



Communication 2015 KOMMUNIKÁCIÓ 2015



KOMMUNIKÁCIÓ 2015





KOMMUNIKÁCIÓ 2015

COMMUNICATION 2015

Budapest, 2015

Székhely
1036 Budapest, Lajos u. 78.

Tel: +36 (1) 250-4910
Fax: +36 (1) 250-4909



Fercom Kommunikációs Kft.

www.fercom.hu

info@fercom.hu

Telephely
1037 Budapest, Pomázi út 15.

Tel: +36 (1) 250-7940
Fax: +36 (1) 250-7939

Cégismertető

A Fercom Kommunikációs Kft. a Motorola Solutions magyarországi disztribútori partnere. Fő tevékenységünk a vezeték nélküli távközlés és rádiókommunikáció, ezen belül analóg és digitális rendszerek szállítása, rendszerintegrációja, telepítése- üzembe helyezése és karbantartása.

Cégünk közel 20 éve rendvédelmi és kormányzati szervek megbízható beszállítója. Termékeinket többek között a Magyar Rendőrség, a Magyar Honvédség, a Nemzeti Adó- és Vámhivatal, valamint nagyvállalatok egész sora használja országszerte nap, mint nap a legnagyobb megelégedéssel. Az országban több helyen saját trónkölt rádiórendszerrel rendelkezünk és üzemeltetünk. A kormányzati partnereink mellett a legnagyobb magyarországi közlekedési, szolgáltató és ipari vállalatok is a Fercom Kft. rendszereit használják. A vezeték nélküli kommunikáció mellett cégünk több éves tapasztalattal rendelkezik speciális biztonsági, katonai és rendfenntartó eszközök forgalmazásában és teljes körű integrációjában. A Fercom Kft. ISO 9001:2000 minősítéssel rendelkezik és minősített NATO beszállító.

Motorola rádió terminálok és rendszerek

Analóg és digitális rádiók és rádiórendszerek

Az analóg rádiók piacán a Fercom Kft. 80%-os részesedést tudhat magáénak, a Motorola csúcsmínőségű készülékeit a kormányzati szervek, gyárak, közlekedési, szállítmányozási és közszolgáltató cégek egyaránt használják. Ezen felhasználók számára természetesen biztosítjuk a lehetőséget a modern digitális technológiákra való folyamatos, akár szakaszos átállásra is.

Az elmúlt 3 évben több mint 25 digitális rendszert telepítettünk, többek között a budapesti Liszt Ferenc Nemzetközi Repülőtér is a MotoTRBO-t, a Motorola digitális rendszerét használja.

Motorola Tetra rádiók és rádiórendszerek

Az elmúlt három esztendőben cégünk több mint 7000 Motorola TETRA terminált szállított a kormányzati Tetra rendszer számára, a megrendelők teljes megelégedésére. A legnagyobb felhasználók a Magyar Rendőrség, Tűzoltóság, egyéb készenléti szervek, valamint a Nemzeti Adó- és Vámhivatal.

Távvezérlő és felügyeleti berendezések, rendszerek

A távvezérlésű alkalmazások és felügyeleti rendszerek alapjául szolgáló Motorola SCADA megoldás (MOSCAD) megoldásunk a közszolgáltató cégek (pl. Fővárosi Vízművek) működését támogatja.



SCI-Network Távközlési és Hálózatintegrációs Zrt.

www.scinetwork.hu
info@scinetwork.hu

A SCI-Network Távközlési és Hálózatintegrációs Zrt. hálózati rendszerintegrációval foglalkozó szakértő vállalkozás. A szűkebb értelemben vett hálózati rendszerek mellett a cég alaptevékenységébe tartozik a mikrohullámú átvitel, a hálózati biztonság és a rendszerfelügyelet is. A SCI-Network teljes körű szolgáltatást nyújt ügyfeleinek a hálózatok terén a feladat felmérésétől kezdve a tervezésen, az eszközszállításon, az üzembe helyezésen, az oktatáson keresztül a garanciális és garancián túli szolgáltatásokig. A folyamatosan gyarapodó létszámmal, bővülő ügyfélkörrel és növekvő forgalommal rendelkező vállalat az informatikai vállalkozások felső harmadába tartozik.

A SCI-Network célja, hogy ügyfelei számára magas színvonalú megoldásokat biztosítson, valamint megismertesse kiváló minőségű termékeit és szolgáltatásait leendő ügyfeleivel.

A vállalat kiemelt figyelmet fordít a minőségbiztosításra, melyet ISO 9001 és AQAP2110 minősítése is tükröz.



Always one step ahead.

