóztatása, ami szoros együttműködést feltételez a az egyes területek között. A jelentés a kritikus infrastruktúrák meghatározásának befejezését sürgeti, ez ugyanis uniós szinten még nem történt meg. Kiemelném, hogy Magyarország már felállított egy tételes listát, amellyel élen jár a tagországok között. A magyar kormány megjelölte azokat a kritikus infrastruktúrákat, amelyekre az ország védelme érdekében különös figyelmet kell fordítani. Éspedig: energiaellátás, közművesíté, közlekedés, szállítás, távközlés, elektronikus adatforgalom, informatikai hálózat, bankrendszer, szolgáltatások, média, ivóvíz, élelmiszer alapellátás, egészségügyi biztosítás. A véleménytervezetben sürgettük a tagállamokat, hogy hozzák létre a maguk CERT-jét, amely még nincsen készen minden tagállamban. Sokáig nyitott kérdésként feküdt az Európai Parlament, az Európai Bizottság és a Tanács asztalán, hogy létrehozzunk-e egy önálló EU CERT-et, a nemzeti CERT-ek fölött.

Úgy tudom, hogy ezt végül elvetették, mivel a legtöbb tagország amellett van, hogy a nemzeti CERT-ek laza szövetségként működjenek együtt, de külön uniós ügynökséget helyezni föléjük nem indokolt. Javaslatot tettem a véleménytervezetben arra is, hogy a kritikus informatikai infrastruktúrák meghatározásába belefoglalhatnánk minden olyan rendszert, amely szenzitív személyes adatokat tartalmaz, például egészségügyi adatbázisok, stb. Kiemeltük a páneurópai gyakorlatok szükségességét is, illetve az egységes fenyegetés-értékelő rendszer mielőbbi létrehozását. Hangsúlyoztuk továbbá az állami és a magánszektor közötti együttműködés jelentőségét, legyen szó akár internetbiztonsági cégekről, szoftver vagy hardver készítőkről, online rendszerek üzemeltetőiről, hiszen a magánszektorra nagyon komoly szerep hárul a közös védelemben, mivel tudásban általában az állami szektor előtt jár. A magánszektort valahogyan rá kell bírni arra, hogy prioritásainak listáján a haszonszerzést sorolja kicsit hátrébb és a védelmet egy kicsit előbbre. Ehhez azonban hozzá kell tennünk valamit. A magánszektor képviselői részéről felmerül rendre az az igény, hogy a jogszabályok ne legyenek olyan szigoruak, hogy ha belépnek egy rendszerbe és ott veszélyt észlelnek, nyugodt lélekkel jelenthessék, ne kelljen attól félniük, hogy megvádolják őket azzal, hogy illetéktelenül léptek be valahova. Ez a szempont megfontolandó, ha ez az együttműködés ára.

A kiberbűnözés és szervezett bűnözés szerteágazó össszefüggéseit éppen csak érinthetjük itt. Tipikus formája a pénzmosás, a felül-alul számlázások, online aukciók, ahol túlfizetik, amit megvesznek. Vagy az online szerencsejáték, amelyen belül külön is megemlíthetők a karibi off-shore-okba áramló pénzek. Ma szervezett bűnözői csoportok felelősek az adatlopások 80-90 százalékáért. Riasztó mértékű az orosz és oroszajkú szervezett bűnözés térhódítása a kíberbűnözés terén. Az orosz és oroszajkú szervezett bűnözés, amelynek érdeklődési köre az ingatlan értékesítéstől, az illegális fegyverkereskedelmen át a műkincs-csempészetig sok mindenre kiterjed, mára élen

járnak a kibertér illegális használatában. Vírusok gyártásával és hálózatok akadályozásával zavarnak meg európai és amerikai weboldalakat. Ráadásul sokszor saját embereiket sikeresen beépítik kiszemelt cégekbe. Érdekes, ahogyan a kiberbűnözés szétrobbantotta, vagy legalábbis átalakította a bűnszervezetek organigramját, ismert maffia-felépítését. Amikor egy szervezett bűnözői kör már elsősorban hackerek láncolatát jelenti, már sem szükség, sem lehetőség nincs a személyes kapcsolatoknak arra a hagyományos, „kézcsókos" változatára, amelyet a Keresztapa című filmben megcsodálhattunk. Jeffrey Robinson, az orosz maffia szakértője szerint az orosz szervezett bűnözés legalább 50 országban megtelepedett, beleértve majdnem minden európai országot, azzal a nyilvánvaló szándékkal, hogy a világ egyik legnagyobb hatalmú érdekcsoportjává váljék. Ismert olyan eset is, amikor egy moszkvai internetes kávézóból törték fel nyugat-európai országok polgárainak bankkártyáit. Az orosz belügyminisztérium felmérése szerint 5006 bűnözői csoport mintegy százezer tagja vesz részt naponta az internetes bűnözésben. Ez megdöbbentő. Azok a szakértők, akiket Oroszországban és az orosz utódállamokban a szervezett bűnözői csoportok beszívnak magukhoz, többnyire igen magasan képzett hackerek, akik lehet, hogy puszta csínytevésként, vagy szórakozásként kezdik a hackelést, ami később főbb megélhetési forrásukká válik. Elemzők szerint szép számban akadnak közöttük olyanok is, akik a volt KGB vagy az FSZB leszerelt, vagy netán még mindig állományban lévő tagjai, az orosz titkosszolgálatok ilyen-olyan szereplői. Részvételük a kíberbűnözésben felveti a „kettős felhasználás" lehetőségét: az üzleti haszonszerzés összekapcsolását a hivatalos szervek részére végzett információszerzéssel.

Végezetül néhány megjegyzés a kiberbiztonság úniós szereplőiről. Az Európai Unió két legjelentősebb intézménye ebből a szempontból az ENISA és az EUROPOL. Az ENISA-ról Suba Ferenc beszámolója után nehéz volna mit hozzátenni, hisz ő avatott ismerője és tevőleges résztvevője is az Európai Információs és Hálózatbiztonsági Ügynökség munkájának. Az ENISA ügye nemrég került a parlament elé, és igen jelentős támogatást kapott szervezeti megújulásához. 2013-ra kell felállnia a Kiberbiztonsági Központnak, amelynek az EUROPOL lesz a gazdája. Erről korábban vita folyt, magam teljesen indokoltnak látom ezt a felállást, hiszen az EUROPOL rendkívül magas színvonalú kibervédelmi egységgel rendelkezik. Hadd utaljak például arra, milyen bravúros módon tártak fel egy 22 országra kiterjedő pedofil-hálózatot úgy, hogy többségében már kihűlt szálakon kellett elindulniuk a rekonstrukciós munkában. Megemlíteném még az Európai Védelmi Ügynökséget, ezen belül a Katonai Parancsnokságot (Military Staff), amely fontos szerepet tölt be a kibervédelem terén. A tavalyi évben megalakult az Európai Néppárt Kiberbiztonsági Tanácsadó Testülete, amelyben hárman vagyunk néppárti képviselők, egyébként európai és tengerentúli rendvédelmi vezetők és szakértők vesznek részt a munkában. Egy olyan konferenciával indítottunk, amely azt a kérdést járta körül, hogy „Kiberbiztonság. Felkészültek vagyunk-e a kiberbűnözés, a terrorizmus és hadviselés megelőzésére?" Az Európai Néppárt szándéka az, hogy a testület aktívan részt vegyen a kiberbiztonságot szolgáló együttműködés előmozdításában.

Zárásként engedjenek meg egy személyes megjegyzést. Azért is örültem annak, hogy az Európai Néppárt szakmai síkon kívánja kezelni a kiberbiztonságot, mert sajnos az Európai Parlamentben elég rossz tapasztalatokat szereztem a szakszerűség és a politikai marketing arányát illetően. Csüggesztő és kiábrándító, ahogyan a rendvédelmi témák vitái rendre emberi jogi show-műsorrá válnak. Ne értsenek félre, az adatvédelem és a személyiségi jogok védelme alapvető jelentőségű feladat. Az azonban elég kártékony, amikor egyoldalúvá, és a rendvédelmi erőfeszítéseket paranoid túlzásokkal megkérdőjelező propagandává silányítják, elsősorban a Parlament baloldalán. Célszerű volna, ha az Európai Parlament egészének a szemléletmódjában helyreállna a kívánatos egyensúly a biztonság (security) és az adatvédelem (privacy) szempontja között.

A MAGYAR JOGHATÓSÁG HATÁRAI A KIBERTÉRBEN, AZ ÜGYÉSZ SZEMSZÖGÉBŐL

Homonnai János

Az elmúlt kb. 15 évben a számítástechnika ugrásszerű fejlődése, elterjedése a nem informatikus végzettségű vagy foglalkozású felhasználók tömegei körében az életviszonyok gyökeres átalakulását hozta magával – az új kommunikációs lehetőségek, az online értékesítési csatornák, banki szolgáltatások igénybe vétele új világot nyitott meg mindenki előtt. A hálózatba kötött informatikai eszközök tömeges elterjedése, a hálózati kommunikáció térnyerése természetszerűleg a bűnözésben, valamint annak üldözésében és az igazságszolgáltatásban is leképeződött. A bűncselekmények elkövetőinek motívumai vagy céljai terén az informatikai fejlődés nem hozott változást, a büntető anyagi jog szabályai ezért nagyobb nehézség nélkül képesek követni a társadalmi szintű változásokat. Ugyanakkor a felhasznált eszközök és az alkalmazott módszerek, különösen azok államhatárokat nem ismerő jellegzetességei olyan kihívásokat állítanak a jogalkalmazók és különösen az eljárási jog elé, amelyeknek nem minden esetben képesek megfelelni.

Az elmúlt években többször is kellett rendőröknek és ügyészeknek választ keresnie olyan kérdésekre, hogy képesek-e igazságot szolgáltatni a sértettnek, akinek bankkártya-adatait internetes vásárlás során megszerezték, és külföldi vásárlásokra felhasználják? Mit tehet az, aki internetes aukción vásárolt és átverték? Mit tehet az, akinek banki adatait adathalászok szerezték meg? Számíthat-e védelemre, akinek banki adatait trójai révén szerezték meg? Reménykedhet-e az igazságszolgáltatásban, akinek számítógépe tönkrement egy vírus miatt, és elvesztek adatai? Tehet-e valamit, akinek feltörték a Facebook profilját? Remélhet-e hatékony intézkedést az a bíró vagy ügyész, akinek személyes adatait külföldi honlapon jogellenesen közzétették? Felelősségre vonható-e az, aki külföldről magyarországi weboldalt, adatközpontot célzott túlterheléses támadással megbénít? Magyarországon felelősségre vonható-e az, aki külföldről, másik külföldi államban számítástechnikai rendszert megbénít – pl. túlterheléses támadással?

A 2000-es évek előtt a kérdéseket a jogásztársadalom nagy többsége nem értette volna, mert nem ismert volna olyan szavakat, amiket ma legtöbben gond nélkül használunk: pl. adathalász, trójai, túlterheléses támadás, zombigép.

Mi a kibertér jogi szempontból?

Ugyanebben az időben a jelen előadás címe is valószínűleg értetlenséget váltott volna ki a magyar jogász – és más foglalkozású hallgatóság – köreiben. Nem csak azért, mert a kibertér fogalma akkor még szinte teljesen ismeretlen volt Magyarországon, hanem azért is, mert a büntetőjog keretei közt a joghatóság nem volt problematikus kérdéskör. Az 1990-es évek elejéig-közepéig egy ügyész leélhette úgy az életét, hogy a Büntető Törvénykönyv joghatóságra

vonatkozó 2. és 3. szakaszainak alkalmazásával soha nem kellett foglalkoznia, az ügyész elé kerülő ügyekben fel sem merült, hogy hiányozna a joghatóság az eljárás lefolytatására. Jól mutatja ezt az is, hogy a bírósági határozatok tára alig tartalmaz olyan döntéseket, amelyek a joghatóság kérdésével foglalkoznának, a joghatósággal kapcsolatban felmerült problémákat elemeznének. A rendelkezésre álló kevés döntés sem a joghatóság és a számítástechnikai bűnözés viszonyát taglalják, külföldi állampolgárságú elkövető külföldön elkövetett cselekményével foglalkozó döntés is csak kettő áll rendelkezésre: 2010-ből, és 1968-ból.

Míg a joghatóság kérdése legfeljebb közönyt, a kibertér említése értetlenséget váltott volna ki 15 évvel ezelőtt. A legtöbb ember számára ma sem teljesen világos, mi is az a kibertér. A kiberteret máshogy értelmezik a számítástechnikusok és a nem számítástechnikusok, a rendőrök, a katonák, a civilek, bárki, aki munkája vagy szórakozás révén számítógépes hálózatokkal kerül kapcsolatba. A kibertér értelmét torzítják a filmekben látott ábrázolások: bár a kibertér „tér" jellege egyértelműen metaforikus, valósága csupán virtuális, az emberi gondolkodásban valós térként jelenik meg, ahol egyik helyről a másikra lehet navigálni. A térbeli megjelenést elősegítik a nyelvi eszközök, ebben a térben navigálnak az emberek, akik egyik helyről a másikra mozognak, szörfölnek, ugranak és visszalépnek. A kibertérben – legalábbis szavakban – bűncselekményeket is el lehet követni, amelyeket a valós világ bűnügyi és igazságügyi hatóságai üldöznek, így teljesen logikusnak tűnik a következtetés, hogy a kibertérbeli bűncselekményekre a való világ hatóságainak van joghatósága. Ugyanakkor a kibertér nem tér, hanem egy olyan absztrakció, amellyel az elektronikus eszközök közti kommunikáció során keletkező adatfolyamot próbáljuk érthetővé, megfoghatóvá tenni. Szigorúan jogászi szemmel, senki nem él, mozog, bűnözik a kibertérben, hanem elektronikus eszközt használ, és adatokat küld más felhasználóknak vagy automatizált rendszereknek, illetve tőlük adatokat fogad. A kibertér tehát közvetítő közeg felhasználók és rendszerek között. Mint közvetítő közeg, számítógépes hálózat, a kibertér egyrészt közvetíti a bűncselekményeket, pontosabban az olyan tartalomközléseket, amelyek bűncselekmény elkövetési magatartásait képezik, másrészt a számítógépes hálózatok, a hálózatok fizikai valóságban létező elemei, a rajtuk közvetített utasítások révén, szoftverjeik manipulálásával maguk is lehetnek bűncselekmény célpontjai, elkövetési tárgyai.

Amikor kibertérbeli elkövetésről beszélünk, valójában nem az elkövetés helyére utalunk, hanem az elkövetés módjára. Az elkövetés hogyanjának kérdésére a válasz: számítástechnikai rendszer útján. Kérdés, hogy ha egy bűncselekmény elkövetése során ezt a közeget is felhasználják, az hatással van-e az államok büntető joghatóságára?

Függetlenül attól, hogy a kibertér kizárólag közvetítő közegként, vagy mint célpont is szerepet játszik-e egy bűncselekmény elkövetésében, a joghatóságot az elkövető fizikai térben betöltött helyzete, jogállása, valamint a cselekmény célpontjának, passzív alanyának vagy sértettjének, esetleg tárgyának fizikai helyzete és jogállása határozza meg.

Joghatóság fogalma, fajtái

A magyar jogban a külföldi vonatkozású ügyekben történő eljárás, a fogalmak és a joghatóságok ütközése részletekbe menő szabályozásának ugyan van hagyománya, azonban nem a büntetőjog, hanem a magánjog területén. A büntetőjogot, és így az ügyészt a közelmúltig elkerülték a joghatóság kérdései, és a joghatóság alatt a gyakorló ügyészek ma sem értenek

mást, mint eljárási jogosultságot, egyfajta országok közötti illetékességet. Minthogy ez az illetékesség szuverén államok igazságügyi szervei közti ügymegosztást jelent, a joghatóság nem csak eljárási jogosultságot, hanem eljárási képességet, hatalmat is magában foglal. A nemzetközi jogirodalom a joghatóságnak ezért több formáját is megkülönbözteti:

- A jogalkotási joghatóság alatt a szuverén államok azon képességét értik, hogy bizonyos cselekményeket, életviszonyokat, személyek jogállását jogszabályokkal rendezzék.
- Jogalkalmazási joghatóság alatt a szuverén államok azon képességét értik, hogy jogszabályaik megsértése esetén a jogsértő személyeket (legyenek akár természetes, akár jogi személyek) bírósági vagy közigazgatási eljárás alá vonják.
- Végrehajtási joghatóság annak képességét jelenti, hogy az állam jogszabályainak teljesítését kikényszerítse, megsértését pedig megbüntesse, bírói, közigazgatási vagy egyéb módon.

Általában a joghatóság mindhárom formája a területi elven alapul: egy állam azokat a cselekményeket, életviszonyokat képes szabályozni, amelyek fizikailag a területén történnek vagy helyezkednek el, azokat a személyeket képes felelősségre vonni, akik területén tartózkodnak és cselekszenek. A területi elv az államok szuverenitásán alapul, és az is következik belőle, hogy egy állam fizikai területén elkövetett cselekményre más állam elvileg nem terjeszthetné ki a joghatóságát.

A XX. és a XXI. század technológiai változásai, különösen a távközlés és a közlekedési hálózatok fejlődése azonban kikezdték a területi elv alapjait. Lehetővé vált, hogy az elkövető úgy kövessen el bűncselekményt egy másik ország területén tartózkodó sértett sérelmére, hogy az elkövetőnek el se kelljen hagynia saját országa területét.

A területi elvet áttörő joghatósági rendelkezések általában – kivételekkel persze – fenntartják a kettős inkrimináció követelményét: erre az állami szuverenitás csorbítatlansága miatt van szükség, a joghatóság kiterjesztése külföldi állampolgár külföldi cselekményére, amely saját országában nem büntetendő, elvileg a külföldi állam szuverenitását csorbítaná.

A területi elv

A számítástechnikai hálózatok sajátos tulajdonságai a területi elv kiterjedtebb alkalmazására nyitnak lehetőséget, az elkövetés helyének értelmezése lehetőséget ad a joghatóság bővítésére. Ahol van a számítógépes bűnözésre vonatkozó külön törvény, az elkövetés helyét értelmező rendelkezéseket lehet beépíteni. Ilyen törvényeket fogadtak el jellemzően az USA több tagállamában.

Például Arkansasban[1] vagy Észak-Carolinában[2] eljárás alá vonható az elkövető, ha a bűncselekményt képező adatátvitel az államba irányul, vagy onnan származik. A legszélsőségesebb szabályozásra Nyugat-Virginia[3] szolgáltat példát, ahol az állam joghatóságát olyan számítógépes bűncselekményekre is megállapították, amelyekben a bűncselekmény elkövetése során az adatok akár csak áthaladnak az állam számítógépes hálózatain.

1 Arkansas Code of 1987, A.C.A. § 5-27-606 (2012) Jurisdiction. http://www.lexisnexis.com/hottopics/arcode/Default.asp.
2 2010 North Carolina Code, Chapter 14 Criminal Law. Article 60 - Computer Related Crime. 14-453.2. Jurisdiction. http://law.justia.com/codes/north-carolina/2010/chapter14/article60/section14-4532/.
3 2011 West Virginia Code, Chapter 61. Crimes and their punishment, article 3c. West Virginia Computer Crime And Abuse Act. §61-3C-20. Personal jurisdiction. http://law.justia.com/codes/west-virginia/2011/chapter61/article3c/61-3c-20/.

Az Európa Tanács Számítógépes Bűnözés elleni Egyezménye (Budapesti Egyezmény) tartózkodik attól, hogy – egy rendelkezés kivételével – speciális joghatósági szabályokat állítson fel, a joghatóságról szóló 22. cikk előírásai alapján az egyezményben részes tagállamoknak az egyezmény szerinti bűncselekményekre olyan joghatósági szabályokat kell megállapítaniuk, amelyek gyakorlatilag megegyeznek az általános – területi és személyi elven alapuló – joghatósági szabályokkal. (Az egy kivételről még szó lesz.) Annak értelmezésében az egyezmény viszont nem segít, hogy melyek a területi elv alkalmazhatóságának szempontjai. Ebből a szempontból a németországi ügyészek vannak a legszerencsésebb helyzetben, mert a német büntető törvénykönyv[4] részletezi, hogy egy bűncselekményt mikor kell a területén elkövetettnek tekinteni, a magyar Btk. viszont nem ad ilyen mankót a jogalkalmazóknak.

A számítógépes hálózatokon elkövetett bűncselekmények esetén az elkövetés tényleges helyének meghatározása egyáltalán nem egyértelmű feladat. A hálózat útján közvetített jogsértő tartalom, például tiltott pornográf felvételek, vagy közösség elleni uszító tartalmak esetén az elkövetés helye lehet annak a számítógépnek az elhelyezkedése, ahonnan a tartalmat feltöltötték. De az elkövetés helyéhez nem tartozik hozzá az a szerver is, ahová a feltöltés történik? A tartalom közzététele ténylegesen csak akkor kezdődik meg, amikor a feltöltés befejeződött: lehetséges tehát, hogy a feltöltés eredete nem is számít, csak az, hogy hová irányul? Amellett is lehet ugyanakkor érvelni, hogy a bűncselekmény elkövetése megvalósul mindenhol, ahol a jogsértő tartalmat el lehet érni.

Még azokban az országokban is, ahol vannak a kiberbűnözés elleni törvények, és ezekben a törvényekben vannak specifikusabb joghatósági szabályok, értelmezési nehézségeket vet fel, hogy a cselekményt hol követték el. Azon kívül, hogy az elkövető ténylegesen hol fejti ki magatartását, hol visz be adatot a számítógépes hálózatba, egyéb tényezők is segíthetnek az elkövetés helyének meghatározásában:

A számítástechnikai eszközök helye

Mint már erre láthattunk példát, egyes államok jogszabályai már akkor is joghatóságot állapítanak meg, ha a területükön lévő számítástechnikai rendszerek akár csak közvetítőként érintettek az adatátvitelben. A cloud computing, a felhő alapú szolgáltatások terjedésére, a torrentezés elterjedtségére figyelemmel valóban előfordulhat, hogy külföldi elkövető külföldön elkövetett és külföldön kárt okozó cselekménye Magyarország érdekeit sérti azáltal, hogy magyarországi szerverek, számítóközpontok kapacitását köti le. Mindezekkel együtt, önmagában mint joghatósági ok, túlzó megoldásnak tűnik, nem beszélve a bizonyítással járó gyakorlati nehézségekről.

A cselekményben érintett személyek tartózkodásának helye

Egyes államok szabályozásában ennek is van szerepe. Például joghatóságot teremthet a sértett tartózkodási helye. A fizikai világban elkövetett cselekmények jelentős részét a sértett jelenlétében követik el. A kibertérben elkövetett cselekmények esetén azonban az elkövetés és a sértett helyének azonossága egyáltalán nem szükségszerű. Ésszerűnek tűnik ezért az olyan értelmezés, amely a sértett cselekménykori tartózkodási helyét is az elkövetés helyével

4 Strafgesetzbuch, § 9 Ort der Tat. http://www.gesetze-im-internet.de/stgb/__9.html.

azonosítja. Egy 2011-es bírósági határozat[5] szerint a magyar bíróság interneten elkövetett aukciós csalás esetén az illetékesség vizsgálata során elkövetés helyének tekintette azt a helyet is, ahol a sértett az elkövető által feltöltött ajánlatot megnyitotta. Ez a döntés a joghatóság megállapítása során is iránymutató lehet.

Különleges joghatósági ok a Budapesti Egyezményben az elkövető tartózkodási helye: ha az elkövető a tartózkodási helye szerinti államnak nem állampolgára, és ez az állam a cselekmény elkövetése helye szerinti államnak az állampolgárságára figyelemmel nem adja ki az elkövetőt, az elkövető tartózkodási helye szerinti államnak le kell folytatnia az eljárást. Például, ha egy állam olyan, a területén elkövetett bűncselekmény miatt kérné Magyarországtól saját állampolgárának kiadatását, amiért akár halálbüntetést is kiszabhatnának rá, a kiadatásra nincs lehetőség, de az eljárást e szabály alapján a magyar hatóságoknak le kell folytatniuk. Ezt az esetet lefedi a Büntető Törvénykönyv azon rendelkezése, mely szerint a magyar törvényt kell alkalmazni a nem magyar állampolgár által külföldön elkövetett cselekményre is, ha az a magyar törvény szerint bűncselekmény és az elkövetés helyének törvénye szerint is büntetendő. Mivel ilyen joghatósági ok esetén az eljárást a legfőbb ügyész rendeli el, az egyezmény kötelező rendelkezésére figyelemmel ezt az intézkedést a legfőbb ügyésznek feltétlenül meg kellene hoznia.

A hátrányos következmények helye

Elterjedt joghatóságot megalapozó körülmény, ha a külföldön, külföldi állampolgár által elkövetett bűncselekmény hátrányos hatásai belföldön jelentkeznek. A magyar bírói gyakorlat az eredmény bekövetkezésének helyét is az elkövetés helyének tekinti, ezt a bíróságok az illetékesség kapcsán hozott határozataiban egyértelműen kimondták. Nem minden bűncselekmény törvényi tényállása tartalmaz eredményt, valamilyen hátrányos következménye azonban minden bűncselekménynek van. Kérdés tehát, hogy az eredmény nélküli bűncselekmények hátrányos hatásainak Magyarországon történő jelentkezése megalapoz-e joghatóságot? A korábban már említett 1968-as döntésében[6] a Legfelsőbb Bíróság a területi joghatóság kapcsán kimondottan úgy foglalt állást, hogy a káros következmények bekövetkezésének helye is alkalmas a magyar büntető joghatóság megállapítására.

Bármilyen egyéb körülmény helye:

Néhány állam igen széles körben ható joghatósági okokat nevez meg törvényeiben: a már említett Nyugat-Virgina a hálózatain átmenő forgalom alapján is megállapítja joghatóságát, Malajzia a számítógépes bűncselekmények körében szinte korlátlanul eljárási jogosultságot teremtett magának, amikor úgy rendelkezett,[7] hogy az olyan számítógépes bűncselekményekre is kiterjed a joghatósága, amelyekben a használt eszközök, programok vagy adatok képesek Malajziában található számítógépekhez történő kapcsolódásra. Az internetprotokoll fő jellemzője, hogy használatával bármilyen számítástechnikai eszköz képes kapcsolódni másik számítástechnikai eszközzel, tehát Malajzia gyakorlatilag korlátlanul kiterjesztette kibertérbeli joghatóságát.

5 BH2011.322 I. Internetes hirdetéssel megvalósított csalás esetén az elkövetési magatartás – a megtévesztés – akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot.

6 BJD 4622

7 Art. 9(2) Malaysia Computer Crimes Act (1997). http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025630.pdf.

A személyi elv

A területi elv mellett, vagy azt követően, a személyi elv a joghatóság másik jelentős megalapozó tényezője.

Az elkövető állampolgársága

A Budapesti Egyezmény is kötelezővé teszi részesei számára, hogy az állampolgáraik által elkövetett cselekményeket üldözzék akkor is, ha területükön kívül követték el. Persze ez nem csak a számítógépes bűncselekményekre vonatkozik, ez az elv általánosságban is megalapítja az egyes államok büntető joghatóságát.

A sértett állampolgársága

Az elkövető mellett a sértett állampolgársága is megalapozhatja a joghatóságot. Ilyen, az ún. passzív személyi elven alapuló joghatósági okot tartalmaznak Németország[8] és Belgium jogszabályai. Az Egyesült Államokban (Computer Fraud and Abuse Act) joghatóságot teremt, ha a bűncselekmény a szövetségi kormányzatra is kihat, tehát ha maga az Amerikai Egyesült Államok a sértett. A passzív személyi elv érdekes alkalmazási lehetőségeket vet fel: országok üldözhetnek elkövetőket kizárólag azon az alapon, hogy a jogsértő tartalom (pl. gyűlöletbeszéd) állampolgáraik ellen irányul. Így akár a magyar hatóságok is eljárhatnak külföldi állampolgárok külföldi weboldalai miatt, amelyek magyar állampolgárok elleni erőszakra uszítanak – ilyenre ez elmúlt időszakban láthattunk valós példát. Erre még majd visszatérek két mondat erejéig.

A védelmi elv

Az elv alapján az állam joghatóságot gyakorol, amikor a határain túl elkövetett bűncselekmény az állam biztonságát vagy alapvető funkcióit fenyegeti. Ez a fajta joghatóság az államok szabályozásában általában megtalálható. Arra, hogy a védelmi elvet a kibertérben elkövetett bűncselekmények körére is ki lehet terjeszteni, példát az Amerikai Egyesült Államok szabályozása mutathat. A kormányzati számítógépek védelme érdekében 2001. évtől az ún. Patriot Acttal (Hazafias Törvény) a joghatóságot olyan, az USA területén kívül található számítógépekre is kiterjesztette, amely felhasználhatóak arra, hogy az USA államközi vagy külföldi kereskedelmét, kommunikációját befolyásolja. Sőt, szövetségi bűncselekménynek minősül, ha bárki olyan jelszavakkal kereskedik, amelyek kormányzati számítógépekbe való behatolást tesznek lehetővé.

Az egyetemlegesség elve

Bizonyos bűncselekmények üldözésére az államok univerzális kötelezettséget vállalnak, a számítógépes bűncselekmények azonban általában nem tartoznak ide. Belgium és Németország azonban egy tipikusan kibertéri cselekmény, a gyermekkorúakról készített pornográf felvételek forgalmazására kiterjesztette univerzális joghatóságát.

8 Strafgesetzbuch, § 7 Geltung für Auslandstaten in anderen Fällen. http://www.gesetze-im-internet.de/stgb/__7.html.

A jelenleg hatályos magyar törvény megjelöli az összes tényállást, amire a védelmi elv és az egyetemlegesség elve alkalmazható, ezek az állam és az emberiség elleni bűncselekmények. E bűncselekmények között vannak olyanok, amelyek felhívással vagy uszítással követhetők el, tehát a kibertérbeli elkövetési mód adja magát, például az alkotmányos rend erőszakos megváltoztatása előkészületét vagy a háborús uszítást manapság leginkább a kibertérben szokták elkövetni. Így ha két szomszédos, tőlünk távoli ország között a fegyveres konfliktus veszélye fennáll, esetleg be is következett, és olyan személy érkezik Magyarország területére, aki akár országában, akár kívülről a háborúra uszított blogjában, vagy weboldalán, ellene az eljárásra a magyar hatóságoknak lehetősége van.

Joghatósági szabályok

A magyar szabályozást nem kívánom részletesen ismertetni, az előbbiekben már utaltam rá, így most csak annyit említenék, hogy a Csemegi-kódextől napjainkig, a mai napon hatályos büntető törvénykönyvig nagyjából azonos módon, a területi elv, az aktív személyi elv (tehát az elkövető állampolgársága), a védelmi elv és az egyetemlegesség elve alapján állapítja meg a magyar joghatóságot. Külföldi elkövető külföldön elkövetett cselekményére a magyar joghatóság csak kettős büntethetőség esetén terjeszthető ki, ez alól kivételt a védelmi elv és az egyetemlegesség elve alapján tesz a törvény. Külföldi elkövető külföldön elkövetett cselekménye esetén azonban az eljárás Magyarország nemzetközi kapcsolatait érinti, ezért a büntetőeljárások megindításáról a legfőbb ügyésznek kell döntenie.

A büntető anyagi jogszabályok folyamatos közeledése ellenére előfordulhatnak olyan cselekmények, amikor a kettős inkrimináció feltétele nem áll fent: például vannak olyan országok, ahol a véleménynyilvánítás szabadsága erősebb annál az érdeknél, hogy valamely csoportok elleni uszítás, gyűlöletbeszéd, esetleg személyes adatok közzététele büntetendő legyen. Ha az elkövetők külföldi szerveren üzemeltetett honlapon magyar állampolgárok egy csoportja elleni gyűlöletre uszítanak, jelentős érdek fűződhet az eljárás lefolytatására, azonban kérdéses, hogy van-e erre a magyar állam szerveinek joghatósága. Ilyen esetben a területi elv fenti szempontok szerinti elemzése segíthet annak eldöntésében, hogy az uszítással okozott káros hatások, az uszítással érintett személyek vagy az adatközlés sértettjeinek lakó- vagy tartózkodási helye, esetleg a jogsértő tartalom Magyarországi számítástechnikai eszközökre történt letöltése megalapozza-e a részben belföldön történt elkövetést. Ilyen kérdésben eddig bírói döntés, érdemi jogértelmezés még nem született.

E körben kiegészítést hoz a szabályozásban a nemrég elfogadott új büntető törvénykönyvünk: A törvény a joghatósági rendelkezések között - a nemzetközi szerződésekben megjelenő tendenciára figyelemmel - újdonságként előírja a passzív személyi elvet. A passzív személyi elv lehetővé teszi azoknak a nem magyar állampolgároknak a büntetőjogi felelősségre vonását, akik külföldön magyar állampolgár vagy jogi személy, illetve egyéb jogalany sérelmére követnek el bűncselekményt, cselekményük azonban az elkövetés helyének joga szerint nem büntetendő. Az egyéb jogalany fogalma még értelmezésre szorul, de az előbb felvázolt esetben megalapozhatja a joghatóságot. Az ilyen cselekmények nemzetközi jellege miatt azonban az eljárás ebben az esetben is csak a legfőbb ügyész döntése alapján indítható meg.

Joghatóság és bizonyítás – a jogalkalmazási joghatóság korlátai

Látható, hogy ha bűnügyi érdek, akarat ezt kívánja, a jelenleg hatályos, de különösen a 2013. júliusától hatályos Btk. alapján a külföldi vonatkozású cselekmények igen széles köre magyar joghatóság alá vonható, a magyar joghatóságot a kibertérben szinte csak a szándék korlátozza, feltéve hogy a cselekménynek van valamilyen magyarországi hatása. Ez azonban joghatóságnak csak a jogalkotási része.

A joghatóság, mint már utaltam rá, képesség és hatalom kérdése is, ezért meg kell vizsgálni, hogy a jogalkotás által létrehozott szabályozás mennyire áll összhangban a valós jogalkalmazási joghatósággal.

Ahhoz, hogy egy büntetőeljárást eredményesen le lehessen folytatni, két dolognak kell rendelkezésre állnia: terheltnek, és az ellene szóló bizonyítékoknak. Amikor a cselekményt Magyarországon követik el vagy magyar állampolgár követi el, a terhelt jelenlétének biztosítására általában bejáratott eszközök állnak rendelkezésre. Más a helyzet, ha külföldi állampolgár által külföldön elkövetett cselekmény esetében kerül megállapításra, hogy a cselekményre a magyar törvény alkalmazható, és az eljárás megindításának feltételei fennállnak. Két eset lehetséges: az elkövető kiadatásának kérése, vagy az eljárásnak a terhelt távollétében történő lefolytatása. A kiadatásnak feltétele a kettős inkrimináció. Mint már említettem, a büntető anyagi jogszabályok közeledése miatt egyre kisebb az esély, hogy ez a feltétel hiányzik: a számítástechnikai rendszereket célzó cselekmények szinte minden országban büntetendők, ugyanakkor a jogsértő tartalom miatt indult eljárásokban előfordulhat, hogy a magyar megkereséseket a kettős büntethetőség hiányában nem teljesítik. Ha mégis megállapítható a magyar joghatóság, a kiadatás zátonyra futása esetén lehetőség nyílik a terhelt távollétében történő eljárásra.

Ekkor azonban a nyomozó hatóság, az ügyész és a bíró újabb problémával szembesül: bár a Btk. joghatósági szabályai lehetővé teszik az eljárás lefolytatását, a büntetőeljárási szabályok nem teszik lehetővé, vagy ha úgy tetszik, nem adnak joghatóságot a bizonyítékok beszerzésére.

Azt, hogy milyen különbségek lehetnek egyes államok valós jogalkalmazási képességei között, legjobban egy a való életből vett példán lehet bemutatni. Két orosz hacker számlájára néhány igen jelentős kiberbűncselekményt rótt az FBI. Vaszilij Gorshkovot és társát azzal gyanúsították, hogy több mint 40 amerikai nagyvállalat számítógépes rendszerét törték fel, pénzügyi adatokat szereztek meg, behatoltak két bank rendszerébe, százezres nagyságrendben hitelkártya-adatokat loptak a Western Uniontól és más cégektől, a PayPalnél hamis hitelkártya adatokkal próbáltak fizetni. Az FBI a két orosz hackert csapdába csalta: egy fiktív, hálózati biztonságtechnikával foglalkozó cég nevében állásinterjúra hívták őket az Amerikai Egyesült Államokba, majd az interjún arra kérték őket, demonstrálják képességeiket. Ehhez preparált, minden billentyűzetleütést rögzítő laptopokat adtak nekik, ők pedig óvatlanul beléptek saját, oroszországi számítógépeikre, és hackeléshez használt programokat töltöttek le. Közvetlenül ezután került sor a letartóztatásukra, majd az FBI a hackerek kifürkészett belépési jelszavait felhasználva bizonyítékként lementette távoli számítógépük adattartalmát. Az eljárás során a védelem természetesen a bizonyítékok beszerzésének, a terheltek számítógépének átkutatását és az adatok lefoglalásának törvényességét is vitatta: megsértették a terheltek alkotmányos jogait, amikor titokban

beszerzett jelszavak révén indokolatlan kutatás tartottak, a kutatáshoz nem állt rendelkezésre bírói felhatalmazás, és nem utolsó sorban azért is jogszerűtlen volt, mert az orosz törvényeket is megsértette. A bíróság a védelmi kifogásokat elutasította: a számítógépekbe való belépést nem tekintette az amerikai eljárásjog szerinti kutatásnak, sőt, úgy tartotta, hogy a számítógépek nem is tartoznak amerikai joghatóság alá, mivel külföldi állampolgár külföldön lévő tulajdonát képezték. Ugyanakkor a bíróság nem tartotta relevánsnak az orosz jogszabályok megsértésére vonatkozó érvelést, mivel az amerikai nyomozó hatóság nyomozati cselekményeire az orosz jog szerinte nem vonatkozik. A bíróság a terheltet végül elítélte. Mindazonáltal a bizonyítékok beszerzése ezen módjának törvényessége még Amerikában sem egyértelmű, egyes vélemények szerint az FBI cselekménye egyértelműen sértette Oroszország szuverenitását. Az orosz hatóságok ezzel annyira egyet is értettek, hogy a nyomozást vezető FBI ügynök ellen büntetőeljárást is indítottak számítástechnikai rendszer elleni bűncselekmény miatt. A középutas vélemények szerint a területen kívüli számítástechnikai adatok a büntetőeljárásban felhasználhatók, ha az adat nyilvánosan hozzáférhető, védett adatok esetén azonban a lefoglalás az adat fizikai elhelyezkedése szerinti állam szuverenitását sérti, kivéve ha ehhez az adott állam hozzájárul. A Budapesti Egyezmény 32. cikkelye egyébként ezt a középutas megoldást alkalmazza.

Mi lenne a helyzet hasonló esetben egy magyarországi eljárásban? A magyar büntető joghatóság alá tartozó ügyekben az eljárást a Be. szerint kell lefolytatni. Jelenti-e ez azt, hogy a Be. alapján olyan bizonyítékokat képes beszerezni a magyar hatóság, amelyek fizikailag nincsenek az ország területén? A Be. hatályra vonatkozó rendelkezései a törvény területi hatályát nem állapítja meg, elméletileg tehát elképzelhető, hogy Magyarország határain kívül végzett nyomozati cselekmény a Be. szabályai szerint történjen. Mégis az a véleményem, hogy a bíróság előtt aggályos lenne olyan bizonyíték felhasználása, amit más ország területéről, szuverenitásának megsértésével, jogsegélykérelem nélkül szerez be az ügyész. Bár büntetőeljárási törvényünk viszonylag új, a bizonyítékok rendszerének megalkotásánál a kodifikálók még nem vették figyelembe azt a lehetőséget, hogy a nyomozó hatóság az ország területéről, mintegy kezét átnyújtva a határon, más országból szerezhet be bizonyítékot.

Kibertérbeli bűncselekményeket általában digitális bizonyítékokkal – dokumentumokkal, metaadatokkal, log fájlokkal, digitális okiratokkal – lehet bizonyítani. Ezt a fogalmat, azonban a Be. nem ismeri, a bizonyítási eszközök között nem sorolja fel, illetve önmagában az adat, mint bizonyítási eszköz jogi sorsa bizonytalan. Az adat önmagában nincs felsorolva a bizonyítási eszközök között, a törvény csak más, a fizikai világban megjelenő bizonyítékhoz kötve ismeri: tárgyi bizonyítási eszköz minden olyan tárgy, ami műszaki eljárással adatokat rögzít. Ez alapján úgy tűnik, hogy az adat csak annak hordozójával együtt bizonyítási eszköz, ezért amikor számítástechnikai eszköz használatával elkövetett bűncselekményt próbálunk bizonyítani, magát a számítógépet, vagy annak az adathordozóját kell lefoglalni. Ha az adat Magyarország határain kívül van, a szokásos eljárás szerint az azt hordozó eszközt nem lehet lefoglalni.

Mindezek arra utalnak, hogy az FBI által alkalmazott trükköt, vagy más olyan eljárást, amellyel egy külföldi számítástechnikai rendszerből a külföldi állam jogsegélye nélkül bizonyítási adatot vonnak ki, Magyarországon nem lehetne törvényesen alkalmazni. Sőt, még a Budapesti Egyezmény 32. cikke alapján nyilvánosan elérhető számítástechnikai adat bizonyítékként való felhasználása is problémákat vet fel: a Be. bizonyítási eszközeivel és eljárásaival

hogyan lehet rögzíteni egy külföldi számítástechnikai rendszer adatait úgy, hogy a létrejövő bizonyíték megfeleljen a hitelesség és a változatlanság követelményének?

Hadd világítsam meg jobban egy példával: nemrég zárult le jogerősen, felmentéssel, annak a vádlottnak az ügye, akit azzal vádolt az ügyészség, hogy külföldi szervereken működtetett szélsőséges honlapon közzétett írásaiban az alkotmányos rend erőszakos megdöntésére hívott fel. A felmentés oka nem a bizonyítékokkal függött össze, a tényállást – az írások közzétételét – a vádlott nem tagadta. Pedig a vádlott ténybeli tagadása esetén a vádhatóság nehéz helyzetben lett volna: a felhívásokat a nyomozó hatóság egy böngészőből kinyomtatta, valamint a weboldalak tartalmát le is mentette. Jobban belegondolva, a bizonyítékok ebben a formában a hitelesség és változatlanság kritériumát nem elégítették ki, a puszta nyomatokkal, valamint a html fájlokkal a vádlott tagadása esetén nem lehetett volna bizonyítani, hogy a vád szerinti tartalom valóban a vádban megjelölt időben, weboldalon megjelent, és a nagy nyilvánosság számára olvasható volt. A helyes eljárás valószínűleg az lett volna, ha szakértő úgy tölti le a jogsértőnek vélt tartalmat, hogy az adatok a tartalommal együtt tartalmazzák a letöltött oldal domain nevét, annak IP címét, a letöltés idejét, és az adatokat így együtt, megváltoztathatatlan formában rögzítik. Az előbbihez hasonló esetben, ha a terhelt még azt is vitatja, hogy a jogsértő tartalom megjelent az Interneten, egy egyszerű nyomat vagy oldalmentés a megjelenés körülményeit hitelesen nem tartalmazza.

A joghatóság valós korlátai a kibertérben

Az előzőekben elmondottakkal nem a számítástechnikai bűncselekmények bizonyításának problematikájába kívántam belemerülni. Csak arra szerettem volna rámutatni, hogy az anyagi jog hiába teremti meg a szabályozás szintjén a joghatóságot, ha az eljárásjog nincs vele szinkronban, és a jogalkotási joghatóság nem esik egybe az jogalkalmazási és végrehajtási joghatósággal. Míg szabályozás szintjén a joghatóságot ki lehet terjeszteni szinte bármire – lásd Malajzia – és a joghatóságot megalapozó elvek alapján szerteágazó szabályokat lehet létrehozni, a jogalkalmazás és a kikényszerítés képessége jóval korlátozottabb. Mindenféle integráció és harmonizáció ellenére továbbra is a szuverén országok korában élünk, ahol még mindig a területi elv határozza meg az eljárás képességét, annak ellenére, hogy a kibertér az államhatárokat – legalábbis bizonyos bűncselekménytípusok esetén – gyakorlatilag eltüntette. Vannak olyan jogrendszerek, amelyek a cél érdekében a területi elvet a bizonyítékok beszerzése érdekében is áttörik, ezzel azonban a többi érintett ország tiltakozását váltják, válthatják ki.

Egy mondatban összefoglalva tehát a címben jelzett határokat: ügyészi szempontból a joghatóság határait mindig is az ügy bizonyításának gyakorlati korlátai vonták meg, és nem az anyagi szabályozás szűkre szabottsága, a joghatóságot a kibertérben tehát nem annyira az anyagi jogszabályok, mint inkább a kibertér gyors fejlődésétől lemaradt eljárási szabályok hiányosságai korlátozzák.

IRODALOMJEGYZÉK

Fekete László (2002): Szabadság, jog és szabályozás a kibertérben. In: *Replika,* 47–48. sz. Forrás: http://www.c3.hu/scripta/scripta0/replika/honlap/47/Fekete.pdf

Peszleg Tibor (2010): A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. In: *Ügyészek Lapja*, 2. szám

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ 2011. II. negyedéves jelentés. Forrás: http://www.cert-hungary.hu/sites/default/files/news/cert_2011_quart_2.pdf

Susan W. Brenner & Bert-Jaap Koops (2004): *Approaches to Cybercrime Jurisdiction.* 4 J. High Tech. L. 1 Forrás: http://www.jhtl.org/docs/pdf/JHTL_Brenner_Koops_Article1.pdf

Szabó Imre (2003): Internetes bűncselekmények, különös tekintettel az internetes csalásra In Dr. Kiss Daisy szerk.: *E-akták. Tanulmányok az internetjog világából.* (Studia Collegii De Stephano Bibo Nominati) Bibó István Szakkollégium Internetjogi Kutatócsoport, Budapest.

AZ ELLÁTÁSI LÁNCOK BIZTONSÁGA[1]

Horváth Attila

Az ellátási láncok biztonsága és a kritikus infrastruktúra védelem kapcsolatáról ma még lehetetlen úgy egy cikket közölni, ha a szerző nem értelmezi a két fogalom tartalmi megközelítéseit. Napjainkra a pénzpiaci, termelési, elosztási és kereskedelmi folyamatok olyan mértékben váltak nemzetközivé, amely korábban elképzelhetetlen volt. Ezzel párhuzamosan ment végbe az ún. reálgazdaságban a beszerzés, a termelés, az elosztási és értékesítési rendszerek diszlokációjának decentralizálása. Az állítás igazságtartalmát kétségbevonók számára egy nagyon egyszerű empirikus módszert lehet ajánlani. Csak azt kell megfigyelniük, hogy az általuk viselt ruhák, vagy használt tárgyak hány százalékát gyártották a távol-keleten? Ez a korábban példátlan integráció nem mehetett volna végbe – felsorolás a teljességre törekvést mellőzi H.A. – a gyártási- szállítási technológiák, logisztikai módszerek, az informatika, stb. fejlődése nélkül. Az új gazdasági trendek elterjedése, a megváltozott fogyasztási szokások és a technológiai fejlődés szükségessé tették az ún. ellátási lánc menedzsment szemlélet elterjedését.[2]

Az ellátási lánc fogalmának meghatározásakor hasonló sokszínűséggel találja szembe magát az a szakember vagy érdeklődő, aki nem elégszik meg egy meghatározás igazságtartalmával, mint a biztonsággal, a logisztikával és a terrorizmussal kapcsolatban. Az alapos kutató ilyen esetekben azzal szembesül, hogy egy-egy fogalommal kapcsolatban a nemzetközi és hazai szakirodalom akár több mint száz, tudományosan is értékelhető meghatározást ismer, és használ. Az ellátási lánccal összefüggő meghatározásokban közös jellemzőként értelmezhető, hogy mindegyikben megjelenik az anyag és információáramlással kapcsolatos szemlélet.[3] Egy állátási láncon belül három fő szakaszon keresztül zajlanak a különböző folyamatok ezek: a beszerzés, a gyártás és a vevők kiszolgálása.[4] Nem kell logisztikai szakembernek lenni ahhoz, hogy valaki elképzelje: egy Európában vagy az Egyesült Államokban fejlesztett, ezekről a helyekről anyagokat felhasználó Kínában gyártott termék, a világ szinte minden pontján megvásárolható legyen, ahhoz az együttműködés megszervezésére nagy hangsúlyt kell fektetni. Egy ilyen bonyolult hálózati rendszerben a kooperáció keretei szükségszerűen át kell, hogy lépjék a hagyományos vállalati- szervezeti kereteket.[5] Az ellátási láncok működése nélkül a globális gazdaság működése elképzelhetetlen lenne. A politikai, gazdasági, pénzügyi kulturális stb. értelemben vett globalizáció elsődleges hatásai, megítélése és megközelítése a nyílt támogatástól az erőszakba hajló radikális elutasításig tarthat. Az ellátási láncok működése egyike azoknak

1 A cikk elkészítésével kapcsolatos kutatást a „Kritikus Infrastruktúra Védelmi Kutatások" TÁMOP-4.2.1.B-11/2/KMR/001 számú projekt támogatta.

2 Knoll Imre: Logisztika-gazdaság-társadalom. Kovásznai Kiadó. Budapest, 2002. pp. 12-16.

3 Szegedi Zoltán: Ellátási lánc-menedzsment. Kossuth Kiadó, Budapest, 2012. pp. 8-12

4 Bowersox Donald J., Closs David J., Cooper M. Bixby, Bowersox John C.: Supplay Chain Logistics Managament. Fourth Edition. Mcgraw-Hill International Edition, New York, 2013. pp. 42-51 p.

5 Szegedi Zoltán, Prenzenszki József: Logisztikai menedzsment. Budapest, Kossuth Kiadó. Harmadik Kiadás. Budapest, 2005. pp. 17-42.

a globalizációs „velejáróknak”, amelyeket a jelenség belső logikája hozott létre és tart fenn, a „káros hatásai” elleni védekezés leginkább úgy eredményes, ha igazodunk a működési mechanizmusához és kihasználjuk az általa nyújtott lehetőségeket. Magyarországon erre leginkább a földrajzi fekvésből adódó kedvező logisztikai adottságok kihasználásával lenne és van mód.

A kritikus infrastruktúra védelem

Az ellátási lánchoz hasonlóan sokat használt és nagyon eltérő módon megközelített kérdéskör a kritikus infrastruktúra védelem. A fogalmi meghatározás és a hosszadalmas fejlődéstörténet helyett ebben a cikkben csak a lényegi értelmezésre van mód, illetve arra, hogy felvázoljuk, hol tart a szabályozás napjainkban Magyarországon. A kritikus infrastruktúra védelem fogalma és módszere az Egyesült Államokból terjedt el, és vált ismertté szerte a világon. Hiba lenne azonban azt gondolni, hogy a történelem folyamán korábban az államok nem foglalkoztak pl. az energiabiztonsággal, a közlekedési hálózatok használhatóságával. Az új típusú megközelítés azért vált szükségessé, mert egyrészt a bipoláris világrendszer felbomlása a korábban kontrol alatt tartott veszélyforrások felerősödését eredményezte (pl. terrorizmus), másrészt a technológia fejlődése az infrastrukturális rendszerek egymástól és a telekommunikációtól való függőségét felerősítette.

A kockázatok felismerését tényleges tettek, egy új szemléletű, komplex módon alkalmazott biztonsági módszer és rendszer bevezetése az Egyesült Államokban következett be. Szakmai vita van arról, mi volt az elsődleges oka annak, hogy Bill Clinton elnök 1998. május 22-én kiadta a kritikus infrastruktúra védelemét szabályzó 63. számú elnöki direktívát. Az elkészítő munkáról készült összefoglaló szerint a létfontosságú rendszerek és létesítmények védelmét főként azért kellett újragondolni, mert az egymással összekapcsolódó infrastruktúra-szektorok egyre sérülékenyebbé váltak, és ráadásul az irányításukat és a vezérlésüket is az infokommunikációs eszközökkel oldották már meg.[6] Más szakértői vélemények szerint a szemléletváltást a terrorfenyegetettség egyre növekvő szintje tette szükségessé.[7] Az „igazságot” valószínűleg a két álláspont között lehet megállapítani: a kritikus infrastruktúra védelem szemléletének és módszerének bevezetését valószínűleg az Egyesült Államokban 1990-es években bekövetkező természeti és civilizációs katasztrófa események, üzemzavarok, a külső és belső terrorizmus veszélyének növekedése egyaránt okozta.

A rendszer kiépülését a 2001. szeptember 11-ei stratégiai jelentőségű terrortámadás-sorozat felgyorsította, illetve módosította. A módosítás a törvényi szabályzástól az intézményrendszer gyökeres változását eredményezte. A már említett terjedelmi korlátok nem teszik lehetővé, hogy az amerikai és európai szabályozás változásait és az intézményi háttér fejlődését egy részletes elemzésnek vessem alá, egy dolog kijelentése megkerülhetetlen: az Európai Unió csak hosszadalmas késedelem után kezdte meg a kritikus infrastruktúra védelemmel kapcsolatos szabályozást.[8] A tagállami egyeztetések mellett a lassú Európai Uniós döntéshozatali mechanizmus sem segítette a megváltozott biztonsági szemlélet és módszer elterjedését. Az értékelhető lépések bekövetkezését a 2004. március 11-ei madridi és a 2005. július 7-ei londoni robbantás-sorozat is kikényszerítette, a két eseménynek nyilvánvalóan hatása volt az első értékelhető Zöld Könyv megfogalmazásáig (2005) és a közösségi szabályok, együttműködési keretek elfogadásáig. Az elvi kérdések elfogadása után a két terrortámadás sokkoló hatása ellenére évekbe telt a közösségi szintű szabályozás kidolgozása, elfogadása és összehangolása. Sokak véleménye szerint, hasznosabb lett volna a kritikus infrastruktúra európai értelmezését megadni és a 2001. szeptember 11-ei terrortámadás-sorozatot követően létfontosságú rendszerekben, létesítményekben és az általuk nyújtott szolgáltatásokban gondolkodni.[9] Egészen biztos, egy értelmezett rendszer bevezetésének szükségességét sokkal könnyebben értelmezett volna a média, és ez által a közvélemény is.

Magyarországon a kritikus infrastruktúra védelem értelmezésével, bevezetésének feladataival az Európai Unióhoz való csatlakozást követően kezdtek foglalkozni. Mind az értelmezés, mind a szabályozás követte a közösségi trendeket. A szabályozás nem maradt el az EU átlagától, annak ellenére sem, hogy a területnek igazából 2010-et követően lett valóban értelmezhető koordinátora az Országos Katasztrófavédelmi Főigazgatóság. Több kormányrendeletet követően a problémakör kezelését az Országgyűlés egy 2012. november 12-én elfogadott törvényben szabályozta, amely szerint a létfontosságú rendszereknek és létesítményeknek (kritikus infrastruktúráknak) az alábbi ágazatai vannak:

1. energetika,
2. közlekedés,
3. agrárgazdaság,
4. egészségügy,
5. pénzügy,
6. ipar,
7. infokommunikációs technológiák,
8. víz,
9. jogrend-kormányzat,
10. közbiztonság-védelem.[10]

A 10 ágazathoz összességében 48 alágazat tartozik. Klasszikus értelemben az ellátási lánc biztonságával összefüggő kérdések a közlekedési ágazathoz tartoznak. A törvényhozó, igazodva a nemzetközi trendekhez, ehhez a szektorhoz sorolta be a közlekedési alágázatokat (közúti, vasúti, vízi és légi) a logisztikai központokat. [11]

Kölcsönhatások, kockázatok, veszélyek az ellátási láncokban

Amennyiben a kritikus infrastruktúra védelmet a biztonság új értelmezése megnyilvánulásaként fogjuk fel, akkor rögtön hozzá kell tenni, hogy a kockázatok a veszélyek elemzését, a rendkívüli helyzetek kezelését az esetlegesen keletkezett károk elhárítását csak rendszerszemlélettel lehet elvégezni. Egy ágazatot vagy egy alágázatot elemezni és vizsgálni nem elég-

6 PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES: PDD 63. URL cím: https://www.hsdl.org/?view&did=456517. p 14.

7 Murray T. Alan-Grubesic H.Tony: Overview of Reliability and Vulnerability in Critical Infrastucture. In.: Murray T. Alan–Grubesic H.Tony (eds). Critical Infrasturcture. Reliability and Vulnerability. Springer-Verlag. Berlin, Heidelberg, New York, 2007. pp. 1–8.

8 Erről a kérdésről lásd bővebben: Bonnyai, Tünde: A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása. Tanulmány, Budapest, 2011. URL cím: http://vedelem.hu/letoltes/tanulmany/tan382.pdf p.61. Horváth, Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 35. p.

9 Horváth Attila: i.m. (2013).

10 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

11 Uo. A kritikus infrastruktúra védelem szempontjából a csővezetékes szállítás sokkal inkább tartozik az energetikához és a vízügyi kérdésekhez.

séges. Erre azért van szükség, mert a biztonság komplex értelmezésének eredményei csak abban az esetben érezhetők, ha a rendkívüli események kezelésére történő felkészülés során, illetve az esetlegesen bekövetkező krízishelyzetek megoldásában figyelembe vesszük az egyes területek, szektorok közötti kölcsönhatásokat, függőségeket, idegen kifejezéssel élve interdependenciákat. Természetesen minden szektor sajátos jellemzőkkel bír, de az egyes rendszerek összekötetésben állnak egymással, ezért pl. egy tartós áramszünet következményei túlmutatnak az energetikai szolgáltatókon.[12] Az elektromos áram szolgáltatásának zavara mellett még számos olyan működési zavart is megnevezhetünk, amely más kritikus infrastruktúra ágazatban vagy alázatban okoz súlyos fennakadásokat. Az ellátási láncok folyamatos és megbízható működését olyan területnek tekinthetjük, amelynek nagy a kitettsége egy másik kritikusnak tekinthető szektortól vagy alágazattól.

Az ellátási lánc biztonsága szempontjából a cél nem lehet más, mint a folyamatos működés fenntartása. Ennek érdekében meg kell előzni az olyan rendkívüli eseményeket, amelyek az anyag és információáramlási folyamatokat megtörik. A kockázatok felmérésére és a veszélyek értékelésére komoly matematikai alapokon nyugvó módszerek állnak rendelkezésre. Azonban a 2001. szeptember 11-ei terrortámadás-sorozatot követően elvégzett amerikai elemzések arra hívják fel a figyelmet, hogy olyan tényezőket is figyelembe kell venni, mint a vallási, kulturális, nyelvi különbségek, sajátosságok vagy akár az üzleti szokások.[13] A szakértők elemzéseiből az következik, hogy a matematikai modellek felállításánál olyan minőségi tényezőket kell kijelölni, amelyek alkalmasak a pontos kvantitatív elemzés elvégzésére, és az eredmények hasznosítására.[14]

A kockázati tényezők számbavételének számos megközelítése létezik, egymás mellett több elfogadható csoportosítást is hasznosíthatunk. Az ellátási láncok valós kockázati tényezők csoportosítására talán a legjobb módszerként kínálkozik egy, az Egyesült Államokban a közelmúltban elterjedt szempontrendszer. Az utóbbi években szakítottak azzal a gyakorlattal, hogy a kockázati tényezőket kiváltó okokra koncentráljanak. Együtt kezelik a várható hatásokat és a kiváltó okokat, így az alábbi veszélyforrásokat különböztetik meg:

- fizikai kockázatok;
- kiber kockázatok;
- humán kockázatok.[15]

Ez a módszer bevezetése alkalmas arra, hogy nem a különböző tényezők közti rangsorolásra, hanem a valós veszélyforrások felbecsülésére szorítkozzanak. A veszélyek és a kockázatok számbavételénél abból kell kiindulni, hogy az ellátási láncok meglehetősen sokszereplős, és sok tényezős rendszert alkotnak. Ennél fogva a sérülékenységük is sok változótól függ, a biztonságot csak az ellátási lánc teljes egészében lehet értelmezni, amely a nyersanyag kitermelőhelytől, a felhasználásig, illetve az újrahasznosításig tart. Ugyanakkor a nagy térbeli különbségek miatt eltérő kockázatokkal kell számolni akár egy ellátási láncon belül a távol-keleten, a nyugat-európai kikötőkben vagy a közép-európai logisztikai szolgáltató központokban.

