Az infokommunikációs közművek biztonsági kockázatai és az információs hadviselés

Várhalmi A. Miklós[1]

Összefoglaló

A távközlésnek, az informatikának és a multimédiának a rendkívüli fejlődése, integrálódása az információs társadalom kialakulásának legfontosabb pillére. Jelentős mértékben járul hozzá a társadalmi, gazdasági fejlődéshez, miközben megnöveli a digitális írástudatlanságnak és a digitális szakadéknak a mértékét is. Kiemelten megnövelte az infokommunikációs biztonsági kockázatokat is. Az internet például a széleskörű és meghatározó hasznossága mellett az informatikai háború, az informatikai terrorizmus eszköze is egyben. A távközlési és informatikai bűnözés terjedése jelentős, a hatékony védekezés szellemi és anyagi ráfordításai napról-napra nőnek. Országos és nemzetközi összefogás nélkül a nemzeti szellemi és pénzügyi források nem tudnak lépést tartani a bűnözéssel. Ennek ellenére jóhiszeműen terjednek az internetes szolgáltatások azzal együtt, hogy ily módon meghatványozzák a kockázatokat. Régen a bűnözőknek a bűnelkövetések helyszíneire kellett utazniuk. Ma már a sokoldalúan összefüggő és elérhető világhálón bárhonnan, bárhova be lehet törni és ott kárt okozni. Kérdés, hogy a támadók vagy a védők lesznek hatékonyabbak?

The security risks of infocommunication infrastructure and the information warfare

Summary

The most important pillar of development of information society is the process of the extraordinary development and integration of telecommunication, informatics and multimedia. While contributing considerably to social and economic development it also increases the digital illiteracy and the digital gap. It especially increased the security risks of info-communication as well. Internet, for example, while being a wide range and decisive utility became the vehicle of war of informatics and info-terrorism. The crime in telecommunication and informatics show a considerably spreading process and the intellectual and financial expenditures of effective defense are growing day by day. Without a nationwide and international cooperation the intellectual and financial resources on national level can not cope with crime. Despite of the foregoing Internet services are spreading even though increasing risks exponentially this way. In the past, criminals had to travel on the site of the crime. Today it is possible to break in from anywhere and make damages to any place. The question is, whether attackers or defenders will be more effective?

1. Bevezetés

Az infokommunikáció fogalma az informatika (számítástechnika) és a kommunikáció (távközlés) konvergenciáját, integrálódását fejezi ki. Az infokommunikációs rendszerek, hálózatok az országos infrastruktúra részeivé váltak és így a közművek rangjára emelkedtek, az energiaellátás, a vízellátás-szennyvízkezelés, stb. mellett. Az infokommunikációs közmű szerepét és jelentőségét tovább növeli az a tény, hogy a többi közműhöz is szorosan kapcsolódik, mivel azok működtetésében, használatában jelentős mértékben vesz részt, mint például távközlési, számítástechnika, elektronizálási, automatizálási vonatkozások.
Az egészségügyi, szállítási, banki-pénzügyi, államigazgatási-közigazgatási, stb. rendszerek támadhatóságában és egyben védelmében is jelentős szerepet játszik az infokommunikációs közmű.

[1] A Magyar Hadtudományi Társaság biztonságpolitikai és nemzetbiztonsági szakértője valamint a Zrínyi Miklós Nemzetvédelmi Egyetem PhD hallgatója (www.varhalmi.hu)

A gazdasági szféra szereplőinek, a gazdasági egységeknek az infokommunikációs biztonsága meghatározó összetevője egy ország gazdasági biztonságának.
Az információs forradalom olyan jellegű és ütemű fejlődést hozott, ahol az infokommunikációnak a társadalmakat, a politikát, a gazdaságot befolyásoló, megváltoztató hatása, előnyei mellett az infokommunikációs biztonsági kockázatok hatványozottan megnőttek.
A biztonság fogalmának jelentős megváltozása, összetettsége miatt is a társadalmak, az emberek ellen irányuló támadások egyik célpontjává váltak a jelentős számú embert, az alapvető létfeltételeket érintő közművek illetve infrastruktúra.
Az adat-információ biztonság és az informatikai biztonság eltérő, de kapcsolódó fogalmak, tárgyalásuk kapcsolódhat vagy elkülönülhet, az aktuális célszerűségtől függően.

2. A biztonság fogalmának megváltozása, szélesebb átfogása[1]

A biztonság a XXI. századra átfogó és összetett fogalommá illetve tényezővé vált, az évszázadokkal ezelőtti katonapolitikai biztonság fogalmának sokkal szélesebb körű értelmezésével, érvényesülésével. A biztonság összetevői, tágabb, átfogó értelmezése alatt a társadalmi (jogi, szociális), politikai (diplomáciai), gazdasági, környezeti (ökológiai), katonai, **informatikai,** pénzügyi, egészségügyi, belügyi biztonságot értik.
A biztonság átfogó értelmezésével párhuzamosan bővült a biztonsági kockázatok köre is. A biztonságpolitikában a hagyományos nemzetállami szereplők mellett egyre nagyobb szerephez jutnak az ún. nem állami szereplők (nemzetközi szervezetek, multinacionális vállalatok, nem kormányzati szervezetek, valamint a nemzetközi bűnözői és terrorista csoportok).
Az átrendeződő nemzetközi rendszer sajátossága, hogy abban egyszerre vannak jelen a hagyományos biztonsági kockázatok és az új, gyakran globális megjelenésű vagy kiterjedésű fenyegetések. Az új típusú fenyegetések és kihívások változatosabbak, kevésbé láthatók és előre jelezhetők. Jellemző tendencia a külső és belső kockázati tényezők közötti határvonal elmosódása.[2]
A biztonság szélesebb értelmezésének előnye, hogy átfogóbb megértési lehetőséget biztosít a fenyegetésekkel és az azokra adandó válaszokkal kapcsolatban.
Az elmúlt évszázad végére jellemző információs forradalom hatására az információs társadalmakat az határozza meg, hogy az **információs hatalom** fontos tényezője lett a hierarchizált világrendszernek szinte minden szintjén. Az **információ=hatalom** elvéhez tartozik alapvetően, meghatározóan és szorosan az elektronikus adat-információ biztonság kérdése is.