A Kapsch Magyarországon a vállalati és intézményi ügyfeleknek professzionális ICT megoldásokat, a távközlési és internet szolgáltatóknak innovatív rendszereket kínál, teljes körű GSM-R, közlekedéstelematikai, valamint Smart Metering megoldásokat szállít.



A tudományos kiadványt lektorálták:

Dr. Fekete Károly alezredes, e. docens

Dr. habil. Kerti András alezredes, adjunktus

Dr. habil. Farkas Tibor százados, adjunktus

Dr. Németh József, adjunktus

Szerkesztette:

Dr. Fekete Károly alezredes, e. docens

Kiadja: NKE Szolgáltató Nonprofit Kft.

Felelős kiadó: Hegyesi József ügyvezető igazgató

Nyomdai munkák: NKE Szolgáltató Nonprofit Kft.

© A szerzők

© A szerkesztő

© NKE Szolgáltató Nonprofit Kft.

ISBN 978-615-5527-55-5

TARTALOMJEGYZÉK

Bevezető	17
--------------------	----

Tudományos közlemények

MEGYERI Lajos: Nikola Tesla	21
---------------------------------------	----

DOBÁK Imre: Mobile communication and migration – Some research aspects of the issue.	27
--	----

PÁNDI Erik: Security structures.	37
---	----

DOMBORA Sándor – HORVÁTH Gergely Krisztián: Az információbiztonság integrált megvalósítása	43
--	----

KOLOZS Csaba: Szálfelügyelet „parancsszóra” – a biztonság mindenek felett . .	57
---	----

NYÁRI László: Smart dust – a védelmi elektronika, informatika és kommunikáció legújabb területe	63
---	----

RÉPÁS Sándor: Nyílt forráskódú kiberbiztonsági szoftverek alkalmazása kritikus információs infrastruktúrák védelme során	69
--	----

Konferencia-előadások

SZARVÁK Anikó: A Missing Thing of Safer Cyberworld	87
--	----

BÓDOGH Attila: Mesterséges intelligencia és a bigdata-elemzések alkalmazási lehetőségei a rendvédelemben	95
--	----

DOMBORA Sándor – HORVÁTH Gergely Krisztián: Az információbiztonság integrált megvalósítása	101
--	-----

KOLOZS Csaba: Szálfelügyelet „parancsszóra” – a biztonság mindenek felett . .	105
---	-----

FARKAS Tibor: Questions and tasks of communication in disaster and crisis situations in Hungary	117
---	-----

TRENCÁNSZKY Imre: Juniper SRX-ek a katasztrófavédelemben, avagy a tűzfal a víz ellen is véd	127
---	-----

NÉMETH József Lajos: The NATO Strategic Communications Centre of Excellence	133
---	-----

FEKETE Károly: Evolution of Military Science: Real and Virtual Worlds.	141
--	-----

SZABÓ Levente – SZABÓ András: Kiképzés a kibertérben	149
--	-----

SCHMUCK András: Üzemeltetés és telepítés távközlési hálózatokon	155
NYÁRI László: Smart dust	161
JOBBÁGY Szabolcs: CISCO CERTIFIED NETWORKING ACADEMY TRAINING, CCNA Routing & Switching	175
PÉTER Attila: National Instruments – LabVIEW Communications System Design Suite	183
NÉMETH József Lajos: Turkey and Strategic Communication.	191
FEKETE Károly: Is there any singularity within the military communication? . . .	199
RÉPÁS Sándor: Nyílt forráskódú kiberbiztonsági szoftverek alkalmazása kritikus információs infrastruktúrák védelme során	207

A tudományos konferencia támogatói:



Kapsch Telecom Kft.



Antenna Hungária Zrt.



Hungaro DigiTel Kft.



NATIONAL INSTRUMENTS™ Hungary Kft.



SCI-Hálózat Zrt.



TOTALTEL Távközléstechnika Kft.



Fercom Kommunikációs Kft.



Equicom Kft.



Hírközlési és Informatikai Tudományos Egyesület



Magyar Telekom Nyrt.



ELSINCO Budapest Kft.



Biztonságpolitikai Szakkollégium



HTEST Hungary Kft.



Enterprise Communications Magyarország Kft.



Professzionális műholdas megoldások bárhol–bármikor



Hungaro DigiTel Kft.