12 Horváth, Attila: i.m. (2013).
13 Cook, Thomas A.: Global Sourcing Logictics. How to Manage Risk and Gain Competitive. Published by Advantege in a Worlwide Marketplace American Management Association. 2007. New York. pp. 8-15.
14 Horváth, Attila: Mi indokolja az ellátási lánc biztonságával kapcsolatos kutatásokat?In: Réger Mihály (szerk.) International Engineering Symposium at Bánki (IESB 2012) Bánki Kari Tudományos Konferencia Kiadvány, Budapest, 2012. pp. 1-13.
15 Tranportation Systems. Critical Infrastructure and Key Resources Sector-Specific Plan as input the National Infrastructure Plan. Department of Homeland Security, Arlington, 2007. 288 p.

A kockázatok újszerű amerikai megközelítése olyan szempontból is hasznosnak tekinthető, hogy megtörte a terrorizmus primátusát, amelyet a közlekedési és logisztikai szektorban elsősorban a közösségi közlekedésben lehetett értelmezni. Az ellátási láncok nemzetközi gazdasági szerepének felértékelődése következtében, a jövőbeni számolni kell az áruszállítási rendszerek esetleges kockázataival is.[16] Ezt a veszélyt még akkor is komolyan kell venni, ha a terrorizmus eddigi történetében a logisztikai létesítmények, áruszállító járművek elleni támadások nem voltak túl gyakoriak. A kockázat realitására a kalózkodás által okozott károk, az áruszállító hajók elleni támadások visszaszorítása érdekében tett erőfeszítések kellőképpen felhívják a figyelmet.[17] Ugyanakkor fontos követelményként jelenik meg a kockázatok folyamatos elemzése, a lehetséges veszélyforrások figyelembe vételével, globális, kontinentális, regionális és a lokális tér sajátosságainak megfelelően.

Csak logisztikai kérdés az ellátási láncok biztonsága?

Az alcímben feltett kérdés egyrészt költői, hiszen egy, a biztonsági tanulmányokban és a logisztikai eljárásokban jártasságot szerző hallgatónak is tudni kell a választ, másrészt mégis fontos alaposabban indokolni a választ, mert igazán csak ekkor tudjuk bizonyítani, milyen súlyú kérdésről van szó. Szándékosan nem a terrorizmus oldaláról keresve a példát, holott ma már tudjuk, hogy a 2001. szeptember 11-ei terrortámadás napokra megbénította az Egyesült Államok repülőtereinek és tengeri kikötőinek forgalmát.[18]

Egy lokális térben keletkezett természeti katasztrófa akár globálisan értelmezhető zavarokat képes okozni. A 2010-es izlandi vulkánkitörés, illetve 2011-ben egy földrengés, és az azt követő szökőár, a fukusimai atomerőmű katasztrófája. A vulkánkitörés hetekre lebénította az észak-európai légiközlekedést, amely nemcsak az utasforgalomra, hanem a légi áruszállításra is súlyos hatást gyakorolt.[19] Különösen hátrányosan érintette azokat az egy termelő függő gazdaságokat, amelyek pl. nem tudták eljuttatni a banántermésüket a nyugat-európai piacaikra. A fukusimai atomerőművel történt rendkívüli eseményeknek pedig olyan súlyos következményei voltak, amelyek az IT és autóiparban néhány multinacionális vállalat ellátási láncának működését veszélyeztették.[20] Ez a két eseménysorozat is egyértelműen bizonyítja, hogy a kritikus infrastruktúra védelemben milyen komplex módon kell felmérni a kockázatokat, és azt állítást alátámasztja, hogy az ellátási láncok sérülékenységi veszélye nagynak tekinthető. Egyben olyan kérdésként kell kezelni, amely biztonsági szempontból meghaladja a beszerzés, a termelés, az elosztás és az értékesítés kereteit.

Az ellátási láncok biztonsága tehát nem szűkíthető le termelési, fuvarozási megbízhatósági kérdéssé. Olyan gazdaságbiztonsági kérdésként ajánlatos kezelni, amely a mai, globalizált gazdaság viszonyai között nem oldható meg csupán nemzeti keretek között és állami feladatként. Az ellátási láncokban bekövetkezett rendkívüli események hatásai túlmutatnak

16 Foltin, Pavel: Security of Logistics Chains Against Terrorist Threats. In. The 17th International Conference The Knowledge-Based Organization. Sibiu (Romania): Nicolae Balcescu Land Forces Academy, 24–26 November 2011. Conference Proceedings 1: Management and Military Science. p 100–105.
17 Horváth Attila: Characteristics of terror-threats in goods transportation. Academic and Applied Research in Military Science.8:(2), Budapest, 2009. pp. 345–355.
18 Cook, Thomas A.: i.m. (2007).
19 Horváth Attila: i.m. (2013).
20 Uo.

a multinacionális vállalatok szervezeti keretein. Az eddigi tapasztalatok szerint az elsődleges következményeket a környezet és a társadalom szenvedi el, a tartósan jelentkező hatásoknak (pl. ellátási zavarok) is a közvélemény elsősorban a társadalmi vonatkozásait éli meg. Ugyanakkor azt is el kell fogadnunk, hogy az ellátási láncok biztonságosabb működési feltételei megteremtéséhez fokozottabb nemzetközi együttműködésre van szükség, amely érinti a nemzetközi szervezeteket, az államokat, a termelő-, kereskedelmi-, logisztikai-, és közlekedési vállalatokat.

Az ellátási láncokkal kapcsolatos biztonsági kérdésekkel kapcsolatban nem szabad figyelmen kívül hagyni a nemzetközi kriminalisztikai szintű problémákat felvető drog- és illegális fegyver, műkincs csempészetet. A kábítószer és a bizonytalan tulajdonú műkincs forgalom lebonyolításának az egyik legegyszerűbb módja, ha legális logisztikai és szállítmányozó vállalkozásokat használnak fel a küldemények továbbítására.[21] Ezért az ellátási láncok biztonságát ilyen értelemben is ki kell terjeszteni.

Az együttműködés területei

Az ellátási láncok biztonságával kapcsolatos kérdések a lehetséges kockázatok, és az esetlegesen bekövetkező rendkívüli események hatásai komplex jellege miatt szoros együttműködésre van szükség, amely meghaladja a kritikus infrastruktúra védelem közlekedési ágazatának kereteit. Az együttműködést ki kell terjeszteni az iparbiztonságra, vagyis a termelési szférára. Nemzetközi szinten olyan világos, szigorúan szankcionált – lehetőleg piaci és pénzügyi következményekkel járó – szabályzásra bevezetésére lenne szükség, amely a termelési költségek mindenáron való „leszorítása" mellett a biztonsági szempontokat is figyelembe venné. Az ipar mellett az agrárgazdasági szektor az, amellyel az ellátási láncok biztonságos működése érdekében kooperálni kell. Az élelmiszer feldolgozóipart és a kereskedelmet nem is lenne célszerű élesen megkülönböztetni, hiszen a szállítási, logisztikai és kereskedelmi eljárások hasonló eljárások szerint működnek. Az elmúlt évek globális, európai és magyar vonatkozású élelmiszer botrányai rámutattak arra, hogy a teljes élelmiszer láncon belül kell értelmezni a biztonságot, vagyis a termelő helyek, feldolgozó üzemek, a kereskedelemi egységek és a felhasználók vonatkozásában.[22] Az egyeztetett eljárások a két szektor között jelentősen megkönnyítenék az áruszállítással, a logisztikai szolgáltatásokkal összefüggő szabályok kialakítását és betartásának ellenőrzését. Az élelmiszer ellátási lánccal való szoros együtt működés az ellátási láncok minden működési területén hasznos tapasztalatokkal szolgálhat a kockázatok és a bekövetkezett rendkívüli események kommunikációjában.[23] Ezen a területen elmúlt évek tapasztalatai bővelkednek olyan mintákban, amelyeket át lehet és kell venni, illetve olyanokban is, amelyeket eleve ki kell zárni.

A szektorok közötti horizontális együttműködés mellett rendkívüli fontossággal bír az érintett termelő, közlekedési, logisztikai és kereskedelmi vállalatokkal is az együttműködés

21 Csaba, Zágon: A szállítási lánc biztonságának aktuális kérdései a missziós feladatok kapcsán. Hadmérnök. 2009, 3. szám. pp. 151-158.

22 Kasza, Gyula-Surányi, József-Lakner, Zoltán- Bódi, Barbara- Deák, Ferenc- Horváth, Attila- Mészáros, László- Szántó, Attila-Danczák, István: Rendkívüli helyzetek és kezelésük az élelmiszer-kereskedelemben - irányelvek tapasztalatok: Élelmiszer Vizsgálati Közlemények 68. évfolyam, 2012. 3-4. szám. pp. 101-117.

23 Kasza, Gyula-Lakner, Zoltán: The bird flu in mind of Hungarian consumers-lessons and experiences of a direct-question survey. Acta Agraria Kaposvariensis. 2006. Vol. 10, No. 2, pp. 229-237.

megszervezése. Erre némi garanciát jelent a már hivatkozott létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényben és a végrehajtási utasításban foglaltak betartása. Valós elmozdulást az jelenthet, ha a vállalatok a kerítés megépítésén, a CCTV kamerarendszerek telepítésén, valamint a biztonsági őrök alkalmazásán túl olyan biztonsági rendszert építenek ki, amelyek kiterjednek a vállalkozás valamennyi tevékenységi formájának biztonságára is.[24] Ehhez azonban a jogszabályi garanciák és a profit veszteség kockázata sem elégséges, valójában az szükséges, hogy a biztonság a szervezeti kultúra részévé váljon.

Az ellátási láncok biztonsága érdekében a nemzetközi együttműködés szükségességét a konténer forgalom nagyságával és kockázataival lehet leginkább alátámasztani. Az Egyesült Államokban több éve végeznek olyan elemzéseket, amelyek az alapján a „forgatókönyv" alapján készül, hogy miként lehet károkat okozni a konténerek felhasználásával a szárazföld belsejében. Ezt az analógiát figyelembe véve Magyarországon sem szabad figyelmen kívül hagyni tengeri közlekedés és a konténeres kombinált szállítás biztonságát.[25] A konténerek elterjedése kétségkívül a globális mértékeket feltétele a kombinált közlekedés folyamatosságának. Ugyanakkor a konténer- és a kikötőbiztonságot illetően komoly viták bontakoztak ki pl. az Egyesült Államok és az Európai Unió között.[26] Az Egyesült Államokban tervezett és koncepcionálisan elfogadott 100%-os konténer átvizsgálási módszer azonban Európában feleslegesnek tűnik.[27] A teljes konténer ellenőrzés és átvilágítás költségei nem állnak arányban a reálisan fellépő kockázatokkal. Ennek ellenére a konténerbiztonságot nem csupán a rendészeti és vámeljárási szempontokból, hanem a kritikus infrastruktúrák védelme szempontjából is komolyan kell venni. A konténer forgalom ma már olyan méreteket ölt, hogy az ellátás folyamatossága biztonsági kérdés, tehát a gazdaság működésének stratégiai kérdései közé tartozik.

Az ellátási láncok biztonsága szempontjából igazodni kell a megváltozott gazdasági körülményekhez is. Jó példát jelenthet erre az Európai Unióban a vasúti privatizáció, amely olyan nemzetközi kötelezettséget jelent, amelyet adottságként elfogadni[28] Egyben azt is jelenti, hogy a külső logisztikai kapcsolatokat jelentő szállítási láncok új szereplőkkel bővülnek. Ez a tény is hangsúlyozza, hogy az ellátási láncok biztonságáról akkor beszélhetünk, ha a gazdasági szereplők, az állam, az érintett szektorok és a fogyasztók együttműködése megvalósul hazai és nemzetközi szinten egyaránt.

Összegzés

A tanulmányban elsősorban arra kívántam felhívni a figyelmet, ha gazdaság biztonságról beszélünk, akkor abba szervesen beletartozik az ellátási láncok megbízható és folyamatos mű-

24 Király, László-Pataki, János: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz. Hadtudomány, 2013. évi elektronikus szám. 15. p. URL cím: http://mhtt.eu/hadtudomany/2013_e_Kiraly_Laszlo_Pataki_Janos.pdf

25 Horváth Attila: i.m. (2009).

26 Csaba, Zágon: A konténeres szállítás biztonsága. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 25 p.

27 Uo.

28 Szászi, Gábor: A vasúti közlekedési alágazat, mint kritikus infrastruktúra. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 35 p.

ködése. Olyan területről van szó, amely nemzetközi szintű szabályzást és eljárásokat igényel. A biztonság ezen a területen csak akkor értelmezhető, ha minden érintett szereplő komolyan veszi a rá vonatkozó kötelmeket és feladatokat. Az ellátási láncok biztonsága tekintetében a hazai kritikus infrastruktúra védelmi ágazatokon belül az agrárgazdasági és a közlekedési szektor fokozottabb együttműködése ajánlott. Fontosnak tartom azt is megjegyezni, hogy olyan területről van szó, amelynek kutatása több tekintetben is alapkutatást igényel, amelybe több tudományterület képviselőinek kell résztvenni.

IRODALOMJEGYZÉK

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

Bonnyai, Tünde: A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása. Tanulmány, Budapest, 2011. URL cím: http://vedelem.hu/letoltes/tanulmany/tan382.pdf p.61.

Bowersox, Donald J., Closs, David J., Cooper M. Bixby, Bowersox, John C.: Supplay Chain Logistics Management. Fourth Edition. Mcgraw-Hill International Edition, New York, 2013. 484 p.

Cook, Thomas A.: Global Sourcing Logictics. How to Manage Risk and Gain Competitive. Published by Advantege in a Worlwide Marketplace American Management Association. 2007. New York. 401. p.

COM (2005) 576 final – Zöld Könyv az európai kritikus infrastruktúrák védelmének európai programjáról. Európai Közösségek Bizottsága. Brüsszel, 2005. 27 p.

Csaba, Zágon: A konténeres szállítás biztonsága. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 25 p.

Csaba, Zágon: A szállítási lánc biztonságának aktuális kérdései a missziós feladatok kapcsán. Hadmérnök. 2009, 3. szám. pp. 151-158.

Foltin, Pavel: Security of Logistics Chains Against Terrorist Threats. In. The 17th International Conference The Knowledge-Based Organization. Sibiu (Romania): Nicolae Balcescu Land Forces Academy, 24-26 November 2011. Conference Proceedings 1: Management and Military Science. p 100-105. ISSN 1843-6722. 897 pp

Foltin, Pavel-SEDLAČÍK, Marek-ŠIKOLOVÁ, Mária: Modification of Critical Path Method by a Portfolio of Security Criterions. In. The 18th International Conference The Knowledge-Based Organization. Sibiu (Romania): Nicolae Balcescu Land Forces Academy, Romania. 14-16 June 2012. P 234-239. ISBN 1843-6722. 341 pp.

Domboróczky, Zoltán: Ellátási láncok és logisztikai szolgáltatások biztonsági aspektusai. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 17 p.

Horváth, Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 35. p.

Horváth, Attila: Városok ellátása és az ellátás láncok biztonsága. Településföldrajzi Tanulmányok. I. évfolyam, 2. szám, 2012, pp. 143-154.

Horváth, Attila: Mi indokolja az ellátási lánc biztonságával kapcsolatos kutatásokat?In: Réger Mihály (szerk.) International Engineering Symposium at Bánki (IESB 2012) Bánki Kari Tudományos Konferencia Kiadvány, Budapest, 2012. pp. 1-13.

Horváth Attila: Characteristics of terror-threats in goods transportation. Academic and Applied Research in Military Science.8:(2), Budapest, 2009. pp. 345–355.

Horváth, Zoltán: Az ellátási lánc újszerű értelmezése a katasztrófa-elhárítási logisztikában. In.: Turcsányi Károly (szerk). Logisztikai a felsőfokú képzésben és a PhD felkészítésben III. MTA IX. Gazdaság- és Jogtudományok Osztály Logisztikai Osztályközi Állandó Bizottság, kiadványa. Budapest, 2013. pp. 97-112.

Izsák Éva: Tér-elmélet és tudományos tudás: Regionális Tudományi Tanulmányok, Budapest, 2012 16:(16) pp. 140-148.

Kasza, Gyula-Surányi, József-Lakner, Zoltán- Bódi, Barbara- Deák, Ferenc- Horváth, Attila- Mészáros, László- Szántó, Attila- Danczák, István: Rendkívüli helyzetek és kezelésük az élelmiszer-kereskedelemben - irányelvek tapasztalatok: Élelmiszer Vizsgálati Közlemények 68. évfolyam, 2012. 3-4. szám. pp. 101-117.

Kasza, Gyula-Lakner, Zoltán: The bird flu in mind of Hungarian consumers-lessons and experiences of a direct-question survey. Acta Agraria Kaposvariensis. 2006. Vol. 10, No. 2, pp. 229-237.

Király, László-Pataki, János: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz. Hadtudomány, 2013. évi elektronikus szám. 15. p. URL cím: http://mhtt.eu/hadtudomany/2013_e_Kiraly_Laszlo_Pataki_Janos.pdf

Knoll, Imre: Logisztika-gazdaság-társadalom. Kovásznai Kiadó. Budapest, 2002. pp. 237 p.

Lakner Zoltán: Turning the Rubik's cube: Socio-economic modernisation, life quality, competitiveness and food reseach, Acta Alimentaria, 37, 4, 2008. pp. 409-413

Murray T. Alan-Grubesic H.Tony: Overview of Reliability and Vulnerability in Critical Infrasturcture. In.: Murray T. Alan–Grubesic H.Tony (eds). Critical Infrasturcture. Reliability and Vulnerability. Springer-Verlag. Berlin, Heidelberg, New York, 2007. pp. 1–8.

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES: PDD 63. URL cím: https://www.hsdl.org/?-view&did=456517. p 14.

Szászi, Gábor: A vasúti közlekedési alágazat, mint kritikus infrastruktúra. Kézirat, megjelenés alatt a Hadtudomány közlekedési kritikus infrastruktúra védelemmel foglalkozó tanulmány kötetében. Budapest, 2013. 35 p.

Szegedi, Zoltán: Ellátási lánc-menedzsment. Kossuth Kiadó, Budapest, 2012. 259.p.

Szegedi Zoltán, Prenzenszki, József: Logisztikai menedzsment. Budapest, Kossuth Kiadó. Harmadik Kiadás. Budapest, 2005. 456.

Tranportation Systems. Critical Infrastructure and Key Resources Sector-Specific Plan as input the National Infrastructure Plan. Department of Homeland Security, Arlington, 2007. 288 p.

CYBERTERRORISM FROM IT FORENSICS PERSPECTIVE

Illési Zsolt

Terrorism and information technology

Cyber threats and reactions are not forming yet a homogeneous system. All those involved –terrorists, organized crime, defence, civil society and business contributors– have different motivations, each with a specific viewpoint and instruments. Based on the presentations, it became clear that the society's dependence on information technology and the resulting new types of challenges cannot be governed as pure technical issues.

In computer security preventive, corrective, and detective controls ensure proper safeguarding of assets. In the centre, there is the user of infocommunication devices and systems who focuses on business objectives. The general user is not aware of the security game around him. There are two other significant players in security process who has lots of attention: the attacker, and the defender. However, there is one another player who is frequently neglected: the pathfinder.

After an offence, the victim and the authorities need evidence to sanction the right wrongdoer for the factual act. But special environments need special expertise to find evidence and to appropriately interpret them in the front of a jury. Judicial (forensic) experts are providing such services.

With the proliferation of information technology the numbers of related cases are increasing simultaneously. As a computer security researcher, I would like to give a special assessment of the relationship between computers and terrorism from the forensic viewpoint.

In my paper I would like point out to the fact that information (or cyber)terrorism is not appropriately defined, but there is a simple way how computer forensics can interpret and handle these issues. My second objective is to highlight some bottlenecks in modern computer forensics to provide adequate answers to the questions of the authorities.

Definition uncertainties

While we are talking about new challenges, such as cyberterrorism we have to face with old problems defining: What do we exactly mean by 'cyber', and what do we mean by 'terrorism'?

The second problem maybe older. Boaz Ganor pointed out that terrorism has no universally accepted definition. However, there are some frequently used concepts that are widely used in terrorism definitions. The top five attributes are the following

- the use of violence and force (82.5%),
- political motivation (65%),
- fear, emphasis on terror (51%),

- threats (47%),
- psychological effects and anticipated reactions (41.5%).[1]

There are some problem distinguishing terrorism from similar violent actions, such as crime and war(fare).

When we are talking about the so called 'cyberspace' we are also face with poorly defined concepts. Different authors using different terms to describe very similar concepts. 'Cyber'[2], 'information', 'computer', and 'computer network' prefixes are equally used with 'terrorism' to describe some violent actions were infocommunication devices or systems are involved. Here we have to add some new elements to violent actions, such as cracking, hacking, systems and hacktivism.[3]

To get a forensically sound approach we have to remember that forensic services support the judicial system in these quests by providing expert interpretation of specific subjects. Crime is an offence against a public law and this offence is always penalized in criminal law. Sanctioning attacks and crimes in times of peace is the privilege of the state in modern countries which adhere to the rule of law. Penalisation rules are determined by the law. Imposing penalties are possible under conditions defined in law. The format and formalities to be followed also laid down in regulations. The court is to decide whether the conditions defined in the law are met. The court is to comply with the law and it is to enforce the compliance. Thus it is not possible to take sanctions in one's own hand for those who become victims of any crime. They have to recourse to the court to vindicate their rights.

From this angle all terrorist activities are classified as criminal activities, so are cracking, hacking and hacktivism. Warfare is the act of nations against nations, but these violent actions are regulated by national and international law. Warcrimes are 'normal' crimes, and they are similarly lassified in criminal law as 'ordinary' crimes. This means that from a legal perspective we have no or little difference between violent actions: what is not prohibited that is not against the law.

If we look closely to the violence, there are four distinguishing factors, the

- motivation,
- target,
- perpetrator,
- execution.[4]

By maping violent actions and these key factors, the differences become more noticeable, as you can see in Table 1.

1 Reference [1]
2 In Hungarian sometimes the term 'kiber' is used.
3 References [1], [2], [3], [4], [5]
4 Reference [6]

Violent actions	Motivation	Target	Perpetrator	Execution
War	political	country	country	- violent (by nature)
Terrorism	political	country government	(international) organisation(s)	- violent (violence works as a device) - use of fear is typical - violence mostly symbolic: misuse of victims
Crime	financial	[any]	individual organisation(s)	- violent (violence works as facilitator)
Hactivism	political	government	organisation(s)	- maybe violent (outcome)

Table 1. Summary of key attributes and violent actions[5]

Let's analyse the 'cyber' issue. Infocommunication resources –especially computers, mobile/handheld devices, computer networks – can be

- target
- implementation / commitment tool / environment
- symbol
- witness

of (computer) crimes.[6]

If these resources involved in a crime they may work as an excellent source of evidence. 'Every contact leaves a trace'. This rule, the Locard's exchange principle, works not only in the physical world, but valid in an information technology environment. The material residues, imprints, and digital evidence objects links the crime scene(s), the victim(s) and the perpetrator(s). Digital evidence objects (DEOs), such as files, data structures, data elements (metadata), and configuration elements (control data, settings etc.), however, DEOs are made up of data which has some nonphysical characteristic (e.g. data can be available in two or more places at the same time authentically) which specifics still not fully exposed by forensic scientist.

There is a wider interpretation of information violence (information operations), adding physical devices and environment, operators to the narrow interpretation and where the final objective is to enhance information superiority of our forces and decrease these capabilities of hostile parties.[7]

Digital evidence, just like its physical pairs (material residues, imprints) is providing answers to the classical forensic questions (5W+1H):

- Who? → Individual(s) involved
- What? → The nature of events that occurred

5 Reference [7]
6 Reference [8] pp. 255–273
7 Reference [9] pp. 160–168

- Where? ⟶ Location of the crime scene(s)
- When? ⟶ Timeline of events
- Why? ⟶ Motivation of the offence
- How? ⟶ Used tools or exploits[8]

Data overflow, system complexity and problems in methodology follow up

Computer forensic investigation is an interdisciplinary domain, where law supplies functional specification, the realisation framework comes from criminalistics, but all these shall be implemented in the field of information technology.

The less investigation issues, the greater criminal investigation effectiveness and efficiency, and as a result forensic labs could:

- increase quality and quantity of available evidence,
- provide appropriate and sufficient documentation,
- make investigations repeatable due to appropriate evidence handling,
- reduce errors due to adequate analysis or interpretation.[9]

The immensely increasing volume of data is an emerging problem within computer forensics. By installing an operating system 10.000-100.000 files are created. Installing applications, adding music, video, document files this number easily goes up to sky high. The use of a computer this number is increased by new, temporary, cached files and the like. Curent New technology and forensic methodology is needed to effectively and efficiently process 'big data cases'.

Technology evolution raised some special issues. First, the move from dead to living system analysis. In the past computer forensic investigator got one or two computers, hard disks or other storage equipments to analyse. The investigator used a labor environment, with This change raises new research areas: we have to understand the effects of forensic investigation process on evidence. In particular we need new methods to deal with virtualised environment. Detecting, imaging, analysing virtual environment is not evident, innovation is needed to catch up with new solutions.

Fight against offences changes from national to international. However forensic institution internationalisation is lagging behind. There is no internationally tested and accepted common / standard methodology, education, research or competence.

Besides the amount of data the proliferation of mobile and handheld devices, and virtualisation also raise the bar of competence to find adequate evidence in cases where infocommunication technology to be analysed. In the next paragraph of my paper I would like to give some examples, why it is getting more and more difficult to give answers to these questions.

8 Reference [10] pp. 58–59
9 Reference [11]

Investigation issues

The 'who issue'

In computer forensic the perpetrator is never present in physical form. All what we can see is computers, user IDs, devices or systems. However computer does not fully represent a natural person, but a criminal procedure may be brought against a natural person, or against a group of natural persons. Police investigators shall provide other (non computer evidence) on the relation between the accused. This requires some extra investigation and special knowledge of the police. This level of competence, luckily I increasing.

If the computer and the perpetrator are connected, there is an issue to bind him to an organisation or a state. In case of international cases this is a very difficult task, because different states may have different legislation on the same behaviour. What is a crime in one country is may not a crime in another one. The Estonian cyberincident[10] is a great example how can a state block the legal claims of another state. State level incidents giving more headaches. What if one natural person is identified during the criminal process it very hard, even if not impossible, to prove the malicious connection between this person and a state. The combination of some national legislation and state secrect are very effectively block a successful investigation.

It is also difficult to separate the real perpetrator and victims. There are some example, when someone was brought to court, and later it turned out that the computer of presumed perpetrator was under the influence of a malicious code, a Trojan horse, which was installed by some third party.[11]

Here I have to call an attention to the great number of organisations/ networks/ systems involved in the commitment of today's computer crime. For example there were over 150 countries involved in the Estonian cyberincident.[12]

The 'what issue'

Logging plays strategic role in decrypting what happened. Everybody thinks that modern computers, and systems record all activities within the borders. Unfortunately this is not so obvious. We have some issues with logs. First, the default settings in most of computer systems in no logging or minimal logging. System administrator, owners due to comfort, ignorance or because of the lack of time / resources do not revise and reset default settings, thus there is no or insufficient residue of the chain of events to provide clues about the nature of events that occurred.

Second, different product logs events differently. They may use different data structure, different number of data fields, and as a result in many cases it is not possible to interconnect these logs, or the result is quite fragmented, which requires lots of manual correction.

Third, some organisation is legally bound to backup logs, some do it for out of best practice, some do not care at all. Different organisations have different retention period. Some

10 Reference [12]
11 Reference [13]
12 Reference [12]

deletes log files within a week, some keep these backups for ages. Sometimes the perpetrator deletes the log files to make detection difficult.

Last, I have to mention that log may contain inconsistent data. The perpetrator may or may not have a possibility to tamper with these data, and the investigator has to decide if the data investigated is original/ modified/ falsified.

The 'where issue'

In physical space it is easy to identify crime scene. In cybercases, however, it is almost impossible. We have a 'virtual' crime scene which may include thousands of sites and computers. There is no such long yellow-black tape to enclose a crime scene this size.

So, we have a question to decide if the scene is the

- location of the perpetrator, or
- location of used systems, or
- location of the target, or
- all above together.

The crime scene may cover countries, or even continents. I already mentioned, the difficulties of investigating transborder crimes; the international character makes this situation even worse.

The 'when issue'

Date and time is not as easy to interpret in computer systems as a layman ay think. The first problem is date representation. In the USA, for example dates are represented as MONTH/ DAY/YEAR, in the UK the format is DAY/MONTH/YEAR, in Hungary we have a YEAR/ MONTH/DAY order. Dates are often represented in short form, where all elements (year, month and days) are represented in two characters. The separator between date element may be '/', '-' or a 'space' etc. It is possible that months are written in text, such as 'May' (English), 'május' (Hungarian) or 'أيار' ('Ayyār', Arabic) etc.

With time data fields we have similar issues. It can be in HH:MM:SS, or just in HH:MM form. Here we also have lots of different element separators.

Both data can be managed on a physical (how data is stored) or in a logical layer (how the data appears in the user interface).

There is no such forensic application which could interpret date- and timestamps correctly. Lots of manual invention is needed to get a consistent date and timeline in a complex case.

If date/time storage were not an issue, we have problem with precision. Some systems synchronizing with external and trusted timeservers, some system administrator thinks that his own time server is a good idea, or even worse, do not let computers update date and time. So, during the investigation, experts have to always ask date and time validity, annd have to figure out means to date/ time synchronisation in all participating systems.

Some counter forensics tool, such as DECAF, confuses date- and timestamps further aggravating this question.

The 'why issue'

In the 'good old times' opposition forces were fighting under their own flags. In cyberspace, however no-flag and false-flag operations are widely employed to cover if an incident is a diversion (like bombing Kassa) or a covert operation.

Unfolding root cause(s) of an operation may require to reveal secret(s) of the attacking and the attacked (country/ countries).

The 'how issue'

Last, but not least we have the difficulties of exactly defining the used tools and exploits due to complex and distributed control structures, the attacker uses one or more command and control machines to access and control a large number of zombie computers,which are attacking the final target.

Encryption is also used both to encrypt communication channels and storages in order to make it extremely difficult to discover and to understand how the crime was committed.

Summary

In this paper I introduced how forensic computer investigators are translating seemingly difficult issues as cyberwar, cyberterrorism, and cybercrime. Identified four key attributes (motivation, target, perpetrator, execution) of differentiating violent acts in cyberspace. I have concluded that all these violences are investigated by judicial experts if they are violating the criminal law, therefore from the computer forensic perspective all violent cyber actions are the same. These are simple investigations, and the purpose of such analysis is to obtain digital evidence objects from the affected computers.

Besides analysing the role and tasks of computer forensics in the war against cyber threats, I gave examples of the key problems of modern computer forensics. Based on these examples I made clear that new approaches,methodologies are required if states would fulfil its sanctioning rules, and make compulsory the law in force.

REFERENCES

[1] Andrew M. COLARIK: *Cyber Terrorism: Political and Economic Implications.* Idea Group Publishing, USA: 2006. ISBN 1–59904–021–2

[2] László KOVÁCS, Zsolt ILLÉSI: Cyberhadviselés. In: *Hadtudomány* Vol XXI. No. 1–2, pp. 29–41. ZMNE, Budapest, 05.2011. ISSN 1215–4121

[3] László KOVÁCS: Az információs terrorizmus eszköztára. In: *Hadmérnök*, Robothadviselés 22.11.2006 special edition. ZMNE, Budapest, 2006. November. ISSN 1788–1919

[4] László KOVÁCS: *Cyber terrorizmus*. Hadtudományi Doktori Iskola, [Online], 2006. http://www.zmne.hu/dokisk/hadtud/terror/lekt_Kovacs_Laszlo.pdf

[5] Zsolt HAIG, László KOVÁCS: *Fenyegetések a cybertérből*. ZMNE, 2008. ISSN 1789–5286

[6] Zsolt ILLÉSI: Számítógép Hálózatok Kriminál technikai Vizsgálata. In: *Hadmérnök* 2009. Vol. IV. No. 4. ZMNE Bolyai János Katonai Műszaki Kar. Budapest 2009. pp. 163-175

[7] Zsolt ILLÉSI: *Information violation (?) and computer forensics.* Óbudai Egyetem, Budapest: 19.11.2011. ISBN 978–615–5018–20–6
[8] Zsolt György BALOGH: *Jogi informatika.* Dialóg Campus Kiadó, Budapest-Pécs, 1998. ISBN 963–9123–19–6
[9] Zsolt HAIG, István VÁRHEGYI: *Hadviselés az információs hadszíntéren.* Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9
[10] Wayne JANSEN, Rick AYERS: *Guidelines on Cell Phone Forensics – Recommendations of the National Institute of Standards and Technology.* Computer Security Division Information Technology Laboratory, NIST Special Publication 800–101. NIST, [Online], 05.2007. http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
[11] Flórián TREMMEL: *Bizonyítékok a büntetőeljárásban.* Dialóg Campus, Budapest-Pécs, 2006. ISBN 963–7296–72–7
[12] Wikipedia: 2007 cyberattacks on Estonia, Wikipedia [Online] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[13] IDGNS: *A Misconfigured Laptop, a Wrecked Life.* PC World, 2008 [Online]. http://www.pcworld.com/article/147213/article.html

A KIEMELT KOCKÁZATÚ SZOLGÁLTATÁSI HELYZETEK A MAGYAR POSTA ZRT.-NÉL, MINT KRITIKUS INFRASTRUKTÚRA ELEMNÉL

Károlyi László

A Magyar Posta Zrt. (továbbiakban: posta) egyetemes postai szolgáltatói státusza, valamint az, hogy a Magyar Köztársaság egyik legnagyobb készpénzforgalmi szolgáltatója, a magyarországi kritikus infrastruktúrák különösen veszélyeztetett kategóriába sorolandó szereplője. Ez a státusza megfelel a fejlett országok besorolási gyakorlatának is. A posta társadalomtörténeti szerepét tekintve különleges társadalmi-államszervezeti szerepet tölt be hazánkban. Tudomásul véve függőségét más kritikus infrastruktúra elemek működőképességétől, egy általános veszélyhelyzetben, amikor sérül a kormányzati, vagy más közigazgatási irányítási rendszer, akkor a posta alternatív megoldást jelenthet.

A posta az egyetlen olyan országos szolgáltató, amely történelmi hagyományai során kialakult technológiáit alkalmazva képes más, kieső távközlési, információ-továbbítási szolgáltatásokat helyettesíteni. Struktúrájából, létszámából, technikai felszereltségéből és technológiájából eredően képes a kormányzati közigazgatás feladatait kiegészíteni, támogatni kiterjedt veszélyhelyzet esetén.

A posta kritikus elemeinek beazonosítása, kapcsolódása az országos szakterületekhez

Az egyetemes postai szolgáltatás négy fő elem működtetésén keresztül valósul meg. A hálózat, amely a településeken a postai szolgáltató helyeket jelenti. A szállítás, amely a küldemények és értékcikkek szolgáltató-, és feldolgozóhelyek közötti mozgatását biztosítja. A feldolgozás, amely postai értelmezésben a küldemények rendszerezését végzi, a kézbesítés, amelynek a feladata a küldemények címzettekhez történő célba juttatása.

A posta függősége más infrastruktúráktól

A posta olyan stratégiai partnerekkel működik együtt, mint a bank-és pénzintézeti-, az informatikai és kommunikációs- szektorok, az energiatermelés és elosztás, a vízellátás-közművek, a közlekedés és szállítás. Ezek az ügyfelek jelentős mértékű küldeményforgalmat bonyolítanak mind levélpostai, mind logisztikai, mind pénzforgalmi termékek/szolgáltatások vonatkozásában.

A posta kiterjedt országos hálózatával, jelenlétével, forgalmával és szolgáltatási formáival nagymértékben függ működési környezetétől. Jelentős a függősége más kritikus infrastruktúrák, úgymint:

- energiaellátás,
- internet-szolgáltatás,
- közműellátás,
- közlekedés,
- hírközlés

állapotától, működési színvonalától

A társadalmilag fontos szolgáltatás kiváltotta hatások közvetítése, akkor járulhat hozzá a kritikusság szerepének fokozódásához, ha ez közvetlenül, vagy egy másik infrastruktúrán keresztül - nagyságrendjében közel azonos módon, illetve társadalmi léptékűvé felerősödve - adódik át a környezetnek (2008/114/EK Tanácsi Irányelv 2. cikk, a) pont). Ez a veszély a Posta működtetése során is fennáll.

A valószínűsíthető veszélyforrások

A postai szervezetek, intézmények, vállalkozások változatos és növekvő számú veszélyeknek-katasztrófáknak vannak kitéve. A postai szolgáltatásokat mind a természeti, mind a civilizációs katasztrófák (beleértve a terrorizmust-kiberterrorizmust is) veszélyeztetik, amelyek elhárítását keletkezésük, kiváltó okaik szerint kezeljük.

A posta terrorizmus általi érintettsége viszonylag alacsonynak minősíthető, ezért a felsorolt fenyegetések bekövetkezésének is kevés a valószínűsége azonban a felkészülési tervekben figyelembe kell venni.

A kiemelt kockázatú postai létesítmények

- A Posta Elszámoló Központ (PEK),
- A Nemzetközi Posta Kicserélő Központ,
- Az Országos Logisztikai Központ.

A postát érintő veszélyek és fenyegetések értékelése

Viszonylag kevés olyan veszély és fenyegetés azonosítható a posta vonatkozásában, amely a szervezet egészét egyetemlegesen érintené. A természeti csapások jelentős részét, ha nem az egészét kizárhatjuk abból a szemszögből, hogy a hálózat egészére, egy időben nem okoz olyan negatív befolyást, amely megbénítja, a posta működését. A posta nagyobb részt nem folyamatos technológiai sor, így egy esetleges zavar, szakaszolás és más egyéb negatív hatás sem okoz lényeges mértékben üzemzavart több szolgáltatási végponton.

A posta egészére gyakorolt negatív hatás tekintetében egyetlen generális következménynyel az informatikai támogatás részleges, vagy teljes sérülése, kiesése járhat. Az informatikai szakterület részleges, vagy teljes kiesése esetén a kiváltás a felvételi, letéti, postahelyi kézbesítési tevékenységek manuális rendre való átállása 2-5-nap.

A posta informatikai és veszélyhelyzet kezelési szakemberei a közelmúltban is elemezték, vizsgálták, hogy mi történik abban az esetben, ha valamilyen ártó szándékú szervezet, vagy személy fizikai, vagy IT „csapást” mér a posta szervezete működtetéséért felelős informatikai-információs infrastruktúrára. Megterveztük a veszélyhelyzet kezelési rendszabályok szimulációs gyakorlaton történő tesztelését; ennek során különböző támadásokat intéznek az integrált infokommunikációs rendszerek ellen, és megvizsgálják, hogy a támadás következtében azok milyen károkat szenvedhetnek el. A szerzett tapasztalatokat beépítjük a szabályozás rendszerébe. Rendszeresek az informatikai havária törzsvezetési gyakorlatok.

A posta az üzletfolytonosságot, a tevékenységek körét fenyegető kockázati tényezőkre elsődlegesen a kockázat megelőzés módszerével ad választ. Az alternatív szolgáltatók alkalmazása, nagy megbízhatóságú berendezések, redundáns, illetve tartalék berendezések kiépítése, és egymástól elkülönített tűzszakaszban tartása, a rendszeresen történő napi mentések, a heti/havi mentések más telephelyen való elhelyezése, alternatív távközlési vagy informatikai hálózati útvonalak kialakítása, megbízható szállítók, üzemeltetők alkalmazása megfelelő védelmet ad.

A kis bekövetkezési valószínűségű, kis üzleti hatású kockázatok a tömeges fertőzés vagy sztrájk, a fűtés meghibásodása vagy munkaállomások, pc-k kiesése az üzletmenet folyamatossági tervekkel kezelhető. Ezekre a kockázatokra a posta azok bekövetkezésekor határozza meg a normál működés visszaállításához szükséges beavatkozásokat.

A szakértői hálózat, kutatói közösségek, tudományos és kutatási programok

A veszélyhelyzetek kezelésére postai szakterületenként szakértő munkatársak kerültek kijelölésre, akik magas szintű szaktudásuk révén részt vesznek a veszélyhelyzetek megoldásában, a tervek aktualizálásában. Valamennyi kompetens postai szervezettel (biztonság, területi igazgatóságok, ingatlan, eszköz, humán, munkavédelem, katasztrófa védelem, kézbesítés) folyamatos az információ megosztás, ez szabályozott keretek között történik.

A postai szolgáltatást igénylő kormányzati és pénzügyi szervekkel együttesen elkészített Együttműködési Megállapodások alapján e szervezetek szakértőikkel is segítik a veszélyhelyzeti együttműködést. A posta biztonsági szakemberei közül többen tanítanak hazai egyetemen, főiskolán, főként biztonságtechnikai, katasztrófa védelmi ismereteket, és tudományos fokozattal rendelkeznek.

Összegzés

A posta jelenlegi felkészültsége (a jogi és belső szabályozás megléte, a tervek kidolgozottsága és naprakészségének fenntartása, az évenként elvégzett felkészítés és gyakoroltatás, a beavatkozáshoz szükséges felszerelések biztosítottsága) a rendkívüli időszakból adódó feladatok végrehajtására alapvetően biztosítja a működés folyamatosságának fenntartását, még ha esetenként szűkített szolgáltatással is.

A postán a kis súlyú következményekkel járó sérüléseinek vizsgálatával igazolható volt, hogy a bevezetett katasztrófavédelmi rendszernek a veszély- és katasztrófahelyzetek megelőzése érdekében végzett tevékenységével, illetve a következmények kezelésével az érintettek teljes körét integrálva jelenleg közel 80%-os készenléttel, hatékonyan látja el a védekezési feladatait.

A kritikus infrastruktúrák közötti interdependenciák felvetik a továbbfejlesztés szükségességét. A védelmi beruházások tervezése és végrehajtása csak ütemezéssel történhet az egyszeri akut költség elkerülése érdekében. Ezzel 3-5 év alatt biztosítható a posta infrastruktúrája teljes védelmi készenlétének elérése.

HIGH RISK SERVICE SITUATIONS AT HUNGARIAN POST LTD., A CRITICAL INFRASTRUCTURE ELEMENT

Károlyi László

The universal postal service provider status and the fact the it is Hungary's largest cash transit service provider render the Hungarian Post Ltd. (hereinafter referred to as the Post) in the high risk category of critical infrastructure elements in Hungary. This category is in line with developed countries' categorization practices. Given the Post's role in social history, it plays a key role in Hungary from the social-state organization perspective. Even considering its dependency on the operability of other critical infrastructure elements, the Post can provide an alternative solution in a general emergency when the governmental and administrational control systems are damaged.

The Post is the only nationwide service provider that can substitute damaged telecommunications and information-transfer services, using its historically refined technologies. Based on its structure, number of employees, technical and technological capabilities, the Post can augment and support government administration in case of crises.

Identifying the Post's critical elements and connection to national areas of responsibility

Universal postal service is based on four pillars. The network, which refers to the postal service points throughout the country. Transportation, which ensures the delivery of mail and value items between service providing and processing locations. Processing, which in postal parlance means the sorting of mail items. Delivery, which means the forwarding of items to the addressees.

The Post's dependency on other infrastructures

The Post cooperates with strategic partners in the financial, IT/telecommunications, energy providing and supply, waterworks-utilities and (public) transportation. These customers have significant delivery turnovers in mail items, logistics and cash products/services.

With its large nationwide network, presence, turnover and service types the Post has a considerable dependency on its operational environment. Dependency is significant on other critical infrastructure elements and their operability and quality, such as:

- energy supply
- internet service

- public utilities
- transportation
- communications

The conveying of impacts of socially significant services can increase the criticality if these are directly or indirectly through another infrastructure – in the same magnitude or socially increased – impacting their environment (Council Directive 2008/114/EC Article 2. clause a)). This danger is inherent in the Post's operations.

Probable sources of danger

Postal organizations, institutions and enterprises are subject to varied and an increased number of dangers and crises. Postal services are jeopardized by both natural and civilizational crises (including terrorism and cyberterrorism). These are handled with a focus on their origins and root causes.

The Post is only lightly prone to terrorism and as a result, the probability of occurance of the listed threats is low. Nevertheless, they have to be taken into consideration in contingency planning.

High risk postal facilities

- Postal Accounting Center
- International Office of Exchange
- National Logistic Center

Evaluation of postal dangers and threats

The number of dangers and threats that universally effect the postal organization is limited. Most, if not all of the natural crises can be excluded since they do not negatively affect or block the operation of the entire postal network.

Postal operations for the most part are not continuous sequences of technological steps. This means that any disturbances, batch stops or other negative effects do not cause major disruptions on multiple servicing end-points.

Only the partial or complete damage or fallout of the IT support may cause general consequences for the Post.

The transition to manual operation of mail acceptance, storage and post office delivery services in case of a partial or complete fallout of IT support is 2-5 days. Az informatikai szakterület részleges, vagy teljes kiesése esetén a kiváltás a felvételi, letéti, postahelyi kézbesítési tevékenységek manuális rendre való átállása 2-5-nap.

The Post's IT and business continuity experts have recently analysed and evaluated scenarios when some malicious organization or person carries out a physical or IT attack against the postal organization's IT infrastructure. We have made plans on how business continuity regulations can be tested in simulation trainings. During these tests various attacks are carried out against integrated IT systems and the damages caused by these attacks are evaluated. The experiences gained during the course of these tests are then fed back to the regulations.

We hold regular IT disaster and business continuity exercises on management level.

The primary risk management tool used by the Post to counter risks jeopardizing its operations is prevention. The following tools provide adequate protection: use of alternative service providers, high availability equipment, installation of redundant or reserve equipment, keeping equipment in separate fire sections, regular daily backups, weekly/monthly backups stored in different locations, use of alternative telecommunications and IT network routes, use and employment of reliable suppliers and system administrators.

Low probability of occurance, low impact risks such as mass infections or strikes, damaged heating systems or workstations, fallout of PCs can be handled with business continuity planning. The required measures to restart normal operations are planned when these risks materialize.

Network of experts, research communities, scientific and research programs

The Post has designated experts from all domains to manage crises. These experts participate in solving crises and updating crisis management plans with their expertise. All stakeholder postal organizations (security, regional directorates, facility and equipment management, HR, work safety, crisis management, delivery) constantly share information in a regulated framework.

The Post has signed Cooperation Agreements with government and financial institutions that rely on postal services. These institutions support crisis management cooperation with their experts based on these Agreements.

Many of the Post's employees lecture in colleges, especially in the fields of security and safety, crisis management and are holders of advanced scientific degrees.

Summary

The Post's current preparedness (existing legal and internal regulations, level of deail and updating of plans, annual education and training, availability of required equipment) to carry out tasks in connection with crises basically supports business continuity, albeit sometimes with a limited scope of services.

The analysis of low impact damages has shown that the Post carries out protection tasks efficiently and with nearly 80% readiness. This is achieved by the integration of all stakeholders, the measures taken to prevent crises and catastrophes and by the handling of impacts.

The interdependencies between critical infrastructure elements render further developments necessary. To avoid significant one-off cost items, security investment planning and execution can only be carried out in a phased way. By this, the complete emergency preparedness of the Post's infrastructure can be achieved in 3-5 years.

SZEZÁM TÁRULJ! A KIBERBŰNÖZŐK, HACKEREK VALÓDI CÉLJA A VÁLLALATI ÉS KORMÁNYZATI RENDSZEREK SÉRÜLÉKENYSÉGEINEK KINCSESTÁRA

Keleti Arthur

Alapvető problémával szembesült az információvédelemmel, kiberbiztonsággal foglalkozó szakma a 2012-ben. Az informatikai rendszerek teljes vertikuma komoly változásokon esett át az elmúlt tíz évben, melynek eredményeként mára a rendszerek összetettek, rendkívül különbözőek (diverzifikáltak) és nagyon gyorsan változóak lettek. Ez egy olyan elkerülhetetlen folyamat, amelyet a felhasználók és a megrendelők gazdag funkciók iránti igényével járó az informatika változás hozott létre ezzel nem kis fejtörést okozva a biztonsági szakembereknek.

A rendszerek bonyolultsága, a felhasználói szokások sokszínűsége és az állandó változás még fontosabbá tette a naprakész informatikai biztonsági rendszerek szerepét, amelyet azonban sajnos még ma is erősen alul értékelnek a vállalati, üzleti és intézményi döntéshozók. Eközben sajnos már a kiberfegyverek piaca is megnyílt és az informatikai térben pénzért ugyanis legálisan vásárolhatóak olyan eszközök, amelyek ismert és széles körben használt informatikai rendszerek még nem ismert sérülékenységeit kihasználva képessé teszik a bűnözőket arra, hogy érzékeny, kritikus információs rendszerekbe hatoljanak be és befolyásolják azok működését, onnan adatokat tulajdonítsanak el vagy egyéb káros tevékenységet folytassanak. Az ilyen támadási lehetőségek sokszínűsége, a hackerek széles motivációs bázisa valamint megtámadható informatikai rendszerek száma komoly kockázati tényezővé emelték a kiberbiztonság hiányát.

Ebben a környezetben érthető, hogy fokozatosan minden informatikát használó szervezet és egyén célponttá vált. A szomorú valóság, hogy a hackerek mára célba vették és sikeresen befolyásolni is tudták több hírszolgálat és hírügynökség tájékoztatási csatornáit. Az Al-Jazeera, a Bloomberg, a Reuters és sok más nagy hírügynökség vagy sajtóorgánum rendszerei fölött átvéve az irányítást a kiberbűnözők híreket hamisítottak és dezinformációkkal igyekeztek becsapni a közönséget. Ez a jelenség egy olyan fenyegető trendre hívja fel a rendvédelemmel, társadalmi mozgásokkal és politikával foglalkozó szakemberek figyelmét, amely a társadalom által ismert és megszokott, megbízhatónak tekinthető információforrások hitelességét kezdi ki és ez alapjaiban változtathatja meg a hozzáállásunkat a közölt tényekhez, információkhoz.

Vállalati informatikai rendszerekben ugyanez a jelenség gazdasági bizonytalanságot jelent, kritikus infrastruktúrák szintjén társadalmi és gazdasági kockázatot hordoz, a rend-

védelem és kiberbiztonság terén pedig kommunikációs zavart, dezinformációs gócpontokat vagy használhatatlan műveleti rendszereket eredményezhet, amely nehezíti a hatékony munkát.

A nemrégiben kirobbant NSA megfigyelési botrány ráirányította a figyelmet arra, hogy a digitális lábnyomok, amelyeket mindannyian hagyunk az interneten valószínűleg elemzés, rögzítés alá kerülnek és ez megfontolt kibertérbeli viselkedésre ösztönözheti a felhasználókat. Ugyanakkor egyben bizalmatlanságot ébreszt a kémelhárítással, nemzetvédelemmel vagy rendvédelemmel foglalkozó területek számára, amely egyértelműen kedvezőtlen. Ezzel együtt viszont felhívja a figyelmet arra a jelenségre, amely az interneten a szakértők által régóta ismert és „mantrázott" problémát hozza közelebb a közemberhez, az identitás lopás lehetőségének kockázatát és az adatszivárgás, adatvesztés lehetőségét. Ez viszont remélhetőleg az állampolgárok és a társadalom óvatosabb, biztonságtudatosabb kibertérbeli viselkedéséhez vezet, amely egyértelműen fokozhatja a közbiztonságot a kibertében.

Eközben riasztó trendeket látunk a világban:

- az Android eszközök 50%-ban találhatóak befoltozatlan biztonsági hibák;
- a rendszereink komplexitása az egekbe szökött;
- Kína kiberbiztonsági piaca 1.8 milliárd USD-ről (2011) évi 45%-os növekedéssel 50(!) milliárd USD-re növekszik 2020-ra (Európa és az USA összesen 16 milliárd USD-t költ majd);
- az ENISA jelentése szerint az incidensek legtöbbje továbbra is rejtve marad.

Ezzel párhuzamosan a kiberbiztonsági problémák kezelésének is sok nézőpontjával kell foglalkoznunk:

- politikai (pl. hacktivisták);
- stratégiai (pl. nemzeti adatvagyon);
- törvénykezési (pl. infovédelmi törvény);
- hadviselési (pl. kiberfegyverek fejlesztése, kiberkémkedés);
- bűnüldözési (pl. gazdasági kiberbűnözés, identitás kereskedelem);
- ipari (pl. SCADA rendszerek);
- katasztrófavédelmi (pl. a létfontosságú rendszerek) § Piaci (pl. üzletmenet folytonosság és jó hírnév);
- adatvédelmi (pl. privát szféra).

A fentiekből következően ma sajnos még messze vagyunk attól, hogy minden érintett szereplő ugyanúgy értelmezze a kibertér fenyegetettségeit. Ezért kommunikálnak a témáról nehezebben egymással az rendvédelmi, államigazgatási, kibervédelmi, vállalati, civil és egyéb gazdasági szervezetek és sajnos a szervezeteken belül is komoly gondok vannak a kibervédelem szükségességének elfogadásával. A 2013-ban elfogadott IT Biztonsággal és információvédelemmel foglalkozó törvény fordíthat ezeken a trendeken, de ennek eredményeire még egy kicsit várni kell. A szomorú helyzetkép az államigazgatásban inkább ez:

- Szándék van.
- Törvény most már van, de még sok kell a gyakorlattá éréséig.
- Szaktudás van, több szervezetben is. De
- a végfelhasználó állami szervezetek legtöbbjénél
  - az erőforrás hiányzik,
  - a biztonsági megoldások hiányoznak,

- Az ISACA 2011-es felmérés alapján:
  - információbiztonsági stratégiával 56% rendelkezik;
  - katasztrófaelhárítási terve 48%-nak van;
  - biztonsági felelős/vezető 37%-ban nincs, ahol van ott is 15%-a számol be HAVONTA a főnökének;
  - csak az intézmények harmadánál látják át nagyobb mértékben felsővezetői szinten az IT kockázatokat (amelyeket ritkán is elemeznek).

A fent vázolt problémákra komplexen értelmezett megoldásokkal igyekszik a T-Systems Magyarország Zrt. hozzájárulni a kibertér védelméhez és a fenyegetettségek megfelelő, kockázatokkal arányos kezeléséhez. A biztonságnak a T- Systemsnél 6 fő és 36 szakmai alterülete van. Relevánsak a jelenlegi témára:

- adatszivárgás elkerülése,
- naplóelemzés, felügyelet és incidens menedzsment,
- mobil biztonság,
- privilegizált felhasználók kezelése.

Ezeket természetesen megelőzik a törvényi előírásokban rögzített kötelező kockázatelemzések és auditok, amelyekben a T-Systems szintén örömmel segít azoknak a szervezeteknek, akik felismerték, hogy a belső kibertér védelme gazdasági stabilitást eredményez a külső kibertér védelme pedig társadalmi felelősség és olyan közügy, amelynek fejlesztése növeli az állampolgárok biztonságérzetét a kibertérben.

HELIKOPTERES TŰZOLTÁS SZABOLCS-SZATMÁR-BEREG MEGYÉBEN

Komjáthy László - Kozák Attila

A Belügyi Tudományos Tanács a kiber bűnözés ellen folytatott küzdelemben résztvevő országos hatáskörű szervek szakmai bevonásával Változó környezet, változó biztonság – Kiber fenyegetések kihívásai napjainkban címmel nemzetközi tudományos-szakmai konferenciát szervezett 2012. szeptember 17-18. között. A TÁMOP-4.2.1.B-11/2/KMR-0001 Kritikus infrastruktúra védelmi kutatások projekt is lehetőséget kapott a bemutatkozásra. A mi kiemelt kutatási területünk (Tűzoltás és az adott terület árvízrizikójának menedzsmentje) kiállítással vett részt a rendezvényen, melyen bemutattuk a nyíregyházi műrepülő világbajnokság betétprogramjaként végrehajtott helikopteres tűzoltást és annak tapasztalatait összegeztük ebben a cikkben.

A gyakorlat célja volt, hogy alternatívát kínáljunk a nehezen megközelíthető helyeken keletkezett tüzek hatékonyabb felszámolásához, ugyanis jelen pillanatban a helikopteres tűzoltás kizárólag a honvédség Mi–8 és Mi–9, illetve Mi–17 közepes szállító helikopterével, valamint vállalkozók bevonásával oldható meg.1

A helikopteres tűzoltásban az elsőként és ma is legelterjedtebben alkalmazott technológia az úgynevezett. bambi bucket. A bambi bucket-et 1982-ben fejlesztette ki a kanadai Don Arney mérnök és a SEI INDUSTRIES. A technológia lényege, hogy a helikopter aljához huzalon rögzítik a vászon, vagy nejlon tartályt. A tartály töltése úgy történik, hogy a helikopter nagy vízfelület felett függeszkedve „meríti meg" majd a kárhelyre érve egy, a bambi bucket alján található nyíláson üríti ki – írja a tanulmányában a szerzőpáros. A módszer azonban nem volt tökéletes, a fennálló problémákra Imreh Lajos a Forgószárny Kft. tulajdonosa és főpilótája dolgozott ki úttörő megoldást.

Ahhoz, hogy a tüzet kellően meg lehessen közelíteni és ne kelljen az ürítéshez a nagy hőmérsékletű tűz feletti légtömegbe repülni, át kell helyezni a kidobás irányát. A Mil Mi–2 típusú gép belsejében, az ülések eltávolítását követően elhelyezett 1,4 köbméteres műanyag tartály kiömlőnyílása a géptörzs bal oldalán került kialakításra. Az elképzelés szerint a hagyományos eljárásokkal szakítva a tűz oltása már nem fentről lefelé merőlegesen, hanem fentről lefelé oldalról történik. Ez a megközelítés lehetővé teszi, hogy a gép eddig elképzelhetetlen mértékben meg tudja közelíteni a tüzet.[1]

A helikopteres tűzoltás hazai úttörője a Forgószárny Kft.

A helikopteres tűzoltás módszerét Magyarországon először a budakeszi telephellyel rendelkező Forgószárny Kft. alkalmazta. A számos tevékenységgel foglalkozó társaság a honlapján

1 1 Kós György - Dr. Komjáthy László: Erdőtüzek helikopteres oltása in: http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/36_Kos_Gyorgy-Komjathy_Laszlo.pdf

(www.forgoszarny.hu) olvasható információk szerint Mi-2 helikoptereivel, Zlin-137T gázturbinás, illetve Zlin-142 merevszárnyú repülőgéppel dolgozik. A tevékenységek között kiemelendő a katasztrófavédelmi tevékenységük.

Az általuk kifejlesztett új tűzoltási módszer lényege, hogy a helikopter belsejében egy speciálisan oda tervezett tartály kap helyet, amelyet közvetlenül egy tömlő segítségével egy közönséges gépjárműfecskendő tölt fel vízzel.

„A módszer óriási előnye a nyílt vízfelszíntől való függetlenség, a nagyon gyors bevethetőség, valamint a jelentős többlet oltóvíz kapacitás, mely ráadásul 100%-ban felhasználható, veszteség nélkül, köszönhetően a zárt rendszernek. Mivel a gép belsejében helyezkedik el, ezért a helikopter manőverezhetősége- így az oltóvíz célba juttatásának pontossága, valamint az egyes fordulókörök sebessége jelentősen megnőtt, ami szintén a hatékonyságot növeli.