3. Információs Forradalom és Társadalom biztonsági kihívásai

Az információs forradalom egyik leglátványosabb fejlődését mutatta, illetve mutatja a számítógépes világháló (Internet) globális méretekben zajló, robbanásszerű elterjedése. A poszt-indusztriális társadalmak egyre nagyobb mértékben támaszkodnak a nagyméretű, globális hálózatokra, amelyek viszont sokkal sebezhetőbbek kis csoportok, vagy akár egyének által indított támadásokkal szemben.
Az információ árú lett, lehet venni és eladni: *"A tipikus amerikai világban az információ sorsa az, hogy áru lesz, venni és eladni lehet. Nem az én dolgom, hogy azon akadékoskodjam, hogy ez a kereskedői álláspont erkölcsös-e vagy nem, durva-e vagy finom. Az én dolgom az, hogy kimutassam: ez az álláspont az információ és a vele kapcsolatos fogalmak félreértéséhez és félrekezeléséhez vezet."* Norbert Wienernek az információelmélet és a modern kibernetika megalkotójának idézett gondolata így nem csupán az információra, hanem az információn alapuló, egyre több titkot felhalmozó információs társadalomra is igaz. Pontosan az információ tömegcikké válása, az információipar tömegtermelése, az információ birtoklásának és manipulálásának hatalmi ággá válása miatt került felszínre a biztonságos információ problematikája. Tökéletesen reprezentálja e problémakört az INTERNET története, mint a globális kommunikációs modell, napjaink információs társadalmának megtestesítője, már-már szimbóluma. Ez a történet azonnal rávilágít az információbiztonság megrendülésének rejtett okaira. Kezdenek összeolvadni az elektronikus információtárolás és továbbítás különböző eszközei egy "mindentudó elektronikus

kommunikátorrá", amely szinte láthatatlanul vezérli, irányítja életünket. Számtalan nemzetközi példa hívja fel a figyelmet az informatika globalizálódása miatt az informatika jelen és jövőbeni környezeti kockázataira, kijátszhatóságára, a puha, liberális adat-információ biztonsági, adat-információ védelmi szemléletre, a hatóságok alkalmazottainak szintjein is. Elképesztően sérülékeny a modern, fejlett társadalmak, a gazdaságilag is erős, katonai (nagy)hatalmak belső és külső informatikai biztonsági helyzete, az ezzel kapcsolatos belbiztonsági felfogások és helyzetek. Mindezt tetézik az emberi jogok, a személyes adatok védelmi vonatkozásai és növekvő kockázatai.
Az információs társadalom kialakulásának előidézője a gazdaság globalizálódása és a vállalatirányítás ebből fakadó válsága, fő motorja a számítástechnika és a távközlés rohamos fejlődése, legfontosabb állomásai a személyi számítógépek elterjedése és a szélessávú adatátviteli hálózatok megjelenése, szimbolikus jelentőségű technológiai újításai az internet és a mobiltelefon.
Mindezek hatására a kifejezés a politika szótárába is bekerült, az informatikai infrastruktúra fejlesztése és az információs írástudás terjesztése kiemelt stratégiai célként jelenhet meg. Ugyanakkor az információs társadalomban élő embernek számos, korábban ismeretlen problémával kell szembesülnie, mint például a korlátlan mennyiségben, de változó minőségben rendelkezésre álló információk értékelése, szűrése és feldolgozása vagy a magánszféra védelme az információk megszerzésére és ellenőrzésére törő gazdasági vagy politikai hatalommal szemben.
Vannak az információs társadalomnak politikai dimenziói is. Az informatika lehetőséget ad a bűnüldözés hatékonyságának, a személyi biztonságnak a növelésére, de a totális diktatúrák (lásd "Big Brother") is jó segítséget találhatnak benne, hiszen olyan vékony a jogi védelem "páncélja". A demokrácia erősítésére is jó, eléggé nyilvánvalóan elősegítette a diktatúrák megbukását azok destabilizálásával, de a demokráciákat is lehet az informatika eszközeivel destabilizálni.
Az információs társadalom elmélete szerint a társadalomban az információ előállítása, elosztása, terjesztése, használata és kezelése jelentős gazdasági, politikai és kulturális tevékenység. Ennek közgazdasági társfogalma a tudásgazdaság, amely szerint az értelem gazdasági hasznosításán keresztül érték jön létre. Ennek a társadalomtípusnak a sajátossága az információ-technológia központi szerepe a termelésben, a gazdaságban, a biztonságban és általában a társadalomban.[3]
Ugyanakkor az állam egyre inkább képtelenné válik a tőkemozgások kontrolljára és a társadalmi biztonság garantálására, ami megnehezíti, hogy az átlag polgár azonosuljon vele.
Az információtechnológiai fejlődésmenet eredményeként az áruk vagy termékek információtartalma igen jelentősen megnőtt az elmúlt ötven évben a nyersanyag- és energiatartalom rovására.
A legtöbb kritikai tanulmány a digitális pénz bevezetésével kapcsolatos tapasztalatokat járja körül, s az állam monetáris politikájának, a jegybankok kompetenciájának súlyos sérülése feletti aggodalmaknak (pl. hogy elveszítik az ellenőrzést a monetáris aggregátumok, a valutaárfolyamok és átváltások, a pénzmennyiség szabályozása felett) ad hangot.
Az információ korában a központi kormányok és elitek, a városi értelmiségi centrumok is elveszítik hatalmukat a média globalizálódásával szemben.
Mindennemű állami ellenőrzés hatástalan a hálózatokba szerveződő kommunikációra nézve, ezért a korszerű információtudományos szemlélet a kvázikaotikus társadalom, mint rendszer modellezésével, megértésével próbálkozik. A tisztességtelen előnyszerzés, a jogszerű, de erkölcstelen spekuláció, ill. a bűnözés világméretű jelenléte a legfőbb veszélyei az internet által megtestesített paradigmának.[4]
Egy nemzetközi konferencia a Net kapcsán a fegyverek, technológiák, emberi szervek, gyermekek kereskedelmét, a bérgyilkosságot, rablást (műkincs, arany, elefántcsont stb.), kábítószert, prostitúciót, nem utolsósorban a veszélyes hulladékok eltüntetése típusú veszélyeket minősítve évi 750 Mrd USD illegális forgalomról számolt be a globális pénzügyi rendszer kapcsán. A legfontosabb hatások a nemzetállamok szempontjából három nagy csoportba rendezhetők. Egyrészt már az államhatalom legmagasabb szintjein is megjelenik a bűnözés (korrupció, befolyással visszaélés, illegális politikai finanszírozás, befolyásszervezés). Másrészt sok állam függőségbe került az árnyékgazdaság nemzetközi összefonódásai miatt (mint pl. az USA a dél-amerikai drogkartellek, a fegyverkereskedelem; az európaiak az olasz vagy az orosz maffia terjeszkedésével). Harmadszor, de nem utoljára, az árnyékgazdaságból származó pénzek szabad áramlása manipulálja a nemzetközi politikát, destabilizálja az egyes nemzetállamokat, nemzetgazdaságokat (mint pl. a japán Yakuza befolyása Délkelet-Ázsiában). Ezért már minden felelős nemzetközi tényező megegyezik abban, hogy az elektronikus pénzügyi folyamatok ellenőrzése elengedhetetlen, a különféle bűnüldözési világkonferenciák pedig már régóta a