2310 Szigetszentmiklós-Lakihegy, Komp u. 2.

tel: 06-1-488-8500 fax: 06-1-488-8501 <http://www.hdt.hu>

FOLYÓÍRATOK

A HTE időszakos kiadványai mellett hagyományosan két folyóiratot jegyez: a **Híradástechnikát** és az **Infocommunication Journalt**. Míg előbbi a hazai szakmai élet történéseit, kérdéseit és működését elemzi, az *Infocommunication Journal* már nemzetközi elemzésre is szert tett. A lap kiadását a Nemzeti Hírközlési és Informatikai Tanács (NHIT) támogatja, szerkesztősége pedig folyamatosan szervez keresztpublikációkat nemzetközi társalópokkal. Az *Infocommunication Journal* elismertségét jelzi, hogy olyan nemzetközi adatbázisokban is szerepel, mint a Scopus, a Compendex és az Inspec.

Amennyiben „up-to-date” részese szeretne lenni az infokommunikációs tér áramlásának, itt találkozhatsz a **Hírközlési és Informatikai Tudományos Egyesületbe történő belépés** feltételeivel: www.hte.hu/belleges.



Kérdéseit, észrevételeit, javaslatait az info@hte.hu e-mail címre készséggel várjuk!

- kiegészülő szakmapolitikai, szakmai véleményalkotás (minisztériumok felkéréseire és társadalmi egyeztetésekben), pl. részvétel a Nemzeti Informatikai Stratégiában, a digitális átállás társadalmi kommunikációjában, az elektronikus hírközlési törvény szakmai véleményezésében, frekvenciaterületek szakmai támogatása, internethasználat jogalkotási javaslattétel
- főiskolák és egyetemek képzési és kimeneti követelmények véleményezése
- külföldi infokommunikációs eredmények honosításának segítése
- kutatásfejlesztési tevékenység támogatása

UTÁNPÓTLÁS BIZTOSÍTÁSA

A HTE ars poetikájában tradicionálisan hangsúlyos szerepet kap a fiatalokkal való kapcsolat-ápolása a **szakmailag széles látókörű és tudományos érdeklődéssel bíró diákok tanulásának és pályakezdésének segítése** – hiszen ők alkotják majd a jövő szakembereit. Az egyesület amellett, hogy az arra érdemes hallgatóknak biztosítja a különböző rendezvényeken, konferenciákon, fórumokon való kezezményes részvételt, és ezáltal a szakmai kapcsolatteremtést is, különböző pályázatokkal hirdeti, amelyek díjazottai anyagi elismerésben is részesülnek. A HTE Diplomatarevé és Szakdolgozat Pályázataira például az ország 15 egyeteméről nevezhetnek, de említsük érdemlő a HTE Akadémia által kiadott tanúsítvány is, amely szintén támogatja a következő infokommunikációs nemzedék szakmai fejlődését.



Nagy Péter
főtitkár
nagy.peter@hte.hu



Bartolits István
főtitkár
bartolits@nmti.hu



Magyar Gábor
elnök
elnok@hte.hu

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET

Levelezési cím / iroda:
1051 Budapest, Bajcsy-Zsilinszky út 12. 502. iroda
Számítási cím / székhely:
1055 Budapest, Kossuth Lajos tér 6-8
Tel.: +36 1 353 1027; Fax: +36 1 353 0451;
E-mail: info@hte.hu; Honlap: www.hte.hu



A Hírközlési és Informatikai Tudományos Egyesület tekintélyes, 65 éves múltjával hazánk infokommunikációs szektorának legatná-
sabb szervezetévé vált. Munkássága a tá-
vközlési és az informatikai iparágtól, a hagy-
ományos postai szolgáltatásokon át, az inter-
netig és a médiavilágig terjed.

Az egyesület közel 60 jogi tagot, valamint majdnem 1000 magánsemélyt számlál. Berkein belül több mint 20 szakmai közösség munkálkodik meg meghatározott célok érdekében, a legjobb tudása szerint.

A HTE amellett, hogy kiemelt, véleményformáló szerepet tölt be a magyar infokommunikációs szakterület szabályozásában, működésében, fejlődésében, hazai és nemzetközi szakmai rendezvények elismert szervezőjeként is jegyzett.

[illegible]SZAKMAI
RENDEZVÉNYEK
SZERVEZÉSE

A HTE naptárában nem telik el hét szakmai találkozás, előadások, kerekasztal-beszélgetések és egyéb szervezett események nélkül, de házigazdája többek között olyan országos szakmai nagyrendezvényeknek, mint

- a projektmenedzserek találkozzát és információcserejét segítő **Projektmenedzséret Fórum**.
- a kimagasló hazai médiatechnikai esemény, a **HTE Médiatek** konferencia, amely az infokommunikációs és alkalmasodások legfrissebb piaci, műszaki és szabályozási kérdéseinek egyik legjelentősebb rendezvénye.