A kifejlesztett helikopter alkalmas a magas épületek, toronyházak oltására, illetve a bennük történő műszaki mentések végrehajtására is. További alkalmazási területei a csarnokjellegű épületek, illetve az ipari és/vagy veszélyes üzemek oltása. A csarnokjellegű épületek oltásánál a nehézséget főként a rálátás hiánya jelenti, a fentről, a levegőből való megközelítés ezt küszöböli ki. A veszélyes üzemek esetében pedig elsősorban biztonsági szempontból indokolt a légi tűzoltás."[2]

Az új technológiánkkal felszerelt helikopter olyan területeken is bevethető, ahol a környezet adottságai, valamint a katasztrófa jellege, súlyossága miatt más technológiák nem alkalmazhatók. A kifejlesztett MI-2 helikopter belső tartályos (1000 liter) technológia hatékonysági mutatói bevetés közben:

- repült idő, körönként: 2-3 perc,
- tartály feltöltésének ideje: kb. 20-30 másodperc,
- óránkénti felszállás: 12-15,
- oltóanyag veszteség: 0%,
- oltóanyag célba juttatása: 100%,
- üzemanyag felhasználása óránként: 320 liter.

Az új módszernek van egy pótlólagos előnye is: a felszerelt forgószárnyas légi jármű egyszersmind alkalmas mentésre is.

Az általuk kifejlesztett eszközrendszer alkalmazható légi kutatás-mentési tevékenység folytatására is, egy infravörös tartomány érzékelésére éjjel és nappal egyaránt alkalmas eszközzel, ami a tüzek gyors felderítése esetén is indokolt.[3]

A langlovagok.hu oldalon 2006. október 26-én publikált cikkében a témával kapcsolatban ez olvasható Dernei Róbert tollából: „Magyarországon napjainkban nagy kiterjedésű, illetve nehezen megközelíthető helyek oltására eddig a fent említett bamby-bucket-es módszer volt a legelterjedtebb légi tűzoltási technológia. Az oltásnál gyakran használták a kisebb teljesítményű MI-2-es helikoptereket (700 literes puttonnyal), illetve bevetettek nagyobb teljesítményű MI-8-as, vagy MI-17-es honvédségi harci helikoptereket is (2000 literes puttonnyal). Igaz ugyan, hogy a nagyobb hasznos terhelhetőségű helikopterek nagyobb oltóvíz szállítására képesek, de lomhaságuknak köszönhetően az óránként szállított vízmennyiség jelentősen elmarad a kisebb víztömeget szállító MI-2-es gép teljesítményétől.

2 http://www.forgoszarny.hu/szolgaltatasainkkatasztrofavedelmitevekenyseg.html
3 3 http://www.forgoszarny.hu/szolgaltatasainkkatasztrofavedelmitevekenyseg.html

1. kép. A Forgószárny Kft. Mi-2-es helikoptere munka közben
Forrás: www.forgoszarny.hu

A gyakorlatban ez annyit jelent, hogy tűzoltásnál, illetve gátépítő/erősítő munkálatoknál, amíg a nagyobb gépek óránként 3-4 forduló teljesítésére képesek, addig a MI-2-es helikoptereknek elegendő 4-5 perc egy kör teljesítésére, azaz óránként 12-15 alkalommal tudnak teljesíteni fordulót. Ha számításba vesszük a nagyobb helikopterek átlagosan 3-4-szeres többlet üzemeltetési költségét, akkor jó esetben is 6-7-szer gazdaságosabban bevethetők katasztrófalehárítási bevetéseknél. Az új technológiának köszönhetően ezt a hatékonysági mutatót most sikerül tovább fokozni nagyjából a kétszeresére."[4]

Helikopteres tűzoltás Szabolcsban – a Kamov Ka 26

A wikipedián fellelhető információk szerint a Ka–26 (NATO-kódja: Hoodlum) az 1960-as években a Szovjetunióban, a Kamov-tervezőirodában (OKB–938) kifejlesztett koaxiális rotorelrendezésű, dugattyús motoros, könnyű többcélú helikopter. Sorozatgyártása az Ulan-udei Repülőgépgyárban és a Kumertaui Repülőgépgyárban folyt 1969-től. A gyártását az 1980-as évek közepén fejezték be, addig összesen 816 darab készült belőle. Elsősorban mezőgazdasági szerepkörben alkalmazták, de használták személyszállításra és katonai célra, futár-feladatokra is. A helikoptert Magyarországon napjainkban mezőgazdasági munkára (például permetezésre, műtrágyaszórásra) használják.

A géptípust 15 ország alkalmazta és néhány közülük (köztük Magyarország is) a mai napig használja, főleg a mezőgazdaságban. A Varsói Szerződés tagállamai közül katonai feladatkörre egyedül Magyarország rendszeresítette az 1970-es évek elején. A Ka–26 helikopter gyártását már az 1980-as évek elején befejezték.[5]

4 http://www.langlovagok.hu/tuzvonal/181_uj-helikopteres-legi-tuzoltasi-modszert-mutattak-be
5 http://hu.wikipedia.org/wiki/Ka-26

2. kép. A Tréner Kft. Ka-26-os helikoptere
Forrás: saját felvétel

A Ka-26 típusú helikopterrel történő tűzoltás tapasztalatai a nyíregyházi Tréner Kft.-nél

A társaság induló gépparkja 5 db Zlin Z-142-es volt. Mára már több mint egy tucat Légi alkalmassági Bizonyítvánnyal rendelkező repülőgép áll rendelkezésre. Többek közt az alábbi gépek találhatók meg gépparkban: Z-142, Z-326M Tréner, An-2, Pa-28 Cherokee, Pa-23 Aztec, C-152, R-26 S Góbé.[6]

A Tréner Kft. jelenleg több Kamov Ka-26 típusú helikopterrel rendelkezik, ezek egyikét alakították át légi tűzoltási feladatra.

A helikopter 40-150 km/h sebességtartományban repül. Terheléstől függően azonban levegőben történő függeszkedést (lebegést) is tud végezni. Tűzoltási feladatoknál a helikopter előnye, hogy a beavatkozás helyén leszállhat leszállóhely igénye kicsi. A leszállóhely közelsége miatt rövid, mintegy 5 perces repülési fordulóidő elegendő a feladat végrehajtásához. Így óránként 12 felszállást is képes elvégezni. A vízzel történő töltési idő megfelelően nagy teljesítményű szivattyúval 20-30 másodpercre rövidíthető. A légi tűzoltást nagy tapasztalatú, földközeli teherrepülésben (mezőgazdasági jogosítás) jártas helikoptervezetők végezhetik.

A tűzoltásra készen állási idő a helikopter feladatainak függvényében változhat. Amennyiben a helikopter és személyzete csak tűzoltási ügyeleti szolgálatot lát el bármely kijelölt területen, akkor a készen állási idő rövid, körülbelül 15 perc, azonban a beavatkozási terület általában nem a repülőtér közelében van, így az átrepülés idejét is figyelembe kell venni a légi tűzoltás megkezdésénél. Más esetben, amikor a helikopter az ügyeleti szolgálattól eltérő feladatot végez, akkor az oltóberendezés átszerelésének és az átrepülés idejét is figyelembe véve a készenléti idő 1órától 6 óráig terjedhet.

A KA-26-os helikopter 600 liter oltóanyagot tud szállítani, nagy előnye azonban, hogy kisebb átalakítás után 800 liter oltóanyag szállítására is képes lehet. Az oltóanyag kibocsájtására kétféle lehetőség is van, a csapóajtót kinyitva 2-3 másodperc alatt az egészet kiengedheti,

6 www.trenerkft.hu

vagy ha a helyzet úgy kívánja a szórókereten lévő szórófejekből finom permetként bocsájthatja ki. A KA-26 típusú helikopter repülési díja: 5.000 Ft/perc+ÁFA, így az óránkénti díj 300.000 Ft+ÁFA/óra.

A helikopterrel történő oltás előnyei

- Először akkor kapcsolódhat be a kárelhárításba, amikor a beérkező jelzések, riasztások alapján a tűzfészek és a veszélyeztetett terület felderítésére van szükség.
- A helikopterek képesek a folyamatos felügyelet fenntartására, a mentési műveletek koordinálására.
- Vannak feladatok amelyek levegőben lebegő helikopterből hajthatók végre. Lebegő helikopterből csörlő segítségével kötélen a mentést végző személy leereszkedhet a földre, és a leeresztett kötéllel személyek, tárgyak a fedélzetre emelhetők.
- A helikopterre szerelt infrakamerával a tűzfészek jól elhatárolható.

3. kép: Ka-26-os helikopter feltöltése gépjárműfecskendőből a nyíregyházi repülőtéren
Forrás: saját felvétel

Gyakorlati tapasztalatok a Szabolcs-Szatmár-Bereg Megyei Katasztrófavédelmi Igazgatóságnál

A 229 településsel rendelkező Szabolcs-Szatmár-Bereg megyében új szervezeti struktúra keretében Nyíregyházán, Mátészalkán és Kisvárdán alakultak meg katasztrófavédelmi kirendeltségek, Fehérgyarmaton egyelőre csak a törzs működik, a vonuló állomány létszámát jövőre töltik fel. Ezen felül 4 hivatásos tűzoltó parancsnokság (Nyírbátor, Kisvárda, Mátészalka, Nyíregyháza) működik. Fehérgyarmaton eddig önkormányzati tűzoltóság működött, ennek laktanyája viszont nem alkalmas a tervek szerint 39 fős állomány befogadására. A katasztrófavédelmi igazgatóság a volt rendőrkapitányság épületének átvételével kibővítené és felújítaná a laktanyát; a beruházás költségeinek fedezésére 200 millió forint értékben nyújtott

4. kép. Vízleeresztés a nyíregyházi légi bemutatón
Fotó: Balázs Attila

5. kép. A Ka-26-os helikopter feltöltése a gépjárműfecskendőn keresztül
Fotó: Balázs Attila

be pályázatot. A pályázat pozitív elbírálása után jövő év januárjában kezdődhetnek meg a munkálatok, a kirendeltség felállítását pedig 2013. december 31-ig kell befejezni.

A fehérgyarmati hivatásos kirendeltség létrehozása igen fontos: a szatmári és beregi térségben egyedül csak Mátészalkán működik hivatásos tűzoltóság, 89 település mentő-tűzvédelmét pedig önkormányzati tűzoltóságok látják el. Ezek ugyan jól működnek, de mellettük szükség van egy hivatásos egységre is; a mátészalkai katasztrófavédelmi kirendeltség nem tudja ezt a nagy területet egyedül ellátni.

A másik, Baktalórántházán létrehozandó őrs a tervek szerint 19 hivatásos tűzoltóval alakul meg, a jelenleg a köztestületi tűzoltóság által használt laktanyát pedig az önkormányzat térítésmentesen átadja a katasztrófavédelem részére. A fejlesztések célja, hogy a riasztást követően 25 percen belül mindenhová kiérjenek a tűzoltók. Ezt az elvárást azonban 11 megyei településen jelenleg nem tudják teljesíteni, itt a kiérkezési idő 25 perc és 30 perc között van

Magyarországon a tűzoltás műszaki mentés 2012. január 1-jével megváltozott, a volt Hivatásos Önkormányzati Tűzoltóságok beintegrálódtak az egységes Katasztrófavédelembe. Az Országos Katasztrófavédelmi Igazgatóság egységesen „Magyarország Szolgálatában a Biztonságért” célt tűzte ki célul a tűzvédelem, polgárvédelem, és az iparbiztonság területén. Az új kihívás új célokat fogalmaz meg a mentő tűzvédelem területén.

Helikopteres tűzoltás ötletét elsőként az adta, hogy más országokban is használnak repülőket tűzoltáshoz. Másodszor Nyíregyházán van az egyetlen repülőoktató iskola az országban és vannak a kötelékükben forgószárnyas repülők (helikopterek), melyet oktatásra és mezőgazdasági célokra is használnak.

Nem utolsó sorban pedig több évtized után 2012-ben Nyíregyháza rendezhette meg a motoros műrepülő világbajnokságot. A zárónapra betétprogramokat kerestek a szervezők. A Szabolcs Szatmár Bereg Megyei Katasztrófavédelmi Igazgatóságnak együttműködési megállapodása van a repülőtér üzemeltetőjével és így lehetőség nyílt a Hivatásos Tűzoltó Parancsnokság állományának a biztosításon kívül egy betétprogram végrehajtásához. A mi módszerünk abban különbözött, hogy egy mezőgazdasági helikoptert alakítottunk át tűzoltáshoz.

Az előkészítést tapasztalatok nélkül, teljesen az alapoknál kezdtük. A kiindulópontot a helikopter a külső tartály adta. Tűzoltáshoz át kellett alakítani a tartály feltöltési rendszerét, így egy gyorscsatlakozós nyomócsonkot szereltünk a tartályra, valamint a gyorskioldós tartályszelepet hidraulikus nyitással és zárással szereltük fel. A betétprogramra három gyakorlási lehetőségünk volt, mely már tűzoltási tapasztalatok gyűjtésére is megfelelő volt. Gyakorláskor az alábbi létszámmal dolgoztunk: helikoptert egy fő vezette, a földi kiszolgálást hivatásos tűzoltó egység végezte. A kiszolgáláshoz elegendő volt egy fél raj, azaz 1+3 fő. A parancsnok irányította a feltöltést, egy fő a gépjárműfecskendőt kezelte, egy fő tömlőt gurított és csatlakoztatta a helikopterhez.

A Feltöltési idő 15-20 másodperc, ennyi idő alatt 600-800 liter oltóanyagot lehet bejuttatni a helikopter tartályába. Az oltóanyag víz, melyet kísérletképpen 1 százalékos vízlágyítással is (habképző anyag) is kipróbáltunk. A légi tűzoltás előkészítése nem igényel sokkal több szakmai tudást, mint a földi tűzoltásnál képzett hivatásos egységeknél. A pilótának elegendő egy 40 órás alapképzés, hogy tisztában legyen a tűzoltói szakfelszerelésekkel, a hivatásos egységeknek pedig egy komoly munkavédelmi oktatásban kell részesülniük, hiszen a művelet alatt a helikopter rotorjai forgásban (felszállási készenlétben) vannak. A parancsnoknak meg kell tanulni a különböző kézkommunikációkat a helikopter pilótájával, aki teljesen ki

van szolgáltatva a földi egységnek. A pilóta és földi egység összehangolásának idejét a három gyakorlat alapján összesen 60 órában állapítottuk meg.

Tapasztalatok

A Nyíregyháza Hivatásos Tűzoltó Parancsnokságnak eddig nem volt tapasztalata a repülőgépes tűzoltás területén, csak szakirodalmak, előttünk végrehajtott gyakorlatok alapján tudtunk tapasztalatokat gyűjteni.

Arra a megállapításra jutottunk, hogy:

- az oltóanyag mennyiség változtatható 200-800 literig
- a maximális feltöltési idő 15-20 másodperc
- az oltóanyag felhasználás 100 százalék
- a légi jármű gyorsan manőverezik, mert a tartály fixen kapcsolódik a géphez
- az átalakításnak nincsen nagy költségvonzata, a gép továbbra is megfelel a mezőgazdasági célokra.
- az oltási hatékonyságot növelte az 1-3 százalékos vízlágyítás mely azt jelenti, hogy a víz felületi feszültségét csökkentettük, kijuttatáskor a tartálynyitó hidraulikus szelepet lehetett szabályozni így a bekevert oltóanyag ütköztetve - keverve lett.

Ezáltal az oltóanyag az égő felületen nemcsak a gyulladási hőmérsékletet csökkentette, hanem egy takaró hatást is biztosított, mellyel kizárta az oxigént az égéstérből, így kombinált oltást értünk el.

Összességében a KA-26-os helikopterrel ugyanazt a hatékonyságot tudjuk elérni, mint amit a Forgószárny Kft a MI-2-es helikopterrel. Lényeges különbségek:

- kevesebb az üzemanyag-fogyasztás,
- az oltóanyag kijuttatását jelenleg háromféleképpen tudja végrehajtani az átalakított helikopter: teljes kioldás, lassú folyamatos tartálynyitás, valamint a permetező szárnyak szórófejeken való kijuttatás (jobb-bal) oldalt,
- illetve külön, csak az egyik oldalt.

Feltételezésünk szerint egy valós esetnél készenlétbe helyezni és bevetni a legoptimálisabb úgy, hogy első feltöltésnél 600 liter oltóanyagot és 2 fő (pilóta és egy tűzoltás vezető) személyzetet visz magával a gép. Ezáltal megvalósítható a légi felderítés és az első oltás. Ezt követően folyamatos EDR-rádiókapcsolaton keresztül a földi kiszolgáló egység már készenlétben lesz a második és további maximális oltóanyag feltöltésre, földi kiszolgálásra.

A gyakorlat és a bemutató által gyűjtött tapasztalatok alapján valószínűnek tartjuk, hogy a helikopteres tűzoltást hatékonyan nem csak erdőtüzek, avartüzek oltásánál lehet alkalmazni, hanem bár ne kerüljön rá sor, nagy kiterjedésű ipari (gumiipar, faipar, papíripar stb.) létesítmények tüzeinek oltásánál is. Nem elhanyagolható szempont, de kis átalakítással akár élettmentésre is alkalmassá lehet tenni a légi járművet az egységes katasztrófavédelmi rendszer mentő tűzvédelmének fejlesztésében.

A cikk a TÁMOP-4.2.1.B-11/2/KMR-0001 Kritikus infrastruktúra védelmi kutatások projekt támogatásával készült.

IRODALOMJEGYZÉK

Kós György - Dr. Komjáthy László: Erdőtüzek helikopteres oltása in: http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/36_Kos_Gyorgy-Komjathy_Laszlo.pdf
Dr. Hadnagy Imre József: Repülőgépek és helikopterek a tűzoltás szolgálatában in: http://vedelem.hu/letoltes/historia/hist16.pdf
http://www.forgoszarny.hu/szolgaltatasainkkatasztrofavedelmitevekenyseg.html
http://www.langlovagok.hu/tuzvonal/181_uj-helikopteres-legi-tuzoltasi-modszert-mutattak-be.html
http://hu.wikipedia.org/wiki/Ka-26
www.trenerkft.hu

CYBERTERRORIZMUS: VALÓS VAGY TÚLDIMENZIONÁLT VESZÉLY?

Kovács László

Az elmúlt években gyakran hallhattuk, hogy a kibertámadások a 2001. szeptember 11-i támadások következményeinél hatványozottabban nagyobb károkat okozhatnak modern, internettel és információs rendszerekkel átszőtt világukban.

Ugyanakkor mindmádig nem következett be egyetlen egy olyan átfogó és kiemelkedő kibertámadás sem, amely megrengette volna a világot. Természetesen kibertámadások és a velük együtt járó károk sajnálatos részei mindennapjainknak, de sem terrortámadás, sem kiemelten nagyobb ország-ország[1] elleni kibertámadás nem történt, tegyük hozzá rögtön: eddig.

Pedig ha jobban belegondolunk, akkor bárki, aki megfelelő tudással, anyagi és technikai erőforrásokkal rendelkezik komoly károkat tudna okozni egy-egy ország információs rendszereinek működésében. Egy ilyen akció motivációja pedig lehet akár a terror, azaz a megfélemlítés is. Ebben az esetben beszélhetünk kiberterrrorizmusról, vagy ahogy a magyar szaknyelvi terminológia is gyakran használja a cyberterrorizmusról.

Természetesen egy támadás mögött nagyon sok ok és motiváció lehet. Ezen okok közül ma a leggyakoribb az anyagi haszonszerzés. Ugyanakkor jelen írásnak nem célja, hogy a kiberbűnözést, az interenetes bűnözést, vagy a kibertérben elkövetett gazdasági bűncselekményeket vizsgálja, maximum abban a kontextusban ahogy az a cyberterrorizmushoz kapcsolódik. (A cyberbűnözés lehet az egyik leghatékonyabb módja annak, hogy a cyberterrorizmus az anyagi errőforrásait akár annonim módon biztosítsa).

A hagyományos terrorizmus és annak hatása a cyberterrorizmusra

Az 1970-es évektől kezdődően, ahogy a szélsőséges terrorista csoportok Európában is megjelentek számos kutatás vizsgálta és elemezte ezeket a csoportokat, az elkövetőket és akcióikat.

A veszély valós volt, hiszen számos európai országnak éveken, sőt évtizedeken keresztül kellett szembenéznie a különböző terrorista akciókkal. Talán még sokak emlékezetében élénken él az olyan terrorcsoportok neve, mint például a Fekete Szeptember[2];

1 A 2007 tavaszán bekövetkezett Észtországot ért támadás természetesen már lehet előfutára egy ilyen támadásnak.

2 1972. augusztus 26. és szeptember 11. között Münchenben rendezték meg a XX. nyári olimpiát. Szeptember 5-én a Fekete Szeptember nevű terrorista csoport nyolc tagja az olimpiai faluban behatolt az izraeli csapat szálláshelyére, ahol két izraeli sportolót megöltek és kilencet túszul ejtettek. Miután az izraeli kormány megtagadta a követelt 200 palesztin fogoly szabadon bocsátását, a terroristák a német kormánytól repülőgépet követeltek a túszok elszállítására. A terroristákat és a kilenc túszt két helikopteren átszállították a fürstenfeldbrucki katonai repülőtérre, ahol egy Boing repülőgép már várakozott, hogy elszállítsa őket valamelyik arab országba. A repülőtéren a német rendőrség túszmentési akciót kezdeményezett, amely olyan szerencsétlenül végződött, hogy a terroristák megölték túszaikat, illetve a tűzharcban öt terrorista és egy rendőr is meghalt. A három további terroristát elfogták. [1]

IRA[3]; Baader- Meinhof Csoport[4] vagy Vörös Brigádok[5], amelyek abban az időben a napi hírek meghatározói voltak a különböző akcióikkal. [3]

Mindezek után 2001. szeptember 11. újra a mindennapok részéve tette a terrorizmust. A Pentagon és a Világkereskedelmi Központ elleni merényletek új dimenziót jelentettek e veszélyek kapcsán, hiszen a világ egyik vezető hatalmát érték komoly terrortámadások.

A szakértők újult erővel kezdték elemezni a terrorizmust, mint a XXI. század egyik meghatározó veszélyforrását. Ha az ezekből az elemzésekből (vagy akár az elemzések módszertanából) levont következtetéseket párhuzamba állítjuk a kibertér ilyen jellegű, nevezetesen terrorista célú felhasználásával, akkor ezek a következtetések segíthetik a cyberterrorizmus megértését. Ilyen megvizsgálandó kérdések lehetnek:

- a háború és a terrorizmus fogalmi és tartalmi elkülönítése;
- az állami terror és a (nem állami) terrorista csoportok vizsgálata;
- a terrorizmus mozgatórugójának (motivációjának) vizsgálata. [3]

Ugyanakkor már a vizsgálatok kezdetén nyilvánvaló vált az azóta is fennálló tény, hogy nem létezik egységesen elfogadott definíció a terrorizmusra, másrészt pedig akárhány megfogalmazást is nézünk, azok számos ponton eltérnek egymástól. Ennek oka elsősorban talán abban keresendő, hogy az adott fogalom megalkotói más és más szemszögből vizsgálják a kérdést, és így természetszerűleg más és más álláspontot is képviselnek.[6]

A sok meghatározásból egy általánosan jól alkalmazható definíció a Magyar Hadtudományi Társaság által megalkotott:

„Terror, megkülönböztetés nélküli támadás: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében." [4]

Minedezek után néhány olyan sarokpont meghatározása kell, hogy következzen, amely a hagyományos terrorizmus kutatásokból levonható, és amelyek nagy valószínűséggel alkalmazhatók a cyberterrorizmusra is.

Amióta az emberiség „feltalálta" a háborúskodást és háborúkat vív egymással, azóta minden háború természetszerűleg erőszakos cselekményeket tartalmaz és félelmet kelt az emberekben. Amiben a háború mégis különbözik a terrorizmustól az az, hogy itt nem elsődleges cél a terrorizálás, a félelemkeltés, hanem az csak egy járulékos tény, hiszen Clausewitzel élve a háború nem más, mint a politika folytatása erőszakos eszközökkel; két élőerő nyílt összeütközése. Egy másik meghatározó különbség a háború és a terrorizmus között az lehet, hogy a háborúkat alapvetően államok vívják, míg a terrorizmus az állammal (vagy több állammal) szembenálló nem állami csoportok, szervezetek jelenítik meg. Ehhez még az a jellemző is hozzájárul, hogy „a terrorizmus lényege egyértelműen a nyílt ütközet tagadása." [3] [6]

Természetesen a történelemben nagyon sok példát láthatunk arra, hogy az állam, vagy az állami hatalmat gyakorlók lépnek fel a terror eszközeivel az ország állampolgáraival szemben. Ez a fajta terror azonban inkább elnyomó, sokszor brutálisan totális befolyása miatt érdemli ki ezt a jelzőt, ellentétben az általunk tárgyalt hagyományos terrorizmus figyelemfelkeltő, demonstráló jellegével. [3]

Későbbi vizsgálataink előtt – amelyek a cybertérben potenciálisan meglévő terrorizmusra irányulnak –, fontos tisztázni, hogy mi, vagy mik azok a motivációk és mozgatórugók, amelyek a hagyományos terrorizmus esetében tapasztalhatók. Fontos ennek kiderítése illetve feltérképezése, hiszen amennyiben ebben az esetben találunk egyértelmű és kézzelfogható indítékot, akkor ennek analógiáján megkereshető a cyber terror esetében az a kiinduló ok, amely az ottani akciókat mozgathatja és motiválhatja.

Az összetett kérdés viszgálható természetesen a terrorszervezet eredeti motivációja irányából is, de a cybertér esetében egy olyan közegről beszélhetünk, amely a nyilvánosság biztosításában megkérdőjelezhetetlen. Megvizsgálva számos terrorakciót közös tényként értékelhető, hogy minden terrorakció egyik kulcseleme a nyilvánosság. Ez az egyik, nagyon sok esetben – eltekintve a hasonló kivitelezési módoktól –, az egyetlen közös a különböző terrorakciók között. Függetlenül az indítéktól, minden terrorszervezet számára létfontosságú a nyilvánosság különböző fokú biztosítása, hiszen csak ezen keresztül lehetséges, hogy a társadalom szélesebb rétegei is kapjanak információt magáról az akcióról, illetve a szervezet céljairól. A terrorszervezet csak így tudja biztosítana, hogy az erőszakos eszközökkel elkövetett akciók a megfélemlítésen, a bizonytalanságon keresztül befolyásolják a közvéleményt, illetve a kormányzatot. Így tehát a terrorakciók a nyilvánosság számára és a nyilvánosság befolyásolására születnek. [3]

Mindezek alapján összefoglalva a következő területek kutatása történt meg mindezidáig a hagyományos- és a cyberterrorizmus közös vonásainak és egymásra hatásainak vizsgálata során:

- a hagyományos terrorizmus és annak alacsony technológiai szintet képviselő eszköz és alkalmazás használata;
- a terrorizmus és az információtechnológia kapcsolata, azaz mire és hogyan használja a terrorizmus az információtechnológiát;
- a kritikus információs infrastruktúrák sérülékenysége, és ezek terrorista szervezetek általi kihasználása, a veszélyeztetett infrastruktúra elemek feltárása, a támadási módszerek csoportosítása, valamint a védekezés módszereinek, eszközeinek és szervezeti kereteinek meghatározása.

Cyberterrorizmus

Az már a kutatások legelején nyilvánvalóvá vált, hogy a terrorista szervezetek ugyanúgy használják az információs kor vívmányait, mint bárki más a világon.

Néhány példa e felhasználásra: [3]

3 1972. január 30-án – amit azóta „véres vasárnapként" emlegetnek – a brit katonák az internálás ellen tüntető tömegbe lőttek, és 13 embert megöltek. Egyes vélemények szerint ez az esemény járult a leginkább hozzá ahhoz, hogy az IRA terrorista szervezetté váljon. Az IRA 1972 februárjában kezdte meg terrorhadjáratát a protestáns és a brit célpontok ellen. Az erőszak megfékezésére a brit kormány felfüggesztette az észak-ír parlamentet és átvette az országrész irányítását, ahol már tizenötezer brit katona állomásozott. Az IRA bomba-merényletekkel és gyilkosságokkal válaszolt erre a lépésre. [2]

4 Andreas Baader és Ulrike Meinhof vezette csoport nevéhez számos – az 1970-es évek elején elkövetett – merénylet és gyilkosság fűződik. Csoportjukat később átnevezték a RAF–Rote Armee Fraktion, azaz a Vörös Hadsereg Frakció névre.

5 Vörös Brigádok – Brigate Rosse, olasz terroristacsoport, amely a 60-as évek végén Renato Curcio vezetésével szerveződött a Trentói Egyetem szélsőbaloldali köreiben. Tagjai lelkesedtek a forradalom eszméjéért, a parlamentáris demokráciát csak álarcnak tartották, amely mögött zavartalanul folyik a kizsákmányolás és az elnyomás. Céljuk az állam meggyengítése és a proletárforradalom kirobbantása volt. Ezt gyújtogatások, robbantások, emberrablások, gyilkosságok útján akarták elérni. Aldo Moro volt olasz miniszterelnök, a baloldallal történelmi kiegyezést kereső kereszténydemokrata politikus 1978. március 16-i elrablásával, majd megölésével politikai válságot idéztek elő. Ők a felelősek a bolognai pályaudvar felrobbantásáért is. Bár a csoport tagjait már a 70-es évek közepétől kezdték letartóztatni és elítélni, aktivitásuk a 80-as évek végéig tartott. A megszűntnek hitt szervezet 2003 őszén ismét hallatott magáról. Az olasz rendőrség ekkor tartóztatott le hat embert, akit Massimo D'Antona kormányzati tisztviselő négy évvel azelőtti, és Marco Biagi tanácsadó 2002-es megölésével vádoltak. [5]

6 Utalnunk kell itt arra is, hogy a terrorizmus meghatározása nagyon sokszor felveti az elnyomó hatalom vs. szabadságharcos mozgalom kérdéseit is.

Tervezés: az internet segítségével a különböző akciók megtervezése során elengedhetetlen kommunikáció rejtett módóon valósulhat meg. Az internetről letölthető és viszonylag könnyen kezelhető titkosító programok segítségével még annak a veszélye is igen kicsi, hogy kommunikációs, kapcsolattartó tevékenységüket a nemzetbiztonsági szolgálatok lehallgassák. A titkos üzenetváltás egy másik módszere lehet a szteganográfia. Ez azt jelenti, hogy látszólag érdektelen és ártalmatlan hordozókba építenek be a kívülállók számára láthatatlan módon információkat. Ilyenek hordózók lehetnek például különböző formátumú képek, ahol a kép digitális jelei közé vannak elrejtve az információk, vagy ilyen lehet akár egy hang fájl is, amely esetében a háttérzaj tartalmazhatja az információt. Mivel ezekben az esetekben nincs semmi, ami a titkos információtovábbításra utalna ezért legtöbbször nem is kerülnek a felderítők látókörébe.

Toborzás, propaganda, pénzügyi támogatás: új tagok verbuválása, toborzása terén szintén hatalmas lehetőségeket nyújt az internet a hagyományos terrorista szervezetek számára. A különböző terrorista szervezetek által fenntartott weboldalakon nyíltan is történik új tagok toborzása. Ezeken az oldalakon a potenciális új tagok meggyőzésére számos megoldás kínálkozik. A webes technikának köszönhetően egy weboldalon lehetőség van felhívni az érdeklődők figyelmét a szervezet céljaira különböző írásokkal, publikációkkal, a szervezet történetének és vezetőinek bemutatásával, az eddigi akciókról készített videók, pedig sokszor le is tölthetők. Lehetőség van továbbá pénzbeli adományok gyűjtésére is e lapok segítségével. Ilyen lapok szép számmal Európában is működnek hiszen a nyugat-európai országok bevándorlói, illetve azok gyerekei között szép számmal akadhat szimpatizáns, aki ilyen módon megszólíthatóak.

Adat- és információszerzés: talán az egyik legnagyobb kihívásként jelentkezik ez a fajta tevékenység napjainkban. A nyugati társadalmak igen nagyfokú információs szabadsága sok esetben azt jelenti, hogy számos létfontosságú infrastruktúra elem tervrjaza, azok támadható pontjai nyiltan elérhetőek az interneten. A terrorista szervezetek számára is adott a lehetőség, hogy a számukra szükséges információkat megkeressék. Mindezeken túl az individualista támadó nagyon sok kész receptet talál pl. a házkészítésű bombák előállítására. Talán erre a legjobb példa a 2013 áprilisában bekövetkezett bostoni terrortámadás, amely előkészületei során az elkövetők a később a tömegben felrobbantott kukta-bombák ötletét és elkészítésének receptjét az internetről töltötték le.

1. kép. Angol nyelvű iszlamista blog [7]

Amennyiben megvizsgáljuk a cybertámadások történelmét, akkor azonban nagyon kevés kimondottan cyberterrorista támadást találunk.

Nagyon sokáig az első és egyetlen cyberterrorista akcióként[7] aposztrofálták az LTTE (Tamil Eelam Felszabadító Tigrisei) nevéhez fűződő támadást, amely során 1997-ben a szervezet aktivistái spamekkel árasztották el a világ különböző országaiban működő srí lankai követségek e-mail postaládáit, válaszul néhány tagjuk bebörtönzésére. Az akció nagy kárt nem okozott, de felhívta a figyelmet az információs rendszerek sebezhetőségére, illetve arra a tényre, hogy a hagyományos terrorista szervezetektől sem áll távol az információs támadás.[3] [8]

1997 júliusában e-mail bombatámadás érte az Institute for Global Communications (IGC) amerikai internetszolgáltatót, akik az Euskal Herria (Baszk Újság) honlapját tartották fenn. A támadás a honlap eltávolítását követelte. [3] [9]

2000 márciusában a Japán rendőrség bejelentett, hogy több mint 150 rendőrségi gépjármű számítógépes rendszerében olyan kémprogramokat találtak, amelyeket többek között követésre, valamint adatlekérésre programoztak. A vizsgálat kiderítette, hogy a gépjárművek fedélzeti szoftvereit az Aum Shinryko terrorista csoporthoz köthető egyik vállalkozás fejlesztette. (Ez a terrorista a csoport követte el a Tokiói metróban, 1995-ben a 12 halálos, és több mint 6000 sérültet okozó szaringáz támadást). A szoftverek segítségével 115 rendőrségi gépjármű helyét követték, amelyek között több civil autó is volt. A további vizsgálatok rámutattak, hogy a csoport több mint 80 japán cég és 10 kormányzati szerv számára szállított szoftvereket korábban. Ezekbe a leszállított szoftverekbe trójai programokat telepíttettek egy későbbi terrortámadás elősegítésére. [3] [10]

2002 októberében az internet legfontosabb infrastruktúrái ellen indult összehangolt támadás. Ekkor a 13 DNS[8] root szerver ellen követtek el DoS[9] illetve DDoS[10] támadásokat. Ez a fajta támadás 2007 februárjában megismétlődött. Szerencsére egyik esetben sem sikerült komoly fennakadást okozni a nemzetközi internet forgalomban, amely egyrészt annak köszönhető, hogy a 13 root szerver több mint 40 helyen tükrözve van. [3] [11]

2003-ban román elkövetők megzsarolták az amerikai National Science Foundation-t (NSF), hogy eladják a szervezet feltört és így nagymértékben feltérképezett számítógépes hálózatának adatait, amennyiben nem kapnak megfelelő anyagi ellenszolgáltatást. Ez a hálózat irányította a Déli-sarkon lévő NSF által fenntartott kutatóbázis energiaellátását és fűtését. Miután bebizonyosodott a fenyegetés valódisága, le kellett választani a kutatóbázis hálózatát. A támadást később terrortámadásnak minősítették. [3] [12]

Megvizsgálva mindezeket a támadásokat, valamint a nemzetközi terrorszervezetek (pl. al-Kaida, Hezbollah) internetes tevékenységeit – weblapjait, webes kommunikációs felületeit –, egyértelművé válik, hogy a terrorista szervezetek is egyre inkább használják az információs rendszereket, magát az internetet, sőt támadásaikat azon keresztül is kivitelezhetik. Ennek kapcsán joggal merül fel a cyberterrorizmus kérdése.

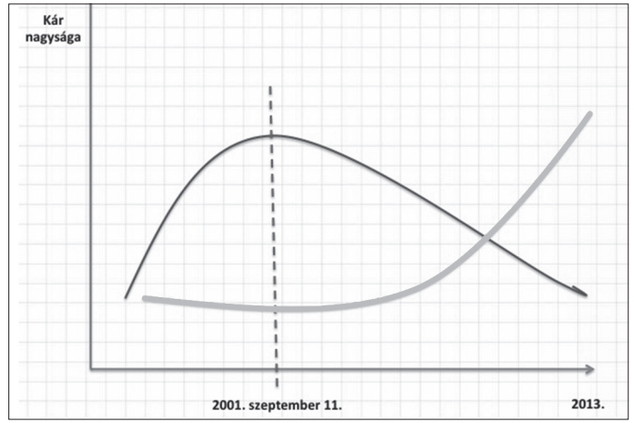
A témában a cyberterrorizmusra vonatkozó egyik legelső meghatározás az FBI úgynevezett cyber részlegének volt vezetőjétől – Keith Lourdeau-tól – származik: „A cyberterroriz-

7 Ezen a helyen azokat a támadásokat is cybertámadásoknak tekintettük, amelyeket hagyományos terrorszervezetek, vagy olyan csoportok, személyek követtek az interneten keresztül, amelyek terrortámadásnak minősíthetőek.
8 Domain Name Server
9 DoS: Denial of Service, azaz túlterheléses támadás.
10 DDoS: Distributed Denial of Service, azaz elosztott túlterheléses támadás.

mus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében." [13]

A cyberterrorizmus egy másik meghatározása röviddel 2001. szeptember 11-e után Dorothy Denning professzortól származik: a *„cyberterrorizmus számítógép alapú támadást vagy fenyegetést jelent, amelynek célja, hogy megfélemlítsék, vagy kikényszerítsék a kormányok vagy a társadalmak részéről az adott terror szervezet politikai, vallási, vagy ideológiai céljainak elérését."* [14]

A meghatározásokból is kitűnik, hogy a terrorista csoportok két, egymástól elkülöníthető célból használják az információtechnológiát. Az első csoportba, azok a terrorista szervezetek tartoznak, amelyek a már említett célokra – propaganda, toborzás, adatszerzés – használják e rendszereket. Gyakran e tevékenységet soft, azaz puha típusú cyberterrorizmus névvel is illetik. A másik – hatványozottan veszélyesebb – csoportba azok a terroristák tartoznak, akik nemcsak ilyen úgynevezett soft tevékenységre kívánják használni a rendszereket, hanem azt, illetve azon keresztül rombolni vagy egyéb erőszakos, hard cselekményeket is végre akarnak hajtani. Célpontjaik között nemcsak az internet szerepel, hanem minden olyan kritikus információs infrastruktúra is, amelyek információtechnológiai eszközökkel, vagy fizikai támadásokkal pusztíthatók. [15]



1. ábra. Világosabb vonallal jelölve a cybertámadások okozta potenciális károk, összehasonlítva a hagyományos terrortámadások által okozott károkkal (szerk.: Kovács L.)

Jelen írás céljai között nem szerepel, hogy ezeket a kritikus (létfontosságú) információs rendszereket (infrastruktúrákat) elemezze, de nagyon könnyen belátható, hogy ezek a rendszerek, illetve ezek egyes, kulcsfontosságú pontjai lehetnek egy adott cyberterror támadás célpontjai. Az ok rendkívül egyszerű. A nyugati társadalmak olyan mértékben kiszolgáltatottá váltak az élet minden területén ezekkel a rendszerekkel szemben, hogy amennyiben azok közül akár egy is, akár időlegesen is kiesik a működésből az beláthatatlan következményekkel jár. Természetesen itt vissza kell utalni arra a korábban tárgyalt kitételre, hogy minden

terrorakció, így a cyberterrorista támadások fő célja a megfelelő nyilvánosság és a megfelelő publicitás biztosítása.

Mindezek alapján felsorolás jelleggel a lehetséges cyberterrorista célpontok:

- energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
- kommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás számítógép-hálózatai;
- pénzügyi-gazdasági rendszer számítógép-hálózatai;
- védelmi szféra riasztási, távközlési, számítógép-hálózatai;
- egészségügyi rendszer számítógép-hálózatai;
- kormányzati és önkormányzati információs rendszerek. [16]

A terrorista célú cybertámadások során alkalmazható eszközök és módszerek nagy hasonlóságot mutatnak a más célú (pl. kiberbűnözés során alkalmazott) támadásokéval. A cyberterrorista ugyanúgy használhat rosszindulatú programokat (férgeket, kémprogramokat, backdoor programokat, keyloggereket), valamint változatos informatikai támadási módszereket (pl. denial of service, distributed denial of service, man-in-the-middle attack, cross site scripting).

A cyberterrorizmus és általában az informatikai támadások vonatkozásában különösen nagy veszélyt jelent a 2010 nyarán megjelent Stuxnet nevű féreg (worm) és annak következményei, hiszen a Stuxnet okozta pánikot követően számos hír látott arról napvilágot, hogy a Stuxnet, illetve az abban megjelenő új informatikai támadási módszerek terrorszervezetek kezébe kerültek. [15]

A hagyományos terrorista szervezetek cybertérben történő tevékenységére jellemző, hogy 2001-ben még csak alig néhány, az al-Kaidához köthető vagy azzal szimpatizáns web-oldalt tartottak számon, ugyanakkor ezek száma 2001. szeptember 11-ét követően gyors növekedésnek indult. Khaled al-Faram szaudi kutató 2007-ben publikált adatai alapján már 5600-ra tette az ilyen weboldalak számát. [15] [17]

Az al-Kaida ezt a tevékenységet saját honlapjain nagyon gyakran digitális dzsihádnak hívta. A digitális dzsihád egyik élharcosa az Irhabi 007 nevet használó marokkói származású fiatal számítógépes zseni Junisz Tszuli volt.

2. kép. Janusz Tszuli, alias Irhabi 007 [18]

Az irhabi arabul terroristát jelent, míg a 007 valószínűleg James Bond-ra utal, hiszen Tszuli Nyugat-Londonban élt egészen 2006-os letartóztatásáig. Irhabi két évig arab és angol nyelvű, dzsihádot hirdető – csak meghatározott felhasználóknak elérhető, jelszóval igénybe vehető – fórumokon szakértői tanácsokat adott az esetenként több ezer látogatónak az internetes sérülékenységekkel, azok kihasználásával, valamint a saját – hálózaton folytatott – tevékenységük minél tökéletesebb titkosításával kapcsolatban. Számos multimédiás anyagot készített és ezek segítségével online oktatásokat is tartott a dzsihádban résztvevőknek. A bérelt szervereken tárhelyet biztosított dzsihádistáknak, hogy olyan anyagokat és szoftvereket töltsenek fel, amelyek különböző internetes támadásokban felhasználhatóak. Naprakész listákhoz jutottak hozzá a fórumozók, amelyben a különböző legújabb webes és egyéb sérülékenységeket mutatták be. [15]

Természetesen mindebből nem szabad azt a téves következtetést levonni, hogy a cyberterrorizmus megegyezne az iszlám terrorizmussal, csakúgy, mint ahogy ez nem igaz a hagyományos terrorizmus és az iszlám kapcsolatára sem.

Következtetések

A jelen írásban megfogalmazottak természetszerűleg csak egy felvillantás erejéig engednek bepillantást a cybertérben folyó – ma már nagyon is reális – küzdelmekbe.

Számos olyan területe van a cybertérben folytatott egyre élénkülő tevékenységeknek, amelyekről nem tettünk említést. Nem beszéltünk az olyan kérdésekről, mint például a hacktivista szervezetek és a terrorizmus kapcsolata, hiszen ezeket a szervezeteket nagyon gyakran és nagyon hibásan aposztrofálják terrorszervezeteknek. Nem beszéltünk a cyberterror elleni védekezés jogi, jogszabályi és szervezeti, vagy akár nemzetbiztonsági kérdéseiről.

Egyet azonban nagy bizonyossággal kijelenthetünk reflektálva az írás címére: a cyberterror jelentette fenyegetést nem lehet túldimenzionálni, hiszen egy-egy ilyen támadás következménye nem csak technikai és anyagi értelemben lenne hatalmas, hanem bizony akár emberéletekben is beláthatatlan károkat okozna. Ezt a – talán nagyon is markáns – megállapítást az is alátámasztja, hogy ma egyre többen rendelkeznek azzal a tudással, amelyek egy-egy ilyen támadás elkövetéséhez szükséges lehet. Az akciók megtervezéséhez pedig számos forrás áll rendlekezésére bárkinek, aki az infokommunikációs eszközöket csak egy kicsit is tudja használni.

A motiváció és az akarat – erre láttunk példát 2001. szeptember 11-én – óriási meglepetésket okozhat ezen a téren is.

A cyberterrorizmus veszélye tehát reális. Ezt a veszélyt nem lehet túldimenzionálni, hiszen függőségünk kritikus információs rendszereinktől rendkívül nagy. Ez a függőség olyan mértékű, hogy amennyiben ezen rendszerek akár időlégesen is vagy csak részlegesen kiesnek a működésből, az nemcsak anyagi, de emberéletekben mérhető károkat okoz gyakorlatilag a nyugati világ bármelyik országában. Tovább növeli a veszélyt, és ezzel a sérülékenységet, hogy ezek a rendszerek olyan interdependenciában, azaz olyan kölcsönös függőségben állnak egymással, hogy egy rendszer vagy rendszerelem meghibásodása számtalan más – nagyon gyakran előre nem is definiálható számú – rendszer működését is megbénítja akár egész földrészeken átívelő volumenben.

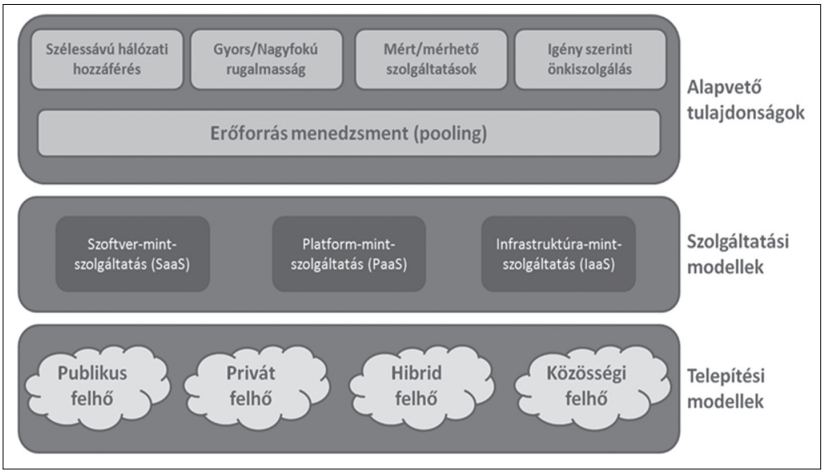
IRODALOMJEGYZÉK

[1] http://www.ezenanapon.hu/main.php?reszletes=414=9=5
[2] http://www.origo.hu/tudomany/tarsadalom/20011106iraes.html
[3] Kovács László: Az információs terrorizmus eszköztára. in: HADMÉRNÖK 2007(1) pp. 1-18. (2007)]
[4] Hadtudományi Lexikon MHTT Budapest, 1995.
[5] http://www.enc.hu/1enciklopedia/fogalmi/poltud/vor_brig.htm
[6] Charles Townshend: A terrorizmus, Magyar Világ kiadó, 2001.
[7] http://ansarullah.co.cc/en
[8] http://konfliktus.index.hu/sritigrisek.html
[9] http://www.bbc.co.uk/politics97/news/07/0719/eta.shtml
[10] http://fas.org/irp/threat/terrorism/sup2.pdf
[11] http://index.hu/tech/biztonsag/hekk0207
[12] http://www.fbi.gov/page2/july03/071803backsp.htm (2008.06.10.)
[13] http://www.fbi.gov/congress/congress04/lourdeau022404.htm
[14] Dorothy E. Denning: Is Cyber Terror Next? http://essays.ssrc.org/sept11/essays/denning.htm
[15] Haig Zsolt, Kovács László, Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. in: FELDERÍTŐ SZEMLE X. évf.:(1-2.sz.) pp. 183-209. (2011)
[16] Haig Zsolt – Kovács László – Ványa László: Kritikus információs infrastruktúrák támadása, védelme. Dunaújvárosi Főiskola Közleményei, XXIX/1. ISSN 1586-8567
[17] http://news.softpedia.com/news/Al-Qaeda-Threatening-The-World-The-Virtual-One-72876.shtml
[18] http://writhink.files.wordpress.com/2009/07/irhaby007.jpg

A SZÁMÍTÁSI FELHŐ BIZTONSÁGI KÉRDÉSEI

Kozlovszky Miklós – Schubert Tamás

A felhőszolgáltatások az informatika egyik legdinamikusabban fejlődő területévé váltak az utóbbi néhány évben. A felhőszámítás (Cloud Computing) paradigma, ötvözi több technológia /elsősorban a virtualizáció, valamint grid számítási (grid computing) és fürt számítási (cluster computing) koncepciók/ előnyös tulajdonságait. A felhőszámítás - Cloud Computing meghatározásakor az Institute for Standards and Technology (NIST) Information Technology Laboratory definícióját szokás idézni[1]: „A felhőszámítás olyan modell, amely lehetővé teszi konfigurálható számítási erőforrások (pl.: hálózatok, kiszolgálók, tárolók, alkalmazások és szolgáltatások) osztott készletének kényelmes, igény szerinti, hálózaton keresztül történő elérését, melyek gyorsan, kevés felügyeleti ráfordítással és szolgáltatói beavatkozással munkába állíthatók és eltávolíthatók”



1. ábra. A felhőszámítás modelljei és alapvető tulajdonságai

Napjainkban minden technikai akadály elhárult az elől, hogy az informatika is - az áram- vagy a vízszolgáltatáshoz hasonlóan - szolgáltatássá váljék. Az utóbbi 5-7 évben a vállalatok felismerve a felhő infrastruktúrák által biztosított előnyöket (kisebb fenntartási költségek) egyre gyorsuló ütemben csökkentik saját infrastruktúra és ezekhez kapcsolódó szakértő humán erőforrás fejlesztéseiket és választják inkább a felhő infrastruktúrákat. A felhő rendszerek jelenleg egymástól elszigetelten, szigetszerű infrastruktúrákként működnek és az alábbi főbb szinteken biztosítanak szolgáltatásokat (a teljesség igénye nélkül):

- IaaS – infrastruktúra nyújtása szolgáltatásként (pl.: Amazon, Microsoft Azure, stb.)
- PaaS – platform nyújtása szolgáltatásként (pl.: Google, Microsoft Azure, Force.com, stb.)
- SaaS – alkalmazás nyújtása szolgáltatásként (pl.: SalesForce, a legtöbb WEB2 alkalmazás, online szoftverek, stb.)
- NaaS – hálózat nyújtása szolgáltatásként (pl.: Cisco, stb.)

Az egyes szigetszerű felhő rendszerek esetében általánosan elmondható, hogy közöttük az átjárás nehezen megoldott. A publikus felhőket használni szándékozó vállalatok jelenleg súlyos döntési helyzetben vannak és valójában a kedvező pénzügyi konstrukciók, vagy a biztonság között kell választaniuk. A felhő infrastruktúrába átültetett (virtualizált) alkalmazások, valamint a vállalatok belső adatainak felhőben történő tárolása csak akkor kivitelezhető, ha a vállalatok megbízhatnak az adott szolgáltatóban. A versenyképesség, megbízhatóság és bárhonnan/bármikor/bárhogyan történő elérhetőség érdekében a vállalatoknak el kell fogadniuk/hinniük, hogy a felhőszolgáltató megfelelően biztonságos, és adataik nem kerülhetnek illetéktelen kezekbe. A felhő szolgáltatóknak ehhez ugyanolyan vagy magasabb szolgáltatási minőséget kell garantálniuk, mintha a felhasználók saját informatikai kapacitással (hardver, szoftver, szakértelem) rendelkeznének. A szolgáltatási minőség az informatikai biztonságot is magába foglalja.

A felhő infrastruktúrák és ezeken definiált szolgáltatások napjainkban már lehetővé teszik akár komplett cégek virtualizált üzemeltetését is, ahol nem csak a számítógépes programok, számítógépek, szerverek, de még maga a hálózat, sőt az adatközpont is teljes egészében virtualizált. A felhő infrastruktúrák teljes helyfüggetlenséget biztosíthatnak, ami egyik oldalról gyors és hatékony adatmigrációt, dinamikus erőforrás allokációt tesz lehetővé, másik oldalról azonban bizalmas adatok esetében problémát jelenthet a nemzeti határok és az adatintegritás garantálása. Kritikus nagyvállalati, illetve kormányzati szintű infrastruktúrák esetében, amikor a kiemelt biztonságot igénylő alkalmazások adatainak nyílt felhőben való tárolása vagy a számítási erőforrások esetleges kiesése nem megengedhető, a nyilvános felhőszolgáltatás (public cloud) helyett adott adatközpontokban megvalósított magán felhőszolgáltatás (private cloud) biztosíthat hatékony megoldást. A kétféle szolgáltatás alap filozófiája és használt technológiája azonos, alkalmazható kibervédelmi megoldásaik jól átfedik egymást.

A számítási felhő vagy Cloud Computing az informatikai szolgáltatások bérleti rendszerű igénybevételével szükségtelenné teheti az infrastruktúra helyi kiépítését. Az informatikai szolgáltatások olcsóbbá válnak, mivel az adatközpontok kihasználtsága többszöröse is lehet a helyi infrastruktúra kihasználtságánál. A vállalati informatikai beruházások a korábbinak töredékére eshetnek vissza, mindemellett a bérleti költségek az igénybe vett szolgáltatással arányosan folyamatosan merülnek fel. Sok jó tulajdonsága mellett a felhőszolgáltatás számtalan kérdést vet fel a rendelkezésre állás és az informatikai biztonság szempontjából.

A kiemelt biztonságot igénylő vállalati alkalmazások esetén nem engedhető meg az adatok felhőben való tárolása vagy a számítási erőforrások esetleges kiesése, ezért a nyilvános mellett létrejött a vállalati adatközpontban megvalósított magán felhőszolgáltatás.

A felhőszolgáltatás öt lényeges jellemzője [2]:

- A szolgáltatás igény szerinti használata (On-demand self-service). A felhasználók egyoldalúan és emberi beavatkozás nélkül foglalnak számítógépi erőforrásokat (szerver idő, CPU teljesítmény, memória, hálózati tárolókapacitás).
- Hálózati elérés. A szolgáltatások távolról, hálózaton keresztül érhetők el a legkülönfélébb eszközök segítségével (PC, laptop, vékony kliens, mobil telefon, PDA).

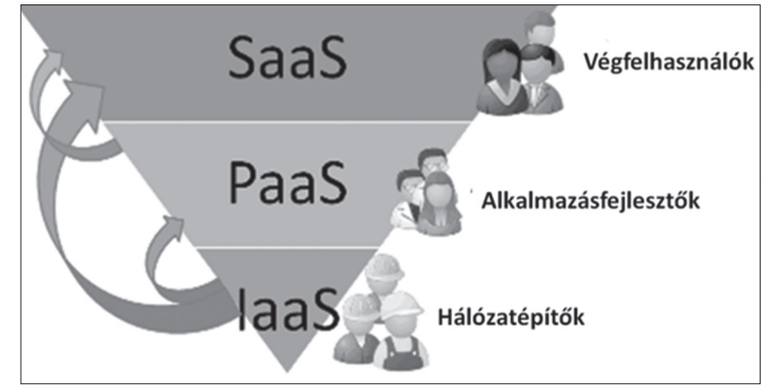
- Erőforrás készlet kialakítása. A szolgáltató számítógépi eszközparkot hoz létre, amelynek erőforrásait a felhasználók dinamikusan, az igényeiknek megfelelően vehetik igénybe. A pillanatnyilag igénybe vett erőforrások helyére vonatkozóan a felhasználóknak általában nincs információjuk, bár egyes megoldásokban bizonyos absztrakciós szinten (pl. ország, adatközpont) lehet választásuk. Az erőforrás alatt többnyire tárolót, processzort, memóriát, hálózati sávszélességet és virtuális gépet értenek.
- Rugalmasság (elasticity). Az erőforrások gyorsan, rugalmasan és gyakran automatikusan rendelkezésre bocsáthatók vagy visszaadhatók (quick scale out and scale in). Az elérhető erőforrások mennyisége a felhasználók számára gyakran korlátlannak tűnik, és bármikor bármilyen mennyiségben igénybe vehető.
- A szolgáltatás mérése. A felhő automatikusan vezérli és optimalizálja az erőforrások felhasználását, amelyet a szolgáltatás típusának megfelelő absztrakciós szinten (tároló, processzor, sávszélesség, stb.) méri. Az erőforrások felhasználását a felhő a szolgáltató és a felhasználó számára átlátható módon monitorozza, szabályozza, és dokumentálja.

Felhőszolgáltatások használata kritikus alkalmazási környezetben (pl.: közigazgatás, államigazgatás, honvédelem, stb.) is lehetséges, csak az adott környezetben elvárt SLA-t (rendelkezésre állás és biztonság) a szolgáltatónak (public, hybrid, private, community) garantáltan biztosítania kell. A felhőszolgáltatások használata kritikus alkalmazási környezetben is alkalmazható, hiszen a felhőszolgáltatás fent vázolt öt lényeges jellemzője olyan előnyöket biztosít, amely csak extrém elvárások esetén szabad mellőzni.

A felhő szolgáltatások alkalmazhatóságának van még 3 paramétere, melyekkel kapcsolatban jelenleg igen intenzív kutatások folynak.:

Felhő szolgáltatási modellek

A 2. ábra szerint az egyes szolgáltatások közvetlenül más szolgáltatásokra épülnek, de nem minden esetben van ez így. Előfordul, hogy egy adott szolgáltatás típust olyan architektúrában valósítanak meg, hogy az igénybe vett szolgáltatások önálló szolgáltatásként nem jelenhetnek meg.



2. ábra. Felhő szolgáltatási modellek

Infrastruktúra – mint - szolgáltatás (Infrastructure as a service - IaaS)

Az infrastruktúra szolgáltatásként történő használata alatt szűkebb értelemben fizikai vagy virtuális számítógépeket értenek, tágabb értelemben a tárolókapacitások, a hálózati infrastruktúra vagy akár egy teljes virtuális adatközpont önálló használataként is értelmezik. Mivel a tágabb értelmezés fenti esetei önálló névvel is rendelkeznek, az IaaS jellemzőit a szűkebb értelmezéshez adjuk meg.

- A szolgáltatók a számítógépi erőforrásokat platform/szerver virtualizációs környezetben bocsátják az előfizetők rendelkezésére, bár igény szerint fizikai számítógépek használatát is lehetővé teszik;
- Az előfizetőknek nem szükséges az eszközöket (számítógépek, tárolók, hálózati berendezések, szoftver licencek, stb.) megvásárolniuk és üzemeltetniük;
- Az előfizetők az erőforrásokat kihelyezett szolgáltatásként vásárolják meg;
- Csak a ténylegesen használt erőforrásokért kell fizetni (pl. óránként);
- A szolgáltatás minősége (QoS) az SLA-ban rögzíthető;
- A szolgáltatás az internet segítségével érhető el;
- Ma már számos szolgáltatás vehető igénybe (pl. Amazon EC2, Amazon S3).

Platform-mint-szolgáltatás (Platform as a service - PaaS)

A Platform magában foglalja a felhő alkalmazás fejlesztésének, tesztelésének, telepítésének és üzemeltetésének teljes életciklusát, valamint sok esetben az ezekhez alkalmazható fejlesztői és üzemeltetői keretrendszereket. A teljes életciklus a felhőszolgáltatásra épül.