globalizálódásról szólnak. Más típusú kihívás együttest jelent a nemzetállamok szempontjából a kölcsönös függőséggel járó második csoport, a katonai tömbök széthullása, két, majd egy szuperhatalom kiemelkedése, s a köréje szerveződő országok kapcsolata, másrészt az új technológiák befolyása a hadviselésre; harmadrészt az emberiségre kifejtett hatások tudatosodása a kockázatkezelés, az információtudatosság terén. További elgondolkodtató hatásokat jelent a nemzetbiztonságban, hogy mindinkább függőségbe kerülnek államok a haditechnikai, technológiai szállítók, ill. a szükséges szakértő munkaerő terén. A katonai technológiák hihetetlenül gyors fejlődése aláássa az egyes országok biztonságát.[5]

4. A köz- és a gazdasági szféra információ illetve informatikai biztonsága

4.1. A közszféra információ illetve informatikai biztonsága[6]

Az informatika védelmére szinte valamennyi intézmény áldoz, ám a stratégiai szemlélet ritkán nyer teret, jellemzően az alkalmazott eszközökre fókuszálnak.
Ahogy az intézményi szférában is egyre több folyamatot gépesítenek, a szervezetek mind jobban függenek informatikai rendszereiktől. Mivel a hatékonyság növelése megfelelő IT-támogatás nélkül nehezen képzelhető el, sőt egyre komplexebb rendszerek alkalmazása a jellemző, a döntéshozók egyetlen választása, hogy igyekeznek felkészíteni folyamataikat és rendszereiket az elképzelhető legrosszabbra, de legalábbis az előre látható összes reális fenyegetés kezelésére. A Magyar Infokommunikációs Jelentés legfrissebb eredményei rávilágítanak, hogy bár a szervezetek döntő többsége tesz bizonyos erőfeszítéseket a kockázatok csökkentése érdekében, a biztonsági tudatosság terén számos intézmény komoly kihívásokkal küszködik.
A Jelentés adatait felszínesen szemlélők azt állapíthatják meg, hogy szinte valamennyi intézmény alkalmaz valamilyen IT-biztonsági, illetve üzletmenet-folytonossági megoldást. Az adatok részletesebb elemzése azonban rámutat, hogy a biztonság megteremtése érdekében tett erőfeszítések legtöbbször kimerülnek az antivírusszoftverek és a tűzfalmegoldások használatában. Az olyan, szofisztikáltabb védelmi megoldások, mint a rendszerhasználat és a hozzáférés naplózása vagy a behatolás-érzékelés, még az intézmények egyötödében sem terjedtek el.
Gyakran hallani olyan külföldi példákat (Németország, USA, stb), ahol értékes - akár kormányzati - adatok gigabájtjai kerültek illetéktelen kezekbe mulasztás, szándékos károkozás vagy véletlen hiba következtében. A veszély mértékét nem könnyű becsülni, de léte bizonyosan belátható.
Ennek ellenére az IT-biztonságot stratégiai szintre emelő tudatos gondolkodás csak a hazai intézmények kis hányadára jellemző. Erre utal, hogy például katasztrófa-elhárítási terve csak minden tizedik intézménynek van, de informatikai szabályzatot is csak az érintett döntéshozók egyötöde követelt meg, biztonsági auditnak pedig kevesebb mint 3 százalék vetette alá magát. Pedig a szabályozási keretek és a cselekvési tervek pontos és részletes definiálása nélkül nehezebb a számonkérés, nem beszélve arról, hogy nehezebb előre vetíteni, mi történik, ha bekövetkezik a baj.
A magyarországi intézmények és vállalatok jellemzően csak a védelem legalapvetőbb elemeit alkalmazzák, míg a szervezet mélyebb rétegeit is átható stratégiai szemlélet igen ritka. Az intézményi szféra szereplőire kevés kivételtől eltekintve jellemző, hogy IT-biztonsági tudatosságuk sokkal inkább az alkalmazott eszközök halmazaiban ölt testet, mint hogy a szervezet működésének egészét befolyásoló filozófiában csúcsosodna ki.