Az egyesület az utóbbi években számos nemzetközi tudományos konferencia és workshop márkájára szervezte meg a konferenciát. A konferencián résztvevők megismerhetik a hazánk szerepét a világ információs társadalomában, a kommunikációs szférában, a média és a HTE nagyrészt rendezvényeiről.

HTEA

Az egyesület szerteágazó kapcsolati hálójának, valamint szakmai taglistájának (amely lefedi az infokommunikációs szektor szinte teljes területét) köszönhetően teret ad a különböző vélemény- és információcsereinek, szakmai párbeszédnek, közös cél érdekében folytatott kollektív munkásságnak.

Lehetőséget biztosít arra, hogy az iparág vállalati képviselői – akár a mindennapi konkurenciájáért is hártható szorítva – kommunikáljon fontos kérdéseikről, kifejtse a jelen nehézségeit illetően jövőbeli elképzeléseit. Mindeközben az egyének szakmai kiemelkedésének, véleményformálásának is útát enged.

A HTE megkérdőjelezhetetlen erőssége, és így több évtizedes elismertségének egyik alapja, hogy mind munkaszámban, mind véleményformálásban **szakaszerű, kiegyensúlyozott és független**, feltűnőmelledik az esetleges politikai vagy éppen vállalati érdekeken.

Bő hat évrizedet és két tucat szakterületet par
mondában összefoglalni szinte lehetetlen lenne,
ezért inkább vázlatpontokban szemléltetjük, mi
minden érinti manapság a HTE tevékenységi
körét:

- 
- hazai és nemzetközi konferenciák szervezése, lebonyolítása
 - szakmai fórumok az internet technológiák és szolgáltatások elterjesztéséhez
 - műsorelosztási és tartalompári technológiai népszerűsítése
 - rádió- és televíziós technológiai ismeretterjesztése
 - projektmenedzsment módszerek terjesztése
 - szakmai folyóiratok, nyomtatványok kiadása
 - nemzetközi kapcsolatok: együttműködés az IEEE, VET és más társaságakkal
 - szakmai díjak odaítélése (pl. Pusztas Tivadar-díj, Kempenen Farkas-díj, Pollák Virág-díj)

Háttérinformációk

A konferencia fővédnöke:

Vass Sándor dandártábornok,
a Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség
csoportfőnöke

A konferencia rendezői:

Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar,
Katonai Üzemeltetési Intézet, Híradó Tanszék
Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség
Hírközlési és Informatikai Tudományos Egyesület, NKE Egyetemi Csoport

A szervezőbizottság elnöke:

Dr. FEKETE Károly
alezredes, e. docens

A szervezőbizottság titkára:

Dr. habil. FARKAS Tibor
százados, adjunktus

A szervezőbizottság tagjai:

Dr. NÉMETH József
adjunktus
JOBBÁGY Szabolcs
százados, tanársegéd

Budapest, 2015. november 11.



Az EQUICOM Kft. 2000 óta van jelen a magyarországi ICT piacon telekommunikációs, informatikai és kábeltelevíziós mérés technikai megoldásokkal. Világviszonylatban is vezető pozíciót elfoglaló beszállítóink innovatív megoldásokat kínálnak az adatátviteli és kommunikációs hálózatok létesítési és üzemeltetési méréséhez, analíziséhez, és monitorozásához. Az évről-évre növekvő piaci jelenlétünk, az ügyfeleinkkel kialakított jó kapcsolat, a technológia központú szemléletünk és a hozzáadott érték növelésére való törekvésünk mellett a beszállítók folyamatos fejlesztési munkájának is köszönhető.

BEVEZETŐ

A Tisztelt Olvasó az évenkénti rendszerességgel megrendezett „Kommunikáció – Communication” tudományos konferencia anyagainak könyvváltozatát tartja a kezében.

A tudományos kiadvány első fejezete szakmai cikkek formájában, magyar és idegen nyelven teszi közzé az aktuális problémákra adható válaszokat, megoldásokat és az elmúlt időszak tudományos eredményeit. A cikkek szerzői többségében társegyetemek, kormányzati és polgári távközlési szervezetek, valamint a versenyszféra tudományos mérnök munkatársai, fejlesztő szakemberei, oktatói, doktoranduszai.

A könyvben közreadott és vizsgált témák időszzerűségét jelzi, hogy a második fejezetben a Nemzeti Közszoigálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Üzemeltetési Intézetének Híradó Tanszéke, a Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnöksége és a Hírközlési és Informatikai Tudományos Egyesület egyetemi csoportja által rendezett „Kommunikáció 2015” nemzetközi szakmai tudományos konferencián elhangzott előadások egy részének szerkesztett változatát, különlenyomatát találjuk.