A PaaS jellemzői, előnyei:

- A felhőalkalmazások fejlesztését, tesztelését, telepítését, futtatását és felügyeletét ugyanaz az integrált környezet látja el (költségek csökkennek, minőség és rendelkezésre állás nő);
- A felhasználói kényelemet, a megfelelő válaszidőt, és a minőséget kompromisszum nélkül biztosítani kell (a hagyományos alkalmazásokéval azonos elvárások);
- A méretezhetőség, a megbízhatóság, és a biztonság járulékos fejlesztés, konfigurálás és költség nélkül biztosítható. Több bérlő kiszolgálása (multi-tenancy) automatikusan biztosítva van. Az adatok tárolásának, továbbításának és a pénzügyi tranzakcióknak biztonságosnak kell lenniük az alkalmazás teljes életciklusában;
- A Web szolgáltatások és adatbázisok elérése eleve alapértelmezett szolgáltatásként biztosított (távoli szolgáltatások és adatok elérése);
- Fejlesztők és fejlesztői csoportok támogatása biztosított. Az együttműködést a platformnak az alkalmazás teljes életciklusában külön konfiguráció nélkül biztosítania kell;
- Az alkalmazásba beépülő mélységi monitorozás segítségével a felhasználók aktivitását, a hibákat és a teljesítmény problémákat rögzítik. Ez az információ segíti a fejlesztőket az alkalmazásaik javításában és a felhasználók újabb elvárásainak megismerésében.

Szoftver-mint-szolgáltatás (Software as a service - SaaS)

A SaaS jellemzői, előnyei:

- Az alkalmazások az internet segítségével érhetők el és felügyelhetők;
- Az alkalmazások kizárólag internet böngészővel érhetők el, helyi installálás nem szükséges;
- Az alkalmazás adatstruktúrája (distributed model) és a program architektúrája lehetővé teszi az alkalmazás egyidejű használatát sok felhasználó számára (multi-tenancy);
- Uniformizált alkalmazások könnyen átültethetők a felhőbe. Az SaaS alkalmazásoknak kellően általánosnak kell lenniük, hogy sok felhasználó is használni tudja;
- Az alkalmazások testre szabása programozás nélkül, kizárólag paraméterezéssel elvégezhető;
- A kommunikáció biztonsága SSL használatával érhető el;
- A felhasználóknak nem kell szoftver licenceket vásárolniuk, kizárólag a szolgáltatásért fizetnek (pl. havidíj vagy felhasználónkénti díj);
- A SaaS alkalmazásoknak rendelkezniük kell mérő és monitorozó szolgáltatással, hogy az előfizetőknek csak a tényleges használatot számítsák fel;
- A SaaS alkalmazásoknak beépített számlázási szolgáltatással kell rendelkezniük;
- A SaaS alkalmazásoknak nyilvános fejlesztői/kapcsolódási felülettel és ecosystem partnerekkel kell rendelkezniük, akik kibővíthetik az előfizetők körét és az alkalmazás piaci részesedését;
- A SaaS alkalmazásoknak biztosítaniuk kell, hogy az ügyfelek adatai és speciális konfigurációi biztonságosan elkülönüljenek más ügyfelek adataitól és konfigurációitól;
- Az SaaS alkalmazások többnyire kifinomult üzleti folyamat konfigurátort biztosítanak az ügyfelek számára;
- A SaaS alkalmazásoknak állandóan új szolgáltatásokkal és képességekkel bővülhetnek;
- A SaaS alkalmazásoknak biztosítaniuk kell az ügyfelek adatainak integritását;
- A szoftver licenceket a szolgáltatók kezelik;
- A költség sok ügyfél között oszlik el;
- A szoftverkarbantartást a szolgáltató végzi;
- A verziókövetést a szolgáltató végzi;
- Az ügyfél hardver költségei csökkennek;
- Tömeges használat esetén a hardver méretezhetősége a szolgáltatónál könnyebben kézben tartható.

Lehetséges hátrányok:

- Hálózati problémák;
- Biztonsági hiányosságok;
- Szolgáltató függőség;
- Korlátozott testre szabhatóság.

Megjegyezzük, hogy a szolgáltatási modellek bemutatásakor itt csak a hagyományos (SPI modellek – Software, Platform, Infrastructure) megoldásokra tértünk ki, az újabb keletű Service Broker-ek által nyújtott lehetőségekre nem.

Felhő telepítési modellek és szolgáltatásaik

A szolgáltatási modellektől (IaaS, PaaS, SaaS) függetlenül négy telepítési modellt dolgoztak ki, melyek mind különböző speciális felhasználói igényeket elégítenek ki.

Nyilvános felhő infrastruktúra (Public cloud)

A nyilvános felhő infrastruktúra a nagyközönség vagy egy nagyobb felhasználói csoport számára nyújt szolgáltatásokat, és a szolgáltatást nyújtó szervezet tulajdonában van.

A felhőszolgáltató vállalatoknak és magánszemélyeknek egyaránt kínál szolgáltatásokat. Néhány példa, amikor a nyilvános felhő a legjobb választás:

- Sokak által használt szabványos szolgáltatás, pl. e-mail;
- Alkalmazások fejlesztése és tesztelése;
- Vállaltok által igénybe vett fokozottan biztonságos SaaS alkalmazás;
- Extra számítási kapacitás igénybe vétele csúcs időben;
- PaaS fejlesztő környezet használata.

Magán felhő infrastruktúra (Private cloud)

A magán felhő infrastruktúra kizárólag egyetlen szervezet számára nyújt szolgáltatásokat, melyet maga a szervezet vagy egy másik fél üzemeltet, és a szolgáltatást igénybevevő szervezet telephelyén vagy azon kívül helyezkedik el.

A magán felhő infrastruktúra használatának leggyakoribb okai:

- A titkossággal és a biztonsággal szemben támasztott fokozott elvárások;
- Irányítási és megfelelőségi követelményekhez történő igazodás;
- A vállalatok már rendelkeznek megfelelő infrastruktúrával, de jobb kihasználásra törekednek;
- A vállalatok a teljesítménnyel és rendelkezésre állással szemben fokozott követelményeket támasztanak;
- Bizonyos esetekben az erőforrások kihasználása elérheti a 90%-ot is.

Közösségi felhő infrastruktúra (Community cloud)

A közösségi felhő infrastruktúrán több szervezet osztozik, és valamilyen közös vonatkozással, érdeklődéssel bíró közösség számára nyújt szolgáltatást. Az üzemeltetést végezheti maga a szervezet vagy egy másik fél, és a szolgáltatást igénybevevő szervezet telephelyén vagy azon kívül helyezkedik el.

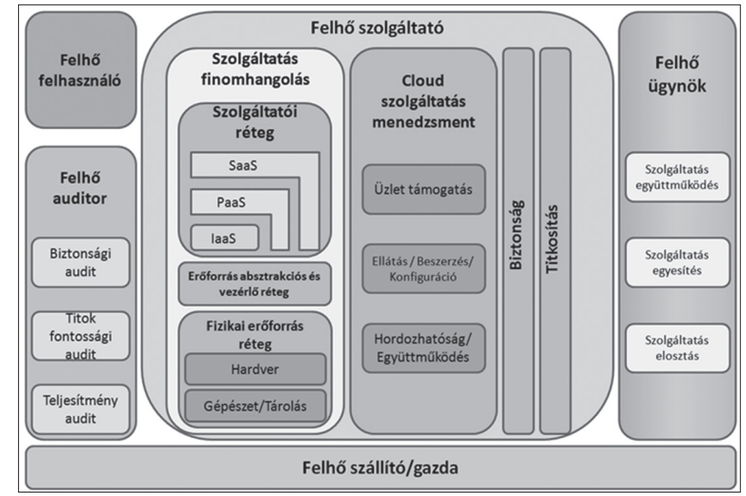
Hibrid felhő infrastruktúra (Hybrid cloud)

A hibrid felhő infrastruktúra két vagy több, más telepítési modellbe tartozó felhő kompozíciója, amely egyetlen felhőként jelenik meg. Az összekapcsolt felhők olyan szabványos vagy gyári protokollal vannak összekapcsolva, amely biztosítja az adatok és az alkalmazások mozgását/ hordozhatóságát.

A nyilvános és magán felhőszolgáltatás esetében alkalmazott technológiák jórészt azonosak. A magán felhőszolgáltatás esetében a beruházási költségek a vállalatnál merülnek fel, az erőforrások jobb kihasználása azonban csökkenti a fajlagos beruházási költségeket. A hibrid felhő a magán felhő összekapcsolása a nyilvános felhő infrastruktúrával.

A felhő számítás referencia modellje

A NIST felhő számítás referencia modellje azonosítja a felhő főbb szereplőit, tevékenységeiket és feladataikat.[3]



3. ábra. A felhő számítás elvi referencia modellje [5]

Az IaaS szolgáltatói modell megvalósítása jelenleg gyártófüggő. A szabványosítási törekvéseket azonban jól mutatja, hogy számtalan nemzeti és nemzetközi testület, munkacsoport, egyesület, szabványosítási szervezet [7] foglalkozik a felhők különböző aspektusainak szabványosításával. Példaképpen az Open Cloud Consortium-ot (OCC) [4] említjük, amely a felhők és a felhők közötti együttműködés keretrendszerével kapcsolatos szabványok fejlesztését támogatja, benchmarkokat fejleszt a felhők vizsgálatára, és segíti referencia implementációk létesítését.

Kritikus informatikai infrastruktúrák

A nemzetközi gyakorlatnak megfelelően azokat az infrastruktúrákat tekintjük kritikusnak, melyek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez, mint például az energiaellátó rendszerek, banki és pénzügyi rendszerek, közlekedés és szállítás, egészségügyi rendszer, kormányzat, kommunikáció- és információtechnológia stb.

A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló Zöld Könyv alapján „kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is

kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak, stb.)". [6]

A kritikus informatikai infrastruktúrával szemben mind a szolgáltatás üzembiztonsága, rendelkezésre állása, mind az informatikai biztonsága iránt fokozott igényeket támasztanak. Ezeknek a fokozott igényeknek a kielégítése többnyire csak együttessen valósítható meg.

A rendelkezésre állást számszerűsíteni kell (pl.: öt kilences). Az informatikai biztonsággal szemben támasztott elvárásoknak egyen szilárdságúaknak kell lenniük a teljes infrastruktúrában.

A rendelkezésre állás és az informatikai biztonság paramétereit szolgáltatási-szint szerződésben (Service Level Agreement – SLA) kell rögzíteni, és mind a szolgáltatónak, mind az előfizetőnek/bérlőnek figyelemmel kell kísérnie.

Security as a Service (SECaaS)

Az elmúlt években egyre több infrastruktúra esetében tudatosan alkalmaznak felhőszolgáltatásokat, de az is előfordul, hogy a felhasználók észre sem veszik, hogy felhő szolgáltat nekik, nem pedig egy helyi szerver. Leginkább azt tapasztalhatják, hogy minden jól és gyorsan működik. A felhő technológiák előnyeinek kihasználása céljából egyre több cég fordul az IaaS, a PaaS, a SaaS, vagy éppen a SECaaS megoldások felé annak érdekében, hogy csökkenteni tudja a vállalaton belül felmerülő költségeket. Bár sokan még kételkednek e technológiák biztonságos voltában, ennek ellenére egyre több informatikai biztonsági eszközöket gyártó cég (pl. McAfee, Panda Security, Symantec, stb.) fejleszt és kínál felhő alapú biztonsági szolgáltatásokat. A SECaaS egy olyan felhő alapú szolgáltatás, ami biztonsági alkalmazások és megoldások távoli igénybe vételét teszi lehetővé általában virtuálisan kiépített csatornán keresztül. Olyan felhőszámítási modell, mely biztonsági szolgáltatásokat menedzsel az interneten keresztül. A SECaaS a Software as a Service (SaaS) modellen alapul.

Kezdetben a Security as a Service megoldásokban csupán áthelyezték a központosított irányítást a felhőbe, majd fokozatosan kiaknázták a felhőszolgáltatásban rejlő erősségeket. A gyártók helyi számítási erőforrást takarítanak meg azzal, hogy a rosszindulatú szoftverek vizsgálatát felhőben bonyolítják ahelyett, hogy a vállalat asztali számítógépein egyenként tennék ezt. Ennek eredményeképpen sokkal több kapacitást sikerült megtakarítani, mintha egyszerűen az ügyfél oldalon végeznénk vizsgálatokat, valamint emellett lehetőség nyílik az egyes számítógépeken felfedezett veszélyekhez kapcsolódó információk összegyűjtésére, könnyen átlátható, fenyegetésekre vonatkozó halmazba integrálására is.

A SECaaS alkalmazásának előnyei

A SECaaS alkalmazásának előnyeit az alábbiakban foglaljuk össze:

- Nincs szükség hardverek vagy szoftverek vásárlására, karbantartására, a SECaaS szolgáltató biztosítja;
- Csökkentett sávszélesség használat;
- A felesleges e-mailek csak a felhőig jutnak el (a bejövő e-mailek legnagyobb része spam);
- Megbízható adatközpont rendelkezésre állás;

- Néhány vállalat SECaaS megoldással egyszerűen össze tudja kötni a vállalat infrastruktúráját és a biztonsági beruházásokat;
- Jellemzően gyorsabb kivitelezés és a külső forrású szakmai hozzáértés miatt rendkívüli mértékben csökken a kockázat;
- Könnyű méretezhetőség;
- Ugyanarra a problémára több szolgáltatás áll a megrendelő rendelkezésére;
- Igénybevétel szerinti költségek;
- A biztonsági feladatok kiszervezésével a szervezetek több időt fordíthatnak a fő feladatkörükre;
- IT-s szakembert nem feltétlenül igényel, nem szükséges a helyszínre küldeni, egyszerűen megoldható a felhő segítségével;
- Alacsony bevezetési költség és még alacsonyabb a használat során felmerülő költség a tulajdonos számára;
- A forgalmazót anyagi érdekeltség köti a megfelelő működéshez, mert, ha a szolgáltatás bevezetése nem sikeres, a szolgáltató elveszti az előfizetőt;
- Az adminisztratív feladatok pl. log fájlok kezelése külső helyen történik, ezáltal időt és pénzt takarítva meg és lehetőséget biztosítva, hogy több idő maradjon a fontosabb feladatokra;
- Folyamatos vírus definíciós frissítések;
- Nincs szükség felhasználói beavatkozásra;
- Web és e-mail biztonság. [9]

A SECaaS alkalmazásának hátrányai

- Egy szolgáltatás esetleges meghibásodása vagy feltörése esetén a felhő nagysága miatt dominó effektus alakulhat ki.
- A cégeknek aggodalomra ad okot egy más cégekkel közösen alkalmazott eszköz használata. Bizalmas információkat nem szívesen adnak ki.
- Bizonyos speciális üzleti területtel foglalkozó vállalatnak szüksége van az ahhoz kapcsolódó alkalmazásokra. Ezek az alkalmazások annyira speciálisak, hogy a SECaaS megoldásokban nem elérhetők vagy egyszerűen nem megoldható a működésük jelenleg.
- Sok SECaaS megoldás esetén még mindig szükséges egy-egy szoftver telepítése a vállalat összes számítógépén az automatikusan elvégezhető telepítések, illetve a frissítések miatt.[9]

A SECaaS szolgáltatások biztosítása még nagyobb kihívás, mint a normál szolgáltatásoké:

- különböző architektúrák, funkciók és megvalósítások;
- nincs egy világszinten elfogadott keretrendszer kialakítva;
- a vállalatok nagy része még nem áll készen ilyen szolgáltatások biztosítására;
- a felhő sebezhetősége (felhő specifikus biztonsági rések):
  - adatok megőrzése;
  - fizikai hozzáférés ellenőrzés;
  - titkosítási kulcsok kezelése;
  - alacsony szinten vagy egyáltalán nem monitorozható az operatív hozzáférés és/vagy a szolgáltatás menedzsment;

- a felhő környezet nem teszi lehetővé, megnehezíti vagy hatástalanítja a hagyományos ellenőrzési eljárásokat (Forensic, havi biztonsági audit, biztonsági értékelések, stb.);
- a felhasznált felhő technológiák is okozhatnak sebezhetőséget: a technológia velejárói (pl.: virtual machine escape), a felhőbe implementálás következményei (pl.: session visszaélés/eltérítés).

A Cloud technológiák szabványosítása

A fentebb kifejtett hátrányokon kívül jelentős problémát jelent a SECaaS biztonsági szempontból kritikus környezetben történő alkalmazásában, hogy a felhő technológiákra vonatkoztatva nincs egységes előírás, a szabványosítás ezen a területen még gyerekcipőben jár. A felhő szabványokkal, ajánlásokkal több szervezet is elkezdett már foglalkozni (cloud-standards.org).

2010 tavaszán a Novell és a Cloud Security Alliance (CSA) meghirdette az iparág első szállító független, számítási felhőkre vonatkozó biztonsági tanúsítási programját (Trusted Cloud), melynek célja a szolgáltatók segítése az ajánlásoknak megfelelő, biztonságos és az ügyfelek meglévő informatikai rendszerével együttműködő megoldások kidolgozásában. Kiterjed a felhőalapú megoldások bevezetésekor kényes területnek minősülő személyazonosság-kezelési, hozzáférési és megfelelőségi megoldások konfigurációira.

Az USA kormánya kezdeményezte a felhő szolgáltatások megrendszabályozására alkalmas ajánlások kidolgozását (mik azok a biztonsági intézkedések, amelyeket egy szolgáltatónak foganatosítania kell, és melyek azok, amiket az előfizetők számon kérhetnek).

2011 februárjában a NIST kiadott egy dokumentumot (ajánlások), melynek célja a felhő számítási környezetek biztonsági követelményeinek meghatározása. Elsősorban a nyilvános felhő szolgáltatásokkal foglalkozik:

- Általános tudnivalók, megfelelőségi és felügyeleti kérdések, az architekturális követelmények.
- Külön foglalkozik az azonosság- és hozzáférés kezeléssel, az adat- valamint szoftverizolációval és az adatvédelmi nehézségekkel.
- Ajánlásokat tesz a rendelkezésre állással és az incidenskezeléssel kapcsolatban.

A Cloud Security Alliance ajánlásai a biztonság minden területére kiterjednek.

A CSA ajánlásai között szerepel többek között, hogy a biztonságnak és az adatvédelemnek már a rendszerek fejlesztési életciklusának tervezési szakaszában meg kell jelenniük (maximális hatékonyság és a minimális költségek), mert a megvalósítás után a biztonsági kérdések kezelése nemcsak bonyolultabb és költségesebb, hanem kockázatosabb is. Továbbá, hogy a szervezeteknek olyan szolgáltatásokat kell választaniuk, amelyek a bevezetés, a konfigurálás és a felügyelet szempontjából is megfelelnek a biztonsági követelményeiknek. [8]

A „számítási felhő biztonsági kérdései" kutatási alprojekt

A kiemelt biztonságot igénylő vállalati alkalmazások esetén nem engedhető meg az adatok felhőben való tárolása vagy a számítási erőforrások esetleges kiesése, ezért a nyilvános felhőszolgáltatás mellett létrejött a vállalati adatközpontban megvalósított magán felhőszolgáltatás. A kétféle szolgáltatás technológiája azonos. A magán felhőszolgáltatás esetén a

beruházási költségek felmerülnek, az erőforrások jobb kihasználása azonban csökkenti a költségeket. A hibrid felhő a magán felhő összekapcsolása a nyilvános felhő infrastruktúrával.

A felhőszolgáltatás alkalmazása összetettsége, elosztott jellege és heterogenitása miatt számos biztonsági kockázatot hordoz magában, és kihívás elé állítja a fejlesztőket, a szolgáltatókat és a felhasználókat. A fejlesztők és a szolgáltatók sokat tettek a felhők informatikai biztonságának fokozása érdekében, de számos biztonságot érintő kérdés megoldásra vár. Ilyen kérdések:

- Felhasználói oldal biztonsági kérdései
- Erőforrás migráció esetén a biztonsági szintek validálása, migrációs keretrendszerek kialakítása
- Hibrid felhő használata esetén a biztonsági szintek garantálása, és transzparens átjárhatóság a különböző rendszerek között
- Szolgáltatói oldal biztonsági kérdései

A kutatási alprojekt célja

A kutatási alprojekt célja az infrastruktúraszolgáltatást (IaaS) nyújtó felhők felhasználókat érintő biztonsági kérdéseinek feltárása, az informatikai biztonságra vonatkozó szolgáltatási szintek kialakítása, amelyek magukban foglalják a felhasználók virtuális gépeit, ezek hálózatait, alkalmazásait, tárolóit. Továbbá egy konkrét felhő implementációra olyan keretrendszer fejlesztése, amely a biztonsági szinteknek megfelelő biztonsági elemeket automatikusan beépíti a futtató környezetbe. A kritikus infrastruktúra védelmi kutatások (TÁMOP-4.2.1.B-11/2/KMR) projekt (2. alprojekt) keretében többek között feltárjuk az infrastruktúraszolgáltatást (IaaS) nyújtó felhők felhasználókat érintő biztonsági kérdéseit,majd részletesen vizsgáljuk a jelenlegi eszközök, valamint általunk fejlesztett informatikai biztonsági szoftver megoldások szolgáltatásként (Security as a Service – SECaaS) történő használatának hatékonyságait és lehetőségeit. A projekt keretében végzett elemzés feltárja a felhő infrastruktúrák jelen implementációiban fellelhető, felhasználókat érintő biztonsági hiányosságokat, biztonsági szolgáltatási szintekre tesz javaslatot, majd egy keretrendszerre épülő konkrét implementációt ad.

Az alprojekthez kapcsolódó K+F+I tevékenységek

A kutatási alprojekt keretében alapvetően infrastruktúraszolgáltatást (IaaS) nyújtó felhők felhasználókat érintő biztonsági kérdéseivel foglalkozunk. Ennek vonatkozásai:

- Védelem külső kiber támadások ellen IaaS felhőszolgáltatást használók számára;
- Sebezhetőség vizsgálat, adott virtuális gépek esetén a gépek biztonsági szintjének ellenőrzése, sebezhetőség vizsgálata;
- Felhasználók adatainak védelme;
- A virtuális gépek közötti biztonságos, titkosított kommunikáció a felhasználó szempontjából transzparens módon;
- A virtuális gépeken, illetve a tároló hálózaton elhelyezett adatok titkosítása a felhasználó szempontjából transzparens módon;
- Adatok áramlásának földrajzi korlátozása, ami nemzetközi infrastruktúrák esetén gyakran törvényi előírás;

A kutatási alprojekt várható eredményei:

- Az IaaS típusú felhőszolgáltatások használóit érintő veszélyforrások módszeres feldolgozása, dokumentálása;
- Az IaaS típusú felhőszolgáltatásoknál alkalmazott virtualizált infrastruktúrák biztonsági szintjének automatikus ellenőrzése, sebezhetőségük vizsgálata;
- A veszélyforrások elhárítását szolgáló automatizmus kidolgozása, és életképességének bizonyítása egy tesztkörnyezetben vizsgált minta-implementációban.

Összefoglalás

Cikkünk első felében bemutattuk a számítási felhők (Cloud Computing) főbb jellegzetességeit, tulajdonságait, gyors elterjedésének okait, előnyeit és hátrányait.

A későbbiekben bevezettük a felhő szolgáltatás fogalmát, áttekintettük a felhők szolgáltatási és telepítési modelljeit, bemutattuk a felhők fejlesztők/gyártók/szolgáltatók funkcionalitás szerinti osztályozását (felhők taxonómiája). Ez az osztályozás jól mutatja a felhők várható fokozott térnyerését az informatikai szolgáltatásokban. Egy további tendencia is megmutatkozik, nevezetesen az informatika minden részfeladatának szolgáltatásként történő megjelenése, és ezek összekapcsolása komplex informatikai szolgáltatások nyújtásában.

Ezt követően a felhők biztonsági kérdéseivel foglalkoztunk, ennek is egy viszonylag újszerű megvalósításával az informatikai biztonság szolgáltatásként történő kezelésével (Security as a Service – SECaaS). Már ma is léteznek felhőből hagyományos infrastruktúra vagy felhő részére nyújtott biztonsági szolgáltatások, de a téma intenzív kutatás alatt áll, és még nem eléggé kristályosodott ki, hogy a biztonság mely területeit lesz képes meghódítani. Végezetül meghatároztuk a cikk hátteréül szolgáló, a „Számítási felhő biztonsági kérdései" c. TÁMOP kutatási projekt (TÁMOP-4.2.1. B -11/2/KMR-2011) céljait, célcsoportjait és kutatási-fejlesztési feladatait, valamint összefoglalást adtunk a cikk tartalmáról és megállapításairól.

A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások" projektnek a cikkhez végzet kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

IRODALOMJEGYZÉK

[1] Mell P., Grance T.: The NIST Definition of Cloud Computing, NIST Special Publication 800-145, National Institute of Standards and Technology, 2011
[2] Hurwitz J,. Bloor R., Kaufman M., Halper F. (2010) Cloud Computing For Dummies, Wiley Publishing, Inc.
[3] Mell P., Grance T. (2011) The NIST Definition of Cloud Computing, NIST Special Publication 800-145, National Institute of Standards and Technology
[4] OpenCrowd (2010) Cloud Taxonomy. http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png
[5] Liu F., Tong J., Mao J., Bohn R., Messina J., Badger L., Leaf D. (2011) NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, Recommendations of the National Institute of Standards and Technology
[6] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final
[7] Szenes, K.(2011): Supporting Applications Development and Operation Using IT Security and Audit Measures (Procds. of 5th IFIP TC2 Central and Eastern European Conference on Software EngineeringTechniques (CEE-SET'2011), Debrecen, Hungary, August 25-26, 2011), to appear in: e-Informatica Software Engineering Journal, http://www.e-informatyka.pl/wiki/e-Informatica
[8] Simmonds P., Rezek C., Reed A. Editors (2011) Seurity Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, https://cloudsecurityalliance.org/guidance/ csaguide.v3.0.pdf
[9] Online-crm: The Realities of CRM SaaS - Advantages and Disadvantages, http://www.online-crm.com/saas_advantages_disadvantages.htm, 2012-04-23

A RENDVÉDELMI SZERVEK HELYE A KIBERVÉDELEMBEN

Krasznay Csaba

Egy ország kibervédelmi feladatait számos katonai, nemzetvédelmi, rendvédelmi és civil szervezet összehangolt munkájával kell megteremteni. Annak érdekében, hogy ez a rendkívül összetett feladat sikeres legyen, több mérvadó nemzetközi szervezet is ajánlásokat tett a felelősségekkel és szerepkörökkel kapcsolatban. Ugyan a szervezetrendszer felépítése országról országra változik, de a legfontosabb feladatokat ezek az ajánlások egyértelműen a belbiztonságért felelős minisztérium alárendeltségébe tartozó intézményekre szabták.

Nincsen ez másképp Magyarországon sem, ahol az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) [1], valamint a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat [2] rendelkezik az ország kibervédelmi szervezeti struktúrájáról. A teljes jogi környezet jelenleg kialakulóban van hazánkban, ezért érdemes áttekinteni, hogy az egyes Belügyminisztérium alá rendelt szervezetek törvényi kötelezettségei és a nemzetközi ajánlások mennyiben vannak egymással összhangban, illetve milyen további jogszabály-alkotási feladatok állnak még a magyar kormány előtt a teljes lefedettség eléréséhez!

Jelen tanulmány az ITU National Cybersecurity Strategy Guide [3], az ENISA National Cyber Security Strategies [4] és a NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) National Cyber Security Framework Manual [5] alapján tekinti át azt, hogy 2013. közepén a magyar kibervédelem felépítése mennyiben felel meg a nemzetközi elvárásoknak, különösen a rendvédelmi szervek tekintetében. A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény [6] 1. § (5) alapján a rendvédelmi szervek közé soroljuk a rendőrséget, a büntetés-végrehajtási szervezetet, a hivatásos katasztrófavédelmi szervet és a polgári nemzetbiztonsági szolgálatokat.

Nemzetközi ajánlások

International Telecommunication Union (ITU)

A távközléssel foglalkozó szervezeteket tömörítő ITU 2011-ben adta ki a National Cybersecurity Strategy Guide című ajánlását, melyben az elsők között kezdett azzal foglalkozni, hogyan kell egy nemzeti kibervédelmi rendszert felállítani. A publikáció 10 lépésben határozza meg a legfontosabb stratégiai lépéseket:

1. A legmagasabb kormányzati szintű kiberbiztonsági felelősség meghatározása. Magas rangú kormányzati felelőst neveznek ki, akinek feladata a nemzeti stratégia kidolgozása és a helyi, nemzeti és globális, szektorok közötti együttműködés elősegítése.
2. Nemzeti kiberbiztonsági koordinátor kinevezése. Olyan iroda vagy személy megbízá-

sa, aki vagy amely átlátja a kiberbiztonsági tevékenységeket az adott országban.
3. Nemzeti kiberbiztonsági tanács létrehozása. Olyan szervezet összehívása, mely a közigazgatás érintett szerveit tömöríti, és feladata azon tevékenységek összehangolása, mely a nemzeti kibertér védelmére irányul.
4. Jogszabályalkotás. Tipikusan az adott országban át kell tekinteni a létező jogszabályokat, és amennyiben szükséges, ki kell egészíteni a büntető-törvénykönyvet és a vonatkozó eljárásrendet a kiberbűnözés visszaszorítása érdekében.
5. Nemzeti kiberbiztonsági keretrendszer kidolgozása. Az ország létrehoz egy olyan keretrendszert, mely tartalmazza a minimális vagy kötelező biztonsági követelményeket olyan területeken, mint a kockázatkezelés és a megfelelőség.
6. Computer Incident Response Team (CIRT) felállítása. Az incidenskezelés nemzeti felelősség, melyet egy CERT /CSIRT képes megoldani. Ez a szervezet elemzi a kiberfenyegetések trendjeit, koordinálja a válaszadást és nyújt információt az érintett felek számára.
7. Kiberbiztonsági tudatosság és oktatás megszervezése. Nemzeti programot kell szervezni a kiberfenyegetésekkel kapcsolatos tudatosság erősítése érdekében.
8. Köz- és magánegyüttműködés a kiberbiztonság területén. A kormányzatnak szorosan együtt kell működnie a privát szféra szereplőivel.
9. Humán képességek fejlesztése a kiberbiztonság területén. Olyan oktatási rendszer kidolgozása, mely a kiberbiztonsággal foglalkozó szakértők tudását fejleszti.
10. Nemzetközi együttműködés. Globális partnerség a mindenkit fenyegető kiberkockázat csökkentése érdekében.

Az ajánlás megnevezi azokat a kormányzati és civil szereplőket is, melyeknek szerepe van a fenti stratégiai feladatok végrehajtásában. Ezen szereplők a következők:

- Kormány, Magyarországon a Miniszterelnökség
- Parlament
- Kritikus infrastruktúrák tulajdonosai és üzemeltetői
- Bíróságok
- Bűnüldöző szervek
- Hírszerző szervezetek
- Információbiztonsági termékek gyártói
- Akadémiai szféra
- Nemzetközi partnerek
- Állampolgárok

A fenti szereplők közül Magyarországon a Belügyminisztérium szervezetei közé tartozik a kritikus infrastruktúrákat felügyelő Országos Katasztrófavédelmi Főigazgatóság, a bűnüldözéssel foglalkozó szervezetek (Rendőrség és a Terrorelhárítási Központ), a polgári titkosszolgálatok közül az Alkotmányvédelmi Hivatal és a Nemzetbiztonsági Szakszolgálat (ezen belül a kormányzati CERT) és részben a Nemzeti Közszolgálati Egyetem, mint akadémiai szereplő. A minisztérium kibervédelemben betöltött fontos szerepe tehát vitathatatlan.

European Network and Information Security Agency (ENISA)

Az Európai Unió kibervédelemmel foglalkozó szervezete, az ENISA 2012 decemberében publikálta a nemzeti kiberbiztonsági stratégiák létrehozását támogató National Cyber Security

Strategies – Practical Guide on Development and Execution című kiadványát. Ebben 20 olyan lépést határozott meg, mely szükséges a nemzeti stratégia létrehozásához.

1. A vízió, a hatókör, a célok és a prioritások meghatározása.
2. Nemzeti kockázatfelmérési szempontrendszer követése.
3. A létező jogszabályok, szabályozások és képességek számbavétele.
4. Tiszta irányítási struktúra felállítása.
5. A fontos szereplők azonosítása és bevonása.
6. Megbízható információátadási eljárások kidolgozása.
7. Kiberbiztonságot számba vevő folytonossági tervek kidolgozása.
8. Kibervédelmi gyakorlatok szervezése.
9. Alapvető biztonsági követelmények meghatározása.
10. Incidensjelentési eljárások kidolgozása.
11. Állampolgári tudatosság emelése.
12. Kutatás-fejlesztés támogatása.
13. Szakértői oktatások és tréningek indítása.
14. Incidenskezelési képességek kialakítása.
15. Kiberbűnözés visszaszorítása.
16. Részvétel a nemzetközi kapcsolatokban.
17. Köz- és magánegyüttműködés kialakítása.
18. A biztonság és az adatvédelem közötti összhang kialakítása.
19. A kibervédelem rendszerének értékelése.
20. A nemzeti kibervédelmi stratégia finomhangolása.

Az útmutató nem nevesíti az érintett szerveket, de a feladatokból és az ezekhez rendelt példákból több helyen is kimutatható, hogy a belügyi szervek természetesen kulcsfontosságúak a stratégia létrehozásában.

North Atlantic Treaty Organisation (NATO)

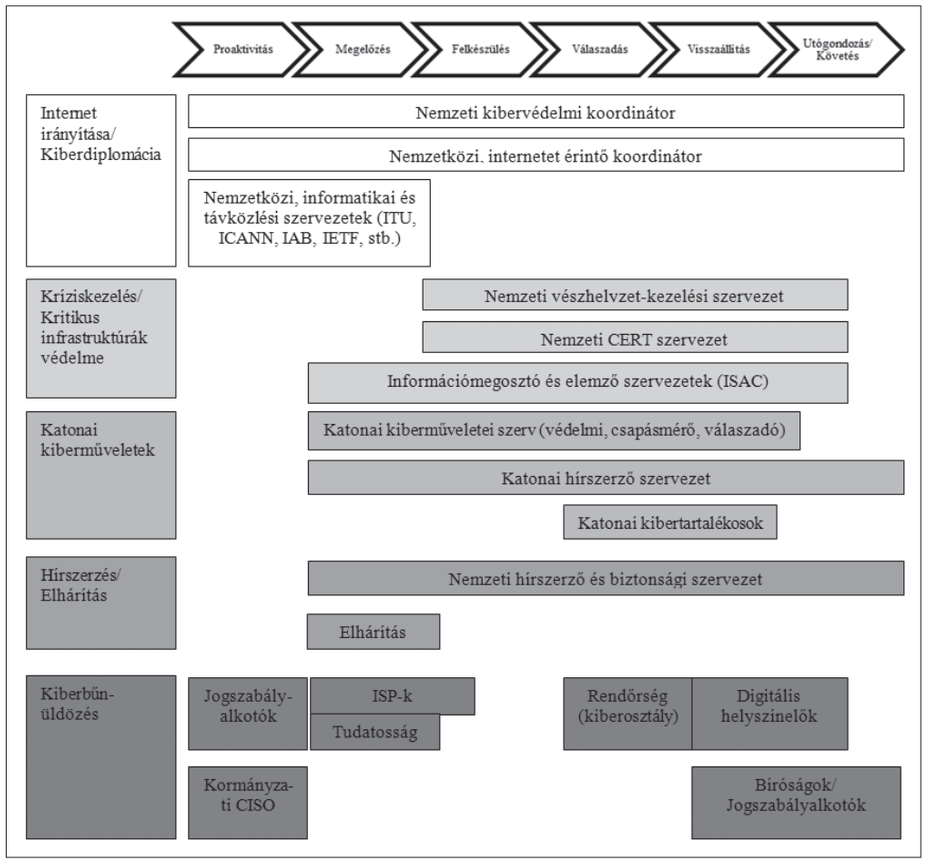
A NATO kibervédelemmel foglalkozó intézete, a Tallinnban működő Cooperative Cyber Defence Centre of Excellence (CCD CoE) gondozásában megjelent National Cyber Security Framework Manual foglalkozik a legrészletesebben a kibervédelem szervezet- és feladatrendszerével. A 2012-ben kiadott kötet az előző ajánlásokkal szemben katonai szemszögből is elemzi a területet.

A nemzeti kibervédelem a tanulmány szerint öt különböző aspektusból vizsgálandó:

- Katonai kibervédelem. A hagyományos területekhez hasonlóan a kibertérben is ki kell építeni bizonyos katonai képességeket, így a saját hálózatok védelmét, a hálózatközpontú hadviselés képességeit, valamint a taktikai és stratégiai kiberhadviselés képességét.
- Kiberbűnözés elleni harc. Ebbe a körbe tartozik az egyént érintő kiberbűncselekmények üldözése mellett a kiberterrorizmus elleni lépések sora is.
- Hírszerzés és elhárítás. Az utóbbi években jelentősen nőtt az államok ellen a kibertérben elkövetett hírszerzési tevékenységek aktivitása, mely indokolttá teszi ezek körültekintő elhárítását, valamint az ország elleni esetleges kibertámadások mielőbbi, titkosszolgálati úton történő felderítését.
- Kritikus infrastruktúra védelem és nemzeti krízismenedzsment. Ez a terület lefedi a

létfontosságú rendszerek védelmét, valamint az esetleges kibertámadás esetén az események informatikai és társadalmi kezelését is.
- Kiberdiplomácia és az internet irányítása. A kibervédelem nemzetközi rendszerének megalkotása esősorban a nemzetközi szervezeteken keresztül, részben bilaterális megállapodásokban lehetséges. Ezért fontos, hogy a kiberteret, és ennek közegét, az internetet irányító szervezetekben a kormányzat aktívan részt vegyen.

A keretrendszer ajánlást is tesz arra vonatkozóan, hogy a fenti feladatokat mely szerveknek kell ellátnia. Ezt egy összefoglaló ábrában tálalja, melyben a kibervédelem feladatrendszerét az egyes életciklus-elem függvényében osztja fel a kulcsszereplők között (lásd 1. ábra).



1. ábra. A kibervédelem életciklus modellje.

Forrás: NATO CCDCOE National Cyber Security Framework Manual

A feladatokhoz rendelt szervezeti egységek jelentős részben a Belügyminisztérium alárendeltségébe tartoznak, megerősítve ezzel azt az előzetes feltételezést, hogy a kibervédelem elsősorban belbiztonsági feladat.

A teljes kibervédelmi struktúra kiépítéséhez a CCD COE keretrendszere 20 javaslatot, illetve tanulságot emel ki, melyet figyelembe kell venni!

1. Minden ország más, ezért egyéni kibervédelmi stratégiát kell kidolgozni!
2. A stratégia csatlakozzon más nemzetek stratégiájához és a nemzetközi szervezetek ajánlásaihoz!
3. Legyen kidolgozva egy olyan frissítési és ellenőrzési eljárás, melynek segítségével a szabályozás mindig a valós kockázatokra adhat választ!
4. Legyen felsőszintű, kormányzati és középszintű, szervezeti koordinációs csoport!
5. Legyenek beazonosítva a kritikus szolgáltatások és infrastruktúrák!
6. Meg kell teremteni a kibertudatosságot, elsősorban a jogszabályalkotók szintjén!
7. Biztosítani kell az információk formális és informális áramlását a szereplők között!
8. Ki kell dolgozni a közös fogalmi rendszert!
9. Olyan jogszabályi rendszert kell létrehozni, mely az alapelveket magas szinten, az operatív munkához szükséges szabályokat rugalmasan változtatható, alacsony szintű rendeletekben szabályozza!
10. A kulcsfontosságú szervezeteknek rugalmasnak kell lenniük az operatív munkában!
11. Ne legyenek lyukak a jogszabályi rendszerben!
12. A szervezeten belüli információáramlást elő kell segíteni!
13. A fenyegetési környezet folyamatosan változik, ezt figyelembe kell venni a jogszabályalkotásban! Ne legyenek elavult szabályozások!
14. Az operatív műveletek esetén a szervezetek között rugalmas együttműködést kell kialakítani!
15. Tisztázni kell az információátadás és az adatvédelem közötti egyensúlyt!
16. Küzdeni kell a digitális írástudatlanság ellen!
17. A nemzetközi kötelezettségvállalásokat a helyükön kell kezelni!
18. Az alapvető információbiztonsági követelmények megvalósítását meg kell követelni!
19. Törekedni kell a nemzetközi interoperabilitásra (műszaki és szervezeti értelemben is)!
20. Tanulni kell más országok tapasztalatából!

Belbiztonsági feladatok Magyarországon

Jogszabályi környezet

A rendvédelmi szervek kibervédelemmel kapcsolatos feladatait számos különböző jogszabály rendezi. A tanulmány írásának időpontjában ezek nem alkotnak egységes, összefüggő, minden feladatot teljesen lefedő rendszert, de a 2012-ben megindult kibervédelmi szabályozás egy későbbi fázisában, a tapasztalatok alapján ezeket a hiányokat pótolni lehet. A legfelsőbb szintű jogszabályok lehetőséget adnak arra, hogy az alsóbb szintű jogszabályok rugalmasan alkalmazkodjanak a változó körülményekhez.

A következő fejezet a rendvédelmi szervek kibervédelmi feladatait tárgyalja. A teljes képhez azonban fontos megemlíteni, hogy az Ibtv. létrehozza az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezeti egységet, a Hatóságot, mely a Nemzeti Fejlesztési Minisztériumon belül kerül felállításra. Emellett fontos szereplő a Nemzeti Biztonsági Felügyelet, mely szakhatóságként működik közre a kibervédelemben,

valamint a Nemzeti Kiberbiztonsági Koordinációs Tanács, melynek feladata a terület stratégiai koordinálása.

Polgári titkosszolgálatok

A nemzetbiztonsági szolgálatok működését szabályozó 1995. évi CXXV. törvény [7] a kibervédelem tekintetében kizárólag a Katonai Nemzetbiztonsági Szolgálatnak ad feladatokat. A polgári titkosszolgálatok tevékenységében a kibervédelem, illetve az informatikai jellegű tevékenység nem nevesített, közvetett cél. A kibervédelmi stratégia azonban nevesíti ezt a célt: „A kiberbiztonsággal összefüggő feladatok ellátását a specifikus szakértelemmel és hatáskörrel rendelkező szervezetekhez szükséges telepíteni, amely szervezetek nem csak egymással, hanem az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködnek. A feladatellátás érinti a nemzetbiztonsági, honvédelmi, bűnüldözési, katasztrófavédelmi és létfontosságú intézmények és létesítmények védelmével kapcsolatos feladatokat ellátó szervezeteket, valamint az elektronikus információbiztonság területén hatósági jogosítványokkal rendelkező intézményeket."

Kibervédelmi feladatot a jogszabályok alapján egyedül a Nemzetbiztonsági Szakszolgálat kap. A szervezet tevékenysége kettős. Egyrészt az Ibtv., illetve annak az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelete [8] alapján kormányzati eseménykezelő központként működik. Másrészt a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet (továbbiakban: BM rendelet) [9] ezt a szervezetet jelölte ki a belügyi szervek vonatkozásában a sérülékenységvizsgálattal összefüggő feladatok ellátására.

Katasztrófavédelmi szervezet

Az Országos Katasztrófavédelmi Főigazgatóság a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény [10] alapján felelős számos kritikus információs infrastruktúra védelmének felügyeletéért. Az Ibtv. ennek a feladatnak a kibervédelmi aspektusait nem részletezi, de több helyen is megerősíti azt, hogy a létfontosságú rendszerelemeket informatikai szempontból is védeni szükséges, ezért az OKF-et és a törvényben nevesített szervezeteket együttműködésre utasítja.

Az OKF emellett eseménykezelő központot működtet Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK) elnevezéssel. Ezt a feladatot a BM rendelet határozza meg számára.

Rendőrség és terrorelhárítás

A rendőrségi és terrorelhárító szervek feladata a kibervédelem egészében rendkívül fontos, de Magyarországon nem pontosan szabályozott. Annak ellenére, hogy az informatikai bűnözés területén mérvadó nemzetközi egyezmény Budapest nevét viseli, a magyar jogrend pedig

részletesen foglalkozik a kiberbűncselekményekkel és azok szankcionálásával, a szóba jöhető szervezetek feladatkiosztásánál ez a terület rendkívül alulreprezentált.

Gyömbér Béla gyűjtése szerint [11] a Rendőrségen belül a területtel célzottan foglalkozik a Készenléti Rendőrség Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztály, a Budapesti Rendőr-főkapitányság, Gazdaságvédelmi Osztály, Számítógépes Bűnözés Elleni Alosztály, illetve a gyakorlatban a hatáskörileg mindenkor illetékes rendőrkapitányságok. A kiberterrorizmus elhárításának érdekében a Terrorelhárítási Központ, Terrorizmus és Számítógépes Bűnözés Elleni Monitoring Egysége folytat ellenőrzési, megelőzési tevékenységet. Hasonló feladatai vannak az Alkotmányvédelmi Hivatalnak és a Készenléti Rendőrség Nemzeti Nyomozó Irodának, de ezek kiberterrorizmussal kapcsolatos tevékenységéről nem áll rendelkezésre nyilvános információ.

Meg kell még említeni a Nemzeti Adó- és Vámhivatal, Bűnügyi Főigazgatóság, Központi Nyomozó Főosztály, Információtechnológiai Osztályát, mely elsősorban a szerzői jogok megsértésével foglalkozik, de potenciálisan alkalmas és képes a kiberbűncselekmények felszámolására.

Egyéb belügyi szervek

A törvényben nevesített rendvédelmi szervek mellett az Ibtv. alapján további szervezetek kaptak feladatokat a kibervédelemben. Egyrészt a BM rendelet szerint a belügyi szervek zárt célú elektronikus információs rendszerei biztonságának központi felügyeletéről a belügyminiszter a Belügyminisztérium Miniszteri Kabinet útján gondoskodik. Másrészt a részben a BM felelősségébe tartozó Nemzeti Közszolgálati Egyetemnek kell bizonyos oktatási és kutatási tevékenységet ellátni. Az Egyetem felelős elsősorban a kibervédelmi szakemberek képzéséért is.

Megfelelés a nemzetközi ajánlásoknak

A nemzetközi szervezetek által kidolgozott ajánlások és keretrendszerek körvonalazzák azt, hogy milyen feladatokat kell ellátnia a belbiztonsági szerveknek a kibervédelmi területen. Az 1. táblázat felsorolja azokat a követelményeket, melyek az ajánlásokból származnak, egyben jelzi azt, hogy jelenleg hatályos magyar jogszabályok szerint melyik intézmény foglalkozik ezekkel a követelményekkel.

Az ajánlásokból eredő feladatok mindegyike lefedésre került, ám ezek különböző érettségi szinten vannak. Az egyes teendők állapota a nyilvánosan elérhető információk alapján a következőképp alakul.

- Jogszabályalkotás: Az Ibtv. és annak végrehajtási rendeletei jó alapot teremtenek a kibervédelem teljes rendszerének kiépítéséhez. Egy magas szintű törvény időtálló keretet ad, a kormányrendeletek kijelölik az intézményrendszert, a miniszteri szintű rendeletek pedig elég rugalmasak a folyamatosan változó körülmények követéséhez. A tapasztalatok alapján erre a rendszerre építhető fel a minősített időszakok kibervédelmi tevékenysége. Szintén jól körülhatárolt a kritikus információs infrastruktúrákkal kapcsolatos feladatrendszer. Hiányzik azonban jogszabályokból a titkosszolgálatok adott területen követendő tevékenységeinek nevesítése, illetve a kiberbűnözés elleni tevékenység kiemelt támogatása.

1. táblázat. Belbiztonsági szervezetek feladatai a kibervédelem területén

Feladatok	Titkos-szolgálatok	OKF	Rendőrség	Egyéb
Jogszabályalkotás				X (BM)
Részvétel a nemzeti kiberbiztonsági tanács munkájában				X (BM)
Nemzetközi együttműködés	X	X	X	X
Köz- és magánegyüttműködés a kiberbiztonság területén		X		
Nemzeti kockázati szempontrendszer meghatározása, kritikus szolgáltatások és infrastruktúrák beazonosítása	X	X		
Nemzeti CERT működtetése	X			
Incidensjelentési eljárások kidolgozása	X			
Kibervédelmi gyakorlatok szervezése	X			
Humán képességek fejlesztése, kutatás-fejlesztés támogatása				X (NKE)
Kiberbűnözés visszaszorítása			X	
A biztonság és az adatvédelem közötti összhang kialakítása	X		X	
Információáramlás elősegítése				X (BM)

- Részvétel a nemzeti kiberbiztonsági tanács munkájában: A Nemzeti Kiberbiztonsági Koordinációs Tanács munkájában a Belügyminisztérium magas rangú képviselővel vesz részt, képviseli a tárca alá tartozó szervezeteket.
- Nemzetközi együttműködés: Mind a BM, mind az egyes szervezetek részvétele kiemelten fontos a nemzetközi együttműködések és szervezetek munkájában. Ennek koordinációja minisztériumi szintet követel meg. Ki kell emelni a Nemzetbiztonsági Szakszolgálaton belül működő CERT nemzetközi kapcsolatokban való részvételének fontosságát, illetve meg kell említeni az Interpol/Europol kiberbűnüldözési kezdeményezéseit, melyben a magyar részvétel hasznos tapasztalatokat hozhat!
- Köz- és magánegyüttműködés: Elsősorban a kritikus információs infrastruktúrák védelmében kulcsfontosságú a sokszor privát kézben levő rendszerelemek üzemeltetőivel való aktív együttműködés. Ez a jelenleg hatósági megközelítésű kapcsolat lényegesen hatékonyabb akkor, ha valamilyen kötetlenebb, pl. egyesületi együttműködés is párosul hozzá. Ilyen kezdeményezés az Önkéntes Kibervédelmi Összefogás (KIBEV) is, melynek célja az érintett szervezetek kibervédelemért felelős személyeinek megszólítása állami és civil oldalról is.
- Nemzeti kockázati szempontrendszer meghatározása, kritikus szolgáltatások és infrastruktúrák beazonosítása: Az Ibtv. rendelkezéseinek értelmében az érintett szervezetek elektronikus információs rendszereit és magát a szervezetet is kockázatalapon be kell sorolni. A kritikus információs infrastruktúrák esetében a rendszerelemeket

és ezek kockázati szempontjait az OKF-nek, illetve részben az Alkotmányvédelmi Hivatalnak kellene meghatározni! Ennek állapotára vonatkozóan nem áll rendelkezésre nyilvános információ.
- Nemzeti CERT működtetése: A Nemzetbiztonsági Szakszolgálat keretében a nemzeti CERT megkezdte működését, a CERT-Hungary korábbi infrastruktúrájára és kapcsolatrendszerére építve. A működés hatékonysága és az esetleges problémák később válnak értékelhetővé.
- Incidensjelentési eljárások kidolgozása: Az Ibtv. által megszabott egyik legfontosabb feladat a kiberbiztonsági incidensek jelentése. Ennek eljárásrendjére nemzetközi ajánlások állnak rendelkezésre, de Magyarországon nem egyértelmű ezek használata.
- Kibervédelmi gyakorlatok szervezése: A CERT-Hungary évek óta szervez kibervédelmi gyakorlatokat, illetve részt vesz ilyen nemzetközi rendezvényeken. Ezek folytatása, illetve kiterjesztése kiemelt fontosságú az elkövetkező időszakban.
- Humán képességek fejlesztése, kutatás-fejlesztés támogatása: Az Ibtv. az információvédelemért felelős személyek képzését kötelezően írja elő, ami fontos lépés a széleskörű tudatosság elterjesztésében. Vannak azonban hiányterületek, elsősorban a szakirányú műszaki felkészítés területén. Ezt, valamint a műszaki és társadalomtudományi irányú kibervédelmi K+F tevékenység támogatását erőteljesen kell támogatni!
- Kiberbűnözés visszaszorítása: Az intézményrendszer szétaprózott, a képességek fejlesztése esetleges, pedig mind az oktatási bázis, mind a nemzetközi kapcsolatrendszer adott ahhoz, hogy Magyarország hatékonyan vehessen részt a kiberbűnözés visszaszorítását célzó együttműködésekben.
- A biztonság és az adatvédelem közötti összhang kialakítása: Az információtechnológia elterjedése lehetőséget kínál arra, hogy az állam érdekeit és törvényeit sértő tevékenységeket célzottan és minden korábbinál hatékonyabban lehessen visszaszorítani. Ez azonban sértheti a magánszemélyek privát szféráját. Meg kell találni a hatékony egyensúlyt a bűnüldözés és az adatvédelem között, hangsúlyozva azt a nemzetközi gyakorlatot, hogy a személyes adatok védelmét érintő csekély jogszabályi lazítás is képes jelentősen növelni a nyomozati cselekmények hatékonyságát.
- Információáramlás elősegítése: A Belügyminisztérium szervezetein belül a kibervédelem feladatainak jelentős része összpontosul. Ez lehetővé teszi azt, hogy a minisztériumon belül olyan szakirányú koordináció épüljön ki, melynek segítségével a szervezetek közötti információáramlás akadálymentessé válik. Nem áll rendelkezésre nyilvános információ arról, hogy ezt a minisztérium hogyan kívánja megoldani, illetve a hatékonyság értékelését is csak később célszerű megtenni.

Összefoglalás

Magyarországon a nemzetközi ajánlásoknak megfelelően épül fel a kibervédelem belbiztonsági struktúrája. Számos területen nemzetközi viszonylatban is élenjáró együttműködések születtek a kormányzaton belül. Az Ibtv. olyan keretet ad, melyen belül hatékonyan oldható meg az ország kibervédelme. Az Ibtv.-t és annak végrehajtási rendeleteit, valamint a korábban elkészült, kibervédelmet érintő jogszabályok tapasztalatait azonban még korai lenne értékelni.

A kibervédelmi szabályozás az operatív feladatok döntő többségét a Belügyminisztériumhoz rendelte. Ennek megfelelően a minisztérium felelőssége és lehetősége is hatalmas. Belbiztonsági területen a kiberbűnözés és kiberterrorizmus elleni tevékenység esetében lehet lemaradást megállapítani. Amennyiben a Belügyminisztériumon belüli kibervédelmi koordináció sikeres lesz, és jól használják ki a rendelkezésre álló tudásbázist és erőforrásokat, ez a lemaradás gyorsan felszámolható.

IRODALOMJEGYZÉK

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[2] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
[3] Wamala, F.: The ITU National Cybersecurity Strategy Guide. International Telecommunication Union, 2011.
[4] National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace. European Network and Information Security Agency (ENISA), 2012.
[5] Klimburg, A. (ed): National Cyber Security Framework Manual. NATO CCD COE Publication, Tallinn 2012
[6] 2010. évi XLIII. törvény a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról
[7] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatok működéséről
[8] 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről
[9] 36/2013. (VII. 17.) BM rendelet a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról
[10] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[11] Gyömbér, B.: Reszkessetek betörők. Szerzői jog a XXI. században blog, http://copyrightinthexxicentury.blogspot.hu/2012/10/reszkessetek-betorok.html

HIGH-TECH BŰNÖZÉS NAPJAINKBAN: A SZELLEMI TULAJDON VÉDELME ÉS A VILÁGHÁLÓ

Krepsz Balázs

A Nemzeti Adó- és Vámhivatal 2011. január 1-én a Vám- és Pénzügyőrség és az APEH szervezetének integrációjával jött létre. A szervezet három pillérét az Adó Főigazgatóságot, a Vám- és pénzügyőri Főigazgatóságot és a Bűnügyi Főigazgatóságot a Nemzeti Adó és Vámhivatalának elnöke irányítja, és az egyes pilléreket a szakmai elnökhelyettesek felügyelik. Az interneten megvalósított jogsértések felderítésében mindhárom szakág együttműködik. Az Adószakmai szakág kijelölt egységei folyamatosan ellenőrzik az internetes kereskedelmet, próbavásárlásokkal, célzott adóvizsgálatokkal vizsgálják az adózással kapcsolatos jogszabályok betartását. A Vám- és Pénzügyőri Főigazgatóság szerveinek feladatai a harmadik országos import tevékenység ellenőrzésére terjednek ki. A szellemi tulajdonnal kapcsolatos bűncselekmény felderítése és a nyomozások lefolytatása a Bűnügyi Főigazgatóság feladata.

A NAV Bűnügyi Főigazgatósága

A szervezet működését a Bűnügyi Elnökhelyettes felügyeli és a Bűnügyi Főigazgató az egyes nyomozó szerveket közvetlenül irányítja. A Bűnügyi Főigazgatóság által irányított nyomozó szervek a Regionális Bűnügyi Igazgatóságok és a Központi Nyomozó Főosztály.

A Regionális Bűnügyi Igazgatóságok feladata a NAV hatáskörébe tartozó bűncselekmények megelőzése, felderítése és nyomozása. 2011-ben országosan több mint 1800 nyomozás indult a szellemi tulajdonnal kapcsolatos szerzői jog megsértése és áru hamis megjelölése bűncselekmények gyanújával. Több mint ezer nyomozás indult hamisított áruk – ruhák, gyógyszerek, műszaki cikkek és egyéb áruk – jogellenes forgalmazása miatt.

A szerzői jog megsértése miatt indult ügyek az alábbi fő kategóriákba sorolhatóak:

- hamis filmeket, zenéket, szoftvereket tartalmazó DVD lemezek árusítása
- matrica nélküli adathordozók jogellenes forgalmazása
- engedély nélküli zeneszolgáltatás
- Illegális fájlmegosztás, illegális letöltő oldalak üzemeltetése (FTP, torrent, linkelős oldalak)
- weboldalak, adatbázisok szerzői jogainak megsértése
- jogellenes szoftverhasználat

A NAV Bűnügyi Főigazgatósága Központi Nyomozó Főosztály feladata a szervezet hatáskörébe tartozó kiemelt ügyek felderítése és nyomozása. A szellemi tulajdonnal kapcsolatos, interneten megvalósított bűncselekmények nyomozására 2011 májusában külön egység, az Információ- Technológiai Osztály létrehozására került sor. Az osztály elsődleges feladata a

jogtulajdonosoknak jelentős vagyoni hátrányt okozó webhelyek folyamatos keresése, monitorozása, bűncselekmény gyanúja esetén a nyomozás lefolytatása, valamint az interneten forgalmazott hamis áruk forrásainak felderítése. Az osztály feladatai közé tartoznak továbbá az aktuális jogsértésekhez kapcsolódó internetes keresések, adatgyűjtések, a nyomozásokat segítő adatbázisok kezelése és a szervezet egyéb egységeinek informatikai, technikai támogatása.

A kalózkodás, hamisítás jelenlegi trendje, hatásai Magyarországon

Illegális szoftverek: A BSA adatai szerint Magyarországon a számítógépekre telepített illegális szoftverek összértéke 113 millió dollár. A világon globálisan az előző években 40%-ról 43 %-ra nőtt az illegális programok száma. Magyarországon ez 42 %-ról 41 %-ra csökkent 2010-re és 2011-ben további csökkenés tapasztalható. A csökkenés ellenére ma Magyarországon minden 10 telepített szoftverből legalább 4 illegális forrásból származik.

Illegális film és zeneletöltés: Becslések szerint az illegális letöltés és a hamis DVD lemezek forgalmazása évente 5-10 milliárd forint bevételkiesést okoz a filmforgalmazóknak, mely elérheti a legális forgalom 30-35 %-át. Még nagyobb arányú bevételkieséssel kell számolniuk a zenei kiadóknak, mivel az adatok alapján a legális zenei értékesítés volumene évről évre csökken. Egyes források az illegális forgalmazás által okozott kár mértékét még magasabbra teszik.

Hamis termékek forgalmazása: A HENT adatai szerint csökkent a hamis termékeket vásárlók aránya Magyarországon, azonban az internetes kereskedelem bővülésével a hamis termékek köre is jelentősen nő. A teljes magyarországi kiskereskedelmi forgalom 1,8 százalékát, 133 milliárd forintot kitevő webáruházi forgalom 2011-ben tovább bővül, és elérheti a 155-160 milliárd forintot melynek kb. 3-5 %-a lehet hamisítvány.