4.1.1. A magyar államigazgatás és közigazgatás egységes adat-, információvédelmi megoldása

Nincs a teljes államigazgatást és közigazgatást átfogó, azonos megbízhatóságú és kézben tartható kockázatú koncepción alapuló irányelv (szabvány csomag), emiatt nincsenek bevezetve és alkalmazva egységes biztonsági szempontokkal kézben tartható infokommunikációs (távközlési és számítástechnikai) védelmi rendszerek sem. Egyes helyeken természetesen léteznek egymástól elkülönülő, különböző megbízhatóságú, szigetszerű megoldások. Amennyiben elismerjük, hogy az „INFORMÁCIÓ HATALOM”, úgy el kell ismernünk, sőt tudomásul kell vennünk az infokommunikációs hálózatokon keresztül szétosztott illetve elérhető információ, a jelentős számú információ-adatbázis elérési pont(szinte minden számítógépes munkahely illetve információs hálózati csatlakozási pont), az adattovábbítási csatornák *emberi és technikai kockázatait* az „INFORMÁCIÓS HATALOM” megőrzésében, illetéktelen vagy jogtalan megszerzésének

megakadályozásában. Minden résztvevő személy és az infokommunikációs hálózatok minden pontja, minden „centimétere" jó lehetőség lehet a *gondatlan vagy tudatos behatolásra*, támadásra, a célinformáció-céladat megszerzésére, az „INFORMÁCIÓS HATALOM" meggyengítésére, megdöntésére.Kétségtelen, hogy az emberiség történetében szinte mindent az érdekviszonyok motiválnak és nap, mint nap érzékeljük a társadalmi, politikai, gazdasági, csoport, emberi, biztonsági, stb. érdekek eltéréseit is. A különböző formában és mértékben, de életszerűen eltérő érdekviszonyok miatt folyamatosan jelen vannak az információk elérésének, megszerzésének lehetőségét jelentősen megkönnyítő, integrált, infokommunikációs hálózatokon a *jogtalan és illetéktelen behatolások*, hozzáférések.
Belföldi és/vagy nemzetközi *(szervezett)bűnözői illetve terrorista csoportok*, más *ellenérdekelt szerveződések* országos esetleg „csak" intézmény méretű államigazgatási, közigazgatási, pénzügyi-gazdasági, katonai, rendvédelmi, közszolgáltatói, környezetvédelmi, infokommunikációs, biológiai, stb. támadásokat, *katasztrófákat okozhatnak*, melynek reális esélyeit és veszélyeit nemzetközi források és példák is igazolják(hackerek behatolásai egyes országok fontos állambiztonsági hivatalainak adatbázisaiba illetve bankrendszerekbe, dollármilliárdos károkat okozva). Ezen okok miatt a magyar Kormány, az államigazgatás, a közigazgatás többboldalú, komplex *adat- és információkezelésének védelme* egységesített irányelveket, központi irányítást, szabályozást, szolgáltatást-üzemeltetést, ellenőrzést követel meg és nem lehet az intézmények önállósági körébe tartozó feladat, továbbá nem lehet a szolgáltatói és termékverseny területe sem. Fontos, hogy ez a komplex adat- és információvédelem nem egyszerűen termékvásárlás, nem egy sztatikus szolgáltatás, nem egy egyszeri szervezés, nem egy egyszeri beruházás, hanem az információbiztonságot veszélyeztető folyamatoknak megfelelően egy folyamatosan változó, egységes szemléletet és végrehajtást igénylő kihelyezett informatikai és rendvédelmi szolgáltatás!
Ennek értelmében ezen terület megfelelő szintű szakmai irányítását, szervezését, kormány közeli szervezetben kell megoldani, mely célszerűen, egyik megoldásként a Miniszterelnöki Hivatal lehetne, különös tekintettel a már odadelegált, oda kapcsolt és bizonyos vonatkozásokban szakmai társterületeket jelentő kormányzati infokommunikáció valamint a Polgári Titkosszolgálatok irányító funkciói miatt is (például az NBH tevékenységei közé tartozik a gazdaságbiztonság, a titokvédelem, biztonsági ellenőrzések, stb). Az új szervezeti egység munkájához tárcaközi (bizottsági) munkára, kapcsolódásokra, együttműködésekre is feltétlenül szükség van.
Másik illetve az előzővel kombinált megoldásként a MeH előző pontban szereplő kisebb szervezeti egységéhez tartozó, meglévő (több is megvizsgálható erre a célra) vagy újonnan szervezendő önálló intézménnyel esetleg egyszemélyes állami tulajdonú részvénytársasággal megfelelő munkamegosztásban is elláttatható a feladat, amely a teljes kivitelezésre is felhatalmazott lehetne. A legoptimálisabb az lenne, ha ez a szervezet látná el közvetlenül minden államigazgatási és közigazgatási szervezetben a teljes adat- és információvédelmet, országos hatáskörrel, a MeH-ből irányítva. Ezzel maximálisan biztosítható lenne az egységes biztonsági szint, a kézben tartható kockázat, az egységes szemlélet és gyakorlat. Természetesen a hatósági, irányítási, kivitelező, üzemeltető, ellenőrzési funkciókat jól elkülönítetten kell megszervezni.

4.2. A gazdasági szféra információ illetve informatikai biztonsága[7]

A világnak tudomásul kellett vennie, hogy az új körülmények között bizonytalan lábakon rogyadozó informatikát nem lehet a korábban megszokott módon használni. Nem elég, hogy kiengedtük a szellemet a palackból, de függővé is váltunk tőle. Ma már az informatikai rendszerek nélkül nem tudunk és nem is akarunk élni. Meg kell tanulnunk tehát az együttélés megfelelő és az eddiginél lényegesen kényelmetlenebb módját.
Tovább bonyolítja a helyzetet, hogy ez mindenkire vonatkozik, senki nem húzhatja ki magát alóla, hiszen az internet arról is gondoskodott, hogy a felelősség mostantól kollektív legyen. Aki kilóg a sorból, az a többieket is veszélybe sodorja.
Jó hír viszont az, hogy már rendelkezésre állnak nemzetközi szabványok, amelyek lehetővé teszik az informatikai biztonsági problémák egységes, mérhető, ellenőrizhető kezelését.
Ebben a környezetben a jelenlegi tendencia az, hogy a világ informatikai beruházásokra fordított összegeinek egyre nagyobb szeletét rabolja el az informatikai biztonság. Ez a Gartner Group előrejelzése szerint hamarosan elérheti a 40%-ot, szemben a korábbi 4-5, illetve a jelenleg átlagosnak tekinthető 10-12 százalékkal.