A tudományos konferencia célja volt a katonai, kormányzati kommunikáció – az EU, a NATO és a hazai hadműveleti vezetés rendszerében elfoglalt – helyének, szerepének értelmezése; képet adni a katonai képzés és felkészítés aktuális kérdéseiről és a velük összefüggésben lévő feszítő problémákról a haderő korszerűsítésével folyamatosan változó környezetben. Erősíteni kívánta a katonai, kormányzati és polgári szakértők szervezett tapasztalatcseréjét és rendszeres kapcsolattartását.

A szervezőbizottság célja, hogy az előadásokon elhangzottak minél szélesebb körben ismertté váljanak, ezért a könyv mellett – online hozzáféréssel – a kiadvány elektronikus változatát is közreadjuk. Néhány tudományos cikket delegáltunk a *Bolyai Szemle* aktuális számába is.

Budapest, 2015. november 11.

Dr. Fekete Károly

TOTALTEL

TÁVKÖZLÉSTECHNIKA KFT



A Totaltel Kft. 100%-ban magyar tulajdonban lévő, 1991-ben alapított budapesti székhelyű társaság. Fő tevékenysége: digitális mikrohullámú rádióberendezések fejlesztése, gyártása és forgalmazása. Társaságunknak jelenleg 22 alkalmazottja van, akik közül 17 magasan képzett mérnök. Kooperáló és beszállító partnereinknél több száz szakember járul hozzá termékeink gyártásához.

Fejlesztési munkánk eredményeként készültek el a TDR típusú mikrohullámú digitális rádióberendezések különböző generációi, amelyek egyre magasabb frekvencián működnek és egyre nagyobb átviteli kapacitásra képesek. Ilyen berendezésekkel vállaljuk kulcsrakészen távközlési és adatátviteli összeköttetések vezeték nélküli megvalósítását nyilvános és magánhálózati alkalmazásokra egyaránt.

Különböző TDR berendezésekből több százat szállítottunk a MATÁV és utódja a T-Com számára. Ilyen berendezések tucatjait üzemeltette az Antenna Hungária Zrt. Szállítottunk berendezéseket állami intézmények és szervezetek számára: egyetemek, NAV, Fővárosi Vízművek, FETIKÖVIZIG stb.

Külön említést érdemelnek a rendvédelmi szervek. A Magyar Honvédség (MH) számára 1993. óta szállítottunk berendezéseket. Szállítottunk ezen kívül összeköttetéseket a Határőrség, a Katonai Felderítő Hivatal és a Nemzetbiztonsági Szakszolgálat számára.

Eddigi működésünk alapján elmondható, hogy a Totaltel Kft. a nagy privatizációs hullámban és import dömpingben egyedüli magyar cégeként méltó partnere tudott maradni a hazai felhasználóknak. A Totaltel Kft. ismert termékeinek kiváló minőségéről, versenyképes áráiról és magas színvonalú szolgáltatásairól.

Munkatársaink tevékenysége felöleli az alábbiakat:

- Rádióhálózat tervezése
- Összeköttetések tervezése
- Hatósági engedélyezés lefolytatása,
- Kulcsrakész projektek megvalósítása, a berendezés fejlesztésétől és gyártásától, a rendszerintegráción át a telepítésig, beleértve a működtető személyzet képzését, és a dokumentálást is.

Fő termékeink:

- TDR-F flexibilis digitális mikrohullámú rádióberendezés 100 Mbit/s sebességig (5, 7, 8, 13, 15, 18, 23, 26 és 38 GHz)
- TDR-F-W nagysebességű digitális mikrohullámú rádióberendezés 350 Mbit/s sebességig (5, 13, 18, 26 és 38 GHz)
- TDR-F-IP5 nagy távolságú digitális mikrohullámú rádióberendezés 2 Mbit/s, azaz 1E1 csatorna átvitelére, sávszélesség takarékos modulációval (1,5 GHz, BW=500 kHz)
- Mikrohullámú antennák, Hálózatfelügyeleti rendszer (MX-MSS és SNMP).

Tudományos közlemények

NIKOLA TESLA

Jelen cikkemben bemutatom Nikola Tesla életét, főbb találmányait, különös tekintettel az energiatovábbításról szóló elméletére, kísérleteire és jelenkori hatására. Nikola Tesla 1856-ban született Smiljanban, a mai Horvátország területén levő településen, egy szerb ortodox pap fiaként.