A kalózkodás és hamisítás amellett, hogy jelentős károkat okoz a legális forgalmazóknak csökkenti az állami bevételeket, a munkahelyek számát és rontja a magyar piac nemzetközi megítélését.

Az illegális letöltés múltja, jelene és jövője

Hamis DVD lemezek árusítása: 90-enes évek közepétől széles körben terjedt el a szerzői joggal védett filmeket, zenéket és szoftvereket tartalmazó hamis DVD lemezek árusítása. A közterületeken, piacokon tartott ellenőrzések során folyamatosan nagy mennyiségű adathordozó lefoglalására került sor. Az illegális lemezek árusítása az internetes letöltési lehetőségek bővülésével folyamatosan csökkent, azonban a mai napig lehet olyan internetes hirdetéseket találni, ahol főként gyűjteményeket kínálnak magánszemélyek eladásra.

DC, DC++ technológia: Az internet rohamos fejlődésével megjelentek olyan weboldalak, ahonnan szerzői joggal védett műveket lehetett közvetlenül, vagy egy belinkelt tároló helyről letölteni. A fájlcserére specializálódott technikai fejlesztésekkel olyan szoftverek jelentek meg az interneten, amelyek lehetővé teszik, a felhasználók otthoni számítógépein tárolt tartalmak egymás közötti megosztását. Az első nagyobb körben elterjedt technológia a DC (Direct Connect) lehetővé tette, hogy nagyszámú felhasználó egy időben csatlakozzon egy

adott szerverhez, és azon keresztül egymáshoz kapcsolódva a megosztott fájlokat akár több felhasználótól párhuzamosan lehessen letölteni. A technológia csak korlátozott sávszélességet és letöltési vonalat nyújtott a felhasználóknak, ezért ez lassan elavult és az új gyorsabb szoftverek vették át a DC HUB-ok helyét.

FTP technológia: A File Transport Protocol (FTP) technológia lehetővé teszi, hogy egy adott szerveren megosztott állományt, a szerver által nyújtott lehető legnagyobb sávszélességgel tudják letölteni a felhasználók. A szerverre feltöltött filmeket, zenéket, szoftvereket és könyveket így bármely otthoni számítógépről a cím és jelszó megadásával közvetlenül lehet elérni. A technológia a lehető legjobb lehetőséget biztosítja az elkövetők részére, hogy a felhasználóktól jelentős illegális bevételre tegyenek szert. A megosztott állományok eléréshez emelt díjas SMS szolgáltatással, banki átutalást vagy internetes fizetést követően adják meg az adott időszakra érvényes jelszavakat a felhasználók részére. A letöltési lehetőségeket különböző weboldalakon hirdetik miközben automatikus levelező és fizetési szolgáltatásokat nyújtanak. A fizetős FTP szerverek működtetésével évente akár több tízmillió forintos bevételre is szert tehetnek az elkövetők. A NAV internetes egységének elsődleges célja a fizetős FTP szolgáltatásokat működtető csoportok azonosítása, a büntető eljárás megindítása, és a jogsértéseket kiszolgáló szerverek lefoglalása. A folyamatos fellépés eredményeképpen a több tízezer felhasználót kiszolgáló szerverek száma jelentősen csökkent.

Torrent technológia: A világon jelenleg legelterjedtebb fájlmegosztó technológia. A kereső (tracker) szerverek egy webcímen érhető el, ahova szabad regisztrációs, fizetős regisztrációs vagy meghívásos rendszerben lehet hozzáférést szerezni. Az egyes felhasználók, vagy működtetők a tracker szerveren egy torrent fájlt helyeznek el, melyet a felhasználók letöltenek, elhelyeznek a saját számítógépeiken futtatott torrent kliensben, majd a rendszer automatikusan, kis szeletekben kezdi letölteni a művet azoktól a felhasználóktól, akik szintén megosztják vagy éppen töltik le az adott fájlt. A torrent szerverek sokáig ingyenesen működtek és a felhasználók csak egymás között cserélték a filmeket, zenéket és szoftvereket. A bűnözők felismerve a rendszer lehetőségét és a kereslet nagyságát napjainkban egyre több esetben – az FTP szerverek működtetéséhez hasonlóan - fizetős rendszerben kezdik működtetni a torrent oldalakat. Sok helyen már a regisztráció is fizetőssé vált, és a prémium szolgáltatások (fizetős arányjavítás, feltöltési kötelezettségek törlése stb.) is jelentős bevételeket jelentenek a működtetők számára. A művek torrent fájljainak feltöltése és azok folyamatos megosztása sok esetben már nem csak a felhasználók közötti adatcsere folyamatában történik, hanem az elkövetők speciális háttér megosztó szervereket (SEED szerverek) működtetnek. A NAV célja elsősorban a vagyoni előnyre törekvő, valamint a különösen nagy vagyoni hátrányt okozó megosztók elleni fellépés.

A jövő technológiái: A legújabb technológiai fejlesztések a decentralizált fájlmegosztás irányába mutatnak. A Tribler a Retroshare és a TOR rendszerek központi szerver nélkül működnek, minden funkciót, a kereséstől a fájlok és a kliensgépek azonosításáig és összekapcsolásáig maguk a hálózatra kötött gépek szolgálnak ki közösen. A decentralizált rendszereken a bűncselekményeket elkövető megosztók azonosítása új feladatok elé állítják a jogvédő és nyomozó szervezeteket.

A Központi Nyomozó Főosztály Információ- Technológiai Osztályának eredményei

2011 májusától az év végéig 11 kiemelt ügyben 10 FTP letöltő oldal ellen indult eljárás. Az érintett tartalom 2011-ben 20000 filmre, 9000 zeneműre, 2000 szoftverre és internetes könyvre terjedt ki. A nyomozások során feltárt, a jogtulajdonosoknak okozott vagyoni hátrány meghaladta a 2,4 milliárd forintot, míg az elkövetők azonosított illegális bevétele több mint 100 millió forint volt. Összesen a tavalyi évben 19 elkövető ellen indult eljárás. A háttér tároló szerverek lefoglalásával számos olyan oldal is megszűnt, amely nem képezte a nyomozások tárgyát, de azok kiszolgálását is az érintett számítógépek végezték. Az eljárásoknak köszönhetően olyan nagy szerverek szűntek meg mint az IWII, palace, apolló, SMS rapid, servehalflife, bravosms, babylon stb. A négy főből álló CINEDUB release team elleni eljárás jelentős nemzetközi visszhanggal is járt. Ez a csapat a premierfilmek megjelenését követő napon jó minőségű, magyar szinkronos filmeket készített, melyek azonnal felkerültek az internetre a torrent és FTP oldalakon keresztül. Az amerikai filmgyártók többek között a CINEDUB csoport tevékenysége miatt sújtotta Magyarországot olyan szankciókkal, hogy a premier filmeket csak hetekkel a nemzetközi bemutatókat követően lehetett bemutatni a magyar mozikban. A nyomozások eredménye, hogy a jobb minőségű premier filmek csak a bemutatót követően nagyobb késéssel jelennek meg az internetes platformokon.

Az osztály több esetben indított nyomozást olyan torrent oldalakkal (pl. Dark Angel, Terracod) kapcsolatban, melyek az FTP szerverekhez hasonlóan, elsődlegesen anyagi haszonszerzés céljából, SEED szerverek használatával működtettek.

A nyomozások több esetben pénzmosás gyanúját is felvetették, és rendszeresen indulnak adóvizsgálatok az érintett cégek és magánszemélyek tevékenységével kapcsolatban.

Az osztály a nyomozásokon kívül folyamatosan végez internet monitorozást és célzott internetes kereséseket is a jogellenes szerverek és a hamisított áruk forrásainak azonosítása céljából (pl. Pangea akció, Vatera aukciók vizsgálata stb.), tovább informatikai és technikai segítséget nyújt a szervezet nyomozó egységei számára.

Az Apolló ügy bemutatása

Az apolló ügy tipikus példája az illegális vagyonszerzés céljából, szervezett körülmények között működtetett warezszerver és az ahhoz kapcsolódó pénzmosási hálózat működésének. A két elkövető az internetes szolgáltató hosting céggel közösen, informatikai szakemberek közreműködésével hozott létre olyan tároló és kiszolgáló szervergépekből álló rendszert, mely alkalmas volt akár több ezer felhasználó egyidejű kiszolgálására. A tárhelyet az interneten keresztül az elkövetők folyamatosan töltötték fel az internetezőket érdeklő, szerzői joggal védett tartalommal, melyet FTP rendszeren keresztül lehetett az otthoni számítógépekről elérni. A felhasználókat e-mailen keresztül keresték meg, és ajánlották nekik a folyamatosan bővülő tartalmat. A szolgáltatásra Banki átutalással és a hosting cég által biztosított emelt díjas SMS szolgáltatással lehetett előfizetni. A beérkező befizetések alapján az elkövetők megadták a szerver elérhetőségét és a meghatározott időszakra érvényes jelszavakat a felhasználóknak, akik ezek birtokában korlátozás nélkül bármikor csatlakozhattak a már működő rendszerhez. A bankszámlákat olyan személyek nevére nyitották, akik a bűncselekmény elkövetésében nem vettek részt, a jogellenes

tevékenységről nem volt tudomásuk. A számlákhoz kapcsolódó netbank szolgáltatáson keresztül több bankszámlán át utalták folyamatosan a pénzt, melyet végül egy cég bankszámlájáról készpénzben vettek fel és juttattak vissza az elkövetőkhöz. A hosting cég vezetői és alkalmazottai is részesei voltak a bűncselekménynek, a rendszer kiépítéséért, működtetéséért rendszeres juttatást kaptak rendszert irányító elkövetőktől. A bűncselekményhez kapcsolódott még a CINEDUB release team, akik a premierfilmek feltöltésével tették vonzóbbá a szervereket, amiért ingyenes prémiumelérést kaptak a tartalomhoz. A bűnözői csoport elleni fellépéssel Magyarország akkor működő legszervezettebb és legnagyobb warezcsoportját sikerült felszámolni.

A nyomozás menete az interneten elkövetett szerzői jogsértéssel kapcsolatos ügyekben

Az eljárás alapja egyrészt a sértettek vagy a szerzőket és kiadókat képviselő civil szervezetek által tett feljelentések, bejelentések, másrészt a nyomozó hatóság által végzett internet monitorozás, internetes keresések eredményei. A nyomozás megindítását követően első lépésként internetes adatgyűjtésre kerül sor, melynek célja a szerver azonosítása a tartalom meghatározása, az elkövetők kilétének tisztázása. A megbízható szolgáltatóktól, bankoktól beszerzett adatok, segítik a bűncselekmény folyamatának előzetes feltárását. Az adatgyűjtést követően helyszíni intézkedés során kerülnek a szerverek fizikailag azonosításra, a hálózati és szervereken talált adatok alapján pedig megkíséreljük a gépek tényleges tulajdonosainak, illetve az azokat használó adminisztrátorok azonosítását. Minden esetben megpróbáljuk a jogellenes tevékenységből származó vagyon felkutatását és biztosítását. A rendelkezésre álló adatok alapján kerül sor a további általános nyomozati cselekményekre, házkutatásokra, kihallgatásokra, adatkérésekre és szükség esetén szakértői vizsgálatokra.

Módszerek és eszközök az internetes bűncselekmények felderítésében:

A nyomozás egyes mozzanatainak végrehajtásához speciális szoftverek és alkalmazások használatára van szükség, melyek az eljárás és az összegyűjtött adatok bizonyítékként történő felhasználásának hatékonyságát biztosítják.

Keresés és monitorozás: Az internetes felhasználók körében a legelterjedtebbek az általános online kereső szolgáltatások mint a google, a yahoo vagy az altavista. Ezek a kereső szolgáltatások azonban sepciális, és folyamatos szakmai keresésre nem alkalmasak. Hátrányuk, hogy az egyes keresőszavakra, vagy azok kombinációira akár több millió találatot is kaphatunk, a keresés így hatékonyan nem szűkíthető. Másik probléma, hogy a találatok folyamatosan ismétlődnek, illetve a rendszeres keresések eredménye is folyamatosan változik. A rengeteg adat feldolgozása így szinte lehetetlen, és lehet, hogy az általunk ténylegesen keresett webhelyek így nem azonosíthatóak. A szakmai keresésre és monitorozásra jóval alkalmasabb eszközök a speciális alkalmazások mint a copernic agent vagy az EU által fejlesztett Osint suite. A NAV által egyre szélesebb körben használt Copy Crawler alkalmazás magyar jogvédők által fejlesztett webes alkalmazás. A keresendő kifejezésekre egy külön működtetett szerver folytat le rendszeresen kereséseket, melyek eredményeit folyamatosan dolgozhatjuk fel úgy, hogy az általunk már azonosított és minősített webhelyeket a rendszer figyelmen kívül hagyja. Így a találatok folyamatosan szűkíthetők és azokból az általunk fontosnak tartott web-

helyek további elemzésére is lehetőség nyílik. Az alkalmazás használatával például a Pangea akcióban közel 300 olyan webhelyet tudtunk azonosítani, ahol feltehetően hamis vagy vény nélküli gyógyszer értékesítés történt.

Webhelyek azonosítása: A webhelyek regisztrátorainak és a kiszolgáló szervereket üzemeltető hosting cégeknek az azonosítását teszik lehetővé a webes whois szolgáltatások. A regisztrátor cég megkeresésével további információkat kaphatunk arról, hogy egy adott webcímnek valójában ki a tulajdonosa, használója.

Egyéb eszközök: Az eljárások során lehet szükség arra, hogy a webes tevékenységünket folyamatosan, reprodukálható módon rögzítsük, melyben segítenek azok a szoftverek (pl. Camstudio), melyek videóban rögzítik a felhasználó tevékenységét. A weblapmentő szolgáltatásokkal (pl. Httrack) teljes weblapok tartalma rögzíthető úgy, hogy az offline módban is az eredetivel azonos módon futtatható, akkor is ha a weboldal megszűnik, vagy tartalma megváltozik. A hálózati elemző szoftverek segítenek abban, hogy a szolgáltató cég szervertermében az éppen folyamatban lévő adatforgalomban részt vevő számítógépeket, felhasználókat azonosítani lehessen, a számítógépeken található log fájlok elemzése pedig a korábbi hálózati forgalom elemzésére adhat lehetőséget.

Hamisítás felderítése az interneten:

A hamis ruházati termékek értékesítését Magyarországon jellemzően távol-keleti származású személyek a közterületeken, piacokon végzik. A hamisított áru egy része importból származik, de több esetben folytatott nyomozást a Nemzeti Adó- és Vámhivatal illegális gyárakkal kapcsolatban. Az internetes kereskedelem terjedésével és a virtuális piacterek megjelenésével egyre gyakrabban jelennek meg főként hamisított gyógyszerek, műszaki cikkek és a ruházati termékek a magyar webhelyeken. Az elkövetők többnyire a már működő aukciós oldalakat (vatera, teszvesz) használják az áruk értékesítéséhez, de előfordul, hogy külön weboldalt hoznak létre az ilyen termékek reklámozásához. Külföldi weboldalakon (pl. ebay, alibaba) is lehet esetenként hamisított termékeket rendelni.

A hamisított áruk forrásainak azonosítása során az eljárás a keresési folyamattal indul, mely vagy automatikus, vagy egy adott termékre, vagy személyre irányuló célzott folyamat. A webhelyről gyűjtött adatok (telefonszámok, e-mail címek, bankszámlaszámok, emelt díjas SMS szolgáltatása, stb.), a weboldal regisztrátori és a szolgáltatóra vonatkozó adatok alapján kíséreljük meg az elkövető azonosítását. A szervereknél történő helyszíni intézkedés során esetenként meg lehet állapítani a rendszeradminisztrátorok, szerkesztők és hirdetők ip. címeit. A vásárlási folyamat nyomon követésével a csomagok feladójára és a kifizetésekre vonatkozó újabb információk merülhetnek fel, mely a nyomozati cselekmények végrehajtását hatékonyabbá teszi.

A bizonyítás nehézségei

Az interneten elkövetett bűncselekmények elkövetőinek felderítését az internet anonimitásából származó problémák nagy mértékben megnehezíthetik.

Az internet felhasználóit elsősorban az ip. címek azonosítják, amelyek bizonyos esetekben manipulálhatóak. A felhasználók proxy szolgáltatások használatával rejthetik saját

azonosságukat, és a webhelyek azonosításának megnehezítésére akár külön átjátszó (proxy, bounce) szervereket is üzemeltethetnek. Ezek a számítógépek csak továbbítják az adatokat, használható tartalommal nem rendelkeznek, így a tényleges tartalom gép azonosítása csak a proxyn átmenő forgalom elemzésével lehetséges. Az elkövetők a szervergépeket sok esetben fiktív cégek, vagy nem létező magánszemélyek nevére szóló hamis szerződésekkel helyezik el, továbbá más, az ügyhöz egyébként nem köthető személyek bankszámláit is használhatják. A lefoglalt számítógépek adatainak titkosításával, az adatok gyors törlésével pedig a saját virtuális nyomaikat próbálják eltüntetni.

A vagyoni hátrány és a sértettek körének meghatározása a gyakorlatban: Az interneten történő jogsértések esetén:

Filmek esetén: on-line terjesztés licencdíja mely jelenleg legalább 800,-USD filmenként az egyes sértettek viszonylatában összesítve. A sértettek meghatározása saját filmadatbázis alapján történik. Hamisított lemezek esetén a vagyoni hátrány a lemezek számához igazodik (korábbi szakértői vélemények és a közös jogkezelők nyilatkozata alapján filmenként 2500 Ft)

Zeneművek esetén: A vagyoni hátrány megállapítása jóval bonyolultabb mivel az internetes terjesztésre általános elfogadott licencdíj eddig nem került kimunkálásra, ezért általában a letöltések száma alapján a korábbi szakértői vélemények és a közös jogkezelők nyilatkozata alapján zenei albumonként 3200,-Ft). A zeneművek kiadóinak azonosítása a MAHASZ adatbázisa alapján történik.

Szoftverek és játékok esetén a vagyoni hátrány egy mű szerzői jogához kapcsolódik, és annak forgalomba hozatalával okozott kárban fejezhető ki, amely a nettó kereskedelmi árnak felel meg. A sértettek ezekben az ügyekben a szoftverek forgalmazói.

A büntető jog és a polgári jog a szerzői jogvédelemben:

A büntetőjogi fellépés elsődleges céljai:

- az illegális szerverek működésére szakosodott bűnözői csoportok felderítése és felelősségre vonása
- a ténylegesen jelentős károkat okozó szerverek lefoglalása, az elkövetők felelősségre vonása és ezzel az illegális lehetőségek körének leszűkítése
- a jelentős vagyoni hátrányt okozó internetes feltöltők felelősségre vonása

A büntetőjogi fellépés eszközei a társadalom széles rétegeit érintő jelenségek végleges megoldására nem feltétlenül alkalmasak. A büntető eljárásnak nem célja nagy számú felhasználó bíróság elé állítása és a vagyoni hátrányt valójában nem okozó tevékenységek elleni fellépés.

A szerzői jogsértések elleni fellépésnek azonban a büntetőjogon kívül olyan eszközei is vannak, melyek fellépésre a jogtulajdonosoknak közvetlenül adnak lehetőséget. Az elektronikus kereskedelemről szóló 2011. évi CVIII. Tv lehetőséget ad a jogtulajdonos számára, hogy a szolgáltató, illetve másodsorban a közvetítő szolgáltatót (pl. hosting cégek) felhívják a jogsértő tartalmak azonnal eltávolítására.

A jogszabályok megfelelő megváltoztatásával, illetve a jogtulajdonosok piaci magatartásának lassú változásával olyan lehetőségek is felmerülhetnek, melyek a széles körű társadalmi

jelenségek megváltoztatását, a jogsértések számának csökkenését szolgálják. Ilyen eszközök lehetnek például a jogsértő weboldalak elérésének korlátozása, erőteljesebb szankciórendszer, az elfogadható árszínvonalat biztosító legális letöltő, szórakoztató oldalak elterjedése.

Az együttműködés fontossága:

A bűncselekmények és egyéb jogsértések felderítése, a jogsértő források azonosítása és visszaszorítása érdekében fontos az érintett civil szervezetek és hatóságok lehető legjobb együttműködésének kialakítása. Ennek érdekében a NAV igyekszik minden együttműködési lehetőséget a leghatékonyabban kihasználni. A legfontosabb partnereink a:

- jogvédő civil szervezetek és egyéni jogtulajdonosok
- HENT
- Nemzeti Média és Hírközlési Hatóság
- NEBEK (Europol, Interpol)
- internet szolgáltatók
- CERT
- Vám- és Adószervezetek nemzetközi együttműködése
- Az EU tagországok egyéb bűnüldöző, ügyészi szervei
- Nemzetközi konferenciák
- Jogsegélyek

Bírósági gyakorlat szerzői ügyekben:

A bírósági gyakorlat szerint a kisebb ügyekben jellemző a pénzbüntetés, megrovás alkalmazása. Ezekben az ügyekben gyakori a közvetítői eljárás, melynek során az ügyészség felügyelete mellett történik az okozott vagyoni hátrány megtérítése, így az elkövető mentesülhet a büntetés alól. Nagyobb ügyekben, az első elkövetés esetén jellemző a megrovás, felfüggesztett szabadságvesztés kiszabása. Kiemelt ügyekben, melyekhez esetlegesen pénzmosás bűncselekmény is kapcsolódik várható letöltendő vagy nagyobb mértékű szabadságvesztés és nagyobb pénzbüntetés kiszabása, de az ilyen jellegű ügyek többsége még folyamatban van, így ítélkezési gyakorlatról még nem beszélhetünk.

KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZEREK SZOFTVERBIZTONSÁGÁNAK KORSZERŰ MEGVALÓSÍTÁSI ESZKÖZEI

Kuris Zoltán

Korunkat információs társadalomként szokás jellemezni. A társadalom gazdasági, politikai és kulturális működésében meghatározó szerepűek a kommunikációs és információs rendszerek.

A társadalom működésének szempontjából kiemelt fontosságúak a kritikus infrastruktúrákat működtető kommunikációs és információs rendszerek, melyek komplex és integrált védelmének biztosítása feltétlenül szükséges, mivel e rendszerek rendeltetésszerű működésének, a benne kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérülése súlyos biztonsági, politikai, gazdasági károkat, ipari katasztrófákat is eredményezhet. A napjainkban kialakításra kerülő elektronikus rendszerek már döntően kereskedelmi forgalomban kapható, így széles körben elterjedt hardvereket és szoftvereket alkalmaznak.

Irányadó szakemberek szerint a kinetikus energián alapuló hadviselés mellett megjelent a kiberhadviselés, annak elmélete és gyakorlata folyamatosan fejlődik, amely a kritikus infrastruktúrák elleni információs dimenzióban megvalósuló hálózati hadviselés informatikai, fizikai és emberi eszközökkel és azok dimenzióiban valósulnak meg[1]. Az utóbbi időben egyre többet lehet hallani a kiberbűnözésről, nagyvállalatok és kormányzati szervek elleni online támadásokról, és az ebből eredő károkról, melyek egyre álcázottabb és szofisztikáltabb kivitelezésűek.

A kommunikációs ás információs rendszerek elleni kiber támadások legnagyobb mértékben a rendszerben alkalmazott szoftverkörnyzet sebezhetőségét próbálják kihasználni. Az információs rendszerek meghibásodásai is legtöbbször szoftverhibákra vezethetők vissza, az incidensek többségének hátterében ugyanakkor emberi mulasztás áll.

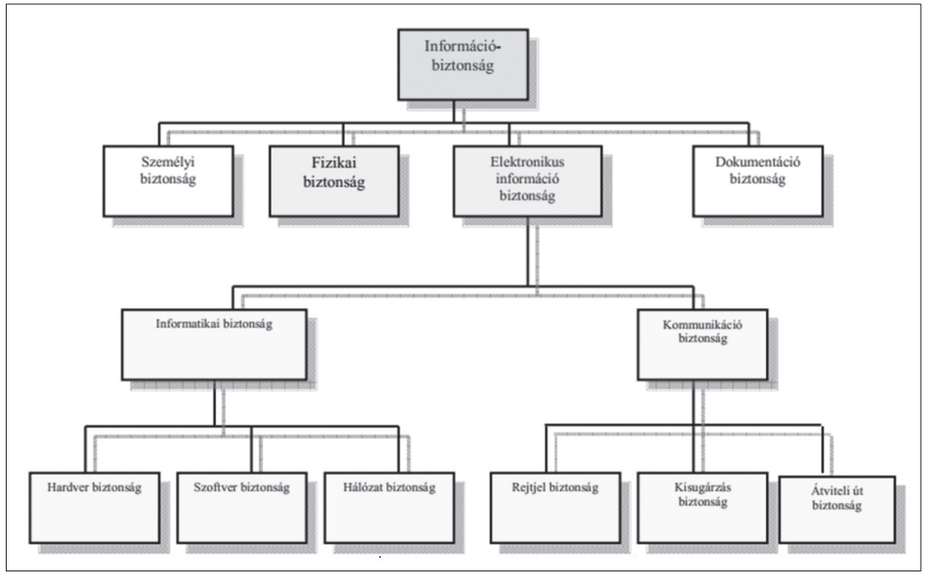
Fontos szempont tehát a szoftveres sebezhetőségéből eredő biztonsági kockázatokat súlyuknak megfelelően kezelni és számolni azzal, hogy elektronikus rendszerekben a szoftverbiztonság akkor tekinthető megvalósultnak, ha az abban alkalmazott szoftverekből eredő biztonsági kockázatok technikai megoldásokkal, bevezetett rendszabályokkal annak kritikusságával arányosan kezeltek a rendszer teljes életciklusában (tervezésétől, rendszerből történő kivonásáig), mely eljárás a szoftverbiztonság szavatolása.

A szoftverbiztonság szerepe a komplex és integrált védelemben

A kommunikációs és információs rendszerek működésfolytonossága, a bennük kezelt információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása komplex és integrált védelem kialakításával valósítható meg. Ennek érdekében összehangolt információ-

1 http://www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf

óbiztonsági rendszabályok megalkotása és bevezetése szükséges a rendszer teljes életciklusára kiterjedően személyi biztonsági, fizikai biztonsági, dokumentumbiztonsági, elhárítási és elektronikus információbiztonsági védelmi intézkedések alkalmazásával. Az alábbi ábra mutatja a komplex és integrált védelem fő területeit, azon belül is részletezve az elektronikus információbiztonság területeit, valamint a szoftverbiztonság helyét a komplex információbiztonsági rendszerben.



1. ábra. A komplex információbiztonság rendszere[2]

A kiemelt, kritikus létfontosságú kommunikációs és információs rendszerek szolgáltatásainak futtatását, abban adatok kezelését a kor követelményeinek megfelelő szerverteremekben üzemelő korszerű hardvert és szoftvert alkalmazó szerver számítógépekkel lehet leghatékonyabban biztosítani, szoftverek tekintetében körültekintően kialakított szoftverbiztonság szavatolási eljárás alkalmazásával.

A szoftverbiztonság megvalósításához a rendszer szoftverkörnyezetének és abban alkalmazott szoftvereknek az alábbi követelményeknek kell megfelelnie[3]:

- Megbízható működés: a szoftver minden körülmények közt végrehajtja feladatát és kiszámíthatóan működik, beleértve az ellenséges körülményeket is, amikor támadás alatt áll.
- Megbízhatóan tervezett: a megbízható szoftver nem tartalmaz olyan sebezhetőséget és gyengeséget, melyet kihasználva manipulálni vagy szabotálni lehet a szoftver megbízható működését. Akkor megbízhatóan tervezett egy szoftver, ha nem tartalmaz olyan tervezési hiányosságot, mely rosszindulatú módon kihasználható lehet.

2 http://hadmernok.hu/2010_4_kuris.pdf
3 https://buildsecurityin.us-cert.gov/bsi/547-BSI.html#dsy547-BSI_dacs

- Fennmaradóképes (Rugalmas): a szoftver a legtöbb ismert támadásnak ellenáll (védekezik) vagy elviseli azokat (továbbra is megbízhatóan működik), amennyire lehetséges számol a további lehetséges támadási formákkal is. Működése helyreállítható a lehető leggyorsabban, alacsony károkkal akkor is, ha a támadást nem tudta elhárítani vagy elviselni.

Fentiek megvalósításához fontos, hogy a szoftverkörnyezetben alkalmazott szoftverek közül a kereskedelmi forgalomban kaphatók rendelkezzenek a megfelelő működésbiztonsági tanúsítvánnyal. Amennyiben egyedi fejlesztésű szoftver kerül alkalmazásra, úgy azt fenti elvek szerint tervezzék, működésbiztonságát tanúsító cég vizsgálja. A működésbiztonság tanúsítványon a szoftverek megbízhatóságát a Common Criteria nemzetközi információbiztonsági szabvány (ISO/IEC-15408) szerinti Evaluation Assurance Level megfelelési szint jellemzi. A hétfokozatú skálája az EAL1-től (funkcionálisan tesztelt) a legszigorúbb EAL7-ig (formálisan igazolt módon tervezve és tesztelve) terjed.

Jellemző, hogy gyakorlatilag alig néhány EAL4(+) (tervszerűen tervezett, tesztelt és átnézett) szintűnél magasabb termék létezik a piacon, a szoftvergyártó világcégek szerverre szánt operációs rendszerei (AIX, HP-UX, Solaris, Windows Server 2008 R2, SUSE és Red Hat vállalatoknak szánt Linux disztribuciója), is csak EAL4(+) besorolásúak. Irányadó szakértői vélemények szerint az EAL4 szint igazából nem túl sok mindent garantál.

Természetesen önmagában az, hogy biztonságos szoftverek kerülnek alkalmazásra nem garantálja azt, hogy az ezekből felépített szoftverkörnyezet, - ami adott esetben fizikailag egymástól több ezer kilométerre lévő szerverparkokban lévő szerverekből kialakított fürtre vagy számítástechnikai felhőre (cloud computing) van telepítve - biztonságos legyen. Ugyanakkor a rendszer jelentőségével arányosan megkövetelendő, hogy a szoftverek biztonsági beállításai, interaktivitásuk körültekintően legyen konfigurálva, a szoftverkörnyezetben működjön rosszindulatú szoftverek ellen védelmet nyújtó biztonsági szoftver, követelmények szerint naplózás és auditálás, üzemezett mentés, és automatizált helyreállítási eljárás legyen megvalósítva.

Kiemelten fontos, hogy kockázatértékelési eljárásban meghatározott időszakonként a rendszerbiztonság felülvizsgálatának részeként a szoftverbiztonság felülvizsgálatára kellő hangsúly legyen fordítva, mert világszerte a szoftverbiztonsági kockázatok növekedése veszélyezteti legnagyobb mértékben a kommunikációs és információs rendszereket. Azt hogy a szoftverbiztonsági kockázatok miként növekednek, az alábbi gondolatokkal lehet szemléltetni.

A szoftverbiztonság növekvő jelentősége

Napjaink trendje, hogy a közszféra és magánszféra nagyobb (domináns) szereplői is egyre nagyobb mértékben veszik igénybe külső szolgáltatók informatikai szolgáltatásait. Pár évvel ezelőtt ennek jellemző formája még az outsourcing volt, a szervezetek internettől elszeparált belső hálózatán, telephelyein üzemelő informatikai eszközöket üzemeltette egy külső cég, a szervezetek csupán saját bérelt vonalakkal rendelkeztek. Megállíthatatlanul terjed a cloud computing (számítási felhő), melynek lényege, hogy külső szolgáltató a telephelyein működtetett hardver infrastruktúrán virtualizációs technológiák korszerű alkalmazásával kínál a vevő igényeihez igazodó szolgáltatásokat, akár virtualizált szervert is. A virtualizált szolgáltatások, szerverek nagy előnye, hogy az erőforrásai dinamikusan skálázhatók így például biz-

tosítható az, hogy egy virtualizált szerveren futó számlázó rendszer a havi egyszeri számla feldolgozási időszakban pl. 10-szer több processzorteljesítményt és memóriát alkalmazzon. A távoli telephelyen futó szerver és a felhasználó által működtetett végponti eszköz (pl. asztali vagy notebook számítógép, táblagép, okostelefon) közötti adatkommunikációs csatorna a védett kommunikáció érdekében jellemzően az internet biztonságos hálózati protokoll (pl. https), vagy virtuális magánhálózat (VPN). A saját szerverparkot üzemeltető szervezetek is gyakran biztosítják egyes dolgozóiknak zárt hálózataik távoli elérését VPN-en keresztül.

Ugyanakkor bebizonyosodott, hogy még a legbiztonságosabbnak tartott VPN megoldások is támadhatók. Ismeretes, hogy 2011. május 21-én katonai hadititkok megszerzése céljából megkísérelték feltörni a Lockhead Martin amerikai haditechnikai nagyvállalat informatikai rendszerét, a cég állítása szerint a támadás ugyan sikertelen volt, de erre reagálva azonnal leállították a VPN-es távoli elérést melyhez az RSA SecureID hardverkulcson alapuló megoldást alkalmaztak[4]. Az eset kapcsán informatikai szakértők azon véleményüknek adtak hangot, hogy többé nem lehet az RSA megoldását biztonságosnak tartani, mely a szegmensben piacvezető. Válaszul az RSA felajánlotta ügyfeleinek a hardverkulcsok cseréjét (40 milliót alkalmaznak világszerte), ami részben beismerésnek is tekinthető.

A Gartner piackutató egyik sajtóközleménye[5] szerint a mobil előfizetések száma 2011-ben elérte az 5.6 milliárdot, 2015-re 7.4 milliárd mobil előfizetést prognosztizálnak. A Nemzetközi Távközlési Egyesület adatai szerint[6] a világ lakosságának 35%-a használ internetet, míg a fejlett országokban a lakosság 74%. A világ pénzforgalma (mely kb. 100-szorosa a tényleges áruforgalomnak) döntően elektronikus tranzakciók keretében zajlik, 2010-ben az Egyesült Államokban a papíralapú pénz már mindössze 10%-a volt csak az összes forgalomban levő pénznek[7].

Az infokommunikációs technológiák fejlődésével és elterjedésével együtt mind több eszköz és szolgáltatás lesz online elérhető, ezzel egyidejűleg dinamikus nő a kibertámadások száma. A Symantec biztonsági cég 2011. évi internetes biztonsági fenyegetettségekről készített beszámolójában[8] kiemelt alábbi néhány adat jól szemlélteti a fenyegetések dinamikus növekedését:

- 80%-kal több támadást detektáltak, mint az előző évben (5,5 millárd támadást).
- A spamak száma előző évhez képest 50 százalékot emelkedett (napi 62 milliárdra becsülik), mely a teljes e-mail forgalom 75%.
- Minden 299-dik e-mail adathalász, minden 239-dik vírusos.
- A 2500 fő feletti vállalatok 50% volt célpontja célzott támadásnak.
- A vállalati vezetők, középvezetők és kutatás-fejlesztési területen dolgozók 42%-nak támadták az elektronikus postafiókját.
- 187 millió embernek lopták el személyes adatát.
- Előző évhez képest 40%-kal, 403 millióra emelkedett a különböző rosszindulatú szoftver (malware) variánsok száma.
- Az év során 4989 új szoftversebezhetőség lett felderítve, átlagosan naponta 8 sebezhetőség kerül felfedésre, melyek különösen veszélyesek (javítócsomagok hiányában nehéz ellenük védekezni, ugyanakkor a sebezhetőség ténye széles körben gyorsan ismertté válik)

4 http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html
5 (http://www.gartner.com/it/page.jsp?id=1759714)
6 http://en.wikipedia.org/wiki/Global_Internet_usage
7 http://www.federalreserve.gov/releases/h6/20110127/
8 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Egyre inkább számolni kell azzal is, hogy a rendszerben használt szoftverek fejlesztésének, működtetésének, jogosult alkalmazásának rendszerében rosszindulatú személy is pozícióba kerülhet, a szoftverbiztonsági rendszert tehát úgy kell kialakítani, hogy ezek a fenyegetések is a lehető legalacsonyabb kockázattal járjanak.

A 2011. novemberi Londoni Kibertér Konferencián mondott beszédében David Cameron brit miniszterelnök évi 1000 milliárd dollárra becsülte a kiberbűnözésből eredő globális károkat[9]. Ugyanekkora károkat becsült Jamie Shea a NATO felmerülő biztonsági kihívásokért felelős helyettes főtitkár is. 2011. december 7-én egy romániai tárgyalást követő sajtótájékoztatón alábbiakat mondta: *„Szinte minden héten van olyan incidens, amely arra emlékeztet bennünket, hogy a kiberbiztonság kapcsolódik életünk szinte valamennyi aspektusához. 1000 milliárd dollár tűnik el évente a globális gazdaságból a kiberbűnözés miatt. Az ipari titkokat, szerzői jogokat, szellemi tulajdont, államtitkot egyre nehezebb megvédeni. A gazdaságok e komplex rendszereken működnek, melyek könnyen megsemmisíthetők”* [10]. A kormányzatok egyre súlyosabb fenyegetésként tekintenek a kiberterrorizmusra.

Sokszor még a legkorszerűbb adatközpontok működését is megbénítja szoftverhiba. Ezek közül ez évben az egyik legnagyobb nyilvánosságot kapott eset volt, amikor a szökőév kezelés szoftverhibája miatt 2012. február 29-én egy teljes napra leállt a világon a Microsoft Azure számítástechnikai felhőszolgáltatás, melyet a világ számos nagyvállalata alkalmaz üzletileg kritikus rendszereihez.

Megalapozott az a megállapítás, hogy a kibertér biztonságának fontosságát ma már az államok vezetése is súlyuknak megfelelően kezeli, Obama amerikai elnök szavai szerint „a kiber-fenyegetettség az egyik legsúlyosabb gazdasági és nemzetbiztonsági kihívás nemzetünk számára”, a múlt évi Londoni Kibertér Konferencián brit miniszterelnök, amerikai alelnök, számos miniszter, nagyvállalat és nemzetközi szervezet vezetője képviseltette magát. Ugyanezen konferenciasorozat ez évi rendezvénye Budapesten lesz. Tavaly év végén hazánk először vett részt a NATO kibervédelmi gyakorlatán, a Nemzeti Biztonsági Felügyelet szervezetében létre lett hozva a kibervédelmi központ.[11]

Szoftverbiztonság szabályozottsága, támogató dokumentumai

A hazai jogszabályi környezetben a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet meghatározza a szoftverbiztonság követelményeit a minősített adatok elektronikus kezelésének szempontjából. Megállapítható azonban, hogy csak a legfőbb követelményeket határozza meg, végrehajtásának módját nemzeti minősített adatok vonatkozásában további normatívák nem szabályozzák.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény megalkotása amely a szoftverbiztonságot kiemelt hangsúllyal kezeli, azért is volt mielőbb szükséges, mert a korábbi az elektronikus közszolgáltatás biztonságáról szóló

9 http://ukinmontserrat.fco.gov.uk/en/news/?view=Speech&id=685398482
10 http://www.infosecisland.com/blogview/18577-NATO-Cybercrime-Drains-One-Trillion-Dollars-from-Economy-Yearly.html
11 http://www.honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat

223/2009. (X. 14.) Korm. rendelet, mely részletesen szabályozta az elektronikus közszolgáltatást nyújtó rendszerekre vonatkozó szoftverbiztonsági követelményeket 2012. április 22-vel hatályon kívül lett helyezve. Ennek következtében a létesülő rendszerek szoftverbiztonsági követelményeinek érvényesítésére (a használatbavételi eljárások során) nincs megfelelő normatív támogatás biztosítva.

Míg a hazai normatív szabályozás hiányos, a szabványok és ajánlások közülük, kiemelten az információbiztonsági irányítási rendszerekkel kapcsolatos ISO/IEC 27000-es szabványcsoporton, az ISO/IEC 15408 Common Criteria és az irányadó NATO és EU szabályozásokon alapul. A KIB 25. számú ajánlásaként kiadott Magyar Informatikai Biztonsági Ajánlás, mely az informatikai biztonság irányítás és értékelését teljes folyamatát lefedi, köztük a szoftverbiztonságot is kiemelten kezeli.

A NATO rendszerek esetén a szoftverbiztonsági követelmények (elvek, módszerek, eszközök) a rendszer teljes életciklusára vonatkozóan a NATO Biztonságpolitikájának támogató direktíváiban pontosan meghatározottak. Ezek közül a szoftverbiztonságot részletesebben szabályzók minősítettek, illetve nem nyilvánosak, ezért nyílt publikációban nem elemezhetők. Viszont „kiemelten figyelemre méltó", hogy mindenki számára elérhető a NATO információbiztonsági weblapja (http://www.infosec.nato.int/). A weblap egyik leghasznosabb szolgáltatása a NATO minősített adatok kezelésére tanúsított hardverek és szoftverek katalógusa, amelyek többsége normál kereskedelmi forgalomban kapható. Tekintettel arra, hogy az itt szereplő termékek alapos bevizsgálást követően lettek engedélyezve NATO minősített adatokat kezelő rendszerekben történő alkalmazásra, más termékhez képest kisebb kockázatúak, tehát ismeretük mindenképpen ajánlott a hazai információbiztonsági szakemberek számára. A termékekhez, köztük szoftverekhez biztonságos műszaki kivitelezési útmutatók tölthetők le (STIG-ek).

Az amerikai Nemzetbiztonsági Hivatal és az amerikai Nemzeti Szabványügyi és Tecnhológiai Intézet információbiztonsággal weblapjain (http://www.nsa.gov/ia/ia_at_nsa/ és http://csrc.nist.gov/) is mindenki számára elérhetően részletes biztonságos konfigurálási útmutatók vannak az elterjedtebb szervereken és végpontokon alkalmazott szoftverekre vonatkozóan. Egy-egy ilyen útmutató, pl. egy szerver operációs rendszer vagy adatbázis-kezelő szoftver esetén jellemzően több száz oldalas, és a szoftverbiztonság összes aspektusára kiterjed.

Az útmutatók első fejezete általánosan meghatározza, hogy az abban leírt eljárások közül melyek mikor követelmények, és mely esetben csak ajánlottak. Jellemzően közös alapelvük hogy az alkalmazott szoftvereknek csak a rendszer rendeltetéséhez szükséges moduljai legyenek telepítve, minden felesleges szolgáltatás legyen letiltva. Ezt követően installálásuk, rendszerspecifikus beállításaik, frissítésük, jogosultságok, monitorozások, naplózások, auditálások, hibadetektálásuk, mentés-helyreállítás menedzsmentjének megvalósítását tárgyalják.

Ezt követően joggal és értelemszerűen merül fel a kérdés, hogyan valósítható meg egy kor követelményeinek megfejlő rendszer biztonságos szoftver architektúra, amely biztosítja szolgáltatásainak működésfolytonosságát, a benne kezelt információk bizalmasságát, sértetlenségét és rendelkezésre állását?

A szoftverbiztonság korszerű megvalósítása

A gyakorlati tapasztalatok azt mutatják, hogy gyakorta olyan kommunikációs és információs rendszerek vannak alkalmazásban világszerte (és hazánkban is) kritikus fontosságú feladatok ellátására, amelyek megalkotása során nem kalkulálták megfelelően a biztonsági kockázatok növekedését, illetve felhasználásuk iránti növekvő igényt, tervezésükkor a biztonsági elvek nem kellő mértékben érvényesültek, architektúrájuk hibatűrés, skálázhatóság szempontjából alulméretezett, ezáltal működésbiztonságuk, támadásoknak történő ellenállásuk a kor követelményeinek már nem megfelelők. Ebből levezethető, a kritikus infrastruktúrák sebezhetőségének növekedése is.

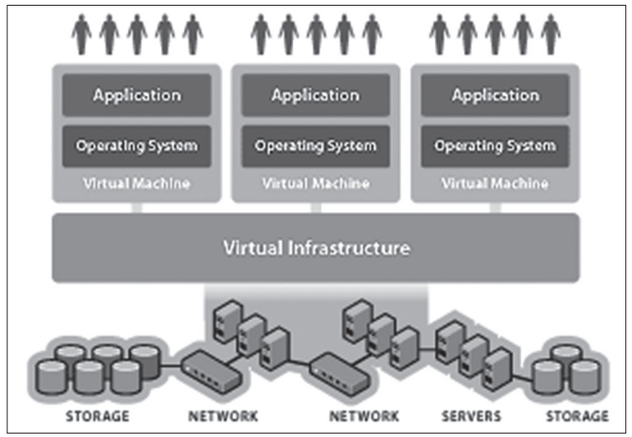
Hibatűrés szempontjából alulméretezett egy rendszer, ha az elvárt rendelkezésre állást nem tudja teljesíteni, ha pl. energiaellátása, adatkommunikációs csatornái, hardverei, szoftverekkel megvalósított szolgáltatásai nem megfelelő mértékben redundáns kialakításúak, egy elemnek a meghibásodása a rendszer teljes szolgáltatás kiesését eredményezheti. (Pl. ha 99.99%-os rendelkezésre állás az elvárt, hetente 1 percet állhat a rendszer.) Skálázhatóság szempontjából akkor alulméretezett egy rendszer, hogyha kapacitása és funkcionalitása nem bővíthető dinamikusan az új és megnövekedett felhasználási igényeknek megfelelően.

Az informatikai infrastruktúrafejlesztések időszakos szervezeten belüli megvalósításához szükséges erőforrásokkal gyakran nem rendelkezik a szervezet, illetve gyakorta költséghatékonyabb havidíjas konstrukcióban külső szolgáltatók adatkommunikációs szolgáltatásainak, szerverszolgáltatásainak igénybevétele. Ezért mind több szervezet választja azt, hogy működése szempontjából kritikus informatikai szolgáltatások és bizalmas információik kezelését is külső szolgáltatok által működtetett informatikai infrastruktúrán valósítsa meg. Ösztönzően hat erre az is, hogy a távközlési szolgáltatók ma már hazánkban is a legkorszerűbb technológiájú adatkommunikációs szolgáltatásokat kínálják (FlexCom bérelt vonal, fényszálas vezetékes, 4GL mobil internet) megfizethető áron. A szervezetek egyre komplexebb szerverszolgáltatásokat vesznek igénybe külső szolgáltatóktól, napjaink számítástechnikai felhő szolgáltatásainak egyik nagy előnye, hogy kiválóan skálázhatók, áraik versenyképesek a saját üzemeltetéshez képest a számos szolgáltatónak köszönhetően, ugyanakkor biztonságos működésük működtetőik üzleti létérdeke is.

Figyelemre méltó ugyanakkor az is, hogy nagyobb szervezetek sokszor a központosítás felé haladva sem bízzák szerverszolgáltatásaik kiszolgálását külső szolgáltató informatikai infrastruktúrájára, gyakran saját szervertermeikben létesítenek privát felhőket (private cloud)!

Összefoglalva, az irodai munkakörnyezetben alkalmazott informatikai szolgáltatások mobil elérése növekvő igény. Ugyanakkor a korszerű szoftverbiztonság megvalósítását egy rendszerben, annak teljes életciklusára a piaci trendekből prognosztizálható fejlődésre, biztonsági kihívásokra tekintettel kell megalkotni!

Ha a szervezet számára lehetséges, korábbi informatikai szolgáltatásainak migrálása, új szolgáltatásainak bevezetése saját informatikai infrastruktúrájának fejlesztésével, akkor célszerű, hogy a hibatűrés és skálázhatóság érdekében a szervereket, aktív hálózati eszközöket, adattároló egységeket (storage) hardver virtualizációs technológiák alkalmazásával privát felhőbe szervezze. Ennek megvalósításában napjaink egyik piacvezető szoftvermegoldása a VMware Virtual Infrastructure, ugyanakkor dinamikusan nő a piaci részesedése a Microsoft Hyper-V megoldásának is. Az alábbi ábra szemlélteti a fentiekben leírtak megvalósítást.



2. ábra VMware Virtual Infrstructure logikai vázlata
Forrás: http://www.vmware.com/virtualization/virtual-infrastructure.html

A virtualizált infrastruktúrán menedzsment konzol szoftver alkalmazással pillanatok alatt hozhatók létre virtualizált szerverek és munkaállomások, erőforrásaik az igényeknek megfelelően dinamikusan változtathatók, alkotóelemeinek állapota, változásuk, üzemeltetésében végrehajtott műveletek egységes felületen naplózódnak, biztosítja azt is, hogy az üzemeltető személyzet feladatainak mértékben tudja csak ezen erőforrásokat vezérelni. A virtualizált számítógépekről könnyen készíthetők mentések, tükörmásolatok a fejlesztési folyamatokhoz vagy kockázatértékelési tesztekhez, melyek az éles szoftverkörnyezet funkcionalitásának bővülését, és biztonságának növelését célozzák, úgy hogy azok működését nem veszélyeztetik. Hiba esetén korábbi állapotba könnyen visszaállíthatók

A virtuális szervereken kiszolgált komplex üzleti alkalmazásokat (pl. vállalatirányítási rendszereket, szervezeti portálok) háromrétegű architektúrába szokás szervezni, melyben az adatok tárolását és hozzáférését tipikusan egy relációs adatbázis-kezelő rendszer (pl. Oracle Database. Microsoft SQL Server szoftverrel), a dinamikus tartalmak előállítását alkalmazásszerver, a felhasználói felületetet jellemzően webszerver szolgáltatja, ez esetben a végponti eszközökön a szolgáltatások igénybe vétele mindössze webböngészőt igényel, így a végponti eszköz lehet akár egy táblagép vagy okostelefon is. Ma már általános biztonsági elvárás, hogy a szerverek közti és a szerver kliens közti kommunikációk titkosított adatcsatornán keresztül történjenek, az adatok védelme érdekében az adatbázis szintű titkosítás alkalmazása, nyilvános kulcsú infrastruktúra (PKI) alkalmazása, mely hitelesítő tanúsítványokat szolgáltat a rendszerben alkalmazott szolgáltatásoknak, eszközöknek és felhasználóknak. Az így megvalósított rendszer biztosítja, hogy a komplex üzleti alkalmazás szolgáltatásai és az abban kezelt információvagyonhoz történő hozzáférés feletti teljes kontrolt, hogy azokat csak a jogosult eszközökről a jogosult felhasználók érjék el.

A szoftverbiztonság lényeges tényezője a komplex végpontvédelem, hardveres és szoftveres megoldásokkal, alkalmazása alapvető elvárás. Az integrált védelmi szoftverek vírusvédelmet, kémprogramok elleni védelmet, hálózati fenyegetésekkel szembeni védelmet (tűzfal, behatolásvédelem) biztosítanak. Követelmény, hogy proaktív fenyegetésérzékeléssel is rendelkezzenek, azaz észleljék az új és gyorsan módosuló rosszindulatú programokat és az ismeretlen fenyegetéseket is felfedjék, aktívan blokkolják a támadásokat. A szegmensben a két piacvezető a Symantec és a McAfee. Az üzleti felhasználásra szánt termékek a végpontokra (szerverek, asztali és notebook számítógépek, táblagépek, okostelefon) központi menedzsmentalkalmazásukból telepíthetők, melyből menedzselhető és felügyelhető az összes végpont.

Nagyobb informatikai infrastruktúrát alkalmazó szervezetek nem nélkülözhetik a szoftverekkel megvalósított automatizált rendszerfelügyeletet mely magába foglalja a működésfelügyeletet, változáskezelést, konfigurációkezelést, verziókezelést, eszközállomány-kezelést, hibakezelést, kapacitáskezelést és eseménykezelést ezek megvalósítását. Ilyen szoftverek pl. a Microsoft System Center (fő elemei Configuration Manager és Operation Manager) az IBM Tivoli és Rational termékcsaládja. A külső szolgáltatók számítástechnikai felhőjén (pl. Amazon EC2, Microsoft Azure) megvalósított informatikai architektúrák automatizált rendszerfelügyelete is biztosított ezek alkalmazásával.

Összegzés, következtetések

Összességében megállapítható hogy a kommunikációs és információs rendszereknek mind komplexebb szolgáltatásokat kell nyújtaniuk, ezért informatikai infrastruktúrájuk egyre összetettebb. Szolgáltatásaik működésfolytonossága, a bennük kezelt adatok bizalmasságának, sértetlenségének, rendelkezésre állásának sérülése súlyos károkhoz vezethet, a kritikus infrastruktúrákat működtető és a minősített adatok kezelő rendszerek esetén ez még hatványozottabban értelmezhető. E rendszerek komplex és integrált védelmén belül egyre fokozottabban kell ügyelni a szoftverbiztonságra, mivel a rendszerek működését gyakran a nem megfelelően kialakított és üzemeltetett szoftver architektúra veszélyezteti. Az ellenük irányuló dinamikusan növekvő támadások döntően a szoftverkörnyezet sebezhetőségét próbálják kihasználni. Ezért fontos hogy a rendszerben megfelelő működésbiztonsági tanúsítvánnyal rendelkező bevizsgált szoftverek kerüljenek alkalmazásra. A kritikusabb alkalmazások fejlesztése során ezért kiemelten fontos tényező az egyedi szoftverfejlesztések biztonsági auditja, a kialakított szoftverkörnyezet működtetésének, változásmenedzsmentjének szabályozottsága, felügyelete, védelme, amelyek automatizálását szoftveres megoldások is segítik.

A szabályozott működéshez fontos hogy a jogalkotók jogszabályokban normatív utasításokban meghatározzák a rendszerek működtetésére vonatkozó követelményeket a társadalom működésében kritikus fontosságú kommunikációs és információs rendszerek vonatkozásában, hazánkban ennek érdekében folyamatban van az információbiztonsági törvény részletszabályozásának megalkotása. A publikációban kifejtett ismeretanyagból is következik, hogy a szoftverbiztonság megvalósításában fontosak és alapvetően szükségesek az információbiztonsági szabványok, ajánlások, információbiztonsággal foglalkozó szervezetek és gyártók biztonságos kivitelezést támogató útmutatói. A korszerű szoftverbiztonság megteremtéséhez a szoftvergyártó cégek a kor követelményeinek megfelelő korszerű szoftvereket kínálnak, melyek centralizált kontrolt biztosítanak az üzemeltetett rendszerre. A külső szolgáltatók által kínált számítástechnikai felhő szolgáltatások egyre inkább költséghatékony alternatívák a saját informatikai infrastruktúra fenntartásával szemben, mind több rendszer

válik online elérhetővé, így a szoftverbiztonság területén belül a proaktív fenyegetettségek elleni védelemre különösen nagy hangsúlyt kell fektetni.

IRODALOMJEGYZÉK

[1] http://www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf (2012.05.12.)
[2] http://hadmernok.hu/2010_4_kuris.pdf (2012.05.12.)
[3] https://buildsecurityin.us-cert.gov/bsi/547-BSI.html#dsy547-BSI_dacs (2012.05.12.)
[4] http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html (2012.05.12.)
[5] http://www.gartner.com/it/page.jsp?id=1759714) (2012.05.17.)
[6] http://en.wikipedia.org/wiki/Global_Internet_usage (2012.05.17.)
[7] http://www.federalreserve.gov/releases/h6/20110127/ (2012.05.19.)
[8] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (2012.05.21.)
[9] http://ukinmontserrat.fco.gov.uk/en/news/?view=Speech&id=685398482 (2012.05.12.)
[10] http://www.infosecisland.com/blogview/18577-NATO-Cybercrime-Drains-One-Trillion-Dollars-from-Economy-Yearly.html (2012.05.22.)
[11] http://www.honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat (2012.05.22.)

DEFINING CYBER-SECURITY: THE ROLE OF NATO IN ENSURING COMMON DEFENSE

Liflander, Christian-Marc

I will not bore you with the genesis of NATO's role in cyber defence. Let's just say: it has been a long and hard climb. Today, however, we are moving fast on the road to take cyber defence where we want it to be – and where it needs to be: in the centre of Allied and partner attention. Cyber defence is finally shedding its image as a playground for geeks, and taking its rightful place as a "must-have" core capability for the 21st century NATO.

In my remarks today, I want to focus on the future – a future that will feature strong public-private partnerships and closer cooperation with partner countries as well as academia. We all know full well: cyber defence is a cooperative exercise. It requires the close interaction of all key stakeholders, public and private; civilian and military; state and non-state; defence and homeland security. NATO is certainly not a "silver bullet" in cyber defence – but it has unique capabilities to offer to Allies and help them achieve enhanced cyber security. Let me very briefly – in a telegramme-style – offer you ten points that describe the role that NATO has in ensuring common defense and where I see NATO going in cyber defence.

First, cyber will get even more attention from our highest political levels. Since the Lisbon Summit, cyber has been given much visibility by our Heads of State and Government. The next Summit will be even stronger on cyber defence. This should help us move forward – but it will also increase the pressure on us to do it right. And this brings me to my second point: we have a robust Cyber Defence Action Plan from last year that we need to fully implement. Currently that is clearly the top priority. All NATO structures will be brought under centralised protection. Last February, a 58 million Euro contract was awarded to upgrade the NATO Computer Incident Response Capability. These efforts now underway will significantly enhance NATO's cyber capabilities over the coming months. And since technology is not standing still, we cannot lean back: a continuous attention will be required also in the future to keep this capability up-to-date.

Third, it is critically important to be aware of how the cyber threat landscape evolves and have indications and warning before cyber attacks targeting our digital networks occur. The recently established Cyber Defence Threat Assessment Cell (CTAC), which will become fully operational in a few months serves as a most useful interface between the tactical/operational level cyber awareness the NCIRC Technical Centre and the warnings and analyses by the intelligence community. Our situational awareness could be further enhanced by using NATO as a platform, a sort of "clearing house" where key stakeholders, Nations and industry exchange relevant information and intelligence to increase our chances of early detection.

Fourth, we will accelerate our efforts in training and education on cyber defence, through our schools and specifically through the NATO Cooperative Cyber Defence Centre of Excel-

lence in Tallinn. The Centre could very well serve as a broad platform for Nations and industry to share best practices and lessons learned and run joint exercises. Our goal is ensure that an ever greater number of officers and civilians understand the cyber challenge. NATO has a fine tradition of educational excellence. We will build on it.

Fifth, capabilities. NATO is about capabilities, and cyber is no exception. To quote the famous military strategist – Ronald Reagan: "I once played a Sheriff without a gun – I was dead 27 minutes into the show". You cannot put it any better. But what does this mean in cyber terms, and what does it mean in times of austerity? It means that Allies need to re-prioritise. That they spend more on cyber even if they are cutting elsewhere. Some are already doing this; other must do it, too. Enhancing cyber defence costs money, but it won't break the bank. Besides, we can save money through multilateral solutions. If we can do it in strategic airlift; we can also do it in cyber. For me, this would really put the "smart" in "smart defence".

Sixth, we will integrate cyber defence into the NATO Defence Planning Process. This process is one of NATO's greatest assets. It makes Nations through the development of force targets concentrate their efforts and build capabilities that the Alliance needs. It gives NATO its unique punch.

Seven, we will work even more closely with partner countries. Cyber defence is a cooperative effort, where no one, however powerful, can go it alone. You cannot build fences that are high enough to keep cyber threats away. NATO can do a lot more if it works with others. And we have a strong and large partnership network , which now reaches from Europe all the way to the Asia-Pacific region. 69 countries are connected through it – that's more than a third of the globe. By working with these partners on cyber defence, we can shape the strategic environment in unprecedented ways. And we are determined to use this opportunity. Similarly, we are establishing standards for future military operations, which will have an impact not only on the NATO Allies but also on the military of our traditional operational partners.

Eight, we want to work more closely with other international organisations, in particular with the European Union. We would defintely do a major disservice to our members states if these two organisations were to fail to get their act together. We need to develop standards together. NATO has already embarked on that road for national CIS that NATO depends on. We also need to harmonise our crisis response procedures. Not doing so is a recipe for failure – and an abdication of our common responsibility to protect our citizens. That's why we will continue to push for a new level of NATO-EU cyber cooperation.