Általában elmondható, hogy a cégek csak valamilyen káresemény (adatvesztés, vírustámadás, a levelezőrendszer leállása, információk kikerülése, hacker-támadás) után kezdenek el foglalkozni a biztonsági kérdésekkel. Ez - bár jellemzően emberi viselkedés -, de semmiképpen sem nevezhető preventívnek, ami pedig ma minden cégnek és szervezetnek alapvető érdeke lenne.
A cégek többségének - talán csak a legnagyobbakat kivéve - általában nincs olyan informatikai stratégiája, ami meghatározná, hogy az informatika milyen módon szolgálja ki a tervezett üzleti célokat, folyamatokat. Gyakran előfordul, hogy a felső vezetésben egyáltalán nem tudatosul, hogy az informatikát milyen módon tudnák a legjobban használni.
Komoly hiányosság, hogy a cégek többségénél nincsenek tisztában a céget fenyegető kockázatok és az üzleti folyamatok fenntarthatósága közötti összefüggésekkel, illetve ennek kapcsán azzal, hogy az informatikai rendszerek hibái milyen óriási közvetlen károkat okozhatnak. Az elvégzett kockázatelemzések eredményei az esetek többségében hatalmas meglepetést okoznak a felső vezetésnek.
Még a legnagyobb cégekre is jellemző, hogy hamis illúzióba ringatják magukat, különösen akkor, ha a cégnél már történtek lépések az informatikai biztonság megteremtésére. Az ilyen rendszerek számtalan esetben sok helyen lyukasak. A hamis biztonságérzet ezeknél a cégeknél is azt eredményezi, hogy valamilyen káreseménynek kell bekövetkezni ahhoz, hogy a szükséges lépésekre rászánják magukat.
A legproblémásabb területek: a jogosultságok és jelszavak feladatorientált, hierarchikus kezelése, a vezetők bizalmatlansága az üzemeltetőkkel szemben, a jelszavak könnyű visszafejthetősége illetve nyílt kezelése, a felhasználóknak indokolatlan jogok biztosítása, a tűzfalak, routerek nem megfelelő beállításai, a mentések laza és szabályozatlan kezelése, a megfelelő informatikai szabályozások és fegyelem hiánya.
Mindezek után, ha összegezni szeretnénk a tapasztalatainkat, azt mondhatjuk, hogy a legnagyobb gondot az okozza, hogy a felmerülő problémákat a legtöbb helyen nem átfogóan, rendszerben gondolkodva közelítik meg, hanem csak egyes részterületeken próbálnak meg eredményeket elérni, és ezek megvalósítására sokszor még mindig elegendőnek tartják az eszközök megvásárlását. A rendszerben gondolkodás egyik összetevője az is, hogy a cég üzleti stratégiájába az informatikának és az informatikai biztonságnak szervesen bele kell illeszkednie. Azonban ezek a stratégiai kérdések ma még nem kapták meg a jelentőségükhöz méltó helyet.
Másrészt még mindig komoly hiányosságokkal küzd az a két terület, amelyik pedig a legnagyobb eredményt hozhatná. Ezek az emberi tevékenységek szabályozása és az oktatás. A statisztikák és az eddigi tapasztalataink is azt mutatják, hogy a biztonsági problémák túlnyomó része (legalább 70-80 százaléka) a nem megfelelően szabályozott emberei tevékenységekre és a szükséges ismeretek hiányára vezethető vissza.
Tudatosulni kellene annak, hogy a biztonság nem teremthető meg pusztán áru és szoláltatás megvásárlásával, hanem minden esetben a szervezet életébe beépülő folyamatnak kell lennie. Ennek megértése alapvető fontosságú minden vállalat és intézmény részére.

4.3. Az informatikai biztonság legnagyobb kockázati eleme az EMBER

Az adat-információ biztonságnak nem a műszaki-technikai feltételek, hanem a műszaki-technikai eszközöket üzemeltető, a dokumentumokat, adatokat, információkat kezelő személyzet, az ember a legnagyobb kockázata. A mai munkavégzés, szervezés, irányítás, végrehajtás és ellenőrzés jelentős része elektronikusan zajlik, számítógépeken illetve távközlő, számítógépes hálózatokon.
Ezek az emberek különböző szerepkörökben vesznek részt az infokommunikációs rendszerekhez való hozzáférésben.Például: tulajdonosi kör; menedzsment, felső vezetés; középvezetők; alsószintű vezetés; ügyintézők; távközlési-informatikai üzemeltetők; karbantartók, takarítók, őrző-védő szolgálat munkatársai; a cég ingatlanjának, ingóságainak kezelését, tervezését, építését, fejlesztését, üzemeltetését, biztonságvédelmét végzők, stb. A felsorolt csoportoknak és tagjainak érdekei, tevékenységei, motivációi, szerepei, felelősségei és kockázati vonatkozásai eltérőek. Az emberi tényezőnek, mint a legjelentősebb biztonsági kockázati elemnek az ellenőrizhetősége is megszervezhető bizonyos kereteken belül jelentős, de nem végezhető el mindenre kiterjedően, azaz a teljes kockázatmentességet nem lehet elérni.
Az alapvető probléma, hogy egy ember gondolkodó, okos lény, miközben azonban szubjektum, érzelmi lény is egyben, azaz az élete egy változó folyamat, ami ismeretlenül-láthatatlanul és kiszámíthatatlanul is befolyásolhatja egyéniségét, tulajdonságait, érdekviszonyait. Tehát a