1875-ben a grazi Politechnikai Intézetben kezdett tanulni. Itt egy német tanár, Poeschl professzor oktatta az elméleti és kísérleti fizikát. Az ő inspirálására kezdett nagyon komolyan foglalkozni az elektromossággal, pontosabban a motorokkal és a generátorokkal. Különösen felkeltette érdeklődését egy motorként és dinamóként is használható egyenáramú szerkezet, amit Párizsból kapott az intézetük. Tesla vizsgálta a készüléket, és észrevette, hogy az nagyon erősen szikrázott a kommutátorok (áramfordítók) miatt. Tesla javasolta a professzorának, hogy javítsák ki a konstrukciót úgy, hogy hagyják el belőle a szikrázást okozó kommutátorokat. Tanára megjegyezte: lehet, hogy nagy dolgokat fog elérni, de ezt sosem fogja megcsinálni, mert ehhez az kellene, hogy az egyenes vonalban ható erőt forgó erővé alakítsa át. Ez legalább annyira lehetetlen, mint az örökmozgó megalkotása.

Tesla 1881 januárjában Budapestre jött, főmérnöki állást kapott a Puskás testvérek által tervezett telefonközpont építésén. A budapesti Városligetben sétálva megjelent neki a megoldás, hogyan kell „orvosolni” a szikrázó problémákkal küszködő egyenáramú motor gondjait. A park porába, egy bottal rajzolta le először a váltóáramú dinamó és motor vázlatát, azét a motorét, amely az egész műszaki civilizációban fordulópontot jelentett. Tesla ekkor jött rá a forgó mágneses mezők használatára, ekkor döbbsent rá, hogy többfázisú áramot is lehet használni.

Budapesti feladatai befejeztével Párizsba ment, az Európai Edison társaságnál talált munkát. A kevés fizetés és a továbblépés lehetőségének a hiánya arra sarkallta, hogy 1884-ben szerencsét próbáljon Amerikában. Az Egyesült Államokban az akkor már híres Thomas Edison alkalmazta. Tesla átalakításokat végzett az Edison által feltalált és kivitelezett egyenáramú elektromos rendszeren, mely New York egyes részein már működött. Majd egyévi munka és több később szabadalmaztatott átalakítás után Edison nem fizette meg a munkáját, ezért Tesla kilépett.

Tesla elképzelése a vezetékes energiatovábbításról alapvetően különbözött Edisonétól. Tesla a nagyfeszültségű, váltakozó áramú energiatovábbítást és -felhasználást látta előnyösebbnek. Az idő később őt igazolta, a ma használt elektromos hálózatok, villamos energiatovábbító rendszerek az ő találmányai alapján működnek. Ebben a

1 NKE, Híradó Tanszék, Hadtudományi Doktori Iskola, doktorandusz (megyeri.lajos@uni-nke.hu).

rendszerben ugyanis sokkal kisebb az átviteli úton elszenvedett veszteség. Kezdetben nagy küzdelem volt a két feltaláló között, Edison nem akarta veszni hagyni a nagy befektetéssel létrehozott egyenáramú rendszerét. Végül a világ első villamos erőművét a Niagara-vízesésnél építették, és az áramot a közeli városba Tesla tervei szerint vezették el. A vízesésnél ma is szobor őrzi a feltaláló emlékét.

Tesla később megalkotta az első fénycsövet, a nevéhez fűződik az első szikratávíró, megteremtette a rádiózás alapjait. Kísérletezett a később Röntgen által szabadalmaztatott úgynevezett X-sugarakkal is. 1891-ben felfedezte az elektronikus eszközökben (például: rádió, televízió) széles körben használatos, róla elnevezett Tesla-tekeracet. Ez a tekercs több száz kV feszültséggel rádiófrekvenciás váltakozó áram indukálására volt képes. Több későbbi találmányában alkalmazta ezt a tekercset. Ezzel például villámszerű elektromos kisüléseket tudott produkálni laboratóriumi körülmények között. Találmányai között szerepel az első fénycső és az első működő szikratávíró is, amelyből a rádió fejlődött ki.

Nikola Tesla a századforduló környékén elkezdett a vezeték nélküli elektromos energiátovábbítással kísérletezni. Laboratóriumában megtalálható volt a valaha épített legnagyobb Tesla-tekeracs, mely képes volt 300 000 W energia generálására. Meggyőződése szerint az elektromos energiát a Föld atmoszférájába pumpálva azt a Föld bármely pontjára el lehet juttatni és ott visszanyerni. Ezt próbálta bizonyítani egy kísérlettel, mikor is 200 utcai lámpát világított ki, vezetékek nélkül, 42 km távolságból. Az ehhez szükséges energia előállítása során gyakran 40 m magasra is felcsapó villámok törtek ki a szerkezetéből. A gyakorlati problémát az jelentette, hogy a befektetett energia sokkal nagyobb volt, mint a visszanyert energia.