Nine, NATO should move beyond its traditional communities and tear down the old separation lines between the defence and the homeland security communities. Cyber defence cannot be effective if we do not link the two together.

My tenth and final point: we will need more public-private partnership. Let's face it: More than 85 % of our cyber infrastructure is owned by the private sector. It is the private sector that produces the technology solutions that we need. And they are the ones who represent the first line of defence. I am aware that this is not NATO's traditional terrain. But let me be very clear: without more private-public partnerships NATO would be left behind the curve. And we want NATO to be ahead of the curve.

Threats arising from cyberspace are increasing both in frequency and sophistication. Protecting our 900 million citizens against such threats is an enormous challenge. It requires

a new understanding of collective defence; a new definition of core, essential capabilities; and it requires new ways of doing business with partner countries, other organisations, and, above all, the private sector. Some have said that this is too complex a challenge for NATO to handle. I disagree. Yes, cyber is a crucial test for our Alliance: NATO can either stand up and be counted, or lie down and be counted out. But I can confidently say to you: We have no intention of lying down.

ROBOTREPÜLŐ RENDSZER FEJLESZTÉS MAGYARORSZÁGON

Molnár András

Az elmúlt évtized, de különösen az elmúlt évek során a robotrepülőgépek fejlesztése és a fejlesztések kapcsán megjelenő prototípusok száma jelentősen megnövekedett. Ezzel egy időben számos területen jelentkezett igény kisméretű (max. 25 kg felszálló tömeg), elsősorban megfigyelésre alkalmas robotrepülőre. Látszólag a kereslet és kínálat ezen a területen mintaszerűen talál egymásra. A terület mélyebb elemzése során azonban nyilvánvalóvá válik, hogy számos megválaszolatlan kérdést kell még tisztázni ahhoz, hogy ezeknek a repülőeszközöknek a mindennapi alkalmazása megvalósulhasson.

Ilyen kérdések többek között – az alkalmazás jogi kérdésein túlmenően – a megbízhatóság, az üzembiztonság, az egyszerű alkalmazhatóság. A kutatás során az alkalmazás jogi kérdései csak érintőlegesen, elsősorban a tesztelések kapcsán váltak vizsgálat tárgyává, mivel a fejlesztések fő irányvonala a repülőgépek műszaki és informatikai területeire koncentrálódott. Ugyanakkor jelentős erőfeszítéseke történtek egy komplex robotrepülő-rendszer kifejlesztésére, mely magában foglalja a repülőeszköz fedélzeti elektronikájának és fedélzeti szoftvereinek, valamint a földi állomás szoftverrendszerének megtervezését és prototípusának kifejlesztését.

Jelen kutatás egy hazai fejlesztés eredményeit kívánja bemutatni, illetve összevetni azokkal az elvárásokkal, melyek biztosítják az autonóm repülőeszközök minimális alkalmazási kockázatát. Az értekezésben választ kívánok adni arra a gyakran felmerülő kérdésre, hogy miért nem elég jó az amatőrök körében elterjedt úgynevezett FPV (First Person View) repülőgép a fenti célokra.

A hobby modellek fejlődése

Pilóta nélküli repülőeszköznek mondhatók a modellezők körében hobby vagy játék céllal készített rádiótávirányítású repülőgépek. Ennek ellenére a gyakorlatban ezeket az eszközöket nem tekintjük valódi pilótanélküli eszköznek. Ennek oka elsősorban az alkalmazás hatósugarában keresendő. Egy klasszikus rádiótávirányítású repülőmodell hatósugarát két alapvető tényező határozza meg. Az első a kezelő „pilóta" látótávolsága. Ez a modell méretétől függően néhányszor 100 métertől néhány kilométer (1-2 km) távolságig terjed. A másik tényező az alkalmazott távirányító rendszer (adó és vevő) hatótávolsága. A kereskedelemben kapható eszközök igazodnak az első tényező paramétereihez, azaz a látótávolsághoz. Egyes esetekben (távcsöves vezetés) a látótávolság megnövelhető. Ebben az esetben jó minőségű távirányítóra, esetleg adóteljesítményt fokozó erősítőre is szükség van. Ilyen alkalmazás lehet például hazánkban is alkalmazott célanyag repítése, ahol fontos, hogy a repülőgépet vezető személy a lőszektoron kívülről irányítsa a modellt.

A mikroelektronika fejlődésével megjelentek a kisméretű kamerák és velük együtt a kis távolságú videó átjátszó rendszerek. Ezek együttes alkalmazása új lehetőségeket nyitott meg az amatőrök körében. A modellrepülőre szerelt kamera képét egy rádióadó segítségével a földön, valós időben megjelenítve a modellező azt a látványt kapja, mintha a gépben ülne. Ezt tovább fejlesztve kialakult a kamera kép segítségével történő modellrepülő vezetés technikája, ami már FPV repülés néven vált közismertté.

Az FPV rendszer látszólag kiküszöböli a látótávolság problémáját, hiszen ha kellően nagy hatótávolságú a videó összeköttetés, akkor a fedélzeti kép alapján a modell vezethető. Szűk keresztmetszet lett a távirányító rendszer hatótávolsága. A gyakorlat során azonban hamar kiderült, hogy a rendszer számos veszélyforrást rejt magában. A kamera képe – amíg az átvitel hibamentes – nem gyengül a távolság növekedtével szemben a hagyományos modell vezetésével, ahol a távolodó gép egyre kisebbnek látszik. A kamera kép elvesztése általában olyan távolságban következik be, ahol már szabad szemmel nem vezethető a modell, így ez az esemény rendszerint a modell lezuhanásával jár. Amennyiben a videó lesugárzó rendszer hatótávolsága nagyobb, mint a vezetést biztosító távirányító rendszeré, úgy a gép vezethetetlenné válása okozhatja annak lezuhanását, miközben a fedélzeti kép hibátlan.

A gépek elvesztésének megakadályozására újabb megoldások születtek. Ezek közül a legegyszerűbb a fedélzeti vevő által vett jel térerejének visszajelzése. Ez az információ hozzásegíti a modell vezetőjét ahhoz, hogy az irányíthatóság szempontjából ne lépje át a biztonságos távolságot. Sajnos, a vevő érzékenysége valóságos körülmények között nem minden esetben van arányban az adótól mért távolsággal. Részben a repülőgép térbeli mozgásából, részben a terepviszonyoktól függő jelterjedésből adódóan előfordulnak vételi kiesések. Ezek az esetek továbbra is gépvesztéssel párosulhatnak. A vétel kiesését egyes rendszerek a fedélzeten elhelyezett másodvevővel vagy másodantennákkal igyekeznek mérsékelni.

Kétvevős megoldást alkalmaz az EmcoTec[1] cég rendszere. Az EmcoTec által gyártott fedélzeti elektronika lehetővé teszi többek közt, hogy az irányítást két vevő által előállított vezérlőjelekkel valósítsák meg. Természetesen egy időpillanatban csak az egyik vevő jelei vezérlik a repülőgépet, de annak vételi zavara esetén a rendszer azonnal átkapcsol a tartalék vevőre. A tartalékvevő antennáját úgy kell elhelyezni a repülőmodellen, hogy annak geometriai tengelye szöget zárjon be az elsődleges vevő antennájának geometriai tengelyével. Ebben az esetben az antenna kedvezőtlen térbeli helyzetéből adódó vételkimaradás jelentősen csökkenthető vagy megszüntethető. Lehetőség van a másodvevőt más frekvenciasávban alkalmazni, ha speciális, kétsávos távirányító adót használunk. Ez tovább növeli a vételi biztonságot, mivel az alapfrekvencia interferenciája esetén is képes megbízható távirányítást biztosítani.

Futótűzként terjed a modellek távirányítása céljából a 2,4 GHz-es rendszer. A gyártók – számos egyéb előny mellett – a diszkrét csatornák felhasználó általi kezelését mellőző megoldást hangsúlyozzák. Ez azt jelenti, hogy a 2,4 GHz-es távirányító rendszerek automatikusan keresik meg a sáv szabad csatornáját, vagy éppen több csatornát felhasználva biztosítják a kapcsolatot. Ezen módszerek csökkentik a felhasználó figyelmetlenségéből adódó interferenciákat (azonos csatornán több adó készülék egy időben történő üzemeltetése), illetve a más zavarforrásokból származó interferenciákat. A 2,4 GHz-es rendszerek legtöbbje rendelkezik

1 EMCOTEC, embedded controller technologies GmbH, Waldstr. 21, D - 86517 Wehringen

2 vagy több antennával, ami a már előzőekben megfogalmazott térbeli antenna helyzetekből adódó vételkieséseket hivatott csökkenteni.

A távirányítás megbízhatóságának növelésével újabb szűk keresztmetszet a fedélzeti elektronika energiaellátása lett. Ezen a területen két különálló szegmens határozható meg. Egyik a szigorúan vett elektronika, illetve vezérlés áramellátási kérdése. Mivel a fogyasztás a gyakorlatban alkalmazott Lithium-polimer akkumulátorok kapacitásához mérten nem jelentős, itt elsősorban a váratlan akkumulátorhibák okoznak problémát. A kontakthibás akkumulátorok ellen a legtöbb gyártó párhuzamosan kapcsolható kétakkumulátoros megoldást kínál. A második szegmens az elektromos hajtású repülőgépek esetén a meghajtó rendszer áramellátása. Ebben az esetben nem ritka a 100A áramfelvétel, ami gyakorlatban a meghajtó akkumulátorok igen gyors kisülését jelenti. A repülési időt, így elsősorban ezen akkumulátorok kapacitása határozza meg. Általában a repülési idő 10 perc és 1-2 óra között mozog. Amennyiben repülés közben lemerül az akkumulátor, akkor a gép biztonságos visszatérése a repülőgép repülési jellemzőitől, a magasságától, a leszállóhelytől való távolságától, valamint a légköri viszonyoktól (elsősorban szél) függ.

Éppen ezért elterjedt a fedélzeten mérhető néhány jellemző adat továbbítása a repülő vezetője felé. Eleinte ezek az adatok elsődlegesen az akkumulátorok állapotára, a repülőgép koordinátájára (GPS), és a repülés sebességére korlátozódtak. Mára egyre több adatra van igény, ami egyre nagyobb sávszélességet igényel. Sok FPV rendszer a telemetriai adatokat a lesugárzott képen jeleníti meg úgynevezett OSD (On Screen Display) rendszerrel. Az OSD rendszer azonban csak informálja a repülőmodellt vezető pilótát a fedélzeten mért paraméterekről. A repüléssel kapcsolatos összes döntés és maga a gép vezetése is a pilóta feladta.

A megbízható adat(kép)-kapcsolat érdekében a fedélzeti RF sugárzók teljesítménye sok esetben az engedélyezett mértéket meghaladó. A teljesítmény fokozása látszólag ugyan eredményre vezet, valójában azonban számos új probléma forrásává válik. A nagyobb teljesítményű adók fogyasztása is növekszik, ami az üzemidő csökkenésével, vagy nagyobb akkumulátorok alkalmazásával párosul. Ez utóbbi esetben a repülési idő fog rövidülni a nagyobb tömegű repülőgép nagyobb energiaigénye miatt. A másik probléma a távirányítást szolgáló fedélzeti vevő „elnyomása” a közeli nagyteljesítményű sugárzó által. Főként a gyengébb minőségű képtovábbítók elégtelen kimeneti harmonikus elnyomása okozza a fedélzeti vevők – beleértve sokszor a GPS vevő – elnyomását. Valódi megoldást a nagytávolságú összeköttetések érdekében az antennák nyereségének növelésével és (vagy) a hatékony modulációs eljárások alkalmazásával lehet találni.

A modell repülőgépen irányított antennák alkalmazása nem hatékony. Ott általában körsugárzó antennát alkalmaznak, ugyanakkor a földi vevőállomásoknál elterjedtek a nagy nyereségű antennák. Ilyen antennák alkalmazása újabb megoldandó feladatot jelent. A nagy nyereség jellemzően az antennának csak egy kitüntetett irányában valósul meg. Éppen ezért az antennákat mindig a repülőgép felé kell irányítani. Ez megoldható úgy is, ha előre tervezett területen végezzük a repülést, és az antennát úgy telepítjük, hogy a gép a teljes repülés időtartama alatt annak „látószögében” maradjon. Ez nem minden esetben lehetséges, mivel a nagy nyereségű antennák látószöge szűk. A problémát az antenna aktív forgatásával lehet megoldani. Az automatikus forgatáshoz azonban szükség van a repülőgép pillanatnyi koordinátáira. Igaz ugyan, hogy ezzel az információval a repülőgép vezetője az OSD rendszeren keresztül rendelkezik, de az automatika számára a képből az adatok csak

igen körülményes módon nyerhetők ki. Néhány rendszer kínál erre is megoldást. Amennyiben hagyományos TV lesugárzó rendszer kerül a repülőgép fedélzetére – ez a leggyakoribb –, akkor az adatok egy része a hangcsatornára modulálható[2]. A földi állomás a hangcsatorna demodulációját követően digitális formában képes előállítani többek között a repülőgép koordinátáit, amit az automata antennaforgató – felhasználva a saját koordinátáját – képes feldolgozni[3].

1. ábra. A szerző által készített nagyfelbontású kép Dunakeszi repülőterének egy részletéről

Képek rögzítése terén két fő irányvonal bontakozott ki. Az első megoldás során a felhasználók nem a mozgókép rögzítését túzték ki célul, hanem a minél nagyobb felbontású fényképek készítését. Ennek egyik elterjedt módszere a több képből utófeldolgozás során elkészíthető nagy területet lefedő, nagy felbontású kép. A módszer érdekessége, hogy számos esetben elegendő egy megfelelő alkalmazással ellátott, úgynevezett okos telefon, amely egységnyi időközönként automatikusan készít fényképeket 4-5 megapixel felbontással. Az utófeldolgozás során nincs szükség arra sem, hogy a képek az adott területről rendezett sorban készüljenek. Számos szoftver automatikusan képes a felvételeket egymáshoz ileszteni és létrehozni a terület nagy felbontású fényképét. Az eljárás érdekessége, hogy az amatőr felhasználók egy adott területről jóval nagyobb felbontású képet képesek létrehozni, mint azt a rendelkezésükre álló képrögzítő berendezés készíteni tudna. Az 1. ábrán látható kép egy 2,5 kg tömegű, 1,5 méter fesztávú elektromos repülőgépre szerelt

2 Molnár, A. (2007). Telemetriai egység kisméretű robotrepülőgépek számára, Robothadviselés 7. Nemzetközi Konferencia és Kiállítás, 2007. november 27., Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest in: Hadmérnök online tudományos lap, konferencia különszám.

3 Molnár, A. (2008). Automata antennaforgató autonóm robotok számára, Repüléstudományi konferencia, 2008. Szolnok, Repüléstudományi közlemények különszám, 2008. április 11.

HTC Desire mobil telefonnal készült képekből az „Image Compose Editor”[4] szoftver segítségével lett előállítva. A felvétel során a repülőgépen lévő mobil telefon kamerája nem volt stabilizálva. A képeket a telefon 1mp-es időpközönként automatikusan készítette. A képek utólagos összefűzése hasonló a panoráma kép készítéséhez, de jóval fejletteb eljárással. A képeket nem kell sorrenben készíteni és az összefűző program számára nem kell megadni az illeszkedő területeket. Mindezt a program teljesen automatikusan végzi. Természetesen a végeredmény minősége javítható, ha a képek készítése során miztosítunk egy olyan pályát, amely a kérdéses területet teljes mértékben és egyenletesen fedi le, valamint biztosítjuk a kamera stabilizálását.

A amtőr alkalmazások során a második elterjedt képkezelési technika nagy felbontású (HD) mozgóképek készítésére irányul. Ebben az esetben olyan kamerákat rögzítenek a repül eszköz fedélzetén, amiket a gyártók extrém körülmények közötti alkalmazásra ajánlanak. Ilyen kamera például az igen elterjedt GoPro[5] kameracsalád. Az eszköz valós időben SD kártyára rögzíti akár 120 fps (képkocka/másodperc) sebességgel a HD minőségű videót. A kamera további előnye a rendkívüli dinamikatartománya, ami repülőgépeken különösen előnyös. A kamera rendelkezik kompozit videó kimenettel, így a kép valós időben a repülőgép irányítója számára is megjeleníthető, igaz jóval gyengébb felbontásban. Ez az élőkép azonban tökéletesen alkalmas a kompozíció folyamatos ellenőrzésére.

A legújabb fejlesztések a rádiókapcsolat megszakadásából adódó károk elkerülését célozzák. Már kereskedelmi forgalomban kapható számos, a repülést támogató eszköz. Ezek legelső példányai a repülés automatikus stabilizálását hivatottak szolgálni. Ilyen eszközök a giroszkópok és az optikai vagy termikus[6] elven működő stabilizátorok. Segítségükkel a repülőmodell vezetése egyszerűbbé, esetenként rövid ideig autonómmá válik. Útvonalrepüléshez azonban nem elégségesek. Szintén kereskedelmi forgalomba kerültek olyan elektronikák[7], melyek képesek a hozzájuk kapcsolt szenzorok segítségével nemcsak stabilizálni, de útvonalon repíteni is a kisméretű modelleket. Az ArduPilot az egyik legelterjedtebb fedélzeti elektronika. Népszerűségét a számos kiegészítő elemen túl a szabadon hozzáférhető nyílt forráskódú szoftver biztosítja. Az ilyen eszközökkel felszerelt modellrepülőgépek már képesek valódi autonóm repülések végrehajtására. Tekintve, hogy a fejlesztés nem csak a szoftvert tette nyíttá, hanem a hardvert is, számos gyártó megjelent olyan kisméretű elektronikákkal, melyekre az Ardu szofverek feltölthetők. Ilyen például napjain egyik igen népszerű Crius All In One elektronikája[8]. A panel (2. ábra) 60-70 USD áron beszerezhető. Tartalmaz mindent (GPS és MODEM kivételével), ami merevszárnyú, vagy multirotoros repülő eszközök autonóm vezérléséhez szükséges. Számos kiegészítő vásárolható a központi egységhez, így könnyen fejleszthető. Az alaplapra integrált 9 szabadságfokú IMU és légnyomásmérő, a panelhez kapcsolt GPS vevővel lehetővé teszi egy többrotoros repülőeszköz egy pont köröli lebegtetését valamint útvonalrepülését.

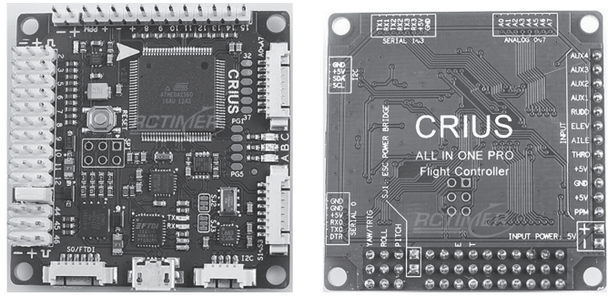
4 http://research.microsoft.com/en-us/um/redmond/groups/ivm/ice/

5 © 2013 Woodman Labs, Inc, http://gopro.com

6 Co-Pilot™ II Advanced Infrared Flight Stabilization System Reference Manual, FMA, Inc. 5713 Industry Lane, Suite 50 Frederick, MD 21704 Sales: (800) 343-2934 Technical: (301) 668-4280 www.fmadirect.com

7 ArduPilot is a family of open source autopilots based on the Arduino platform. http://www.diydrones.com/notes/ArduPilot (2011)

8 http://www.rctimer.com/download/Crius_AIOP_Manual_MWC.pdf



2. ábra. A CRIUS AIO robotpanel[9]

A Crius AIO panelen is futtatható ArduCopter program képes együttműködni a személyi számítógépen futtatható ArdupilotMegaplanner10 földi szoftverrel[10]. A szoftver alkalmas a repülőeszköz konfigurálására (pl. Szabályzók PID beállítása, kiegészítő elektronikák aktiválása, stb.), az autonóm üzemmódhoz szükséges útvonaltervezésre, valamint megfelelő MODEM esetében a repülés valósidejű megfigyelésére (virtuális pilótafülke). A nyílt forráskód filozófiája a földi szoftver esetében is igaz, így bárki fejlesztheti, illetve készíthet a repülőeszközzel kommunikáló saját rendszert. Mára már elérhetővé váltak okos telefonokon futtatható, a PC-s szoftver funkcionalitását biztosító programok, így az ilyen rendszerrel ellátott hobby drónok rendkívül kompakt eszközökké válhatnak.

Az ArdiPilot beállítása, köszönhetően a széles felhasználói körnek és az általuk üzemeltetett fórumoknak akár közepes felkészültséggel rendelkező felhasználó számára is megoldható. A rendszer meglepően stabil. Az alapbeállítások jó kiindulási alapot biztosítanak. A fórumok a berepülés során tapasztalt jelenségek alapján igen jó iránymutatást biztosítanak, így az amúgy összetett PID szabályzók beállítása, illetve hangolása is könnyen megoldható.

Következtetések

A hobby modellek fejlődését követve látszólag kialakult a mai értelemben is robotrepülőnek tekinthető eszköz. Minden kétséget kizáróan megállapítható, hogy a legmodernebb hobby eszközök felhasználásával készíthető autonóm repülésre alkalmas modell. Nem szabad azonban figyelmen kívül hagyni azt a tényt, hogy az ilyen módon összeállított rendszer elemei nem professzionális céllal készültek. Mindez azt jelenti, hogy a modellek csak korlátozott feltételek mellett viselkednek megfelelő módon. A biztonságnak, a hobby kategóriáknál, elsődlegesen a modell tulajdonosa számára a modell megmentése tekintetében van jelentése. Az alkalmazott kamerák és a képtovábbító rendszerek képminősége is elsősorban a modell kezelőjének élményét hivatott biztosítani. Ezek a képek alig alkalmasak felderítésekre vagy

9 http://www.rctimer.com/download/Crius_AIOP_Manual_MWC.pdf
10 www.diydrones.com
Arduplane: code.google.com/p/ardupilot-mega/wiki/home?tm=6
ArduCopter: code.google.com/p/arducopter/wiki/ArduCopter?tm=6
ArduRover: code.google.com/p/ardurover/wiki/Overview?tm=6

megfigyelésekre, és még kevésbé alkalmasak speciális képfeldolgozó eljárásokkal megszerezhető információk szerzésére.

Az újabb irányzatok azonban (több képből összeállított nagy felbontású fotó, vagy fedélzeten rögzített HD minőségű videó) már felderítési igényeket is képesek kielégíteni. Mindezt a kereskedelemben szabadon beszerezhető eszközök segítségével. Ez azt is jelenti, hogy amatőr eszközökkel sámos civil felhasznló készíthet egy adott területekről olyan, igen jó minőségű felvételeket, amiket eddig csak a fejlett katonai eszközöket birtokló, állami felügyelett alatt működő egységek voltak képesek elkészíteni.

Természetesen az itt megfogalmazott hátrányok a jelen technikai színvonal figyelembevétele mellett igazak. A mikroelektronika és a szoftvertechnológia rohamos fejődésével prognosztizálható a hobby rendszerek képességeinek és minőségének további fejlődése, ami egyre közelebb juttatja a modellrepülőgépeket az olcsó robotrepülőgépek kategóriájához.

Fontos megjegyezni, hogy a nyílt forráskódú rendszerek számos új lehetőséget hordoznak magukban. Természetesen hátránnyal járhat, hogy a forráskódot bárki módosíthatja különösebb szakértelem nélkül. Ebben az esetben a rendszer megbízhatósága drasztikusan csökkenhet. Ugyanakkor fontos látni, hogy számos olyan fejlesztő is hozzájuthat a rendszer elemi részeihez, akik érdemben képesek azokat módosítani, továbbfejleszteni. Ebből következik, hogy megfelelően képzett amatőrök kezében is kifejlődhetnek olyan rendszerek, melyek alkalmazásával hatékony és megbízható robotrepülőgépek hozhatók létre.

A fejlődési trendeket elemezve a közeljövőben várható, hogy amatőr szerveződések képesek lesznek akár 100 km hatótávolságú autonóm repülőeszközök elkészítésére. Ezzel együtt a robotrepülőgépek üzemeltetési kérdései jelentősen meg fognak változni, mivel az eszköz birtoklása széles körben el fog terjedni.

Az AirGuardian rendszer

Az AirGuardian rendszer egy komplex, repülő és földi állomást magában foglaló rendszer. A fejlesztés során párhuzamosan készült a repülő robot elektronika, a fedélzeti robot program, a földi antennaforgató és annak programja, valamint a teljes földi állomás szoftverrendszere. Az egyidejű fejlesztésnek köszönhetően a részegységek együttműködése tekintetében optimális.

Célkitűzések

Az AirGuardian rendszer az alábbi célkitűzések elérése érdekében valósult meg.

1. Fedélzeti elektronika
   - Kompakt, lehetőségekhez mérten kisméretű és -tömegű elektronika, amely nem igényel vezetékeken csatlakozó további modulokat.
   - Modul rendszerű elektronika, amely lehetőséget biztosít bővítésekre, illetve optimalizálásra az adott felhasználásokhoz. A modulok csatlakoztatása kártya rendszerű, így az elektronika az egységes szerkezetet a bővítések során is megőrzi.
   - Univerzális kommunikációs felület, ami lehetővé teszi a legtöbb RF modem csatlakoztatását, valamint a lehetőséget biztosít vezetékes kapcsolatra földi beállítások során egy hordozható számítógéppel USB felületen keresztül.
   - A robotelektronika képes tárolni a repülőgép alap paramétereit, valamint az aktuális

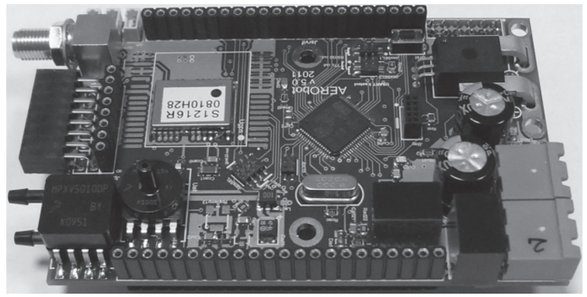
útvonalat legalább 200 fordulóponttal és a hozzájuk tartozó paraméterlistákkal.
- A fedélzeti program képes teljesen önálló működésre, azaz a földi állomással történő kommunikációvesztés ne okozzon a repülési feladat végrehajtásában akadályt.

2. Földi antennafogató egység
- Kompakt egység, amely nem igényel további, vezetéken csatlakoztatott modulokat.
- Automatikus önkalibráció a telepítést követően.
- A repülőgép automatikus követése.
- Szükség esetén az AirGuardian földi szoftvere utasítások formájában képes mozgatni az antennát.

3. Földi szoftverrendszer
- A földi szoftver és a rendszer további egységei (antenna, repülőgép) kapcsolata automatikus. Megfelelő beállítás esetén a felhasználónak nem kell a kapcsolat megteremtése érdekében semmilyen konfigurációt végeznie.
- A földi szoftver akár egy hordozható számítógépen is működőképes, de több számítógép hálózatba kapcsolása estén, a szolgáltatások bővülése mellett, elosztott rendszer formájában is működhet.
- A földi szoftver képes a repülés adatainak eltárolására a későbbi visszajátszás érdekében.
- Alkalmazható a felhasználó által kalibrált tetszőleges térkép.
- A szoftver rendelkezik több, az adott feladat szempontjából leghatékonyabb nézettel.

A fedélzeti elektronika

A fedélzeti elektronika a fenti szempontok figyelembevételével modul rendszerűre készült. Az elsődleges felhasználás szempontjából (robotrepülőgép) két részegység szükséges. Ezek a robot panel (AERObot 5.0 alaplap, 3. ábra) és a szervópanel (AERObot 5.0 szervópanel, 4. ábra).

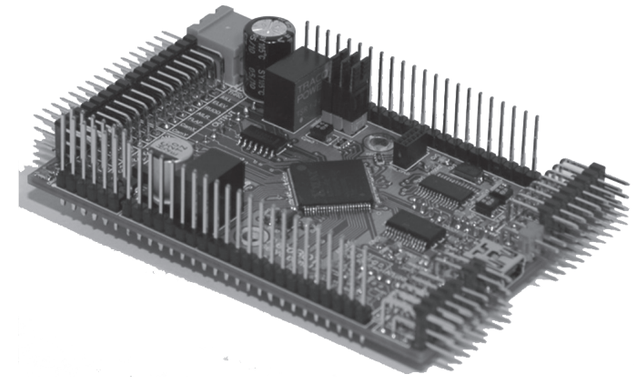


3. ábra. Az AERObot 5.0 alaplap

A robotpanel tartalmaz minden olyan egységet az Inerciális Mérő Egységet kivéve (az angol terminológiában használatos mozaikszóval: IMU), amely a repülőgép autonóm repülése szempontjából szükséges. Ennek megfelelően a panelhez elektromosan csak az IMU és a GPS antenna csatlakozik, illetve a hajtómű áramfelvételének mérése esetén annak a tápvezetéke.

További csatlakozások a statikus és dinamikus nyomást bevezető csövek, melyek a repülőgépre szerelt Pitot-csőtől juttatják el a nyomást a panelra szerelt szenzorokhoz. Az alaplaphoz szendvicsszerűen csatlakoztathatók a bővítő modulok. Ilyen például a szervó panel. A panelhoz természetesen még csatlakoztathatók további elektromos eszközök (ultrahangos magasságmérő, fordulatszámmérő, hőmérsékletmérő stb.), de ezek az elemi működéshez nem feltétlenül szükségesek.

Annak érdekében, hogy egy hagyományos értelemben vett távirányított repülőgépbe egyszerűen beépíthető legyen a robotegység, kifejlesztésre került egy úgynevezett szervó panel. Ennek feladata, hogy a robot által előállított vezérlőjeleket a repülőgép kormányát mozgató szervómotorokkal össze lehessen kötni. Az egység további feladata, hogy átkapcsolási lehetőséget biztosítson a távirányított és az autonóm üzemmódok között. Ezt a funkciót az egység külső utasítás (távirányítóról küldött parancs) vagy belső parancs (földi szoftver) hatására lehet aktivizálni. A biztonság növelése érdekében az átkapcsoló elektronika két független távirányító vevő jeleit kezeli úgy, hogy vételkimaradás esetén átkapcsol a másik vevőre, ha annak jelei megfelelőek. Teljes vételkiesés esetén (egyik vevő sem szolgáltat megfelelő jelet) az egység automatikusan robotirányításra vált, mivel az nem igényel közvetlen földi kapcsolatot.



4. ábra, az AERObot 5.0 szervópanel

A két egység együttes alkalmazása egy fejlett fedélzeti robotegységet alkot. Segítségével nemcsak a repülőgép automatikus vezetése, hanem a robotrepülőgép hasznos terhét jelentő elektronikai egységek alapszintű kezelése (például, kamera ki-/bekapcsolás, speciális adatrögzítés vagy zavaró eszközök ki-/bekapcsolása) is megvalósítható. A robotpanel további bővítési lehetőséget biztosít. A szervópanelhez hasonló módon csatlakoztatható olyan speciális további egység, amely bővíteni képes a rendszer szolgáltatásait. Ilyen bővítés lehet egy szenzorpanel, amely képes a levegő összetételét analizálni. Az eredményeket a robotpanel a hozzá kapcsolt modem segítségével az egyéb telemetriai adatok mellett továbbítja a földi állomásra, ahol az valós időben megjeleníthető és kiértékelhető.

A fedélzeti elektronika minden beállítást – beleértve az utoljára beprogramozott útvonalat is – nem felejtő memóriában tárol. Ebből következik, hogy a rendszer a bekapcsolást

követően – amint a GPS lokalizálta a pozíciót – azonnal üzemkész. Nincs szükség start előtti kalibrációra, illetve paraméter beállításra. A bevetés útvonala elkészíthető a kitelepülést megelőzően. Szükség esetén azonban minden paraméter és az útvonal is, repülés közben is módosítható.

A földi elektronika

A rendszer földi elektronikája az antennaforgató egységben kapott helyet. Ennek feladatai a rádiófrekvenciás kapcsolat biztosítása a repülőgéppel, a vezetékes adatkapcsolat a földi számítógéppel, valamint a földi, nagynyereségű antenna mozgatása úgy, hogy az a repülés során mindig a repülőgép felé nézzen.

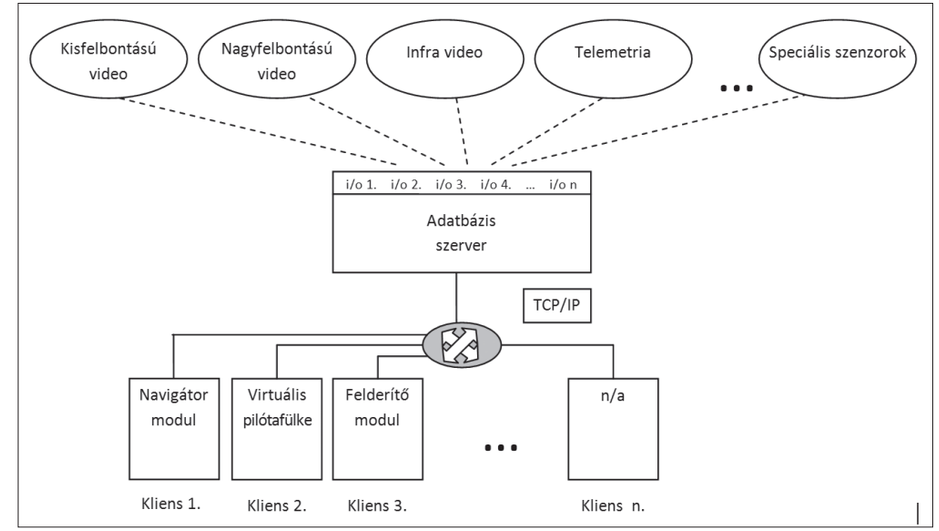
Az antennaforgató tervezése során kiemelt szempont volt, hogy a felsorolt funkciókat egy egység valósítsa meg, azaz ne kelljen a funkcióknak megfelelő részegységeket kábelekkel, a helyszínen, összeszerelni. Ennek megfelelően az antenna a hozzá tartozó elektronikával és forgató mechanizmussal egy kompakt egységet alkot, melyet egy háromlábú műszerállványra szerelve lehet a terepen azonnal üzemkész állapotra hozni. A forgató további szolgáltatása, hogy a kitelepítést követő saját pozíció meghatározása egy beépített GPS segítségével történik. Az antenna iránykalibrációja szintén egy beépített elektronikus iránytű (mágneses szenzor) segítségével valósul meg. További praktikum az antenna körbeforgásának korlátozásmentessége, mivel a forgó és az álló rész között vezeték nélküli adatátvitel valósul meg. Ennek a megoldásnak köszönhetően nem szükséges az antennát alaphelyzetben tárolni, illetve indítani. A két (2) szabadsági fokkal rendelkező antenna képes a repülőgép irányát és magasságát követni.

A földi szoftver

A földi szoftverrendszer kliens-szerver architektúrájú. A szerver feladata többrétű. Biztosítja a repülőgép felől érkező adatok fogadását, illetve a felhasználó által adott parancsok továbbítását a repülőgép számára. Az adatforgalmat képes akár soros porton, akár USB-n vagy hálózaton, TCP/IP szabványú csomagok formájában kezelni. A szerver további feladata az adatok (bejövő és kimenő) archiválása, illetve a hozzá kapcsolódó kliensek kiszolgálása. A szerver a felhasználó számára transzparens módon üzemel.

A felhasználó a rendszerrel alapvetően a kliensalkalmazásokon keresztül érintkezik. A kliensek hálózati protokollon (TCP/IP) keresztül csatlakoznak a szerverhez. Ebből adódóan akár több munkaállomáson is nyomon lehet követni a repülést, illetve elemezni lehet annak adatait. Mivel a repülőgép számára ugyanazokon a klienseken keresztül lehet utasításokat küldeni, a kliensek felhasználói autentikációval vannak ellátva. Ennek megfelelően a felhasználó több szerepkör (pilóta, navigátor, felderítő, adminisztrátor) közül választhat. A szerepkörök úgy lettek kialakítva, hogy az adminisztrátor kivételével minden felhasználó csak a feladatainak megfelelő adatokhoz fér hozzá, illetve annak megfelelő utasításokat adhat. Így például a pilóta vezetheti a repülőgépet, de nem módosíthatja az útvonalat vagy nem kezelheti a felderítő kamerát, míg a navigátor csak az autonóm repülés útvonalát kezelheti.

A szoftver jól skálázható. Lehetőség van több munkaállomásból felépített földi vezérlőállomás kiépítésére vagy olcsó, egyetlen számítógépet alkalmazó irányítópult kialakítására.



5. ábra. Az AirGuardian földi szoftverrendszerének logikai vázlata

Ez utóbbi esetben célszerű adminisztrátor szerepkört alkalmazni, mivel ez minden funkció elérését biztosítja.

Az AirGuardian lehetőséget nyújt régi küldetések visszajátszására is. Ebben az esetben természetesen minden rögzített adat szinkronban jelenik meg, mivel a rögzítés időcímkékkel együtt történik.

Az AirGuardian által használt térkép akár a felhasználó által is a rendszerbe illeszthető. Ennek érdekében a programcsomag része egy kiegészítő modul, amely fő feladata a térképi adatbázis szerkesztése. Ez lehetőséget ad egy meglévő térkép módosítására, vagy egy teljesen új térkép szerkesztésére és kalibrációjára. Ez utóbbi szolgáltatás biztosítja azt, hogy a felhasználó saját – akár titkosan kezelt – adatállományát felhasználhassa anélkül, hogy azt másik fél (szoftverfejlesztő) számára telepítés és kalibráció céljából átadja.

Következtetések

Az AirGuardian rendszer számos kísérlet bizonyította a fejlesztés elején kitűzött célok elérését. A kísérletek során a fedélzeti elektronika megbízhatóan üzemelt. A redundáns rendszerek (RC vevők, tápegység) átkapcsolása hiba- és tranziensmentes. Az átkapcsolás tényéről csak a fedélzeten rögzített adatok utólagos elemzéséből lehet következtetni, azaz a felhasználó számára a repülés során nem érzékelhetők.

Az antennaforgató egység megfelelően alkalmazható a repülőgép követésére. A rendszer nem igényel különösebb operátori beavatkozást. Telepítést követően csupán észak felé kell fordítani az egységhez kapcsolt irányító modul segítségével. Az északi pozíció meghatározása egy LCD panel segítségével könnyen kivitelezhető. Ezt követően az antenna egység GPS modulja lokalizációját kell megvárni, ami jellemzően 1-2 perc. Amint a repülőgéptől érvényes

telemetriai adatok érkeznek, az antenna automatikusan ráfordul a repülőre, és folyamatosan követi annak mozgását. Hosszan tartó vételkimaradás esetén az antenna manuálisan, a hozzá kapcsolt irányító modul segítségével a gép várható érkezési iránya felé fordítható, így biztosítva a lehető leghamarabbi automatikus követés visszaállását.

A pilótanélküli robotrepülőgépek polgári alkalmazásának lehetőségei

A polgári felhasználás tekintetében számos területen alkalmazhatók autonóm, kisméretű pilóta nélküli légi járművek. Németországban és Svájcban már alkalmaznak infra kamerákkal felszerelt robotrepülőgépeket az aratási vadkárok megelőzése céljából. Látható tartományban üzemelő kamerák segítségével pedig a növényzet elszinteződése alapján lehet következtetni esetleges kártevők (gombafélék) megjelenéséről, illetve a betegség terjedéséről. Mindezek alkalmazása jelentős előnnyel járhat. Ugyanakkor a haszon számításánál figyelembe kell venni a robotrepülők bekerülési és üzemeltetési költségeit.

A technika fejlődésével és a gyártási számok növekedésével várható, hogy meg fognak jelenni a piacon a katonai drónok árához képest lényegesen kedvezőbb árú, polgári felhasználású eszközök. Szolgáltatási jellegüket tekintve két nagy csoportot határoztam meg:

(1) Képi megfigyelést végzésére alkalmas repülő szerkezetek, melyek fedélzetén látható fény tartományában vagy infra tartományban üzemelő kamerák vannak elhelyezve. Az ilyen eszközök esetében elvárás a kép stabilizálása, amely történhet a kamera vagy kamera rendszer mechanikai stabilizálásával, a kép utólagos elektronikus (szoftveres) stabilizálásával, esetleg a két eljárás együttes alkalmazásával. További elvárás, hogy a képi információ valós időben jelenjen meg a felhasználó számára, ami nagy sávszélességű adatátvitelt igényel. A képi információ sávszélesség igényének csökkentése érdekében számos fejlesztő alkalmaz digitális képtömörítést és ezzel együtt digitális átvitelt. Ez a módszer jelentős mértékben növeli meg a továbbított kép minőségét (analóg esetben jónak mondható az 400-420 TV soros kép, ami a számítógépeken jellemző módon 480*576 vagy 560*480 pixeles felbontásnak felel meg, digitális átvitel esetében pedig nem ritka a HD képminőség, ami 720*480 tól 1920*1080 pixeles felbontásnak felel meg). A digitális rendszerek kiváló képminősége mellett egy jelentős hátrány jelenik meg. Az átvitelhez szükséges sávszélesség csak abban az esetben csökkenthető jelentősebb mértékben az analóg átvitelhez képest, ha a kép tömörített formában kerül továbbításra. Bár számos tömörítő eljárás ismert, a hatékonysága miatt napjainkban az MPEG-4 eljárás a leggyakoribb. A tömörített adatfolyam szükségszerűen növeli a képrögzítés és kép megjelenítés közt eltelt időt. Ennek egyértelmű oka a kép tömörítésének (adó oldal) és dekódolásának (vevő oldal) időigénye. A digitális átvitel esetén az analóg rendszerekkel megegyező módon folyamatos videó jelenik meg a megfigyelő oldalon, de az eredeti rögzítéshez képest a digitális rendszer jelentős (a tömörítéshez és dekódoláshoz használt eszközök kialakításától és a tömörítés mértékétől függően változó, néhány 100 ms-tól néhány másodpercig terjedő) késleltetéssel bír. Ez gyakorlati szempontból azt jelenti, hogy a digitális rendszerek által sugárzott kép megfigyelésre kiválóan alkalmas, ugyanakkor a repülőeszköz vezetésére csak korlátozottan, vagy egyáltalán nem alkalmas. Természetesen a késleltetés idejével kapcsolatos megállapítások jelen technikai színvonal esetén érvényesek. Nagy valószínűséggel a technika, különösen a nagy sebességű, célszámítógépek fejlődése várhatóan az értekezésben jelzett késleltetési időket jelentősen csökkentik majd.

A vizuális megfigyelés esetén gyakran megjelenő igény a képi tartalom bizonyos mértékű automatikus elemzése vagy átalakítása, hogy a megfigyelő hamarabb észrevehesse a számára fontos információt. A kép speciális manipulálása (átalakítása) bizonyos határokig gyorsan megvalósítható. Ilyen lehet például a kép átszínezése például infra kamerák esetében, ahol a szürkeárnyalatos képet úgy módosítják, hogy a hideg területek kék, a meleg területek piros színűek legyenek. Sok esetben a kép módosításának egyik célja, hogy kiemeljük a lényegi információt. A hőképek esetében például gyakori eljárás, hogy a szürke árnyalatos képen csak egy előre beállított hőmérséklet feletti területeket színezünk ki. Ez a módszer nagymértékben megkönnyíti például eltűnt személyek megtalálását.

A képek tartalom szerinti elemzése már sokkal nagyobb számítási kapacitással rendelkező feldolgozó egységeket igényel az előbb ismertetett egyszerű manipulálásokhoz képest. A tartalom szerinti elemzéssel speciális objektumok jelölhetők ki a képen. Ilyen lehet például földön álló repülőgépek automatikus felismerése. Lehetőség nyílik a képpontok mozgásvektorainak elemzése által akár ismeretlen, mozgó hátterű képen is felismerni mozgó objektumokat (földön haladó járművek). Igaz ugyan, hogy az imént említett lehetőségek civil alkalmazások esetén ritkán szükségesek, de az eljárások alkalmasak olyan intelligens kameramozgató rendszer kialakítására, amely nagymértékben megkönnyíti a vizuális megfigyelést akár nem katonai robotrepülőgép alkalmazása során is. Ilyen lehetőség az automatikus objektumkövetés. Ebben az esetben a felhasználó által megjelölt, számára érdekesnek tartott objektumot igyekszik a rendszer folyamatosan a kép közepén tartani, így lehetőség nyílik egy kiválasztott terület pontosabb megfigyelésére. Készíthető olyan rendszer is, amely nem csupán a kamera mozgatásával oldja meg az objektum követést, hanem utasításokat ad a robotrepülőgép fedélzeti elektronikája számára és ezáltal olyan repülési pályára állítja a repülőgépet (jellemző módon körözés az objektum körül), hogy a célterület folyamatosan megfigyelhető maradjon.

(2) Adatgyűjtésre kialakított repülő szerkezetek, melyek elsősorban nem képi információkat rögzítenek. Ilyen eszközök lehetnek például a levegő összetételét vagy szenyyezettségét mérő szenzorokkal ellátott robotrepülőgépek. A mért adatokat folyamatosan sugározzák a földi megfigyelő és feldolgozó állomásnak, vagy a fedélzeten rögzítik azokat. Igen gyakori mgoldás, hogy mindkét adatkezelési módszert alkalmazzák, így lehetőséget biztosítanak a valós idejű elemzésre, valamint a vételi zavaroktól mentes adatok utólagos feldogozására.

Az adatgyűjtésre kialakított robotrepülőrendszerekkel kapcsolatos elvárások eltérnek a képi információk megszerzésére kifejlesztett rendszerektől. Az adatgyűjtés során általában nem cél a stabilizált szenzor platform, valamint az adatok továbbítására nem szükséges nagy sávszélességű átvitel. Számos esetben azonban lényeges lehet nagy távolságú, megbízható adatszolgáltatás, valamint a felhők feletti repülés, ami magában foglalja szükség esetén a felhőben történő repülés képességét. A felhőben történő repülés természetesen csak korlátozott esetekre értelmezhető és általában nem elvárás a zivatarfelőkben történő mérés. A felhőben, vagy erősen ködös időben történő repülés kizárja az optikai ellven működő horizontbecslést és az arra épülő szabályzást.

Bizonyos esetekben a mérés jellege megköveteli, hogy a mérést végző robotrepülőgép ne szennyezze be a mérés helyét. Ilyen mérési feladat lehet a lékörben mért szennyező anyagok terjedésének vizsgálata, ami az adott terület rendszeres (akár óránkénti végy még nagyobb gyakoriságú) újramérését jelenti. Ilyen mérések során a repülőgép hajtóművének emissziója

zavarhatja a mérést. Éppen ezért az elektromos meghajtású robotrepülőgépek ideálisak lehetnek az adott terület ismételt mérését megkövetelő felhasználások esetében.

A két csoport meghatározásának oka a fentiek alapján is látható jelentősen eltérő fejlesztési szempontok alapján indokolt. Tekintettel arra, hogy a polgári alkalmazások elterjedésének egyik jelentős korláta a robotrepülőgépes rendszer bekerülési költsége, a fejlesztések során indokolt olyan optimalizálásokat és kompromisszumokat alkalmazni, melyek a rendszer árának jelentős csökkenését eredményezhetik. A robotrepülőgépek esetében jelentős költségek takaríthatók meg oly módon, hogy azok a költséges alrendszerek nem kerülnek kifejlesztésre, illetve beépítésre, amelyek az tervezett feladat ellátásához nem szükségesek. Például vizuális felderítésre tervezett repülőgép esetén szükséges a kamera mechanikai és/vagy optikai stabilizálása, ugyanakkor nem vizuális adatgyűjtő rendszer esetén az említett drága rendszer elhagyható.

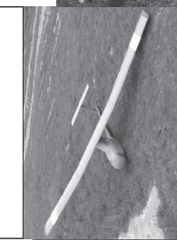
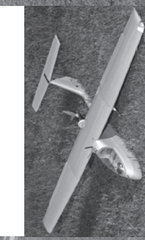
Összegzett következtetések

A kutatás során egyértelműen kirajzolódott egy, a robotrepülőgépekkel kapcsolatos felhasználói igény, amely az alábbi szempontoknak megfelelő rendszer kifejlesztését tette indokolttá:

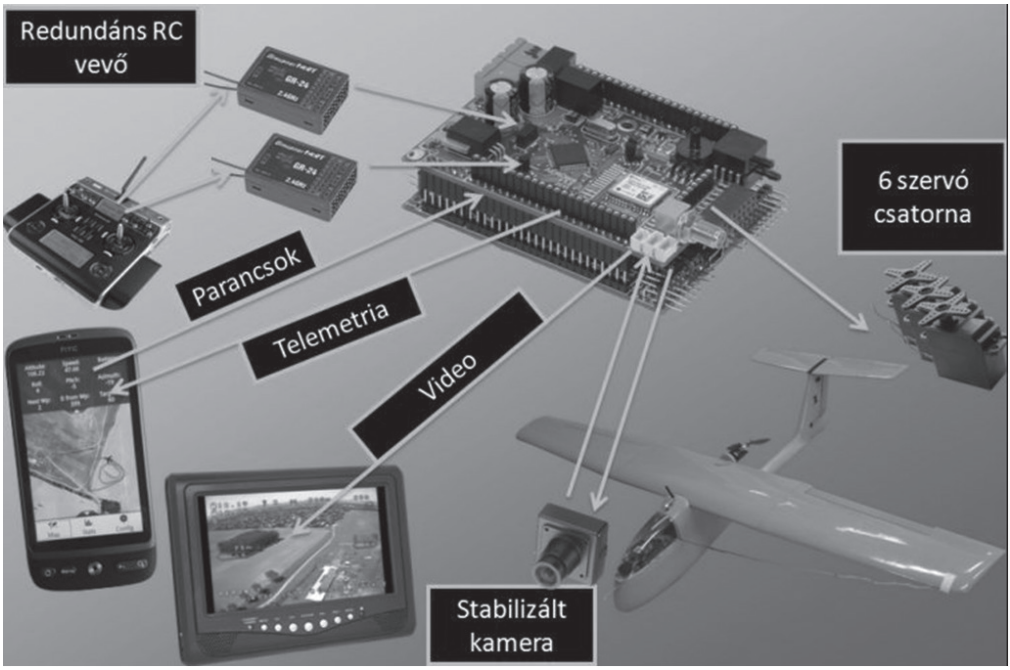
1. A felhasználó által egyszerűen konfigurálható rendszer. Ez többek között jelenti a repülőgép alapparamétereinek egyszerű és gyors beállíthatóságát, az alkalmazott rendszereket elfedő, felhasználóbarát kezelőfelületet, valamint a rendszer által alkalmazott térképek felhasználó által történő egyszerű cseréjét.
2. A repülési adatok valós idejű megfigyelésének széleskörű kiterjesztése. Ez jelenti a több kliensen nézhető és elemezhető adatokat megjelenítő rendszert.
3. A hazai fejlesztésben rejlő rugalmas továbbfejlesztési lehetőség.
4. Széles palettával rendelkező robotrepülőgépes szolgálat kialakításának lehetősége. Ez elsődlegesen a feladatokhoz optimalizált hasznos terheket szállító konténerek vagy akár komplett repülőgépek flottáját jelenti. Ebben az esetben a felhasználó, vagy a szolgáltató a mindenkori igényekhez legjobban igazodó eszközt tudja alkalmazni, ami költség- és feladathatékony.

Az AERObot tesztelése és elemzése során az alkalmazott repülőgépeket az 1. táblázat foglalja össze. A kísérletek során azért történt több repülőeszközön a vizsgálat, hogy kellő mennyiségű tapasztalat álljon elő a robotrendszer képességbeli határainak megállapítására. Az elvégzett kísérletek jól igazolják, hogy az AERObot v5.0 rendszer a kitűzött célokban megfogalmazott paraméterű kisméretű robotrepülőgépek esetében megbízhatóan alkalmazható.

A földi állomás tekintetében sikerült egy olyan rendszert kifejleszteni, ami megbízhatóan és hatékonyan képes a repülőgép és a kezelő személyzet kiszolgálására. A program alkalmazható egy vagy több, hálózatba kapcsolt számítógépen egyaránt. Kiegészítő modulja segítségével a felhasználó saját térképállományt hozhat létre, melyet kalibrációval, valamint egyedi azonosító pontokkal láthat el. A térképállományok exportálhatók más AirGuardian rendszerekhez.

A repülőgép neve	Chelidon	Fun Cub	BHE – 03	Sky Walker	Tiger 60
					
Gyártó	Dr. Molnár András. Speciális robotrepülésekhez fejlesztve.	Multipex. Távirányítású repülőmodell.	BHE, Bonn Hungary Kft. Speciális robotrepülésekhez fejlesztve.	Hobby King. Távirányítású repülőmodell.	Carl Goldberg Products LTD. Távirányítású repülőmodell.
Meghajtás	Elektromos, 22V, 1300 W, elektronikusan kommutált, 6,7:1 áttételű, belső forgórészes.	Elektromos, 12V, 500 W, elektronikusan kommutált, külső forgórészes.	Elektromos, 22V, 1300 W, elektronikusan kommutált, külső forgórészes.	Elektromos, 12V, 500 W, elektronikusan kommutált, külső forgórészes.	10 ccm, alkoholos, 2 ütemű.
Felszálló tömeg	6 kg	3 kg	16 kg	3,5 kg	4,5 kg
Szárnyfesztáv	3,6 m	1,4 m	3,5 m	1,6 m	1,5 m
Repülés során mért legnagyobb szélsebesség	40 km/h	30km/h	58 km/h	15 km/h	36 km/h

1. táblázat, az AERObot rendszer tesztelése során alkalmazott repülőgépek főbb adatai



6. ábra, az AERObot rendszer vázlatos felépítése

A megvalósított komplex rendszer főbb elemeit a 6. ábra szemlélteti. A tervezés eredményeképp a rendszer egyes elemei önálló alrendszerként is hasznosíthatók, így lehetőség nyílik a már meglévő robotrepülőrendszerek kiegészítésére vagy új fejlesztésekben részegységként történő felhasználásra.

A tanulmány a TÁMOP-4.2.1B-11/2/KMR-2011-0001 azonosítási számú Kritikus infrastruktúra védelmi kutatások című pályázat támogatásával valósult meg. A szerző köszönetet mond az Európai Unió és az Európai Szociális Alap által nyújtott támogatásért.

A KATONAI ERŐ ALKALMAZÁSÁNAK TAPASZTALATAI AZ ÁRVÍZI VÉDEKEZÉSBEN

Padányi József

A változó biztonsági környezet a Magyar Honvédség feladatait sem hagyta érintetlenül. Olyan új kihívások jelentek meg vagy erősödtek fel, mint terrorizmus, az éghajlatváltozás okozta katasztrófák (elsősorban a növekvő számú és intenzitású árvíz). A csökkenő források nehezítik az átalakítást, legyen az a szervezet, a kiképzés és képzés, vagy az eszközrendszer korszerűsítése. Mára letisztultak a feladatok, és ha lassan is, de megkezdődött az átalakítás. A tisztképzés rendszere 2013-tól teljesen megújul, újraszervezzük a tartalékos rendszert, újraszabjuk nemzetközi szerepvállalásunkat, és nagyobb hangsúlyt kapnak a honi területen végrehajtott feladatok. Hasonló kihívásokkal – még ha más-más hangsúllyal is – néz szembe a legtöbb haderő. A következőkben a Magyar Honvédség előtt álló kihívásokat és az arra adott válaszok néhány területét mutatjuk be, különös tekintettel az árvédekezésben betöltött szerepére. (Kritikus infrastruktúra védelmi kutatások, TÁMOP-4.2.1.B-11/2/KMR)

Nemzetközi kitekintés

A katonai erő alkalmazása a katasztrófák elleni védekezésben mára megkérdőjelezhetetlenné vált. Nem volt ez mindig így, hiszen még a nyolcvanas évek végén is komoly viták folytak arról, szabad-e a katonai képességeket ilyesmire használni. A politikai ás katonai körülmények változása, a hagyományos szembenállás megszűnte után ez a vita gyorsan nyugvópontra jutott. Egyrészt néhány katasztrófa bizonyította a katonai erő alkalmazásának nélkülözhetetlenségét ezen a területen – például az Andrew hurrikán, (1992 Egyesült Államok) – másrészt eltűnt a hagyományos ellenség és a katonák egy pillanatra légüres térben találták magukat. Cinikusan fogalmazva azt is mondhatnánk, hogy kapóra jött egy új feladat. Mindez oda vezetett, hogy a katonai doktrínákba, biztonsági stratégiákba nagyobb hangsúlyt kapott ez a terület. Ezt követték a szervezeti és technikai fejlesztések, egyre nagyobb teret engedve a többrendeltetésű szervezeteknek és eszközöknek. A következőkben néhány példát mutatunk be a katonai erő és a katasztrófák elleni védekezés kapcsolatáról.

Svájc

A svájci haderő feladatait három pontban foglalja össze a svájci Alkotmány:
- Az ország függetlenségének és területi épségének fegyveres védelme.
- A civil hatóságok támogatása.
- A nemzetközi béketámogatásban való részvétel.[1]

1 http://www.vtg.admin.ch/internet/vtg/en/home/themen/auftraege.html Letöltve: 2012. június 17.

A hatóságok támogatása alatt elsősorban a rendőrség támogatását értik a nemzetközi konferenciák és egyéb jelentős események során. A katasztrófák elleni védekezésben akkor vesz részt a haderő, ha gyorsan képes a tűzoltóság, az egészségügyi és polgári védelmi szervezeteknek segítséget nyújtani.

Horvátország

A horvát haderő feladatai között is meghatározó szerepet játszik a katasztrófák elleni védekezés, a civil hatóságok támogatása vészhelyzetben és a kutató-mentő műveletek. Az ország helyzeténél fogva ez leginkább a pusztító erdőtüzek elleni küzdelemben valósul meg. A horvát légierő eszközei között 6 db AT-802 és 6 db CL-415 tűzoltó repülőt találunk, melyek minden évben élesben vizsgáznak. Nem volt ez másképp 2012 júliusában sem, amikor Selce körzetében vettek részt a kiterjedt erdőtűz oltásában.[2]

A horvátok a felkészülésre is nagy hangsúlyt fektetnek. A horvát hadsereg tűzoltásra felkészített csoportosítása minden évben gyakorlattal készül a nyári időszakra. A MI-8 típusú helikopterek tűzoltókat és felszerelést szállítanak a veszélyeztetett pontokra, gyakorolva a kötélen való leereszkedést, a kommunikációt, a tengerparton való repülést.[3]

A tűzoltó repülők gyakorolják az oltást, a vízre szállást és a vízfelszíni feltöltést. Nagy hangsúlyt fektetnek a civil szervekkel való együttműködésre, hiszen a tűzoltás során viszonylag kis területen kell, extrém körülmények között kell együtt dolgoznia a civil és katonai mentőerőknek.

A horvát légierő sajátos feladata a szigetekről való betegszállítás is, elsősorban olyankor, amikor gyorsan és nehéz körülmények között kell repülni, vagy beszállítani.

Cseh Köztársaság

A cseh haderőben egy műszaki dandár adja a katasztrófák elleni védekezés fő erejét. A dandárba szervezett alegységek egy része kifejezetten a katasztrófák – elsődlegesen az árvizek – elleni védekezésre szakosodtak. Kiképzésük, eszközeik és vezetési rendjük mind ennek a feladatnak lettek alárendelve. Az elmúlt évtizedben számos alkalommal bizonyították felkészültségüket. Természetesen a hadsereg más erői is igénybe vehetők katasztrófahelyzetben, így a légierő szállítói kapacitása, vagy az egészségügyi szakemberek.

Anélkül, hogy tovább részleteznénk más országok alkalmazási elveit és tapasztalatait, a következőkben csak utalunk a katonai erő alkalmazásának elveire:

A kanadai kormány általában nem alkalmazza a katonai erőt katasztrófahelyzetben, de ha más szereplők lehetőségeit meghaladja a védekezés, akkor lehetővé teszi az erők és eszközök bevetését.