felvételekor, esetleg bizonyos időközi ellenőrzéseken még megbízhatónak ítélt személyt a egészségügyi (egészségromlások, balesetek, szenvedélybetegségek, idegi-szellemi változások, stb), családi (házasság, válás, gyermekszületés, haláleset, stb), pénzügyi, vagyoni, politikai, erkölcsi, vallási, egzisztenciális, egyéb körülményeiben beállt változások oly módon befolyásolják, hogy zsarolhatóvá, lefizethetővé, megvehetővé illetve befolyásolhatóvá, sőt deviáns, világmegváltó, igazságosztó, pénz-vagyonellenes akaratának érvényesítőjévé válik. Az adat-információvadászok számára ennek kihasználása a legegyszerűbb és legolcsóbb, mert egy vagy több személy megvásárlása sokkal kevésbé kockázatos, mint egy bizonyos fokig védett műszaki-technikai rendszer megcsapolása, lehallgatása és sokkal olcsóbb is.
Egy példa az előzőekre: ***„Az informátor az életét félti."*** *… Az a férfi, aki nemrég adócsalók adatait adta el a német hírszerzésnek, és ezzel kirobbantotta országa egyik legnagyobb adóbotrányát, félti az életét, és új személyazonosságot kér a hatóságoktól. Állítólag attól tart, hogy befolyásos külföldiek bosszút állnak, amiért lebuktatta őket. Henirich Kieber újabb levelet írt a BND-nek, a német hírszerzésnek, ám ezúttal nem adócsalókat lebuktató adatokról számolt be, hanem azt kérte: adjanak neki új személyazonosságot, mert félti az életét…. Kieber 2006 januárjában vette fel a kapcsolatot a BND-vel "Júlia" kódnév alatt. A 2000 banki ügyfél számlaadatait tartalmazó DVD átadását követően a tanúvédelmi programnak köszönhetően új személyazonosságot kapott a német hatóságoktól. Az ügyről egyre több információt derített ki a német média, például azt is, hogy ki volt a rejtélyes informátor, és hogyan zajlott az adatcsere. Így került nyilvánosságra Kieber neve, és az, hogy 2001 áprilisában kezdett a liechtensteini LGT banknál dolgozni: az intézet adatait, dokumentumait kellett digitalizálnia az informatikához kiválóan értő alkalmazottnak. Ez magyarázza azt, hogy a lopott adatokat tartalmazó DVD félelmetes részletességgel tartalmaz adatokat az adócsaló ügyfelekről: szerződések, a megbeszélések percre pontos időpontjai, kézzel írott megjegyzések. 2003 januárjában hagyta ott banki állását, és zsebében az aranyat érő lopott adatokkal kísérletet tett illetékes kezekbe juttatni. Több ország adóhivatalánál is kopogtatott (Liechtensteinnel, Amerikával és Angliával is felvette a kapcsolatot), míg végül a német hírszerzésnél figyeltek fel rá 2006-ban, és még nem kevés pénzt is hajlandóak voltak fizetni neki: összesen 4.6 millió eurót utaltak Kieber számlájára, azonban ironikus módon az adólevonások miatt "csak" 4.2 millió ütötte a markát. …. A Németországot és több más nyugat-európai államot is érintő adóbotrány reflektorfénybe állította a banktitkosság kérdését is. Kieber esete ugyanis bebizonyította, hogy a banki ügyfelek adatait egy klikkeléssel CD-lemezre vagy USB meghajtóra lehet menteni, azt pedig zsebre vágni. Kieberhez egy másik lebuktató is csatalakozott: Rudolf Elmer a svájci Julius Bar bank gazdag ügyfeleiről mentett le adatokat, és sétált ki velük az épületből - igaz, ő nem kért pénzt az értékes információkért. "Azt akarom, hogy a svájci pénzügyi világ őszintébb, morálisabb és etikusabb legyen" - nyilatkozta a Der Spiegel német politikai hetilapnak….*
A dán kormány ezzel szemben közvetve bírálta a német hatóságok módszerét, amellyel illegális úton szerzett banki adatok révén jutottak adócsaló állampolgárok nyomára. Kristian Jensen adóügyi miniszter kedden a Borsen című üzleti lapnak nyilatkozva kijelentette: "Nem áll szándékunkban lopott adatokat felhasználni. És nem is fizetünk lopott adatokért." Azzal kapcsolatban, hogy a német hírszerzés (BND) ötmillió eurót fizetett egy informátornak az általa felkínált adatokért, a dán miniszter elmondta: erkölcsi problémát lát abban, ha megjutalmaznak egy bűnözőt az általa lopott információkért. "Nincs ínyemre ez a magasztos orgazdaság. Etikai szempontból ez nem megfelelő módszer a korrekt adófizetés biztosítására" - fogalmazott Jensen.
A liechtensteini példa felbátoríthat más banki alkalmazottakat is hasonló illegális illetve törvénytelen üzletkötésre, a bankok hírnevének további lejáratására, a pénztulajdonos cégek és magánszemélyek elbizonytalanítására. Lehetnek további „világmegváltó, igazságosztó" alkalmazottak, akik üzleti-kitörési lehetőséget látnak hasonló titkosszolgálati vagy rendőrségi kapcsolatfelvételekben. Ezt meg kell előzni és ellensúlyozni!

4.4. Az információs illetve informatikai biztonság rendvédelmi feladat

Az adat-információ biztonság nem informatikusi, hanem rendvédelmi szemléletet, feladatot és felelősséget igényel. Az informatika fejlődésével együtt jelent meg az adat-információ védelem illetve biztonság egyre nagyobb jelentőségű problémája. Az infokommunikáció (távközlés és számítástechnika) biztonsága az igen fejlett rendszerek sokoldalú, rugalmas, óriási szolgáltatás kínálattal rendelkező konfigurálhatósága és programozhatósága miatt széleskörű kockázatokat is

hordoz az üzemeltetők, a kezelők, a felhasználók miatt. Az üzemeltetők és a kezelők részben informatikusok illetve informatikai ismeretekkel rendelkező személyek. Általában ők végzik a konfigurálásokat, programozásokat, jogossági beállításokat, védelmi szoftver beállításokat, mentéseket, stb. Viszont az informatikusok, a kezelők szemlélete általában messze van a rendvédelemtől, a vagyonvédelemtől, az érdekvédelemtől, hiszen a képzésük, ismereteik, a gyakorlatuk, a szemléletük, az egyéniségük ettől jelentősen eltérő. A cégek vezetői ezt általában nem látják át illetve ők sem kezelik rangján ezt a kérdést. A távközlési és számítástechnikai rendszerek védelmét, biztonságát egy külön belső ellenőrzési-védelmi-rendészeti (belbiztonsági, belső elhárítási!) szervezeti egységben lévő szakemberekkel kell biztosítani. Mivel az információ=hatalom, így a rendszergazdák, a kulcs informatikusok, a képzettebb kezelők-felhasználók kezében van a „hatalom", hiszen ők mindenhez hozzáférhetnek. Ennek ők tudatában is vannak, mert általában igen értelmes emberek! Viszont ez a monopol helyzetük jelenti a legkomolyabb kockázatot!