Elméletei között szerepelt, hogy ha a Földet övező ionoszférát bizonyos frekvenciájú energianyallal gerjesztjük, az ionosféra fényt bocsát ki, mely alkalmas lehet világításra. Tesla Colorado Springsben megépített egy óriási tornyot, a „globális, vezeték nélküli energiaátjátszó központot”, melynek alapja az atmosféra mint átjátszó közeg elektromos energiát vezető képessége. Maga az átjátszó állomás mintegy 18 emelet magas volt, melynek tetején egy 20 méter átmérőjű dóm volt. Tesla állítása szerint szerkezete képes 100 MV feszültségű, 1000 A áramerősségű energia előállítására, melynek energiaszintje eléri a 100 GW teljesítményt.

Sajnos a kísérletek az anyagi erőforrások kimerülése miatt abbamaradtak, és a tornyot 1917-ben lebontották. Életében 146 szabadalmat (ebből 112-t Amerikában) jegyeztek be a neve alatt. Barátai közé tartozott Mark Twain, a híres író, akivel megosztotta tudományos felismeréseit, merész gondolatait. Tesláról nevezték el a tesla (mágneses indukció) SI-mértékegységet. A világ egyik legjelentősebb és leghíresebb feltalálója, tevékenységét elsősorban az elektromosság és mágnesesség területén fejtette ki. Több fontos elméleti munkán és szabványon kívül a nevéhez kötődik a többfázisú villamoshálózat vagy a váltóáramú motor is.

Nikola Tesla 1943. január 7-én hunyt el New York-ban. A St. John-katedrálisban szászak vettek részt a gyászszertartásán. Végrendelete értelmében halála után hamvait,

személyes tárgyait, könyveit és dokumentumait Belgrádba szállították, ahol múzeumot nyitottak életművének.

NIKOLA TESLA ÚJRAFELFEDEZÉSE

Napjainkban számos, egykor Tesla által feltalált vagy az ő ötletét továbbgondolva kifejlesztett elektronikus eszközt használunk. A mai napig kísérleteznek elméletei alapján és az általa feltalált Tesla-tekerccsel. A nagyhatalmak is érdeklődnek találmányai iránt, ennek két jellemző példáját emelem ki.

1. Az orosz Tesla-torony 40 km távolságra van Moszkvától, a „Nagyfeszültségű Marx és Tesla generátor Kutató Intézet” nevet viseli. Célja energia kinyerése villámokból, de más célokra is használták. Ez a projekt a méreteiben különleges: a világon ez a legnagyobb (ismert) Tesla-torony (1. ábra).



1. ábra: Az orosz Tesla-torony

2. Az USA által életre hívott HAARP-program (High Frequency Active Auroral Research Program, azaz nagyfrekvenciás aktív sarki fény kutatási program) ionoszférát kutató létesítménye – Ionospheric Research Instrument (IRI) – a sarkvidéki térség legnagyobb beruházása a magas légkör vezetőképességének vizsgálatára, mely az alaszakai Gakona közelében, az amerikai légierő területén található. Működését 2007-ben kezdte meg. A HAARP hivatalosan egy tudományos kezdeményezés, melynek célja

az ionoszféra viselkedésének és tulajdonságainak tanulmányozása, illetve az eredmények alkalmazása a kommunikációs és felügyeleti rendszerek kialakításában, polgári és védelmi célokra egyaránt. Két fő részből áll: egy nagyfrekvenciájú (High Frequency) adóberendezésből és az antennarendszerből. Az antennamező 180 darab derékszögben felállított, kereszt alakú dipól szerkezetből áll (2. ábra). Az adó teljesítménye 3,6 MW.



2. ábra: A HAARP antennarendszere

Az antennarendszerrel az adó által előállított nagy energiájú hullámokat az ionoszféra különböző rétegeibe sugározzák tudományos célokból. A HAARP-programot sok misztikum és legenda övezi. Az interneten számos történet kering a létesítmény állítólagosan létező titkos projektjeiről, amelyek az időjárás befolyásolásától a földrengéskeltésen át (a „hívők” szerint egy ilyen legutóbb 2013. április 5-én rázta meg Észak-Koreát, és rongálta meg nukleáris berendezéseit) egészen a Földet támadni szándékozó földönkívüli lényektől megvédő fegyverek létezéséig terjednek.