Belgiumban egységes szemlélettel, mintegy egymást kiegészítő erőforrásként kezelik a civil és katonai szereplőket katasztrófa helyzetben. Alapelv, hogy jó időben és a megfelelő helyen alkalmazzák a szükséges forrásokat.

A francia megközelítés is abból indul ki, hogy ha szükség van rá, azonnal igénybe kell venni a katonai erőt, csökkentve a károkat és a veszteséget.

2 http://www.focus-fen.net/index.php?id=n283787 Letöltve: 2012. július 24.
3 http://www.osrh.hr/default_en_news.asp?id=686 Letöltve: 2012. július 24.

Az angoloknál egyértelműen amellett álltak ki, hogy ha a katonai erő alkalmazása tűnik a legjobb megoldásnak, akkor azonnal igénybe kell azt venni.

A hazai helyzet

Jogszabályi háttér

A Honvédelmi Törvény egyértelműen meghatározza a Magyar Honvédség feladatait. [1] A honvédség legfontosabb feladata a haza fegyveres védelme. Ezen túl meghatározó – és mint a tapasztalat mutatja – igen gyakori a „közreműködés a katasztrófavédelemmel összefüggő feladatok végrehajtásában." A honvédség fejlesztése során ennek a feladatnak a követelményei is megjelennek. A katasztrófavédelmi feladatok során a honvédségi szervezetek katonai függelmi rendszerben, saját parancsnokaik vezetésével vesznek részt a munkában. Ennek során legfeljebb 200 fő 21 napi időtartamot meg nem haladó igénybevételéről a Honvéd Vezérkar főnöke, az ezt meghaladó létszámú vagy időtartamú igénybevételről a honvédelemért felelős miniszter dönt. A 3000 főt meghaladó igénybevételről a honvédelemért felelős miniszter – a döntéssel egyidejűleg – az Országgyűlés honvédelmi ügyekkel foglalkozó bizottságát tájékoztatja. Látható tehát, hogy a feladat pontosan körülhatárolt rendben és módon történik.

A Honvédelmi Törvény kiemelt figyelmet fordít a feladatok megfogalmazása során azon társadalmi elvárásoknak, amelyek a civil környezet közvetlen támogatását szolgálják. Így nevesítésre kerültek a tűzszerész feladatok, az állami protokoll feladatok, a hadisír gondozás, valamint az állami közfoglalkoztatás támogatása.

A 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról is foglalkozik a kérdéssel. [2]

„A védekezést és a következmények felszámolását az erre a célra létrehozott szervek és a különböző védekezési rendszerek működésének összehangolásával, az állampolgárok, valamint a polgári védelmi szervezetek, a gazdálkodó szervezetek, a Magyar Honvédség, a rendvédelmi szervek, a Nemzeti Adó- és Vámhivatal, az állami meteorológiai szolgálat, az állami mentőszolgálat, a vízügyi igazgatási szervek, az egészségügyi államigazgatási szerv, az önkéntesen részt vevő társadalmi szervezetek, valamint az egyesületek és az erre a célra létrehozott köztestületek, továbbá nem természeti katasztrófa esetén annak okozója és előidézője, az állami szervek és az önkormányzatok (a továbbiakban együtt: katasztrófavédelemben részt vevők) bevonásával, illetve közreműködésével kell biztosítani."

A Nemzeti Biztonsági Stratégia amellett, hogy foglalkozik a biztonsági környezet változásával, egyúttal a honvédség feladatairól is szól:

„A globális éghajlat- és környezetváltozás, a szélsőségesebbé váló időjárás hatásai, a nyersanyag- és természeti erőforrások kimerülése, az egészséges ivóvízhez jutás és a világban egyre súlyosabb formában jelentkező élelmezési gondok komoly biztonsági kockázatot hordoznak magukban, konfliktusok forrásaivá válhatnak. A globális, a térségben vagy Magyarországon keletkező környezeti, civilizációs és egészségügyi veszélyforrások nem csupán az ország, de a térség biztonságát és fejlődését is veszélyeztethetik. Magyarországra ráadásul földrajzi adottságainál fogva fokozottan hatnak a Kárpát-medence szomszédos országaiban keletkező környezeti és civilizációs ártalmak, az árvizek, a víz- és levegőszennyezés. A környezeti veszélyforrások közvetve hatással vannak a lakosság egészségi állapotára.

Természeti és ipari katasztrófák. Az egyes ipari, biológiai, vegyi és különösen nukleáris létesítményekben zajló folyamatok ellenőrizhetetlenné válása tömeges méretekben veszélyeztetheti vagy károsíthatja az emberi egészséget, a környezetet, az élet- és vagyonbiztonságot. További kockázatot jelent a veszélyes áruk közúti, vasúti, vízi, légi és csővezetékes szállítása.

A Magyar Honvédségnek rendelkeznie kell olyan képességekkel is, amelyekkel tevékenyen hozzájárulhat a természeti vagy ipari katasztrófák következményeinek felszámolásához. [3]

Jelenleg csak tervezet a Nemzeti Katonai Stratégia, amely ágazati szintre bontja le a fenti feladatokat. [4] A tervezett Stratégia a Magyar Honvédség megújulásának egyik fontos dokumentuma, mely ágazati stratégiaként figyelembe veszi a Nemzeti Biztonsági Stratégiában lefektetett irányelveket. Az ország Alaptörvényével, a védelmi szféra tevékenységét meghatározó jogszabályokkal, az Észak-atlanti Szerződés Szervezete Stratégiai Koncepciójával, valamint az Európai Biztonsági Stratégiával összhangban kijelöli számunkra az előttünk álló időszak stratégiai szintű célkitűzéseit, és iránytűként szolgál a Magyar Honvédség megújításának feladatához.

A dokumentum megfogalmazza azt, hogy a honvédelem ügyét nem lehet a biztonság más területeitől elválasztva, önmagában értelmezni és kezelni. A biztonság nem katonai vetületeinek egyre inkább megnő a fontosságuk, ez ugyanakkor nem jár együtt a katonai szegmens szerepének csökkenésével. A biztonsági kihívások kezelése túlnyúlik az egyes szakminisztériumok hatáskörén, és összehangolt kormányzati együttműködést kíván meg.

A stabilitás ellen ható folyamatok között – összhangban a korábban ismertetett dokumentumokkal – kiemelt figyelmet kap a terrorizmus elleni harc, a kiber fenyegetés, az energiabiztonság, az éghajlatváltozás és az ebből eredeztethető, növekvő számú és súlyosságú katasztrófahelyzetek.

Ennek megfelelően fogalmazódnak meg a Magyar Honvédség feladatai is. A Magyar Honvédség alkalmazására jellemzően válságkezelő műveletekben kerül sor, sok esetben Magyarországtól jelentős távolságra, szélsőséges természeti és éghajlati viszonyok között, nehezen megközelíthető terepen. A válságok kezelése során a hálózatközpontú hadviselés, a precíziós fegyverek és modern technikák, a civil-katonai együttműködés, a pszichológiai hadviselés, valamint a különleges rendeltetésű erők széles körű alkalmazása szükséges. A válságkezelésre általában olyan, az alapfeladatát ellátni képtelen, gyenge államokban kerül sor, ahol irreguláris, félkatonai szervezetekkel, felkelőkkel, fegyveres csoportokkal, nemzetközi zsoldos és terrorista csoportokkal szemben kell a biztonságot megteremteni és fenntartani.

Egyre többször van szükség humanitárius célú beavatkozásra és segítségnyújtásra, illetve egyre gyakrabban van szükség arra, hogy humanitárius szükséghelyzetben katonai erőt alkalmazzunk a beavatkozás elsődleges eszközéül. A válságok kizárólag katonai erővel nem kezelhetőek, kezelésük összetett civil és katonai erőfeszítést, együttműködést igényel, különös tekintettel az azonos műveleti területen működő katonai és polgári szakemberek egymásrautaltságára. A katonai és a civil erőfeszítések nem választhatóak el élesen egymástól. A műveleti területen nem csupán állami, hanem számos nem állami szereplő is meghatározó módon jelen van.

A jogszabályok adta kereteken belül a Honvédelmi Minisztérium és a Magyar Honvédség megalkotta belső szabályzóit és létrehozta az igénybe vehető erők és eszközök igénybevételi rendjét.

Gyakorlati tapasztalatok

Fontosnak tartjuk hangsúlyozni, hogy a Magyar Honvédségnek kiemelt feladata a katasztrófák elleni védekezésben való részvétel. Kötelesség és lehetőség arra, hogy bizonyítsa felkészültségét, hasznosságát. Az éghajlatváltozás következtében szaporodó katasztrófahelyzetek – hazánkban elsősorban az árvíz – következményeinek felszámolásában meghatározó a Magyar Honvédség szerepvállalása. Mondom ezt azért is, mert vannak törekvések ezen szerep relativizálására, a katonai erő szerepének lebecsülésére.

Az árvédekezésben végzett katonai szerep jelentőségét mutatják azok a tények, amelyek az elmúlt néhány év adataiból következnek.

1. táblázat. A honvédség szerepe az árvizi védekezésben

Időpont	Résztvevő katonai erő létszáma (fő)	Kirendelt technikai eszközök száma (db)
2000. április 7. – május 12.	4260	553
2001. március 5. – március 28.	2399	150
2002. augusztus 13. – augusztus 24.	3025	175
2006. március 31. – május 10.	10 695	643
2010. május 17. – május 23.	455	55
2010. július – július 11.	3071	390

Forrás: A Magyar Honvédség képességei és a katasztrófaelhárítás kihívásai 2000-2011. Zrínyi Média 2012.

Nemcsak az árvédekezés jelent feladatot katonáinknak. A 2010-ben bekövetkezett vörösiszap katasztrófa következményeinek felszámolásában is szükség volt a Magyar Honvédség erőire és eszközeire. Elsősorban azok a képességek kerültek előtérbe, amelyeket a gyorsaság és az egyediség jellemez. A honvédség 2200 katonával és 400 technikai eszközzel segítette a mentés és helyreállítás munkáját. Legfontosabb feladatai voltak:

- folyamatos helikopteres felderítés és sebesültszállítás;
- légtérzár fenntartása a kárterület körzetében;
- sérültek kórházi ellátása;
- radiológiai és vegyi felderítés, elemzés;
- szennyezett személyek és eszközök földi és légi mentesítése (635 fő, 31 749 eszköz, 98 km út);
- romeltakarítás;
- kitelepítés feltételeinek megteremtése (4 000 tábori ágy, 8 000 készlet ágynemű);
- hídépítés;
- üzemanyagszállítás, hűtőkonténerek biztosítása.

2012-ben bozóttűz pusztított Bugac körzetében. Az oltási munkákba bekapcsolódtak a honvédség helikopterei és járművei. Az oltás során alkalmazásra került az 1994-ben rendszeresített, légi tűzoltásra szolgáló, több mint ezer liter vizet szállító Bambi Buck is.[5]

Itt kell szólnunk arról a szervezetfejlesztésről is, amelynek eredményeképpen – hosszú előkészítés után – 2002-ben létrejött a Tisza Többnemzeti Műszaki Zászlóalj. Az egység létrehozásának célja, hogy a Tiszán levonuló árhullámok ellen legyen egy hatékony, gyorsan bevethető, kellő felkészültséggel és kiváló eszközökkel rendelkező katonai szervezet. Olyan szervezet, amely bármely érintett országban képes és kész segíteni. Magyarország, Románia, Szlovákia és Ukrajna egy-egy műszaki századot bocsátott rendelkezésre, amelyek adott esetben készen állnak a feladatra. Az egység tehát virtuális szervezet, de komoly erőforrás és évente tart közös gyakorlatot.

Az alkalmazás elvei

Melyek azok az előnyök, amelyek a katonai erő alkalmazása mellett szólnak?

- A katonai erő teljes logisztikai háttérrel rendelkezik, így igénybevétele esetén a védekezés irányítóinak nem kell külön gondoskodni az ellátásról, a pihentetésről, a technikai eszközök feltöltéséről, esetleg szállításáról, az egészségügyi támogatásról. Komplett mentőerő érkezik, teljes eszközrendszerrel. Különösen fontos ez akkor, amikor egyéb beérkező erők sokszor a saját ellátásukról sem tudnak gondoskodni. A 2010-es árvízi védekezés során nem egy esetben tapasztaltuk azt, hogy a védekezésre átcsoportosított erők és eszközök rövid idő alatt alkalmatlanná váltak a feladat ellátására. Nem volt megszervezve a pihentetésük, ellátásuk, logisztikai támogatásuk.
- A katonai erő saját vezetés-irányítási rendszerrel rendelkezik, eszközrendszere kompatibilis a többi erő eszközeivel.
- A katonai erő olyan speciális eszközökkel rendelkezik, amelyek más szervezeteknek nincs. Nehéz terepjárók, kétéltűek, légi járművek, mobil világítás technika, nagyteljesítményű víztisztító berendezések, logisztikai eszközök (sátor, főzőpont, stb.).
- A katonai erő olyan szaktudással rendelkezik, amelyek más szervezeteknél nem, vagy csak korlátozott mértékben van meg. A robbantás, a hídépítés (úszó és állóaljzatú egyaránt), légi szállítás és mentés, egészségügyi kapacitás (égésspecialisták), a búvármunkák, a felderítés minden formája csak néhány kiragadott példa ebből a szaktudásból.
- A katonai erő alkalmazásának elvei itthon és külföldön is hasonlóak, bár hangsúlybeli eltérések adódhatnak. Az elmúlt évtizedekben felhalmozódott tapasztalatok mind az árvédekezés, mind más katasztrófahelyzetekre jól hasznosítható alkalmazási elveket adtak.
- A katasztrófa megelőzése illetve a következmények felszámolása meghaladja a védekezésben érintett szervezetek erejét.
- Az igénybevétel több előnnyel járjon, mint hátránnyal.
- Az igénybevétel ideje, nagysága és kiterjedése legyen arányban a szükséglettel.
- Biztosítottak legyenek a helyzetnek megfelelő, minimálisan szükséges feltételek és körülmények.
- Az erők és eszközök gazdaságos felhasználása, tartalékképzés.

Összefoglalás

Az átalakuló Magyar Honvédség életében vannak olyan biztos pontok, amelyeket egyetlen változtatás sem érint. Az egyik ilyen a haza védelme, a másik a honi területen végrehajtott

feladatok, mint a katasztrófák elleni védekezésben való részvétel. Az átalakuló biztonsági környezet új hangsúlyokat teremt, melyre hazánk igyekszik gyorsan reagálni. Nem könnyíti meg a döntéshozók helyzetét az sem, hogy az ország védelmi költségvetése soha nem volt ilyen alacsony. Ilyen körülmények között nehéz, de nem lehetetlen azon képességek megőrzése, amelyek biztosítják a katasztrófák elleni védekezésben való további hatékony részvételt. Ehhez azonban az is kell, hogy minden érintett a megelőzésre helyezze a hangsúlyt, hiszen a megelőzött katasztrófánál nincsen gazdaságosabb és biztonságosabb megoldás.

IRODALOMJEGYZÉK

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

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

A Kormány 1035/2012. (II.21.) Korm. határozata Magyarország Biztonsági Stratégiájáról, Magyar Közlöny 2012. 19. sz.

Nemzeti Katonai Stratégia (tervezet).

A Magyar Honvédség képességei és a katasztrófaelhárítás kihívásai 2000-2011. Zrínyi Média Budapest, 2012. ISBN 978 963 327 534 4

A SZÁMÍTÁSTECHNIKAI IPAR ÉS A KIBERBŰNÖZÉS ELLENI KÜZDELEM: LEHETŐSÉGEK ÉS KORLÁTOK

Précsényi Zoltán

A kiberbűnözés[1] – azaz tágan értelmezve a digitális térben elkövetett, illetve folytatott, törvénybe ütköző cselekedetek, illetve tevékenységek – számos tekintetben új kihívások elé állítja a bűnüldöző hatóságokat.

Nagy léptékű szervezett bűnüzés

A kiberbűnözés rendkívül sokrétű és szerteágazó, a legkülönfélébb államigazgatási, kereskedelmi, társadalmi és egyéb szektorokat egyöntetűen sújtja, ezért feltérképezése körülményes és semmiképp sem teljes körű.

Elkövetési módjai a technológiai fejlődéssel együtt haladnak, változnak és finomulnak, ami folytonos lépéselőnyt biztosít a bűnözőknek a védekezőkkel szemben, illetve szüntelenül próbára teszi a bűnfelderítő, bűnüldöző, nyomozó és büntető hatóságokat, úgy a technológiai képességek és anyagi erőforrások, mint a naprakész szakértelem területén.

Ugyanakkor a kiberbűnözés volumene óvatos becslések szerint is globális szinten a kábítószerkereskedelem mértékével vetekszik[2], s ahhoz hasonlóan rendkívül szervezett keretek között zajlik, javarészt egy önszabályozó, párhuzamos és illegális piacgazdaság jellemzőit magára öltve. A támadó eszközök, a törvénytelenül szerzett eszmei és tárgyi javak (adatok, szellemi termékek, pénzügyi eszközök, stb.) – de sokszor még maga a bűnelkövetés is – virágzó és dinamikusan növekedő áru- és szolgáltatási kereskedelem tárgyát képezik, kiélezett innovációs versennyel a különféle szereplők között. Például számos, a fekete kereskedelem útján beszerezhető vagy bérbe vehető[3] kártevő program egyfelől ön- és másolásvédelemmel ellátva, valamit a vetélytársak termékeinek blokkolására vagy eltávolítására alkalmassá téve kerül forgalomba. A forgalmazó pedig – megfelelő ellentételezés fejében – jótállással, -ügyfélszolgálattal, és egyéb prémium szolgáltatásokkal jár a megrendelők kedvében, pontosan úgy, mint a hagyományos kereskdelemben, csak éppen minden törvényes kereten kívül[4].

A bűnelkövetés, a bűnelkövető eszközök, valamint a vonatkozó és járulékos orgazdaság tehát egy határokon átívelő, integrált, és jól üzemelő, kompetitív és folyamatosan növekvő

1 Európa Tanács, CETS 185. sz. 2001. november 23-i, ún. Budapesti Egyezmény, második fejezet, első szekció

2 Symantec, Norton Cybercrime Report, 2011: http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

3 Symantec, White Paper on Attack Kits and Malicious Websites, 2011: https://scm.symantec.com/resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf

4 Symantec, White Paper on the Underground Economy, 2008: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

piacgazdaságként is leírható. Ezzel szemben a bűnüldöző szervek létszámban, felkészültségben, intézményközi és nemzetközi szervezettségben, technikai és anyagi erőforrásaikban is csak nehezen és komoly energiaráfordítással állhatják a versenyt[5].

Technológiai eszközökre szakosodott bűnözés

A kiberbűnözés további sajátossága, hogy elkövetési eszközei a infokommunikációs technológiák manapság szó szerint korlátlan lehetőségeit aknázzák ki, gyakran sokkal kreatívabban és innovatívabban, mint azt a legitim szereplők teszik. Valahányszor egy új technológia kerül a törvényes piacra, valóságos „törési verseny" veszi kezdetét a kiberbűnözők körében, akik rendkívül komoly anyagi és technológiai hátterük révén megdöbbentően rövid idő alatt képesek célirányosan „feltörni" a legújabb készülékeket vagy programokat, s olyan módon alkalmazni azokat, amilyen felhasználásra adott esetben azokat soha nem is tervezték, olyan területeken, amelyeken soha nem is lettek tesztelve[6]. Nagy feltűnést keltett például, mikor kiderült, hogy a Stuxnet féreg egy kiskereskedelmi forgalomban kapható szerverüzemeltető operációs rendszer nyomtatásvezérlőjén keresztül volt képes urándúsító centrifugák fizikai tönkretételére[7].

Ez egyúttal rávilágít arra is, hogy a kiberbűnözőknek számos esetben önkéntelenül is segítségére van a jóhiszemű vagy gondatlan technológia-felhasználó, aki tudatlanságból, gazdaságossági megfontolásból vagy egyéb okból nem rendeltetésszerűen használja az adott technológiát, elmulasztja a legalapvetőbb védekezési lépések megtételét, s ezáltal saját maga is támadási felületet biztosít.

Ezen felül persze komoly kihívást jelent a technológia saját sebezhetősége is, amely az esetek egy részében talán tervezési vagy kivitelezési hiányosságokra is visszavezethető, számos más esetben azonban a termék tervezett rendeltetésén kívüli felhasználás során merül fel. Gyakran egy-egy sebezhetőség nem is egy konkrét technológiát érint önmagában, hanem annak a terméknek egy vagy több másik technológiával való együttes alkalmazásakor lép fel és/vagy válik relevánssá. Klasszikus példa erre, amikor egy elektronikus dokumentumolvasó szoftverben olyan sebezhetőség merül fel, ami nem az adott szoftvert vagy az abban megnyitott adatállományt kompromittálja, hanem az alatta futó operációs rendszert támadja, illetve fertőzi meg.

A sebezhetőségek egyetemes kiküszöbölését, sőt megelőzését hízelgő dolog a technológiák gyártóitól elvárni, és csábító ötletnek tűnhet egy ezirányú jogszabályi kötelezettség előírása. Gyakran említett példa e tekintetben az autóiparé, miszerint a gépjármű üzemszerű és biztonságos működéséért a gyártó vállal felelősséget. Az összehasonlítás azonban rendkívül félrevezető, ugyanis ez a jótállás is csak a gépjármű rendeltetésszerű használatának határáig terjed. Nem fedi le a karbantartás elmulasztásának, a szabálytalan közlekedésnek, és pláne nem a gépjármű bűnelkövetésre való felhasználásának lehetőségét. Ha a hasonlatot konzekvensen végigvezetjük, akkor gyorsan kiderül, hogy:

5 Európai Bizottság, COM(2012)140 sz., 2012. március 28- i közlemény az Európai Kiberbűnözési Központ létrehozásáról

6 Például lásd az alábbi, nyílt forrású útmutatót törvényes felhős szolgáltatások törvénytelen célokra való alkalmazásáról: Thomas Roth, Breaking encryptions using GPU accelerated cloud instances, 2011: https://media.blackhat.com/bh-dc-11/Roth/BlackHat_DC_2011_Roth_Breaking_encryptions-wp.pdf

7 Symantec, W32.Stuxnet Dossier, 2011: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

- Az üzemszerűen és szabályosan használt fékrendszer hibájának kijavítása valóban a gyártó felelőssége, pontosan úgy, ahogy a jótállási idő alatt tönkremenő számítógép javítása vagy cseréje is[8].
- Viszont ugyanez semmiképp nem lehet igaz például arra az esetre, mikor egy terrorista bombát rejt el az autóban: szigorú technikai értelmében sebezhetőségnek számít az, hogy az autó alkalmas egy bomba elrejtésére, azonban ezért nyilván nem terhelheti felelősség az autó gyártóját. Ugyanígy méltánytalan dolog lenne az infokommunikációs hardverek és szoftverek gyártóit felelősségre vonni azért, mert termékeik alkalmasak bizonyos szándékos vagy gondatlan, rendeltetés-idegen, vagy egyenesen rosszindulatú, kártékony felhasználásra.

Márpedig a kibertér egyik legalapvetőbb jellemzője, hogy minden felhasználó saját belátása szerint, mindenféle külső kontroll nélkül használja készülékeit, programjait, adott esetben azok tervezett rendeltetésétől radikálisan eltérően, sőt azzal merőben ellentétesen. Nem csak arról van szó, hogy „mindenki azt rak a gépére, amit akar, és azt csinál vele, amit jónak lát", de ezen túlmenően még azt is figyelembe kell venni, hogy a magánélet, a személyes adatok és a szólásszabadság védelméhez való alapvető állampolgári jogokkal[9] összeegyeztethetetlen lenne az ehhez kifejezetten hozzá nem járuló technológia-felhasználókat bármilyen módon a technológiák gyártóinak ellenőrzése alá vonni. Ilyen körülmények között pedig nem elvárható, hogy az utóbbiak szavatolják termékeik jogszerű vagy rendeltetésszerű használatát.

A bűnüldöző hatóságok szempontjából egy adott bűncselekmény felgöngyölítése során a technológiai kihívás tehát nem pusztán a fejlődéssel való, idő-, pénz- és energiaigényes lépéstartás, hanem annak puszta feltárása is, hogy ki, hol, mikor és milyen hardvereket és szoftvereket használ(t), milyen célból, milyen körülmények között, milyen összefüggésekkel és következményekkel, tekintettel a lehetséges, valószínű, illetve kizárható ok-okozati összefüggésekre, a felmerülő szándékosságra vagy gondatlanságra, jó- vagy rosszhiszeműségre, vagy például az áldozat(ok) saját magatartásának vagy cselekedeteinek esetleges jogszerűtlenségére. Ezen kérdések megválaszolása már önmagában rettentő komplex feladat, melyet minden konkrét esetben külön-külön és fokozott körültekintéssel kell elvégezni, még mielőtt bármilyen nyomozati következtetés egyáltalán levonhatóvá válna.

Határokon átívelő bűnözés

A következő tény pedig még tovább – és talán még nagyobb mértékben – nehezíti a bűnüldözés feladatát: A kibertér technológiai hátterének adottságai lehetővé teszik, hogy a kiberbűnözés sokszor szinte teljes mértékben függetlenítse magát mindennemű állam- és közigazgatási határoktól. Egyesek úgy tartják, hogy a kibertérben a hatóságok hagyományos illetékessége irreleváns. A valóság azonban talán még ennél is sarkosabb: a hatóság területi illetékessége igenis releváns, mégpedig elsősorban mint a hatékony bűnüldözés egyik legkomolyabb akadálya.

Nem véletlen például, hogy a „botnet" néven ismert támadó infrastruktúrákat üzemeltető szervezetek a zombi hálózataik irányító központjait tudatosan különböző államok területein

8 Lásd 1999. május 25-i, 1999/44/EK sz. európai parlamenti és tanácsi irányelv a fogyasztási cikkek adásvételének és a kapcsolódó jótállásnak egyes vonatkozásairól, EUHL L171/12, 15/4 kötet, 1999.7.7.

9 Lásd Európai Alapvető Jogok Chartája, 8-ik és 11-ik cikkelyek, EUHL C 364/1, 2000.12.18.

szórják szét, és szükség esetén percek alatt, más esetekben néhány perces rendszerességgel változtatják „digitális székhelyüket", ezáltal megnehezítve akár a lokalizálásukat, akár – és főleg – minden nemű fizikai rajtaütést. Nem is beszélve arról, hogy a „digitális elkövetés" helyszíne sokszor semmilyen fizikai közelségben nincs a tényleges elkövetők hollétével, sőt még ha talán lenne is, akkor sem lenne feltétlenül bizonyítható[10].

Ugyanakkor téves és elhamarkodott következtetés lenne oda konklúdálni, hogy a hatóságok területi illetékessége csak akadályként merülhet föl ebben a vitában: az elkövetők ugyanis végső soron mindig természetes személyek, az elkövetés eszközei pedig mindig fizikai eszközök, vagy legalább is bizonyos fizikai eszközökön futó algoritmusok. Márpedig mind a természetes személyek, mind az igénybe vett fizikai eszközök helymeghatározása igenis lehetséges, sőt szükséges. A bűnüldözés eljárásai tehát azonosak a minden más bűnözési forma ellen alkalmazottakkal, csak az elkövetők beazonosításához vezető nyomozati cselekmények a legtöbb esetben számos határon átívelnek, technológiai hátterük pedig a máshol megszokottnál sokkal bonyolultabb, szofisztikáltabb, sőt némely esetben – főleg egy-egy nyomozás kezdeti szakaszában – akár teljesen ismeretlen[11] is lehet a hatóságok előtt.

Kiemelt szerep a számítástechnikai ipar számára

A fent leírtakból következik, hogy a kiberbűnözés elleni küzdelem területén kiemelt szerep jut a magánszektornak, azon belül is a hardvereket, szoftvereket gyártó, és szolgáltatásokat nyújtó ipari szereplőknek.

A számítástechnikai ipar egyfajta állandó strukturális áldozata a kiberbűnözésnek, hiszen minden bűncselekmény valamilyen technológia alkalmazása, feltörése, eltérítése, meghamisítása vagy egyéb fel- vagy kihasználása révén kerül elkövetésre. Ezért aztán az ipar saját jól felfogott érdeke, hogy a tőle telhetőt megtegye saját termékei és saját felhasználói védelmében; a termékeiben felmerülő sebezhetőségeket lehetőség szerint orvosolja; jóhiszemű, törvénytisztelő ügyfeleit óvja a kibertámadásoktól vagy legalább azok következményeitől; lehetőségeihez és jogosítványaihoz mérten együttműködjön a hatóságokkal az egyes bűncselekmények felderítésében.

Egyúttal az ipar sok esetben jobb és mélyebb ismeretekkel rendelkezik saját technológiáiról, mint a nyomozó és bűnüldöző hatóságok, s így például a kölcsönös információcsere számos esetben kölcsönös előnyökkel is jár, mind a bűntények felderítése, mind a technológiák hatékonyabb védelmezése szempontjából.

Végül sok technológia-gyártó nemzetközi szinten tevékenykedik, ezért területi lefedettsége számos nemzeti bűnüldöző hatóság illetékességét felöleli, könnyebbé téve ezáltal az alapvetően határokon átívelő kiberbűnözés globális feltérképezését, a védelmi eszközök hatékonyabb terítését, a különböző országokban megfigyelt jelenségek közötti korrelációk feltárását, vagy éppen a több illetékes hatósággal való egyidejű kooperáció előmozdítását. A Symantec évente kiadott Internet Security Threat Report című jelentésének legfrissebb számát[12] például lényegesen bővebb betekintést ad a kiberbűnözés világtrendjeibe, mint tehetné bármelyik szuverén állam saját hatósága. Ennek oka az, hogy a Symantec ügyfél-bázisa, illetve az ügyfelek által – és az ő hozzájárulásukkal – elhelyezett több mint 240.000 támadás-érzékelő szenzor majdhogynem az egész világot lefedi, páratlan érzékelési és elemzési lehetőségeket biztosítva a cég számára. Ennek a szenzorhálónak (Symantec Global Intelligence Network) a kiépítése hosszú évek beruházásának eredménye, ám az így létrehozott egyedülálló kereskedelmi potenciálon és versenyelőnyön is túlmutat az így szerzett tapasztalatok és tanulságok közérdekű megosztása, ezért is terjeszti a Symantec nyilvánosan és ingyenesen többek között a hivatkozott jelentést is.

Mindezek ellenére azonban a számítástechnikai ipar sosem volt, és sosem lesz bűnüldöző hatóság: nyomozási vagy egyéb eljárási jogköre nincs, közhatalmi eszközökkel vagy előjogokkal nem rendelkezik, és minden tevékenységét köteles a polgári és büntetőjogi felelősség korlátain belül folytatni. Ez pedig alapvetően behatárolja a kiberbűnözés elleni küzdelemben vállalható szerepét.

Amit az ipar megtehet

Az ipar nagyvonalakban három területen járulhat hozzá a kiberbűnözés megelőzéséhez, kivédéséhez, illetve felderítéséhez.

Figyelemfelhívás, ismeretterjesztés, oktatás

A kibertér minden résztvevője saját digitális tevékenységeinek, szerepének és az azzal járó felelősségének megfelelően kell, hogy tájékozódjon az adott szerepvállalással járó kockázatokról, gondoskodjon azok kezeléséről, ide értve különösen a kiberfenyegetéseknek való kitettséget, valamint a védekezés lehetséges eszközeit. Jóllehet, mára a kiberbiztonság ugyanolyan alapvető fontosságú szemponttá nőtte ki magát, mint a fizikai biztonság, a tényekben azonban mind a hatóságok, mind a gazdasági szereplők, és különösen az egyéni felhasználók (fogyasztók) körében érzékelhetően alulértékelt marad a kiberkockázatok ismeretének, megértésének, reális felmérésének és gyakorlati kezelésének fontossága. Az ilyen irányú információ iránti kereslet és fogékonyság kiépülése még mindig nagyon kezdeti stádiumban jár, noha a számítástechnikai ipar különféle eszközökkel igyekszik saját ügyfelei, partnerei, illetve a nagyközönség számára megkönnyíteni a kiberbiztonsági tájékozódást, illetve védekezési és készültségbeli felzárkózást. Az alábbi néhány Symantec publikáció és termék jól illusztrálja, hogy az ipari szereplők milyen jellegű anyagokkal járulhatnak hozzá a kiberfenyegetésekkel kapcsolatos információk szélesebb körű terjesztéséhez, a felhasználók tájékoztatásához, a szakemberek képzéséhez.

A fentebb említett Internet Security Threat Reporthoz hasonló módon a Symantec szenzor-hálózatának segítségével rendszeres és naprakész információt gyűjt az Interneten megfigyelt jelenségekről. A Norton Cybercrime Index például naponta frissülő helyzetjelentést ad a globális szinten mért vírustevékenységekről, a spam (levélszemét) forgalom volume-

10 Symantec, beadvány az Egyesült Államok Nemzetbiztonsági és Kereskedelmi Minisztériumainak közös nyilvános konzultációjára a zombihálózatok elleni küzdelem eszközeiről és lehetőségeiről, 2011. november 14: http://www.nist.gov/itl/upload/Symantec-Comments-to-BotNet-FRN-11-14-11.pdf

11 Különösen nulladik napi sérülékenységek esetén

12 Symantec, ISTR volume XVII, 2012. április: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

néről, aktuálisan kiemelt témáiról, forrásairól, cépontjairól, a hálózatalapú (pl. botnet-) támadások intenzitásáról, vagy a pillanatnyilag leggyakrabban „mérgezett" keresőszavakról (SEO poisoning, azaz „kereső motor optimizáció mérgezés"[13]). Az így gyűjtött információt és a vonatkozó biztonsági ajánlásokat a cég a Norton Cybercrime Index weblapon[14], illetve mobil alkalmazásokon keresztül ingyen bocsátja a nagyközönség rendelkezésére, hogy így segítse elő a leggyakoribb fenyegetések felismerését és kivédését. Ideális esetben egy körültekintő internetező ugyanolyan természetesen tájékozódhatna napi rendszerességgel az aktuális kiberfenyegétesekről, mint teszi azt az időjárás, a közlekedés vagy például a tőzsdei árfolyamok tekintetében. Az információ puszta kínálata azonban csak nagyon lassan és fokozatosan vonja maga után az eziránt való érdeklődés kialakulását és növekedését. Ezzel együtt az ilyen jellegű beruházások beindítása és fenntartása akkor is nagyon szükséges, ha igazán csak hosszú távon válnak majd gyümölcsözővé.

Ugyanez igaz az évente kiadott Norton Cybercrime Reportra is[15], amely évről évre lefolytatott nemzetközi mérések és közvéleménykutatások révén igyekszik felbecsülni a kiberbűnözés által az egyéni felhasználóknak okozott kárt, beazonosítani a leggyakoribb és legkockázatosabb cselekedeteket és magatartásokat, illetve tájékoztatást és jótanácsokat adni a hatékony védekezés eszközeiről. Ezen jótanácsok („best practices") széles körben terjesztett digitális és nyomtatott anyagok formájában is[16] rendszeresen eljutnak a végfelhasználókig, a hatékonyság határát tehát ismét nem annyira a tájékoztatási anyag terjedelme vagy tartalma, mint inkább a közönség tájékozódási hajlandósága és fogékonysága határolja be.

A fentieken túl a hozzáértőbb felhasználók, szakemberek számára a Symantec rendszeresen ad ki alaposabb elemzéseket is egy-egy új víruscsaládról, kiberbűnözési trendről vagy támadási technológiáról[17]. Ezek az elemzések – nyilván anonimizált adatok alapján – de valós ügyfeleknél feltárt támadások és fertőzések tanulságait vonják le, az anyagok közzététele pedig azt a célt szolgálja, hogy segítsen a tágan vett kiberbiztonsági közösségnek felvérteznie magát a legújabb fenyegetésekkel szemben. Bár ezek az anyagok erősen technikai jellegűek és számottevő szellemi befektetést és annak megfelelő eszmei értéket képviselnek, ingyenes és publikus terjesztésük előbbre való közösségi érdek, s egyben hosszú távon megtérülő befektetés. Csak úgy, mint a 2011-ben indított Norton Cybersecurity Institute, amelyen keresztül a Symantec a bűnüldöző hatóságok szakembereinek célirányos képzését, ismereteik elmélyítését igyekszik gyakorlati úton előmozdítani[18].

13 Röviden: automatikus kereső szolgáltatások megtévesztése abból a célból, hogy az éppen legnépszerűbb keresőszavakra – pl. „foci vb", „Kate Middleton", „London Olympics" – kapott találatok minél nagyobb valószínűséggel irányítsák bizonyos fertőzött, kártékony tartalmakat terjesztő weblapokra a gyanútlan internetezőt. Lásd a Symantec vonatkozó blogját : http://www.symantec.com/connect/blogs/evolution-seo-poisoning

14 http://cci-web.finedesigngroup.com/flashApp (mgj: Flash animáció)

15 Symantec, Norton Cybercrime Report 2012: http://www.norton.com/2012cybercrimereport

16 Lásd például itt: http://us.norton.com/articles/

17 Például Symantec, The Elderwood Project, 2012: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf, vagy Symantec, Trojan.Neloweg, 2012: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Trojan_Neloweg_Bank_Robbing_Bot_in_the_Browser.pdf

18 http://www.symantec.com/about/news/release/article.jsp?prid=20110504_01

Védelmi eszközök, termékek és szolgáltatások

Az ipar klasszikusabb, hagyományos értelemben vett kereskedelmi szerepe a védelmi technológiák gyártása és forgalmazása, függetlenül egyébként az adott termék vagy ipari szereplő saját üzleti modelljétől. Egyazon ipari szereplő nyújthat például hardvert, szoftvert és szolgáltatást, nyílt és zárt forráskodú termékeket, igyenes és fizetős alapon, egyszeri befizetéses és periódikusan megújuló előfizetéses konstrukcióban, fizikai tárolón és online letölthető formában, végpontra telepített termékként és a felhőből nyújtott szolgáltatás formájában egyaránt. Fontos szempont, hogy – a fentebb leírtaknak megfelelően – a gyártók és szolgáltatók ezeket a termékeket és szolgáltatásokat legjobb tudásuk szerint, piaci verseny alapján és a rendeltetésszerű használat korlátain belül forgalmazzák. Tehát a hatékony kibervédelmi eszközök piacának innovatív és versenyképes mivolta nagy mértékben függ attól, hogy a termékekkel és szolgáltatásokkal járó gyártói és forgalmazói felelősség mennyire marad meg egy kiszámítható üzleti kockázatnak. A jelenlegi jótállási szabályok szigorítása és a forgalmazói vagy gyártói felelősség kiterjesztése, bár politikailag olykor kecsegtetőnek tűnhet, valószínűleg nem segítene fokozni az általános kibervédettséget, ugyanis az ipari szereplők a minél hatékonyabb és innovatívabb termékek fejlesztése és piacra dobása helyett inkább a felelősségi kockázat kezelése (minimalizálása), azaz a régebbi, jobban ismert, ám kevésbé hatékony termékek és szolgáltatások szinten tartása révén versenyeznének[19]. Ami, tekintettel a kiberbűnözők roppant kreativitására és innovatív képességére, inkább megsokszorozná a támadási felületeket, mintsem befoltozná azokat.

Ezzel szemben nagyon fontos, hogy a folytonos technológiai fejlődés során a gyártók és szolgáltatók mindenkor gondoskodjanak a készülékeikben, szoftvereikben, szolgáltatásaikban felmerülő hiányosságok és sebezhetőségek mielőbbi kijavításáról. A már leírtaknak megfelelően minden ipari szereplő tisztában van az ehhez fűződő saját érdekével, és igyekszik is mindent megtenni az esetleges hibák elhárításáért. Két szempontot fontos itt figyelembe venni.

Egyfelől gondoskodni kell arról, hogy a gyártók közötti információcsere a jövőben is olyan gördülékenyen és akadálymentesen folyhasson, mint jelenleg (azaz ne kerüljenek polgári, kereskedelmi, büntető, adatvédelmi, verseny- vagy egyéb jogi akadályok például az újonnan felfedezett sebezhetőségekre vonatkozó információk gyors, iparon belüli cseréjének útjába). Ugyanakkor hasonlóan kontraproduktív lenne előírni például minden újonannan felfedezett sebezhetőség azonnali nyilvánosságra hozatalát, ugyanis a kiberbűnözők jó eséllyel mindenkinél, és leginkább a védekezőknél gyorsabban képesek „ráugrani a résre". Éppen ezért tanácsos az új sebezhetőségeket csak a vonatkozó javítás publikálásával egyidejűleg nyilvánosságra hozni, és fontos, hogy az ilyen megfontolásból való információvisszatartáshoz ne kapcsolódjon hátrányos törvényi vagy egyéb jogi következmény.

Másfelől tudatosítani kell a felhasználókban, hogy a termékek, különösen a szoftverek frissítése jóllehet jogilag fakultatív[20], ám a kiberbiztonság szempontjából nem opcionális. Sokatmondó megállapítása például a Symantec korábban hivatkozott Internet Security Threat

19 Vö: Európai Bizottság 2012. július 26-i, COM(2012)417 sz. közleménye az európai biztonsági iparpolitikáról, különösen annak 4.2.4-es szakasza a polgári jogi felelősség korlátozásáról

20 Bár elmulasztása a vonatkozó szerződéses feltételek szerint adott esetben akár a garanciáról való lemondással, vagy egyéb jogvesztéssel is járhat a felhasználó számára.

Reportjának, hogy a 2011-es év folyamán legtöbbet kihasznált szoftver-sebezhetőségre az adott gyártó már négy éve kiadta a javítócsomagot. Mindazok, akik ezen sebezhetőségen keresztül estek kibertámadás áldozatává, saját mulasztásuk következményével szembesültek. Ezért is lenne méltánytalan a gyártókra hárítani a technológia gondatlan vagy nem rendeltetésszerű alkalmazásának, karban nem tartásának felelősségét. Olykor elhangzik az érv, miszerint a tíz évvel korábban vásárolt gépnek vagy programnak a mai kihívásokkal szemben is védettnek kéne lennie. Ez azonban sem jogi, sem piaci alapon nem elvárható, méghozzá azért nem, mert a termék rendeltetésének való megfelelését az eladás pillanatában kell értékelni, az utána való szintentartás pedig már egy külön, általában zárt határidejű szolgáltatás. Ennek ellenére, ugyancsak saját jól felfogott érdekében, a legtöbb gyártó igyekszik a termékeit azok avulása, amortizációja, sőt piaci kivezetése után is még sok évig biztonsági frissítések révén támogatni (vö. egy lejárt garanciájú gépkocsi, egy tükörsimára használt gumiabroncs, vagy egy csonkig kopott fékbetét).

Szakértői segítségnyújtás és információcsere

A harmadik terület, amelyen az ipar hatékonyan járulhat hozzá a kiberbűnözés elleni küzdelemhez, a felderítő és bűnüldöző szervekkel való együttműködés. Ezen a téren az ipar kétségtelenül elmélyült ismeretekkel és tapasztalatokkal rendelkezik a kibertér egyes szegmeinseit alátámasztó technológiákról, s az ilyen fajta szakértelem értékes kincs nem csak a piaci verseny keretében, hanem a hatóságok számára is. Ezzel az értékkel azonban mindenkinek illik tisztában lennie: az információ vagy szakértelem alapvetően nem ingyenesen áll rendelkezésre, de ha adott esetben még ingyenesen is kerül átadásra, például méltányossági alapon, akkor sem feltétlenül szabadon felhasználható, továbbadható vagy megosztható.

Szemben a korábban említett, ingyenesen és publikusan terjesztett technikai elemzésekkel, a Symantec, számos más ipari szereplőhöz hasonlóan, egyedi szerződéses konstrukciókban, és/vagy ad hoc magán- és közszféra közötti együttműködések keretében is oszt meg bizalmas információt, bocsát rendelkezésre szakértelmet a bűnüldöző szervek részére. Ez azonban mindig a megfelelő jogi garanciákkal és a vonatkozó jogszabályi előírások teljeskörű tiszteletben tartása mellett történik, ami többek között azt is jelenti, hogy ilyen együttműködésekről általában semmilyen konkrétum nem megosztható. Lehet szó konkrét nyomozati cselekmények során nyújtott technikai segítségről, szolgáltatásként elvégzett rendszer-, információ- és hálózatbiztonsági feladatok teljesítéséről, konkrét kártevő kódok visszabontásáról és elemzéséről, stb. Általánosan a Symantec tapasztalatai szerint az az együttműködés lesz sikeres és gyümölcsöző, amelynek során a felek egyetértenek és megegyeznek az alábbiakban:

- Konkrét célt fogalmaznak meg (egy adott művelet elvégzése, egy adott ügy felderítése, egy adott infrastruktúra védelme, egy adott információtípus rendszeres cseréje…), és ahhoz tartják magukat;
- Világosan megállapítják a felek közötti szereposztást és a vonatkozó felelősségeket;
- Kellő időt és energiát fordítanak a kölcsönös bizalom kiépítésére, nem csak intézményi szinten, hanem a gyakorlatban együttműködő szakemberek között is;
- Méltányosan osztják meg a projekttel járó feladatokat és költségeket (hogy mind a befektetés, mind a haszon kölcsönös legyen, s egyik felet se terhelhesse méltánytalan jogi, kereskedelmi, hírnévbeli vagy egyéb teher pusztán az együttműködésben való részvétel miatt);
- Nem tágítják a konkrét együttműködés kereteit további feladatok, további területek felé, mert az megbonthatja az eredeti egyensúlyokat, s ezáltal alááshatja a fáradságosan kiépített kölcsönös bizalom alapjait;
- És végül lezárnak és befejezettnek tekintenek minden olyan együttműködést, amely teljesítette a kitűzött céljait, vagy okafogyottá vált.

Amit az ipar nem tehet meg

A fentiekkel nagyjából be is zárul az ipar számára nyitott lehetőségek köre. Ezen túlmenően minden kiberbűnüldözési cselekmény megfelelő illetékességet, jogkört, hatósági jogosítvány, közhatalmi jogokat igényel, melyekkel az ipar nem rendelkezik, nem is ruházható fel, legalább is a demokratikus hagyományú jogállamok alkotmányos rendjeinek legtöbbjében.

Az ipar nem megfigyelő vagy ellenőrző szerv

A politikai döntéshozók olykor igen ellentmondásos elvárásokat fogalmaznak meg az iparral szemben: Egyfelől igyekeznek a lehető legszigorúbb feltételekhez kötni az ipar és a bűnüldöző hatóságok közötti bármilyen nemű együttműködést, különösen az információ- és adatcsere területén, különösen akkor, ha az ilyen információcsere során az állampolgárok személyiségi vagy egyéb szabadságjogai vélt vagy valós csorbát szenvedhetnek[21]. Másfelől azonban felismerik, hogy a kibertérben az ipar kivételes információszerzési lehetőségekkel rendelkezik, s ennek megfelelően a kiberbűnözés elleni küzdelemben való ipari részvételt és együttműködést néha túlbuzgó módon is próbálják szorgalmazni, például akár büntetőjogi felelősségrevonással is fenyítve a bűnmegelőző vagy bűnüldöző hatóságokkal elégtelenül együttműködő szereplőket[22]. Jóllehet, evidensnek tűnik, mégis számtalanszor tisztázásra szorul az a tény, hogy az ipar minden körülmények között csak a vonatkozó jogszabályok betartása mellett működhet együtt a hatóságokkal: egyfelől se törvényi előírásokat, se szerződéses kötelezettségeket nem szeghet meg önkényesen, másfelől a hatóságok elvárásainak, konkrét igényeinek is csak jogszerű eljárások keretében felelhet meg.

Konkrétan ez azt jelenti például, hogy az ipari szereplők külön kifejezett ezirányú hozzájárulás vagy más jogszerű felhatalmazás híján se saját ügyfeleik, se harmadik felek fölött nem gyakorolhatnak ellenőrzést vagy felügyeletet; önhatalmúlag nem élhetnek kényszerítő eszközökkel még saját jogaik érvényesítése érdekében sem; közvetlenül vagy közvetetten személyesnek minősülő adatot csak a személyes adatok védelmére vonatkozó hatályos jogszabályi előírások által engedélyezett esetekben, az azokban meghatározott feltételek szerint oszthat-

21 Lásd például Európai Parlament, Axel Voss,. saját kezdeményezésű jelentés a személyes adatok Európai Unión belüli védelmének átfogó megközelítéséről (2011/2025(INI)), 2011. június 22, A7-0244/2011, 6-ik sz. bekezdés: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0244+0+DOC+PDF+V0//HU

22 Lásd például Európai Parlament, Monika Hohlmeier, első olvasati együttdöntési jelentés-tervezet az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról (COM(2010)0157 – C7-0293/2010 – 2010/0273(COD)), 2011. november 24, 12-es és 13-as módosítások: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-476.089+01+DOC+PDF+V0//HU&language=HU

nak meg bárki mással, még akkor is, ha ez a kiberbűnözés elleni küzdelem során hasznos vagy célravezető lehet[23]. Hasonlóképp a számítógépes rendszerekbe való behatolás, működésük befolyásolása, az azokban tárolt adatok megszerezése, az azok révén folytatott távközlések lehallgatása vagy eltérítése, illetve az ilyen célú termékek fejlesztése is csak akkor nem minősül önmagában kiberbűnözésnek, a kiberbűnözés elősegítésének, vagy arra való felbujtásnak, ha mindez a meghatározott jogszabályi lehetőségek keretén belül történik, például az érintettek beleegyezésével, vagy harmadik feleket hátrányosan nem érintő módon biztonsági kutatási és fejlesztési célból, vagy kifejezetten megalapozott és indokolt esetben jogszerű hatósági utasításra, igazságügyi felügyelet mellett, a közrend védelmében[24].

Az ipar nem nyomozó szerv

A fentiekből következik az is, hogy az ipari szereplőknek nincs se joguk, se hatáskörük nyomozati cselekmények folytatására, vagy kiber- (vagy egyéb) bűncselekményekkel kapcsolatos tények megállapítására és azok jogi minősítésére. Például amikor a Symantec egy ügyfelénél illetéktelen külső behatolási kísérletet vagy nem kívánatos adatszivárgást észlel, és erről tájékoztatja az ügyfelet, akkor csupán annyit tesz, hogy megállapítja az előzetesen, közös megegyezés útján meghatározott adatforgalmi, rendszerüzemeltetési, hálózatbiztonsági normáktól mért eltérést; a rendelkezésre álló adathalmazok alapján megállapítja az incidens során jogszerűen a látókörébe kerülő és beazonosítható készülékek, hálózatok, szoftverek érintettségét; adott esetben foganatosítja a szintén megállapodásos alapon kikötött, releváns, technikai jellegű biztonsági és védelmi ellenintézkedéseket; illetve mindezt szükség és igény szerint közli az ügyféllel. Mindezen megállapítások és lépések, illetve az ezekre vonatkozó naplóbejegyzések (logok), jegyzőkönyvek adott esetben akár bizonyítékként is felhasználhatók egy későbbi bűnügyi nyomozás során, azonban:

- Az incidens érzékelése és saját technikai nomenklatúra szerinti naplózása semmilyen formában nem tekinthető jogi minősítésnek (azaz a Symantec nem állapítja meg, hogy kiberbűncselekményről, rendszerhibáról, gondatlanságról, netán legitim behatolásról vagy, tegyük fel, kiberbűnüldözési nyomozati cselekményről van-e szó);
- Az incidens során aktív eszközök, rendszerek, algoritmusok azonosítóinak rögzítése semmilyen formában nem bizonyítja vagy vélelmezi konkrét személyek vagy szervezetek aktív vagy passzív érintettségét (például bizonyos személyi azonosítók alkalmazásának megállapítása egy adott esetben egyszerű adattechnikai kérdés, viszont azt már csak a nyomozó hatóság állapíthatja meg, hogy ezen azonosítók alkalmazása az adott esetben jogszerű volt-e vagy sem, és bizonyíthatja-e egy vagy több konkrét személy tevőleges részvételét a cselekmény elkövetésében);
- Az incidens során vagy nyomán foganatosított biztonsági és védelmi ellenintézkedések pusztán technikai jellegűek, nem pedig jogi lépések (egy kibertámadás sikeres kivédése önmagában se nem zárja ki, se nem súlyosbítja az adott támadás esetleges bűncselekménykénti minősítését).

Röviden és tömören: a Symantec feladata kimerül a rendszerek normálisnak tarott működésétől való eltérések észlelésében és a szükséges technikai korrekciók kivitelezésében. Viszont kizárólag a bűnüldöző és nyomozó hatóságoknak van illetékessége és hatásköre annak megállapítására és értékelésére a rendelkezésre álló információk alapján, hogy az adott incidens során történt-e kiberbűntény, ha igen, ki követte el, ki ellen, hol, honnan, milyen eszközökkel, milyen célból, stb.

23 2003-ban módosított 1995. október 24-i, 95/46/EK sz. európai parlamenti és tanácsi irányelv, EUHL 1995L0046, 2003.11.20, 7-ik cikkely

24 Európa Tanács, CETS 185. sz. 2001. november 23-i, ún. Budapesti Egyezmény, 6-ik cikkely, második bekezdés

Az ipar nem bűnüldöző szerv

A Symantec következetesen tartja magát ahhoz az álláspontho, miszerint ezen kérdések saját hatáskörű megválaszolásának akár kísérlete is súlyos szereptévesztés lenne egy ipari szereplő részéről. Ez méginkább igaz az esetleges jogsértések jóvátételére, jogállami keretek között való szankcionálására, pláne megtorlására. Ilyen lépések meghozatalára jogállami keretek között kizárólag a hatóságok jogosultak, polgári és büntetőjogi alapon, adott esetben nemzetbiztonsági vagy honvédelmi megfontolások – és jogosítványok – mentén. Ennek megfelelően például nem az ipar tisztje:

- Illetéktelenül szerzett információkat visszaszerezni vagy megsemmisíteni;
- Büntetéseket vagy egyéb jogi következményeket és ellenintézkedéseket foganatosítani;
- Ellentámadási cselekményeket kezdeményezni vagy folytatni.

Jóllehet, a kibertér infrastruktúrájának, rendszereinek, szolgáltatásainak, tágan vett eszközeinek és vívmányainak fejlesztője, birtoklója, üzemeltetője, sok esetben haszonélvezője nagy mértékben a privát szféra, azon belül is az ipari szereplők közössége. Azonban ez a tény az utóbbiakat semmilyen közhatalmi attribútummal nem ruházza föl. Az ipari szereplők – szakértelmük, technológiai hátterük, nemzetközi hatósugaruk, valamint a birtokukban lévő információk révén – nyilván hosszabb távon is megkerülhetetlen résztvevői és tevékeny közreműködői maradnak a kiberbűnözés elleni küzdelemnek. A bűnüldözés elengedhetetlen eszközeivel – alkotmányos felhatalmazással, hatáskörrel, területi illetékességgel, valamint végrehajtási jogkörrel – azonban kizárólag a közhatalom rendelkezik. A két szektor egymásra utaltsága tehát nyilvánvaló, a szerepek különválasztása pedig létfontosságú.

A NEMZETI KIBERBIZTONSÁGI STRATÉGIA

Suba Ferenc

A társadalmi és gazdasági folyamatok egyre nagyobb hányada zajlik az Interneten, ez a „virtualizálódás" hozta létre a kibertér fogalmát. A kibertér létező valóság, ahol globálisan 2 milliárdnál több, Magyarországon 3 millió felhasználó jelenik meg, az egyének társadalmi életet élnek, csoportok és pártok szerveződnek, a gazdasági élet szereplői pedig szolgáltatásokat nyújtanak, pénzt és árukat mozgatnak. A kibertér egyben az a szféra, ahol az államok egyre gyakrabban érvényesítik nemzetbiztonsági, illetve nemzetgazdasági érdekeiket védekező vagy támadó jelleggel a kibertér nyújtotta lehetőségek felhasználásával. A kibertér nincs tekintettel az állami határokra, eszközeit és infrastruktúráját meghatározó mértékben az üzleti szektor szereplői tulajdonolják, működtetik és ellenőrzik. További jellegzetessége, hogy a kibertérnek nincs irányító központja, új elektronikus információs rendszerekkel (mint például a mobil internet vagy az informatikai felhő) naponta bővül és állami eszközökkel csekély mértékben szabályozható.

Fentiek figyelembevételével került meghatározása a kibertér fogalma, miszerint a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a Magyarországon található, a globális kibertér részét képező elektronikus információs rendszerekből és ezen elektronikus rendszereken keresztül adatok és információk formájában Magyarországra irányuló és hazánkban megjelenő társadalmi és gazdasági folyamatok összességéből áll. Nemzetbiztonsági szempontok alapján kiemelendő, hogy a kibertér fogalma magában foglalja azon kibertérben zajló társadalmi és gazdasági folyamatokat is, melyekben Magyarország érintett.

A decentralizált, gyorsan növekvő, államilag nem szabályozott kibertér egyre nagyobb biztonsági problémákat vet fel, ebben a környezetben a névtelenség és a követhetetlenség mögé bújva szinte következmények nélkül lehet hírszerző tevékenységet folytatni, kormányzati és üzleti rendszereket tönkretenni, mások tulajdonát törvénytelen eszközökkel elvonni. A kibertérből jövő támadások eredetét ezért szinte lehetetlen megállapítani, leginkább a kibertámadások céljából, eszközrendszeréből és nagyságrendjéből lehet következtetni arra, hogy hagyományos kiberbűnözés vagy államilag finanszírozott támadás ellen kell védekezni. Fentiek alapján a kibertérben megjelenő veszélyek forrásuk szerint négy nagy csoportba oszthatók: állami vagy üzleti hírszerzés, bűnözés, terrorista csoportok, valamint aktivista egyének vagy csoportok.

A fenti veszélyek okán a közigazgatás és a társadalom működését lehetővé tevő informatikai infrastruktúrák illetve a nemzeti adatvagyon védelme, vagyis a kiberbiztonság fenntartása kiemelt feladattá vált, amely következtében alapvető kormányzati igény és egyben feladat a kiberbiztonság biztosítása. Az állam kiberbiztonsága az információs társadalmak biztonságának szerves része lett: kiberbiztonság nélkül nem képzelhető el sem a nemzeti adatvagyon,

sem az államműködés szempontból létfontosságú infrastruktúrák biztonságos működtetése.

Kiemelendő továbbá, hogy a nemzeti adatvagyon és a létfontosságú infrastruktúrák működésének kiber-kitettsége olyan szintre emelkedett napjainkra, hogy egy infokommunikációs katasztrófa valószínűsíthetően ugyanakkora vagy akár nagyobb károkat képes okozni a magyar szuverenitás védelme, illetve a nemzetgazdaság működése számára, mint a hagyományos biztonságpolitikai kihívások, vagy egyes természeti katasztrófák.

A kibertérben megjelenő veszélyek és a lehetséges válaszlépések számbavételével határozható meg a kiberbiztonság jelentése, miszerint a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

A kibertérben fellépő veszélyek nem pusztán virtuális fenyegetések, kihatnak a fizikai világra is, mivel a kibertérhez kapcsolódó kommunikációs, irányító és ellenőrző rendszereiken keresztül a létfontosságú rendszerek és létesítmények folyamatos és biztonságos működése nagymértékben függ a kibertér még kialakítandó biztonságától. Biztonságpolitikai szempontból egyértelműen érzékelhető, hogy a biztonság- és védelempolitika szárazföldi, légi, tengeri és űr dimenziója mellett a kibertér, mint az ötödik biztonságpolitikai dimenzió jelent meg, ami rövid időn belül a legfontosabb biztonságpolitikai dimenzióvá válhat.