5. Informatikai biztonság a Magyar Köztársaság Nemzeti Biztonsági Stratégiájában (2004)

A rendszerváltozás után végbement euro-atlanti integrációs folyamat során Magyarország olyan integrációs szervezetek tagjává vált, amelyekben a tagállamok stabilitása a közös értékek, a demokrácia és jogállamiság, az emberi jogok és alapvető szabadságjogok érvényesülésének biztosításán alapul, és ezek megvédéséért készek és képesek egymást segíteni. Magyarország biztonsági helyzete szilárd, biztonságának alapvető garanciája a NATO és az EU keretein belül folytatott együttműködés. Magyarországot nem fenyegeti katonai agresszió, és az egyéb hagyományos fenyegetések kockázata is minimális. *Ugyanakkor új fenyegetések és kihívások jelentek meg, amelyekre csak nemzeti erőfeszítéseinket összehangoló kormányzati fellépéssel, képességeink tudatos fejlesztésével és rugalmas alkalmazásával, valamint széleskörű nemzetközi együttműködéssel lehetséges hatékony választ adni.*
A nemzeti biztonsági stratégiára épülve összehangoltan készülnek el azok az ágazati stratégiák, többek között katonai, nemzetbiztonsági, rendvédelmi, gazdasági-pénzügyi, humánerőforrás-fejlesztési, szociálpolitikai, informatikai és **információvédelmi**, katasztrófavédelmi és környezetbiztonsági területen, valamint a terrorizmus elleni küzdelem területén, amelyek az átfogóan értelmezett biztonság területén határozzák meg a teendőket.

II.1.6. Az információs társadalom kihívásai

A hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Az információs forradalom vívmányainak mind szélesebb körű megismertetése, az oktatás színvonalának emelése kulcsfontosságú érdek, ami közvetve pozitív hatással van a gazdaságra, a társadalom életére és az ország érdekérvényesítő képességére. Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára.

III.3.7. Információs rendszerek védelme

A technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű és biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között.

6. Nemzeti Operatív Válságkezelő és Koordináló (Infrastruktúra) Biztonsági Központ

Egy ország, egy nemzet életképességének, stabilitásának, nemzeti és nemzetközi tekintélyének egyik fontos jellemzője a védelmi, védekező képessége. Ez függ a nemzetközi szövetségektől, együttműködésektől és hangsúlyosan a nemzeti szemlélettől, igényességtől, szervezéstől, személyi és pénzügyi ráfordításoktól. Magyarországon az Önkormányzati és Területfejlesztési Minisztérium (ÖTM) keretein belül működik, a miniszter irányításával működik a Kormány katasztrófavédelmi tevékenységét előkészítő és szervező Kormányzati Koordinációs Bizottság, mely a minisztériumok és a hatóságok képviselőiből áll. Titkárságot, Veszélyhelyzeti Központot és Operatív Törzset működtet. Kezeli a kritikus infrastruktúra védelmet is, más érintett hatóságok bevonásával együtt.
A Belügyminisztérium után az ÖTM-ben működik a Nemzeti Helyzetértékelő Központ is, mely a ez egyes minisztériumok hatáskörét meghaladó polgári válságkezelést és Nemzetbiztonsági Kabinetet hivatott információkkal történő ellátását végzi. A terrorizmus elleni fellépés is ide tartozik.
Az infokommunikációs biztonsággal alapvetően a Nemzeti Hírközlési Hatóság, CERT (Computer Emergency Response Team) foglalkozik a Rendőrséggel és a Nemzetbiztonsági Szolgálatokkal együtt.
A meglehetősen szétosztott védelemi funkciók helyett a jövőben például létrehozható egy Nemzeti Operatív Válságkezelő és Koordináló (Infrastruktúra) Biztonsági Központ, amely egy olyan sokoldalú információ érzékelő, gyűjtő, tároló, feldolgozó és hasznosító csúcsszerv, egyben a legfelső vezetési pont is. Jelenleg ilyen még nincs Magyarországon, pedig az érzékeny, gyors és dinamikus reagáláshoz, a szoros, de rugalmas operatív együttműködéshez sokkal célszerűbb, gazdaságosabb és hatékonyabb lehetne, más nemzetközi példák alapján is.

7. Információs – hálózati - vezetési hadviselés (halott nélküli háborúk)

A hálózatközpontú hadviselés legfontosabb eleme az információk megszerzésének és felhasználásának radikálisan új módja, amely gyökeresen átalakítja a haderő vezetési rendszerét is, hiszen lehetővé teszi, hogy minden információ a vezetés minden szintjén egy időben álljon rendelkezésre és ennek megfelelően a döntések mindig a lehető leggyorsabban, és a lehető legalacsonyabb szinten történjenek. Ez lehetővé teszi a minimális erő alkalmazását is, elkerüli a „baráti tűzből" esetleg adódó problémákat, minimálisra redukálja saját veszteségeinket és a járulékos pusztítást is.
Az információ megnövekedett jelentőségét az újfajta elektronikai-távközlési-informatikai, valamint vezetési technológiák viharos fejlődése tette lehetővé, amely a hadügy folyamataiban is szükségszerűen érvényre fog jutni: "A hadseregre is érvényes az a megállapítás, hogy a jövőben a siker egyik döntő tényezője az információ megszerzése, alkotó módon történő felhasználása, az információs és vezetési fölény megszerzése lesz. Amelyik fél az információhoz előbb fér hozzá, és azzal jól tud gazdálkodni, az nyer, amelyik fél erre nem képes, az veszít. Ilyen egyszerű törvények fogják megszabni a további fejlődés útját."[8]
Az információs hadviselés olyan egységes elgondolás alapján végrehajtott tevékenységek rendszere, amely valamely állam részéről egy másik állam működési rendjének befolyásolására vagy megtörésére, továbbá a saját állam hatékony működőképességének megőrzésére irányul a saját információs képességek megvédése, fejlesztése és alkalmazása, valamint a másik állam hasonló képességeinek bénítása, zavarása vagy megsemmisítése révén.
A "döntő fölény a megfelelő helyen és időben" elve szintén nem annyira az ellenség megsemmisítésre, mint inkább a kezdeményezés megragadására, az ellenség hadműveleti felépítésének, harcrendjének, működési struktúrájának megbontására irányul, az ellenséges csapatok pusztítása ennek csupán egyik - bár eleddig legfontosabb - eszköze. A hadászati-hadműveleti tevékenységek alapvető célja nem az ellenség harcoló alakulatainak minél nagyobb arányú megsemmisítésén, hanem ezen csapatok vezetési rendszerének, hadkiegészítési rendjének, hadműveleti felépítésének, együttműködésének, felderítési-logisztikai-műszaki és tűzrendszerének megbontásán keresztül érhető el elsősorban. Ez az ellenséges szándékról való lemondatás és a

háborúk megnyerésének hatékony eszköze volt a múltban, szerepe a 21. században a működési struktúrák közvetlen megbontása révén jelentős mértékben növekedni fog.
A műszaki-irányítástechnikai fejlesztés elsődleges oka nem egyszerűen a katonai siker mindenáron való kikényszerítésében rejlik, hanem abban, hogy a korszerű módszerek és technika alkalmazása számottevően csökkentheti az élőerőben és az anyagi javakban bekövetkező veszteségeket, amely a politika mozgásterét jelentős mértékben bővítheti adott konfliktus kapcsán. A minimális veszteségre való törekvés az utóbbi években különösképpen előtérbe került a békefenntartó műveletek és fegyveres biztosítási tevékenységek során, amely megköveteli különböző nemzetiségű, rendeltetésű és harcértékű alakulatok hatékony együttműködését, a műszeres felderítés és az automatikus tűzvezetés egységben történő alkalmazását, az információk továbbításának és feldolgozásának automatizálását, a vezetési-döntéshozatali folyamatok optimalizálását, végső soron pedig a rendszerszemléleti alapokon nyugvó, új típusú katonai gondolkodásmód kialakítását.
Megnőtt azoknak a beavatkozási pontoknak a száma, amelyekre történő ráhatással jelentős zavarok kelthetők a szervezetek működésében, és ezekre a társadalom egésze a funkcionális függőségek kiterjedt rendszere következtében sokkal gyorsabban és hevesebben reagál, mint korábban. A korszerű társadalmakban lényegesen egyszerűbb nehezen megállítható, pozitív visszacsatolásos elven működő, öngerjesztő, káros folyamatokat elindítani az államszervezet és gazdaság működésében, mint azt megelőzően bármikor; valamely hiba, funkcionális zavar következményei sokszor nem vagy csak kevéssé prognosztizálhatók, azokat a vezetés sok esetben képtelen oly módon modellezni, hogy a zavar elhárítása érdekében azonnal és hatékonyan be tudjon avatkozni.
A stratégiai információs hadviselés "fegyverei" közé tartoznak az ún. HERF-fegyverek (High Energy Radio Frequency), amelyek nagy energiájú rádiójeleket sugároznak a kijelölt célpontra, amelyek áramkörei érzékenyek a túlterhelésre. Az EMP/T (Electromagnetic Pulse Transformer) fegyverek a HERF fegyverekhez hasonló elven mûködnek, csak sokkal hatékonyabbak. Egy lakott településen "felrobbantott" EMP/T bomba tönkretenné a kommunikációs és elektronikus berendezések mûködését, leállna pl. az elektromosáram-szolgáltatás, melynek következménye polgári nyugtalanság, a közrend megbomlása lehet.
További fegyverként hasznosíthatóak a rendszerbehatolások, ugyanis az egymással összekapcsolt számítógépes rendszerekbe viszonylag könnyû a behatolás, ami komoly biztonsági kockázatot von maga után.
A jövő háborúja: távközlés, informatika, hadművészet című cikkből vett idézettel: “Az információs hadviselés már nemcsak a képzelet terméke, hanem létező rész az Egyesült Államok szárazföldi, tengeri és légi erőinek arzenáljában. Arthur Cebrowski altengernagy, az amerikai vezérkar irányítási, ellenőrzési, távközlési és számítógépes főigazgatója a közelmúltban nyilvánosan kimondta: a távközlési-informatikai hadviselés megjelenése legalább annyira megváltoztatta a hadművészet és a stratégia alapképleteit, mint annak idején az atombomba. Ám nem a végpusztulás réme által, hanem ellenkezőleg: azzal, hogy puskalövés nélkül meg lehet bénítani az ellenség hadseregét, sőt egész gazdaságát, bankrendszerét, egészségügyi ellátását, iparát: mindent, amit komputerek tartanak nyilván és segítenek irányítani. Meg lehet fosztani a vezérkart és a kormányt az információ továbbításának lehetőségétől. Kevesen halnak meg, talán egy ház sem dől össze, a legyőzött ország gazdasága mégis hosszú évekig romokban hever.”[9]

IRODALOM

[1] Várhalmi Miklós: Szabadság és Biztonság, előadás Athénben, 2005 (www.varhalmi.hu)
[2] Resperger István: Kockázatok, kihívások és fenyegetések a XXI. században, ZMNE tanulmány, 2006
[3] Molnár László: Az információs társadalom felé
[4] Manuel Castells 1997 = Manuel Castells: The Information Age, II.k. Oxford, Blackwell
[5] Csorba József: A globalizáció az információs társadalommal kapcsolatos információtudományos gondolkodásban
[6] Szilágyi Szabolcs: A közszféra IT - biztonsága, www.terminal.hu, 2008.06.03.
[7] KÜRT Kft: Az információbiztonság Magyarországon

[8] Dr. Várhegyi István: Az információs hadviselés, Új Honvédségi Szemle, 1996/7. sz.
[9] Népszabadság, 1997. november 3.