A kibertérben való tevékenység elérkezett arra a gazdasági és politikai befolyásolási képességi fokra, s ennek következtében a kibertér biztonságának kérdése arra a nemzeti biztonságpolitikai szintre, hogy a korábbi technikai részletszabályok helyett átfogó és összetett szabályozást igényel. Magyarországgal szövetséges EU és NATO tagállamokban kormányzati koordinációs szervezetek alakultak, együttműködési fórumokat alapítottak a közigazgatás, a gazdasági (üzleti), a tudományos (akadémiai) és civil szférák között, szakosított intézményeket működtetnek. Kiberbiztonsági stratégiákat alkotnak, kiberbiztonsági törvényeket fogadnak el, nemzetközi együttműködéseket alakítanak ki, tudatosító és képzési programokat indítanak be, valamint üzleti motivációs rendszereket állítanak fel a nemzeti kiberbiztonsági helyzet javítására.

A Nemzeti Kiberbiztonsági Stratégia gyökereiben a 2001-ben elfogadott ún. „Budapest Konvenció”-ig nyúl vissza, amely egyrészt nemzetközi fontosságú konkrét magyar hozzájárulás a globális kiberbiztonság területén, másrészt napjainkig az egyetlen jogi kötőerővel bíró, referenciaként használt nemzetközi dokumentum. Az Egyezményben megfogalmazott alapelvek mindmáig érvényesek, és nemzetközi szinten is széles körben elfogadottak.

A stratégia kapcsolódik:

- Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozathoz,
- a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényhez, azon belül a létfontosságú rendszerek és létesítmények hálózatbiztonsági környezetének kialakításához,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényhez (Infobizt. tv.)
- az Európai Parlament által 2012. november 22-én elfogadott, A kiberbiztonságról és védelemről szóló, 2012/2096(INI) számú határozatához.

A stratégia alapelve az átfogó és összehangolt megközelítés:

- melyben kormányzati és nem-kormányzati, katonai, rendvédelmi és civil, nemzeti és nemzetközi, gazdasági és politikai eszközök egyaránt megfelelő hangsúllyal szerepelnek,
- ahol a felelősségek letisztázva, összehangoltan fogalmazódnak meg,
- amely a kormányzati és a magánszféra önkéntes együttműködésére, önkéntes információ-megosztásra építve a kormányzat és az érintett szférák közös erőfeszítésével kerül megvalósításra.

A stratégia alapvető célja, hogy Magyarországon az informatikai eszközök, rendszerek és szolgáltatások, valamint az elektronikus hírközlési infrastruktúra és szolgáltatások üzembiztosak legyenek, továbbá megfelelő szintű felkészültséggel és védelemmel rendelkezzenek a kiberfenyegetések és kibertámadások ellen.

A stratégiához kapcsolódóan a törvény a kormányzati koordináció céljából a Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) létrehozásáról rendelkezik, amelyre a Miniszterelnökség irányításával az érintett minisztériumok és hatóságok bevonásával kerül sor. A Tanács tevékenységén keresztül elősegíti a kiberbiztonság szabályozását, támogatja a források hatékony felhasználását, felügyeli a nemzeti kiberbiztonsági stratégia és akcióterv teljesülését, folyamatosan követve a kibertér változásait, szükség esetén javaslatot tesz ezek megújítására, a Miniszterelnökség által delegált kiberbiztonsági koordinátoron keresztül ellátja az egységes magyar álláspont kialakítását és képviseletét a nemzetközi politikai együttműködésekben.

Az együttműködés erősítése érdekében a Tanács létrehozása mellett olyan egyeztető fórum is kialakításra kerül, amelyben a kormányzat kijelölt képviselői és a civil, a gazdasági (üzleti) és a tudományos szektor meghatározó szereplői tudnak együttműködni a kiberbiztonság növelése érdekében. A fórum működését középvezetői szintű munkacsoportok segítik. Az együttműködés kiterjed az 1249/2010. (XI. 19.) kormányhatározattal létrehozott Kritikus Infrastruktúra Védelmi Tárcaközi Szakmai Munkacsoporttal történő kapcsolattartásra is, amely az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi Irányelv végrehajtását segíti elő. Az együttműködési rendszer egyben kezeli a Kritikus Infrastruktúra Védelmi Konzultációs Fórummal és a Fórum munkáját segítő munkacsoportokkal történő kapcsolattartást is, melyek elsődleges feladata a kormányzati szereplők és a civil szféra kritikus infrastruktúra-védelemmel kapcsolatos együttműködésének megteremtése.

A stratégia alapján a megelőzés, felkészülés és ellenőrzés céljára ún. szakosított intézményeket szükséges működtetni. Ilyen speciális szakértelemmel és hatáskörrel rendelkező szakegységet képeznek a rendőrség, valamint a Nemzeti Adó- és Vámhivatal szervezeti keretein belül működő, a számítógépes bűnözés elleni harcra szakosodott egységek, valamint az Országos Katasztrófavédelmi Főigazgatóságon is kialakításra került a kritikus infrastruktúrák informatikai védelméért felelős szervezeti egység. Ugyanezen körbe tartozik az Infobiztv. végrehajtására a Nemzeti Fejlesztési Minisztérium keretei között kialakított elektronikus információbiztonsági hatóság, valamint a Nemzeti Biztonsági Felügyelet is, amely felkérésre sérülékenység vizsgálatot végezhet. Magyarország nemzetbiztonsági szolgálatai a kibertérben fellépő fenyegetések elhárítására és információszerzésre szakosodott szervezeti egységeket alakítottak ki. A Magyar Honvédség ellátja a katonai célú

kommunikációs és információs rendszerek működtetését és védelmét, fokozatosan alakítja ki kibervédelmi képességeit, felhasználva az önkéntes tartalékos rendszerbe jelentkező szakértőket is. Mindezen szakosított intézmények munkáját a Nemzeti Média és Hírközlési Hatóság, mint szakhatóság, kormányzati felkérésre segítheti. Az említett szervezeteken kívül további közigazgatási szervezetek és állami intézmények látnak el a hatásköri jogszabályokban lefektetett kiberbiztonsági feladatokat.

A kiberbiztonsági események operatív kezeléséhez kapcsolódó alapfeladatot lát el az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által minősített kormányzati eseménykezelő központ, valamint ágazati esemény- illetve incidenskezelő központok (CERT-teket). Kiemelendő, hogy a szakosított intézmények kiberbiztonsági tevékenységük során együttműködnek a személyes adatvédelem és a titokvédelem kapcsán hatósági feladatokat ellátó hatóságokkal.

A magyar kibertér biztonságának szabályozása több lépésben történik meg. Elsőként a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvénnyel Magyarország gondoskodott a kritikus infrastruktúrák védelméről, érintve azok hálózatbiztonsági követelményeit. Második lépésben a 2013. évi L. törvény útján a kormányzati elektronikus információbiztonság területe kerül szabályozásra, amely felhatalmazást ad a kapcsolódó végrehajtási szabályok kormányrendeleti és/vagy miniszteri rendeleti szintű további szabályozására. Ezen jogszabályokat egészítik ki azok az operatív együttműködési megállapodások, melyek egyrészről a kormányzati szervek közötti munkafolyamatokat rendezik, másrészt a magyar kibertér nem kormányzati tényezői és a kormányzati szervek közötti kapcsolatok jogalapját teremtik meg.

A nemzetközi együttműködés területén igen sikeres és elismert Magyarország eddigi részvétele a különböző nemzetközi együttműködési struktúrákban, többek között:

- az Európai Unió tagországai által önkéntes alapon szerveződött Európai Kiber Válság Együttműködési Keret (European Cyber Crisis Cooperation Framework) munkacsoportjában,
- az Európai Hálózati és Információbiztonsági Ügynökség, az ENISA által kialakított képességfejlesztő együttműködésekben,
- az International Watch and Warn Network tagállamok „kibervihar” (Cyberstorm) típusú nemzetközi együttműködései keretében lezajlott nemzetközi gyakorlatokon,
- a Meridian konferenciasorozathoz hasonló kormányzati együttműködésekben.

A jövőben még hangsúlyosabban és koordináltabban szükséges részt venni a szabad és biztonságos globális kibertér kialakításáért felelős nemzetközi együttműködésekben, ezért kiemelt figyelmet kell fordítani a 2012-es Budapesti Kibertér Konferencia utókezelésére.

A stratégia alapján Magyarország fenntartja élen járó szerepét a kiberbiztonsággal összefüggő hazai és nemzetközi konferenciák szervezésében. Szakosított intézményein, a civil, a gazdasági és a tudományos terület szereplőivel kialakított együttműködéseken keresztül támogatja a kibertér biztonságos használatát célzó és figyelemfelhívó médiakampányokat, valamint a kiberbiztonsági gyakorlati tudást átadó honlapok működtetését.

Az oktatás és kutatás-fejlesztés terén Magyarország kiemelt figyelmet fordít arra, hogy az általános, a közép- és felsőoktatásban, valamint a szakmai továbbképzésekben a kiberbiztonság szakterülete integrálódjon az informatika oktatásába. Speciális képzési formát igényel a kormányzati tisztviselők alap- illetve továbbképzése, annak érdekében, hogy az informatika

szakterületen dolgozó kormányzati tisztviselők megfelelő tudás birtokában képesek legyenek az e-közigazgatást egyre szélesebb körben alkalmazó magyar közigazgatás elektronikus információs rendszereinek működtetésre. Magyarország stratégiai partnerség kialakítására törekszik azon egyetemi és akadémiai kutatóhelyekkel, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását.

A stratágia alapján Magyarország a kiberbiztonság lényegi elemének tekinti a gyermekek egészséges fejlődését lehetővé tevő környezet kialakítását és fenntartását, melyet minden érintett területen prioritásként kezel, megvalósítva a Gyermekbarát Internet Európai Stratégiájának célkitűzéseit. A gyermekvédelem területén kiemelt partnerének tekinti az online gyermekvédelem terén eredményeket elért civil szervezeteket.

Az üzleti motivációs rendszerek kialakítása kapcsán a stratégia kiemeli, hogy az informatikai és hírközlési közbeszerzések kiberbiztonsági követelményeinek meghatározása során Magyarország abban érdekelt, hogy azok a lehető legmagasabb szintű kiberbiztonsági védelem kialakítására ösztönözzék a közbeszerzéseken résztvevő informatikai és hírközlési eszközgyártókat és szolgáltatókat, kiemelt hangsúlyt fektetve a nemzetközi biztonsági tanúsítási szabványoknak való megfelelésre. A magyar kormány törekszik egyben arra, hogy a gazdasági élet szereplőivel közösen dolgozzon ki olyan ösztönző intézkedéseket a gazdasági élet szereplői számára, amelyek a kiberbiztonság fokozását célozzák.

A Nemzeti Kiberbiztonsági Stratégiában meghatározott feladatok ellátására munka- és intézkedési terv készült el, amelynek végrehajtását a Miniszterelnökség irányítása alatt álló Nemzeti Kiberbiztonsági Koordinációs Tanács irányítja és ellenőrzi. A munka- és intézkedési tervben meghatározott feladatok és mutatószámok követik az Európai Hálózati és Információ Biztonsági Ügynökségnek a nemzeti kiberbiztonsági akciótervekre vonatkozó ajánlását.

AZ ADATVÉDELMI HATÓSÁGOK SZEREPE: JOGSZERŰSÉG ÉS JOGELLENESSÉG HATÁRA AZ ADATOK KEZELÉSE SORÁN

Szabó Endre Győző

A Nemzeti Adatvédelmi és Információszabadság Hatóság képviseletében arról kívánok szólni, hogy hol húzódik a ránk leselkedő kockázatok kivédése érdekében felhasznált adatok kezelése kapcsán a jogszerűség és a jogellenesség határa. Ésszerűen adódhatna a válasz, hogy a jogszerűség és jogellenesség határát éppen a jog jelöli ki. A bemutatandó példák és az összetett társadalmi viták azonban arra mutatnak rá, hogy a jogalkotó által nem egyetlen tollvonással eldönthető problémákról van szó. Gyakran érezhető törésvonal látszik húzódni már a különböző megközelítések között is. Úgy tűnik, mintha a kiindulópontok is eltérőek lennének.

Azok a kollégák, akik most ennek az eseménynek a biztonságáért felelnek, nyilvánvaló, hogy akkor fognak fellélegezni, ha a napot úgy zárhatják, hogy minden állami vezető, résztvevő biztonságban elhagyta az épületet, a vacsora után biztonságban hazaért, nem kerülnek elő gyanús csomagok, és minden további incidens nélkül zárult a konferencia. Logikus az a felvetés, hogy az egyének szűk értelemben vett biztonsága nélkül nincs is értelme az emberi jogok kiteljesedéséről beszélni, hiszen az, akinek a léte veszélyben forog, nehezen tudja szabadságjogait gyakorolni. Kétségtelen ugyanakkor, hogy az itt és most feladatain túl vannak az ember szabadságjogaival kapcsolatban más megfontolások is. Akkor, amikor az itt és most biztonsága érdekében szükséges korlátozások túlzónak tűnnek, méltán merül fel a kérdés: kínálja-e az adott esetben szűkülő szabadságunk azt a kibontakozási lehetőséget, amely az emberi méltóságból fakad, illetőleg az emberi lét lényegét jelenti? Marad-e tér az egyén tehetségének, emberi lehetőségeinek kibontakozására, amely túlmutat az itt és most kérdésén? Olyan kibontakozási lehetőségekről, az ember alaptermészetéből fakadó szabadságigényről van szó, amelyért a történelem során sokan képesek voltak életüket áldozni.

Nyilvánvaló, hogy mind a két említett megközelítés legitim, hiszen közösen őrzött értékeink védelmét tűzik ki célul. A különbség leginkább a hangsúlyok között húzódik. Érdemes ennek a törésvonalnak a mentén elemezni néhány vitát az elmúlt évekből, amelyek rámutatnak arra: a jogszerűség és jogellenesség határát sokszor nehéz megtalálni.

Adatmegőrzés

Az Európai Unió által előírt adatmegőrzési kötelezettség értelmében a tagállamok hat és huszonnégy hónap közötti időtartamra írják elő a telekommunikációs szolgáltatást nyújtók számára a forgalmi adatok megőrzését. Nincs szó a kommunikáció tartalmának, csupán a forgalmi adatoknak a megőrzéséről. A jogszabályt az európai adatvédelmi biztos az Eu-

ropai Unió által valaha megalkotott legerőteljesebb jogkorlátozással járó jogszabályának minősítette. A tagállami átültetés nem volt zökkenőmentes, tudjuk, hogy több országban, így például Németországban, Csehországban, Romániában alkotmányellenesnek ítélték az átültető jogszabályokat.

Az irányelv átültetése Magyarországon is vitát váltott ki. Közismert, hogy Magyarországon az adatmegőrzés szükségességével kapcsolatban jelentős esemény volt a romagyilkosságok feltételezett elkövetőinek kézre kerítése. Az adatmegőrzés szükségességét a közvélemény előtt nagyban alátámasztotta a romagyilkosságok felderítése, amelyre nem kerülhetett volna sor (vagy legalábbis nagyobb nehézségek árán kerülhetett volna csak sor), ha az elektronikus hírközlési szolgáltatók által megőrzött adatok nem állnak a nyomozó hatóság rendelkezésére. Az adatmegőrzés tehát egy olyan területnek tűnik, ahol hosszú évek vitái és tapasztalatai nyomán lassan nyugvópontra jutunk. Az egyén magánszférájáért aggódók természetesen továbbra is némi idegenkedéssel és gyanakodással tekintenek a megőrzési kötelezettségre, de várhatóan ez a vita lecseng a következő években. Sok múlik azon is, hogy fény derül-e a tárolt adatokkal való esetleges visszaélésekre. Bízunk abban, hogy a tárolt adatokat csupán a jog keretei között, a jogalkotó által meghatározott célokra használják fel.

PNR (Passanger Name Records) adatok kezelése

A légi utasok adatainak bűnüldözési célból történő felhasználása szintén tipikus példája az elvi természetű vitáknak. A bűnüldöző szervek annak fontosságát hangsúlyozzák, hogy szélesebb körű adatokból részletesebb elemzéseket tudnak elvégezni a fennálló kockázatokra nézve, ilyen módon pedig a biztonság erősíthető. A magánszféra védelmében fellépők azt a kérdést teszik fel, hogy csupán azért, mert valaki repülőre száll, miért kerül automatikusan a bűnüldöző szervek látókörébe? Miért kell a rájuk vonatkozó adatokat széles körben kezelni? Az adatkezelés számos körülménye vitás lehet az érintett adatok körétől kezdve a megőrzés idején át az adatokhoz hozzáférő hatóságok köréig és a felhasználás lehetséges céljáig. Azt azonban senki sem vitatja, hogy a repülés különlegesen veszélyes üzem, a közlekedési nemek között a leginkább kitett a terrorista fenyegetéseknek, és ezért az átlagosnál erősebb kontrollt igényel. Az Európai Unió jelenleg tárgyalja a PNR adatok európai kezelésével összefüggő irányelvet. Arra számítunk, hogy lesznek vitáink, sőt, hosszúra nyúló vitáink európai szinten is e kérdés kapcsán. Abban azonban teljes az egyetértés, hogy a repülés biztonsága magától értetődően prioritást élvez, ennek jegyében kell vitás kérdéseinket rendezni, ideértve a személyes adatok kezelésének szabályait is.

Közterületi megfigyelés

A közterületi térfigyelés szerte a világon viták kereszttüzében áll. Megszűnik-e a magánszférához való jog azáltal, hogy olyan területre lépünk, ahol egyébként mások előtt jelenik meg az egyén? Ha nem, mi a terjedelme ennek a „nyilvános magánszférának”? A leggyakoribb kérdés, amelyre a legritkábban kapunk pontos és számokkal alátámasztott választ: mennyit javít a köz biztonságán a közterületen elhelyezett kamera? Javítja-e országos szinten a bűnügyi statisztikákat? Csökken-e a bűnözés által okozott társadalmi költség, vagy a költség azonos marad, egy átstrukturált bűncselekményi statisztika mellett?

Szintén kérdés, hogy mi történik a kamera képét közvetítő monitor mögött? Jut-e elég energia a bűnüldöző szerveknél arra, hogy minden egyes jogsértés esetén eljárjanak? Ha erre nem jut elég erőforrás, vajon mi alapján döntenek a szankcionálandó, illetve adott esetben következmény nélkül maradó cselekmények között? Objektív alapokon tud-e maradni a különbségtétel? Ha ez nem érvényesül, milyen intézkedésekkel szavatolható mégis, hogy a bűnüldöző szervek eljárása minden tekintetben diszkrimináció nélküli maradjon? Az adatvédelem nyelvén szólva: mi garantálja azt, hogy a különböző adatalanyokról rögzített azonos adatok azonos következménnyel járnak az egyes egyénekre nézve? Olyan kérdések ezek, amelyeket érdemes észben tartani, keresni rájuk a választ, és arra számíthatunk egyébként, hogy rendszeresen találkozni fogunk ezekkel a felvetésekkel az elkövetkezendő években. A közterületi térfigyelés jövőjét az egyre inkább összekapcsolódó rendszerek jellemzik. Az egyes műveletek összetettebbé válása nem véletlenül irányítja a jogszerű adatkezelés határai iránt érdeklődő szakértők figyelmét a közterületi térfigyelés felé.

Közösségi oldalak

A közösségi oldalakon való regisztráció, az ebből fakadó kérdések és problémák ma már nem jelentenek újdonságot. A közösségi hálókon nyilvánosan elérhető adatok révén az egyénre leselkedő kockázatok széles körben megvitatottak ma már. Adatvédelmi jogi szempontból mégis nagyon érdekes kérdésről van szó: az egyén önként kíván egy virtuális közösség tagjává válni, ugyanakkor az ott feltüntetett adatai a virtuális közösség „alkalmi látogatói” számára is elérhetővé válnak. Lehetőség van természetesen különböző „privacy beállítások” révén egyfajta virtuális remeteként tengetni virtuális napjainkat, de ez a fajta közösségi lét mégis csak kevés változatosságot ígér. Minél nyitottabb az egyén, annál több közösségi élményre számíthat a virtuális térben. De mi keresnivalója van adott esetben a nyomozó szerveknek, vagy mondjuk a leendő munkáltatónak a virtuális közösségben? Adatvédelmi szempontból mi csak arra tudjuk felhívni a figyelmet, hogy senki által nem hitelesített információkat fog találni a nyomozó, a munkáltató, amikor az egyes adatlapokat böngészi. Az adatok minősége tehát kétséges. Egyébként a nyilvános adatok jogszerűen hozzáférhetőek bárki által, adatvédelmi jogi szempontból ezzel kapcsolatban nem merül fel további kérdés. A nyilvános adatok sem használhatóak fel azonban korlátozás nélkül: a személyiség védelmének jogi eszközei akkor is rendelkezésre állnak, ha adott esetben a személyes adatok védelmét szolgáló szabályok nem nyújtanak már védelmet az egyén számára.

Milyen szerep hárul az adatvédelmi hatóságokra az említett ügyek kapcsán?

Az adatvédelmi hatóságok nem jogalkotó, hanem jogalkalmazó szervek. Véleményüket meghallgatják és ideális esetben figyelembe veszik a jogalkotás során, ugyanakkor a jogalkotást követően nincsen már mozgásterük: a jogalkotó által tételezett jognak kell érvényt szerezniük. Így van ez a magyar adatvédelmi hatóság, a Nemzeti Adatvédelmi és Információszabadság Hatóság esetében is, amely 2012. januárjában alakult. A magyar jogalkotó az Alaptörvény megalkotása révén lezárta az adatvédelmi ombudsmani időszakot, és helyébe az európai társhatóságok sorába illeszkedő hatóságot hozott létre. Az új hatóság az ombudsmani mozgástérnél erősebb jogosítványokkal felruházva őrködik a személyes adatok védelméhez, valamint a közérdekű adatok megismeréséhez való jog érvényesülése felett.

Az adatvédelmi hatóság az új szabályok szerint jogosult hatósági eljárást lefolytatni, tehát

a közigazgatási eljárás általános szabályait alkalmazza munkája során. Azokban az esetekben indul formális közigazgatási eljárás, amelyekben a személyes adatok védelme ezt indokolttá teszi. Egyéb esetekben a hatóság ombudsmani típusú eljárást indít, úgynevezett vizsgálati eljárás keretében jár el. Akkor alkalmazza ezt a „puhább" eljárást, amikor remélhető, hogy az érintett által panaszolt ügy hatósági fellépés nélkül is orvosolható.

A vizsgálati eljárás az elnök döntése alapján bármikor átválthat hatósági eljárásba. A hatósági eljárás mindig hivatalból indul, az érintettnek közvetlenül nincs jogosultsága hatósági eljárást indítania. A hatósági eljárás során érvényesül a közigazgatási eljárás minden részletszabálya: határidőkkel, formális bizonyítási eljárással, határozathozatallal és természetesen a jogorvoslati lehetőséggel. A magyar adatvédelmi hatóság határozatai csak a törvényszék előtt támadhatók meg.

Határozatában a hatóság végső soron bírságot is kiszabhat. Ha áttekintjük az adatvédelmi hatóság által hozott határozatokat, látjuk, hogy a legsúlyosabb büntetést egy kibertérben megvalósult jogellenes adatkezelés miatt szabtuk ki. Az adatkezelő ingatlan portált üzemeltetett, ahol 30 napos, állítólag ingyenes hirdetési időszakot követően az ingatlan hirdetés elhelyezéséért már fizetni kellett. A hozzánk eljutott beadványok egybehangzóan arról számoltak be, hogy nem tudták a hirdetést törölni, akár a 30 napos időszakban voltak, akár már azon túl. Ha pedig valaki nem rendezte tartozását, akkor a törlés jogával már nem is élhetett, így viszont újabb és újabb időszakok után kellett fizetnie. Az eset kapcsán sokan bűncselekmény gyanúját említik, és bár az adatvédelmi hatóság ebben a kérdésben nem dönthet, a nyomozó hatóságot tájékoztattuk az esetről. Az ügy pikantériája, hogy a szerver Szlovákiában található, Révkomáromban. Bár az adatkezelő várhatóan vitatja a magyar joghatóság meglétét, úgy ítéltük meg, hogy nem férhet kétség a magyar adatvédelmi hatóság jogosultságához az eljárás lefolytatására és végső soron a bírság kiszabására. Figyelembe vettük, hogy szinte kizárólag magyarországi ingatlanokat hirdettek a honlapon, az adatokat magyarországi gépekről, magyar polgárok töltötték fel; ezen túl az ingatlanok iránt értelemszerűen zömmel magyar felhasználók érdeklődtek, mindezek alapján pedig a magyarországi adatkezelés megállapíthatósága már nem volt kérdés, hiszen ezeket a műveleteket a hazai szabályozás önálló adatkezelési műveletekként nevesíti. A határozatot az adatkezelő megtámadta a bíróság előtt, és a bíróságnak a joghatóság kérdésében is állást kell majd foglalnia[1]. Mi a magunk részéről az adatalanyok helyzetét rontó körülményként értékelnénk, ha ilyen ügyekben a bíróság azt mondaná ki, hogy a hatóság nem járhat el, ha az adatkezelésnek bizonyos műveletei az országhatáron kívül esnének.

Következtetések

Amint látjuk, számos kérdés áll még nyitva a konferencia által tárgyaltak közül. A bűnözés elleni küzdelem, a biztonságunkat közvetlenül fenyegető körülmények erőteljes állami és adott esetben nem állami kontroll után kiáltanak, egyszersmind ezen intézkedések tervezése és végrehajtása során nem áldozhatunk fel olyan értékeket, amelyek az egyén szabadságától és szabadságérzetétől elválaszthatatlanok. Az eredetileg feltett kérdés, hogy hol húzódik a jogszerű és a jogellenes adatkezelés határa, nehezen válaszolható meg a jog eszközeivel, esetről

1 Az ügyben indult bírósági eljárás várhatóan 2013-ban zárul le

esetre vitázva juthatunk közelebb a válaszokhoz. Az említett példák azt mutatják, hogy a viták nem csak szükségesek, hanem képesek is arra, hogy sokáig reménytelenül ellentétes álláspontokat végül megbékítsen egymással. A társadalmi viták bonyolultak, az Európai Unió szintjén még bonyolultabbak, ezért türelemre van szükség minden résztvevő oldalán. Abban azonban bizonyosak lehetünk, hogy amennyiben nem hagyjuk magunkat a gyakran változó közhangulattól befolyásolni, nem engedjük, hogy akár a vita tárgyát, akár annak menetét terrorista vagy bármilyen fenyegetettség kívülről befolyásolja, akkor a vitáink, ha hosszúra nyúlnak is, olyan eredményhez vezetnek, amely megóvja közösen vallott értékeinket, mind rövid, mind hosszú távon. A jog nyelvén szólva: ha a vitákat nyugodt légkörben, pillanatnyi kétségek és hangulatok befolyása nélkül folytatjuk le, akkor bizonyosak lehetünk afelől, hogy vitáink és megoldásaink alkotmányos mederben maradnak.

AZ OKOSTELEFONOKKAL KAPCSOLATOS KIHÍVÁSOK, VESZÉLYEK

Szabolcsi Zsolt

Napjainkban a számítástechnikai eszközök és berendezések használata és alkalmazása mindennapos tevékenységgé vált. Gyakorlatilag elengedhetetlen kellékei az élet minden területén végzett tevékenységünknek. Ezen eszközök palettája rendkívül széles, kezdve a személyi számítógépektől az okostelefonokig. Az információs társadalmak korát éljük. Az egyre nagyobb társadalmi igények miatt szinte már nincs is olyan eszköz, mely ne tartalmazna valamilyen mikroprocesszort, de inkább mondhatni mikroszámítógépet, amelyek valamilyen – legalább minimális szintű – szoftveres döntéshozatali mechanizmust alkalmaznak.

A számítástechnikai eszközök és rendszerek használatával drasztikus mértékben nőtt meg az információáramlás, melyek vezetékes és vezetéknélküli technológia alkalmazásával kerülnek továbbításra. Korunk információs forradalma, a közösségi oldalak elterjedtsége és rendszeres használata új lehetőségeket nyitott meg a társadalom számára, melyeket nem csak maguk a felhasználók, hanem a különféle szervezetek – beleértve a titkosszolgálatokat és rendvédelmi szervezeteket – is felhasználnak az információk beszerzésére. Az információs forradalom azonban nem csak a legális felhasználást teszi lehetővé, hanem lehetőséget és teret ad a számítástechnikai rendszerek, hálózatok, alkalmazások feltörése útján bűncselekmények, illetve információk megismerésére, gyűjtésére, módosítására.

A mobil telefonok vonatkozásában meg kell ismerni egy új fogalmat, ez pedig az okostelefon fogalma. Jelenleg nincs konkrét fogalmi definíciója, de gyakorlatilag ide sorolható minden olyan telefon, melynek a műszaki paraméterei egy számítógép képességeivel felérve képesek az általános számítási feladatok ellátására. Az okostelefonok forradalma 2007-ben indult meg az iPhone megjelenésével, noha korábban is léteztek már okostelefonok. Az első okostelefonnak a 2002-ben megjelent Nokia 7650-es készülék tekinthető, majd az ezt követően megjelent további modellek, melyek symbian operációs rendszerrel és S60 felülettel működtek. Ezek a készülékek képesek voltak multimédia tartalom lejátszása mellett számos alkalmazás használatára, melyet a programozók és alkalmazásfejlesztők részére kiadott fejlesztői környezet biztosított. Számos, addig ismeretlen funkciók kezelésére készített alkalmazás látott napvilágot. Gyakorlatilag szinte az összes korszerű okostelefon-platformra fejlesztett alkalmazás elődei már ekkor megjelentek.

A korai okostelefonok elterjedését azonban gátolta a relatív bonyolult használat és az ismeretlenség, illetve az igények hiánya. A közösségi oldalak és egyéb szolgáltatások gyerekcipőben jártak, vagy még nem is léteztek, így a társadalomnak nem volt még igénye ezen eszközök képességeinek kiaknázására.

Az áttörést az iPhone készülék hozta el. A kor igényeinek eleget téve rendkívül jól és egyszerűen használható felhasználó-barát kezelőfelület, a kapacitív érintőképernyő által biztosított, átgondolt felhasználó-interfész és a látványos, gyors operációs rendszer mögé

tett alkalmazásbolt nem várt sikereket hozott, ezáltal megváltoztatva az egész mobiltelefon iparágat.

A rendkívüli sikert meglovagolva újabb modellek jelentek meg és a megváltozott igényekre azonnal reagáló IT cégek egymást túlszárnyalva iszonyatos mértékű fejlesztésbe kezdtek ezen a területen, szinte elsöpörve minden korábbi rekordot. Az Apple által fejlesztett iPhone által használt iOS mellé felzárkózott a Google által fejlesztett Android platform, mely egyes területeken túl is szárnyalta azt. Az elmúlt öt év alatt rendkívül nagyot fordult a mobiltelefonok világa. Az okostelefonok mellett megjelentek a tablet PC-k (továbbiakban: tablet) és mára már a phablet-ek is a kategória részét képezik.

Az okostelefonok esetében HD , majd napjainkra a full HD felbontású megjelenítés is teret hódított. A tárolható és kezelt adatok tekintetében az okostelefonok felérnek egy kisebb tárolási kapacitású, de közepes számítási teljesítményű számítógéppel. A hagyományos mobiltelefonokkal ellentétben az okostelefonok több magos processzorral, beépített grafikus processzorral, több csatornás GPS modullal (GPS, Glonass), Wi-Fi, Bluetooth, NFC hálózati és 2G, 3G, LTE mobilkommunikációs képességekkel

A hagyományos mobiltelefonok, illetve az okostelefonok GSM-rendszerű adatforgalma (klasszikus működés) esetében a titkosszolgálatok megfelelő képességekkel rendelkeznek a lehallgatás és a GSM rendszeren történő egyéb adatforgalom ellenőrzése tekintetében.

A mobiltelefonokkal kapcsolatos visszaélési lehetőségek terén meg kell említeni az illegális és legális információgyűjtési lehetőségeket. Nyilvánvaló, hogy egy adott ország hatóságai a saját törvény-rendszere alapján felhatalmazást nyer valamilyen módon az információk megszerzésére (lehallgatás, híváslista, telefonok adatainak lementése stb.). Azonban nem csak a hatóságok érdekeltek az információk megszerzésében, hanem magánszemélyek és magánynyomozó-irodák és bűnelkövetők, bűnszervezetek is.

A hagyományos mobiltelefonok esetében a telefonon tárolt adatok megszerzése szakértelmet és megfelelő eszközt igényelt. Ahány telefon, annyiféle csatlakozó, kábel és adattárolási megoldással kellett szembenézni.

A hagyományos és az okossá vált mobiltelefonok tekintetében a megszerezhető adatok az alábbi táblázatban kerültek összehasonlításra

1. táblázat. Megszerezhető adatok köre

Hagyományos telefon	Okostelefon
Hang SMS, MMS Médiafájlok	Hang SMS, MMS Médiafájlok Dokumentumok GPS adatok SNS adatok E-mail és egyéb fiókok adatai Felhasználói jelszavak Egyéb adatok

A hagyományos telefonokkal történő összehasonlítás fontos ténye az, hogy a készülékekből történő közvetlen adatszerzés szakértelmet és megfelelő csatlakozási felületet kívánt. Az okostelefonok rendkívül felhasználóbarát kezelőfelülete és az egységes csatlakozási felület az adatszerzést, adatkinyerést, adattovábbítást nagyon könnyűvé és egyszerűvé tette.

Az okostelefonokkal kapcsolatban meg kell említeni a közösségi oldalakat is, melyek önmagukban is kihívást jelentenek a rendvédelmi hatóságoknak, azonban az okostelefonok elterjedésével ez kihívás sokkal fenyegetőbbé és nagyobbá vált. Gyakorlatilag az összes okostelefon „személyes feketedobozként" is értelmezhető. Egy aktív okostelefon felhasználó egyrészt nagy adatforgalmat bonyolít le, melynek ellenőrzése szükséges lehet. Továbbá az okostelefonokon rendkívül sokrétű és nagy mennyiségű adat tárolható, és kerül is tárolásra, mely adatok megszerzése lehet rendvédelmi, titkosszolgálati és természetesen bűnelkövetési érdek is.

Az okostelefonok elterjedésével új fenyegetésekkel szembe kell nézni. A teljesség igénye nélkül ilyenek lehetnek:

- Érzékeny adatok szivárgása az IT rendszerből.
- Belső adatok kijuttatása
  - beépített, bővített memórián keresztül,
  - azonnal az internetre (felhőbe),
  - közvetett módon közösségi oldalakra,
  - egyéb tárhelyekre (ftp, torrent, stb.),
  - fényképek azonnali kijuttatási lehetősége.
- Trójai és más, vírusok, férgek szándékos, vagy szándékolatlan bejuttatása a belső rendszerbe .
- Ellenőrzés nélküli csatlakozás.
- Könnyű elkerülni a lebukást.

A közösségi oldalakon fellelhető információk megismerése és elemzése számos lehetőséget rejt magában. Nem csak a felhasználók által megadott szöveges adatok, hanem a feltöltött fénykép(ek) és videó-felvételek alapján is következtetéseket lehet levonni azok személyiségére, kapcsolati körének feltérképezésére, érdeklődési körére vonatkozóan.

A teljesség igénye nélkül néhány példa:

- háttér körülmények: anyagi források (milyen a lakás berendezése, műszaki eszközök, hová ment nyaralni és az kb. mennyibe kerül stb.);
- fontos kapcsolatok: az emberek azzal szerepelnek közös fényképen, akik számukra valamilyen oknál fogva fontosak (barátok, barátnők, közeli munkatársak stb.);
- érdeklődési kör: milyen irányultságú érdeklődése, mi foglalkoztatja (a videók, tovább osztott fényképek alapján).

A különféle szolgálatok az alábbi törvényi felhatalmazás útján bírói engedély nélkül folytathatják az ilyen irányú adatgyűjtő tevékenységüket.

A közösségi hálózatokból nyert adatok egy része az OSINT[1] tevékenységhez kapcsolódik, de egyes adatok megismerése és megszerzése Magyarországon TIGY tevékenység során külső engedély meglétét igényelheti.

A közösségi oldalakból szerzett információ, mint hírszerzés nem csak a felhasználói ada-

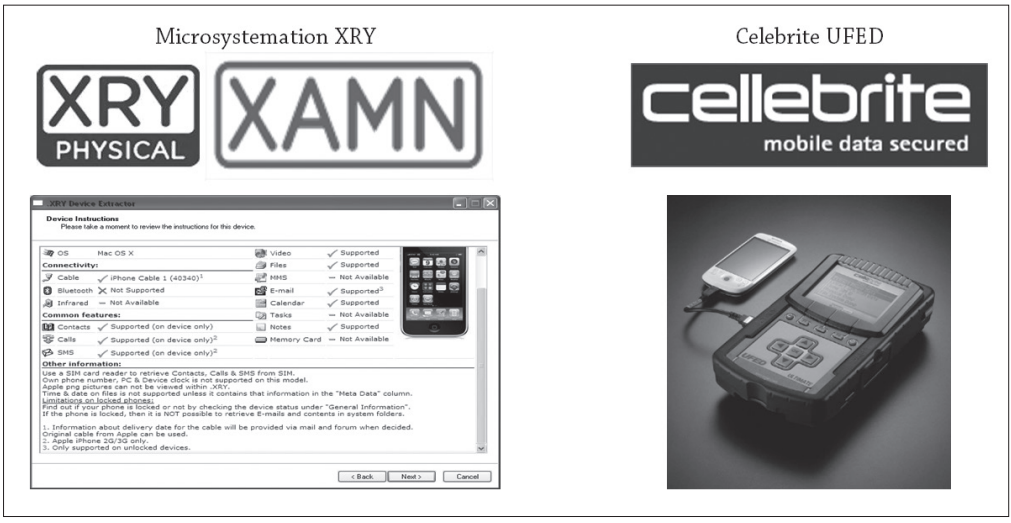
1 OSINT = Open Source Intelligence (Nyílt Forrású Hírszerzés)

tok, hanem az egyes fórumok tekintetében csoportok vonatkozásában is lehetőséget nyújt az adott csoport tevékenységének, céljának és jövőben tervezett csoportos tevékenységük megismerése, és adott esetben arra történő felkészülés szempontjából.

Természetesen itt meg kell jegyezni, hogy a közösségi hálózatokból történő információgyűjtés nem kizárólagosan a titkosszolgálatok tevékenysége. Ezt az „információ forrást" napjainkban a rendvédelmi szervek, magáncégek és magánszemélyek is rendszeresen alkalmazzák.

A hagyományos készülékeken közvetlenül tárolt adatokhoz történő hozzáférés esetében kijelenthető, hogy készülék típustól, gyártótól függően különböző csatlakozó felületek, protokollok és eljárások alkalmazásával az adatok kinyerése sokszor nehézkesen, vagy egyáltalán nem oldható meg. A telefonok adatainak kinyerésére azonban két ismert (nagy), jól alkalmazható szakértői eszköz és szoftvercsomag létezik.

1. kép. Mobilszakértői alkalmazásaok



A fenti két szakértői alkalmazás támogatja a hagyományos és az okostelefonok adatainak kinyerését, melyhez a szükséges támogatás mind a folyamatos szoftverfejlesztésben, mind a készülékekhez történő csatlakozási eljárások, csatlakozók, átalakítók tekintetében biztosítva van.

A NEMZETI BIZTONSÁGI FELÜGYELET KIBERVÉDELMI TEVÉKENYÉGE

Zala Mihály

A Nemzeti Biztonsági Felügyelet 1999. január 1-én jött létre Magyarország titokvédelmi szervezeteként, azzal a céllal, hogy a NATO titokvédelmi hatósági szerepkörét betöltse. A Felügyelet feladatai 2003-ban, Magyarország EU csatlakozása előtt egy évvel kiegészültek az EU titokvédelmi hatósági funkciókkal, 2007-ben pedig a Felügyelet a nemzeti titokvédelmi szerepkört is átvette.

A 2009-es év ismét nagy változást hozott a Felügyelet életében a minősített adat védelméről szóló 2009. évi CLV. törvény elfogadásával, amely alapjaiban újraszabályozta a honi titokvédelem struktúráját. A törvény 2010. április 1-jei hatályba lépése óta a Felügyelet egyfajta „titokvédelmi főhatóságként" működik a Közigazgatási és Igazságügyi Minisztérium szervezeti keretében.

Ugyanakkor a Felügyelet fejlődése azóta sem állt meg: a 2010-es kormányváltás után Magyarországon is megindult az törekvés, hogy más EU-s és NATO-s tagállamok mintájára hazánkban is nagyobb hangsúlyt kapjon a kibervédelem. Ebben nagy szerepet kapott a Nemzeti Biztonsági Felügyelet, ugyanis a Felügyelet a klasszikus titokvédelmi funkciókat ellátó szervezeti egységein túl 2011 óta már egy kibervédelmi egységgel is rendelkezik. A Cyber Defence Management Authority (a továbbiakban: CDMA) egy 15 fős szervezeti egység a Felügyeleten belül, melynek feladata a magyarországi, azon belül pedig elsősorban a kormányzati információs rendszerek sérülékenység vizsgálata, valamint a létfontosságú infrastruktúrák kibertámadásokkal szembeni felkészítése.

Ezen feladatkör-bővítés indoka az, hogy a kibervédelmi megelőző funkciók kiépítése során kiderült: napjainkban a klasszikus titokvédelmi feladatok a nemzetbiztonsági kockázatoknak legfeljebb 10 százalékát fedik le. Egy kibertámadás esetén ugyanis nem az a legnagyobb kockázat, hogy a támadók bejutnak egy adott rendszerbe, és abban kárt tesznek, hanem az, hogy ott jogosulatlanul hozzáférhetnek védett dokumentumokhoz, anélkül, hogy ezt a rendszer üzemeltetői valós időben realizálnák. Ez nagyobb kihívást jelent, mint a klasszikus titokvédelmi feladatok.

A Felügyelet nem fegyveres vagy rendvédelmi szerv, hanem egy kormánytisztviselőkből álló szervezet, amely alapvetően civil jelleggel bír. Ennek a szerkezeti felépítésnek vannak előnyei és természetesen hátrányai is. Előnye, hogy a Felügyelet a társadalom azon rétegeivel is kialakíthat kapcsolatot, ahol a fegyveres, vagy rendvédelmi szerveknek ez szinte lehetetlen lenne. Ilyen például a hackerekkel való kapcsolat is: néhány évvel ezelőtt a hackereket még üldözték tevékenységük miatt, mára azonban egyre több szervezet igyekszik a saját hasznára fordítani a hackerek tudását, és egyre több európai országban fordul elő az a tendencia, hogy már a kormányzati munkába is bevonják a hackereket. Ezen

gyakorlat hazai átültetéséhez azonban szükséges a megfelelő kommunikációs csatornák kiépítése a kormányzat és hackerek között, amihez nagyban hozzá tud járulni a Felügyelet a saját eszközeivel.

Noha a Felügyeleten belül működik egy tanúsító osztály is, amely rejtjelző eszközök hatósági tanúsítványát állítja ki, sajnos a mindennapi használatú szoftverek titokvédelmi vizsgálatával Magyarországon még senki sem foglalkozik. Pedig komoly zavarokat okozhat akár a Windows 2000 használata is, amelyet 2003 óta már nem támogat a Microsoft sem, ennek ellenére számos helyen, információ és tudás (illetve beruházási lehetőségek) hiányában, a mai napig használják. A megfelelő szoftver kiválasztásában a szervezeteknek segíthet a NATO nemrégiben közreadott listája, amelyen szerepelnek a NATO által ajánlott szoftverek és biztonsági beállítások.

Napjaink kiber-problematikájának egyes elemei

Az internetes bűnözés

Mára már az egyik legkomolyabb kihívást jelenti a bűnüldöző szervek számára az internetes bűnözés. Az éves bevétel, amelyet az internetes bűnözés termel, folyamatosan növekszik, csak erre az évre 400 milliárd dollárnyi bevételt prognosztizáltak. Noha sokan azt gondolják, hogy a pornográfia ennél jóval nagyobb bevételt hoz, de valójában nagyságrendekkel elmarad ettől az összegtől.

A kibertérben több mint 5 milliárd eszköz van használatban, és körülbelül 2 milliárd felhasználóról beszélhetünk, de egyes előrejelzések szerint ez a szám 2022-re már 3 milliárdra fog emelkedni. Jelenlegi adataink szerint naponta átlagosan 300 millió kompromittációra kerül sor, megközelítőleg napi 1 millió felhasználót érintve. Egy kompromittált információ átlagos becsült anyagi kára vagy következménye pedig 133 dollárnál kezdődik.

Az ’ (aposztrof)

Az ’ (aposztrof) szűrésével sok problémát el lehetne kerülni, azonban ezt a jelet sem a rendszergazdák sem pedig a rendszerek nem szűrik. A Felügyelet nemzetközi szervezeteknél folytatott munkái során is számtalan alkalommal tapasztalta, hogy sajnálatos módon az ’ (aposztrof) szűrés hibái mindenhol megvannak.

Ez a problémakör nagyszerűen ráirányítja a figyelmet arra, hogy a jelentős következményekkel járó kopromitációkból eredő károk túlnyomórészt elkerülhetőek lennének, ha a rendszerek üzemeltetői valóban rendelkeznének a legalapvetőbb szakmai ismeretekkel, és azokat a gyakorlatban is használnák, különösen az ún. webes sérülékenységek tekintetében.

A fejlesztések

A rendszerfejlesztők nem egyedi fejlesztéseket árulnak, hanem sajnálatos módon ugyanazt a terméket adják el több vevőnek is egyedi fejlesztésként. Így viszont csak használat közben derül ki a gyanútlan megrendelő számára, hogy nemhogy nem egyedi az általa megrendelt fejlesztés, hanem ugyanaz a motorja, ugyanaz az SQL sérülékenység és ugyanazok a hibák jellemzik, mint

a számtalan, más szervezeteknél kivitelezett, szintén „egyedinek” titulált fejlesztéseket. És ez a probléma nemcsak Magyarországon, hanem külföldön is általánosan jellemző.

A fejlesztéssel kapcsolatban a legnagyobb hiba az, hogy a biztonsági elemeket senki nem tudja, vagy akarja beépíteni a fejlesztés költségvetésébe, mert azok nélkül költséghatékonyabban kivitelezhető a beruházás. Az esetek 90 százalékában a webes szolgáltatások nincsenek tűzfallal védve, és sokszor egy szerveren több szolgáltatás, több honlap is fut, azok összes sérülékenységével együtt, és ha ezek közül csak egy is sérülékeny, akkor már a többi sem lehet tökéletes biztonságban.

A legolcsóbb megoldás természetesen az lenne, ha már a fejlesztés, vagy még inkább a tervezés során integrálnák a rendszer biztonsági elemeit, mert amikor a rendszer már üzemel, akkor már késő a biztonságot figyelembe venni biztonsági szempontokat és a rendszerbe beépíteni. Ez azért is kiemelendő, mert gyakran EU-s forrásokból valósul meg az informatikai rendszerfejlesztés finanszírozása, és ezeket a rendszereket öt évig üzemben kell tartani. Tehát ha a fejlesztés eredményeként egy nem biztonságos rendszer jön létre, akkor azt még öt évig kell használni, ellenkező esetben a forrásokat vissza kell fizetni.

A motiváció mibenléte

A területet jellemző legjelentősebb probléma legegyszerűbben egy fikcióval mutatható be. Képzeljünk el egy országot, ahol sok informatikai rendszer működik. Képzeljük el, hogy ezek a rendszerek egymással össze vannak kapcsolva, ezek mindegyike, kisebb-nagyobb módon ugyan, de sérülékeny. Tételezzük fel, hogy az informatikusok nyereségszerzés céljából visszaélnek a tudásukkal és igyekeznek rávenni vezetőiket arra, hogy minél nagyobb összeget költsenek el a fejlesztésekre. Tegyük fel, hogy a politikusok sem értenek mindehhez, hiszen manapság még nem mindenkinek kézenfekvő az informatika: a politikusokat félre lehet vezetni ezen a területen, és így nem tudják a megfelelő döntést meghozni, mert nem kapják meg a támogatást ahhoz, hogy jó döntést hozzanak.

Képzeljünk el egy olyan országot, ahol az informatika és információbiztonság a korrupció melegágya, ahol akár százmilliárdok is elfolyhatnak így. Képzeljünk el egy olyan országot, ahol a magáncégek immáron nem a megfelelő fejlesztésekben érdekeltek, hanem abban, hogy lehetőleg minél több politikust és minél több informatikai vezetőt győzzenek meg arról, hogy az általuk forgalmazott rendszereket, és eszközöket vásárolják meg. Nemrégiben egy NATO konferencián vázoltuk fel ezt a fikciót a résztvevőknek, és kértük őket arra, hogy minden aktualitástól mentesen tegye fel a kezét az, aki nem ismer rá a saját országára. Senki sem jelentkezett.

A kiszervezés, azaz „outsourcing”

Amikor az első számítógép megérkezett hazánkba, majd az első munkahelyekre, az emberek elkezdték ezeken az akkor új és korszerű típusú gépeken végezni a munkájukat, aztán a számítógép lassan felváltotta az írógépet és az ún. leírókat. Aztán megérkezett az internet, eljutott az államigazgatásba is, és ma már ott tartunk, hogy nélkülözhetetlen eszköze lett a napi munkavégzésnek. De a 80-as, 90-es évek végén még nem állt még rendelkezésre a tudás az új technikáról, az új eszközökről. Ezért az állam ezeknek a rendszereknek a fejlesztését, üzemeltetését, és karbantartásának feladatát kiszervezte külső cégekhez. Ez hosszú évekig,

gyakorlatilag két évtizedig így zajlott. Igaz, hogy már akkor is voltak néhányan az államigazgatásban, akik értettek az informatikához, de ezeket a feladatokat mégsem rájuk bízták.

Aztán lassan a világ ráébredt arra, hogy a kiszervezés mekkora problémát okozhat. Ez nemcsak hazánkban, hanem Európa más országaiban és Amerikában is így zajlott. A politikusok is rájöttek, hogy ezt a széles feladatkört az államnak saját magának kell ellátnia, legalábbis ami a védelmet illeti. Az államnak viszont nemcsak a hadsereg, a rendőrség és egyéb szervezetek irányítását kell magához vonnia, hanem az informatikai rendszerek védelmének feladatát is. Ugyanez érvényes a NATO-ra és az EU-ra is. És ezek a folyamatok mindenhol megindultak.

Az NBF álláspontja a kezdetektől az volt, hogy a kibervédelem kizárólag állami feladat lehet. Meglátásunk szerint három résztvevő van jelenleg ebben a szférában a piacon, a védelem vonatkozásában: az üzemeltetők, a felhasználók, illetve a harmadik szereplő lenne az állam, vagyis 2011 óta a CDMA megalakulását követően a Nemzeti Biztonsági Felügyelet.

Feladatai ellátása során a Felügyelet ugyanis SQL sérülékenység vizsgálatot végez, megkeresi a rendszerek gyenge pontjait, kiszűri a humán tényezők által generált nagy mennyiségű hibákat, és felhívja a vizsgált üzemeltető figyelmét ezen hibák kijavításának fontosságára, hiszen alapvetően az a Felügyelet álláspontja, hogy a hibák megelőzése lényegesen olcsóbb, mint a probléma bekövetkezte esetén a következmények elhárítása. A megelőzés akár bérből és fizetésből végrehajtható. A Felügyelet azon kollégái, akik sérülékenység vizsgálatával, elemzésével és az ezekre adható válaszok kidolgozásával foglalkoznak, fizetésért dolgoznak. Ezt a feladatot a Felügyelet kollégái látják el, mert a Felügyelet az általános gyakorlattal ellentétben nem köt külsős cégekkel szerződést, akik akár több millió forintért vállalnák el ugyanazt, amit a mi kollégáink bérből és fizetésből ugyanúgy meg tudnak csinálni. Azonban ezzel a kapcsolatban még nem történt meg a jogi szabályozás.

Oktatás, tudatosság növelő képzések

Az egyik legfontosabb téma a kiberbiztonság területén a tudatosítás és a megfelelő oktatás. Húsz évvel ezelőtt, ha valaki kellő szorgalommal rendelkezett, el tudta sajátítani a számítógép kezelésével kapcsolatos alapvető tudást, ma már azonban külön kell foglalkozni az eltérő célcsoportokkal és azok eltérő igényeivel és szükségleteivel, azaz a felhasználókkal, a fejlesztőkkel, az üzemeltetőkkel és a döntéshozókkal.

Ennek a legfőbb oka az, hogy a sérülékenységek az esetek 80%-ban bérből és fizetésből kijavíthatóak. Hogyan lehetséges ez? Az általunk tapasztalt tömeges hibák jelentős részét képzett informatikusok és rendszergazdák követték el. Hiszen hiába biztonságos egy szervezet internetes rendszere, ha az informatikus a főnöke kérésére például hétvégén, azért, hogy ne kelljen bemennie, otthonról, vpn segítségével próbál kiküszöbölni egy hibát. Így azonban, az interneten keresztül kompromittálódhat a cég informatikai rendszere. Vagy egy másik példával élve, szintén hiába jól megkonstruált egy adott védelmi rendszer, ha az informatikus felettese kérésére kikapcsolja a védelmi eszközöket. Ezért nagyon fontos, hogy az informatikusok és a rendszergazdák a lehető legjobban fel legyenek készülve a kritikus helyzetekre, és a lehető legnagyobb tudással rendelkezzenek. Ugyanis ha az informatikusok megfelelően fel vannak készülve, akkor nem kell feltétlenül drága technikai eszközöket vásárolni a védelem érdekében. És éppen ezért nagyon fontos a vezetők képzése is, hogy megértsék a kockázatokat.

Annak érdekében, hogy az informatikusok megfelelő képzésben részesüljenek az NBF alapképzés és egyéb képzések elindítását kezdeményezte a Nemzeti Közszolgálati Egyetemen. A Felügyelet már külföldön is tartott speciális képzéseket, és a tervek között szerepel, hogy a jövőben a veszprémi Pannon Egyetemen lennének képzések a hazai kormányzat illetve piaci szereplől és külföldiek részére is. 2011-ben a Felügyelet együttműködési megállapodást írt alá az egyetemmel erre vonatkozóan.

Fiatalkorúak

A kibervédelmi kérdések tárgyalása során nagy hangsúlyt kell helyezni a gyerekek megfelelő tájékoztatására is. Gyermekeink nap mint nap használják az iwiw-et, a Facebookot, a Twittert, és ezáltal nagy veszélynek vannak kitéve. Fontos, hogy már az általános és középiskolákban is legyen a helye az informatikai és információbiztonsági képzésnek, hogy a gyerekek megtanulják, amit kiraknak az internetre, azt onnan soha többé nem lehet leszedni. Mert ki tudja, melyik szerveren, de az ott fog maradni.

A Nemzeti Biztonsági Felügyelet eddigi és jövőbeni kibervédelmi szerepvállalása

A Nemzeti Biztonsági Felügyelet több oktatási programot is tartott már, továbbá részt vett rendszer- és biztonságerősítő munkákban, projektekben is. A Nemzeti Fejlesztési Minisztériummal folyamatban van a Felügyeletnek több közös projektje is, amelyek célja, hogy a központi gerinchálóra csatlakoztatott rendszerek és több jelentős létfontosságú rendszer vizsgálatára sor kerülhessen. A projekt eredményeként több rendszert is sikerült magasabb biztonsági fokra emelni, de fontos látni, hogy a folyamat még csak most kezdődött el, és egy konkrét vizsgálat megtörténte nem jelenti annak a végét is egyben.

A Felügyelet 2011-ben részt vett a NATO kibervédelmi témájú (NATO Cyber Coalition Excercise) hadgyakorlatán is, amely az első ilyen témájú gyakorlat volt hazánk életében. A gyakorlaton az Alkotmányvédelmi Hivataltól a honvédelmi tárcán át, a katasztrófavédelemig sok magyar szereplő vett részt. A hadgyakorlat módot adott arra, hogy az a kör, amely incidensek kezelésében érintett, vagy érintve lehet, tudjon együtt dolgozni, és kiépítve a szükséges kommunikációs csatornákat ezeknek a tapasztalatoknak később is hasznát vehesse. Az idei hadgyakorlatra, amely ősszel kerül megrendezésre, a Felügyelet munkatársai írják a nemzetközi forgatókönyvek meghatározó részét, illetve készítik elő a technikai kíhívásokat tartalmazó részeket. Ez nagy megtiszteltetés a Felügyelet számára.

Napjainkban gyakran találkozhat az átlag állampolgár is az Anonymous jelenséggel kapcsolatos hírekkel. A legnagyobb kockázatot azonban nem az ilyen és az ehhez hasonló csoportok jelentik, akik kitesznek a honlapunkra valami oda nem illő dolgot, vagy kicserélik a honlap tartalmát. Az igazán nagy kockázat az, amikor nem is látjuk, mit visznek el, vagy milyen tartalmakat tesznek be a szervereinkre, illetve webes szolgáltatásaink közé.

A Nemzeti Biztonsági Felügyelet igyekszik külföldön is szerepet vállalni az informatikai rendszerek biztonságával kapcsolatos irányelvek kialakításában. Ennek érdekében napi kapcsolatot alakítottunk ki az EU-val, és a NATO-val. Ugyanakkor a Felügyelet arra törekszik, hogy együttműködjön mindazokkal, akik segítségre szorulnak az informatikai rendszerek védelme,

vagy a sérülékenység kezelésének témájában. Egy jól működő rendszerhez ugyanis nemcsak a technikai, hanem a már többször említett humán tényezők megfelelő működése is szükségesek.

A Felügyelet a jövőben azt szeretné elérni, hogy a kormány, a felhasználók és a gazdasági élet szereplői a lehető legszorosabban együttműködjenek, mert enélkül szinte lehetetlen megoldani a felmerülő problémákat. Fontos, hogy a gazdasági élet szereplői bátran fejlesszenek, néhány évvel előre is lássanak, és a kormány majd eldönti, hogy melyik fejlesztést veszi igénybe. Ugyancsak egy jövőbeni álom a megfelelő jogi szabályozás kialakítása, vagy az egyes szereplők közötti aktív információcsere megvalósítása. A problémákat csak úgy lehet megoldani, ha feltárják őket egymás előtt. Ha ezek mind megvalósulnának, akkor Magyarország még akár kibernagyhatalom, legalábbis európai kibernagyhatalom is lehetne.

KÖZLÉSI FELTÉTELEK

A szerkesztőségünk csak olyan kéziratot fogad el közlésre, amelyek a rendészeti szakma történetéhez, feladataihoz, gyakorlati munkavégzéséhez kötődő tudományterületek legújabb kutatási eredményeivel, hazai és nemzetközi tapasztalataival foglalkoznak.

A szerkesztőségünk max. 50 000 karakter terjedelmű kéziratot fogad el, amelyet Word szövegszerkesztővel, Times New Roman betűtípust, 12-es betűméretet, sorkizárt rendezést, szimpla sortávolságot használva kell szerkeszteni (alcímek számozás nélkül, félkövér kiemeléssel, lábjegyzet a lap alján, irodalomjegyzék a közlemény végén). A kéziratot a magyarrendeszet@uni-nke.hu email címre kell elküldeni. A kiadvány fekete-fehér nyomdatechnikával készül, kérjük ezt figyelembe venni. Amennyiben a kézirat képet vagy más objektumot tartalmaz (diagram, táblázat), azokat kérjük külön fájlban is elküldeni, és a szövegben a helyét a fájlnévvel megjelölni.

A közlésre felajánlott anyagot kérjük nyomtatott formában is a szerkesztőség címére megküldeni.

Mellékelni kell a rezümét max. 3000 karakter terjedelemben magyar és angol nyelven. A szerző nevét, ha van rendfokozatát, tudományos fokozatát, beosztását, szolgálati vagy munkahelyének megnevezését, telefonszámát, címét, illetve azt a címet is ahová a tiszteletpéldányt küldhetjük.

A szerkesztőség fenntartja a jogot a kéziratok stilizálására, korrigálására, rovatokon belüli elhelyezésére, tipografizálására. A szerkesztőség a kéziratot nem őrzi meg és nem küldi vissza.