Nikola Tesla munkásságát a mai napig misztikum övezi. Találmányait sokan sokféleképpen magyarázzák, népszerű az írott és elektronikus sajtóban is. Önálló Facebook-oldala van, és számos összeesküvés-elmélet hivatkozik vélt vagy valós felfedezéseire. Mivel saját nyilatkozata szerint hitt az UFO-k létezésében, és találmányait színpadiasan, misztikusan mutatta be, sokan földöntúli képességeket tulajdonítanak neki. Tény, hogy az elektromágneses jelenségek vizsgálatakor – elutasítva kora szaktekinvélyeinek az álláspontját – több területen is korszakalkotó áttörést ért el, amit véleményem szerint zseniális gondolkodásának és kitartásának köszönhetett.

IRODALOMJEGYZÉK

- [1] TESLA, Nikola: *Experiments with Alternate Currents of High Potential and High Frequency*. N. Y., AIEE, Columbia College, 1891.
- [2] BIRD, Christopher – NICHELSON, Oliver: Nikola Tesla: Great Scientist, Forgotten Genius. In: *New Age Magazine*, February 1977, Annual 2006 for the Croatian Academy of Engineering.
- [3] www.skory.gylcomp.hu/tesla/tesla.html
- [4] www.sasovits.hu/anyag/feltalal/tesla.htm
- [5] <http://wignerjenoszakkollegium.hu/kiskor/?q=node/4>
- [6] www.haarp.alaska.edu/haarp/
- [7] www.ewao.com/a/1-teslas-legendary-tower-built-and-tested-in-russia

MOBILE COMMUNICATION AND MIGRATION – SOME RESEARCH ASPECTS OF THE ISSUE

Nowadays Europe is confronted with the mass of migrants. The mobile communication equipment, the developing communication and IT applications, and even the widely used social networking sites undeniably have been in the background of all these population movements. Lots of studies were reported in media drawing attention to the complexity of the topic and also to the role of information and communication technologies (hereinafter: ICT) and especially smartphones, which are related to migration. This short essay wishes to draw attention to the linkage between migration and mobile communication and to flash on some research directions on the international scene.

It is fact, that global accesses to information, the achievement of social, political and economic conditions have high importance in recent days, which can not be done without the various ICT solutions. The global ICT sector rapidly develops, and in the terms of its dynamism, it is worth to see the ITU (International Telecommunication Union) statistics:

- „In 2015 there are more than 7 billion mobile cellular subscriptions worldwide, [...] and globally 3.2 billion people are using the Internet of which 2 billion are from developing countries.”¹ „By end 2015, 34% of households in developing countries have Internet access, compared with more than 80% in developed countries”.²
- Nevertheless it also marks the gap between the two parts of the world. While the ICT solutions have become an indispensable part of everyday life in the developed areas of the world, in Africa it is still only one in five people who uses the Internet every day, and the rate of penetration of mobile networks is significantly lower than in the developed world.

A published UN research study in 2009³ summarizes the relationship between migration and communication technologies and its significance. Concerning the glo-

1 SANOU, Brahim, director of the ITU Telecommunication Development Bureau, May 2015, Telecommunication Development Bureau, International Telecommunication Union. www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (2015. 09. 01.)

2 ICT Facts & Figures, SANOU, Brahim, director of the ITU Telecommunication Development Bureau, ICT Data and Statistics Division, Geneva, May 2015, Telecommunication Development Bureau, International Telecommunication Union. www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

3 HAMEL, Jean-Yves: Information and Communication Technologies and Migration United Nations Development Programme. In: *Human Development Research Paper*, 2009/39.

balization, technological and infrastructural development it also points out, that the largest online communities (according to ITU data) were in Asia and China in 2009, but these statistics are similar nowadays. We could realize that the ICT infrastructure continuously develops in those countries, which play the role of migration sender, and more and more people (eg. in Africa) are connected to the Internet or have access to mobile telephony capabilities. It is also a peculiarity, that the widespread usage of wired communication is simply left out from the development process in many regions, and the population immediately faced with mobile phone systems, or reaching the World Wide Web. The development of ICT is worth to be highlighted by some statistical data of the related countries:

- One of these indicators is the “Percentage of Individuals using the Internet” that shows different levels of development in the past ten years. While, for example, 4.32% of the population in Syria used the Internet in 2004, this rate reached 28.09% in 2014. Similar increases can be seen for example in Turkey, where during the same period 14.58% to 51.04%, in Nigeria, where 1.29% to 42.68%; in Libya, where 3.53% to 17.76 the proportion of Internet users have risen. By contrast, in Afghanistan, it is only one in 15 people (6.39% of the population), or even in Iraq, every 10th people (11.3% of the population) use the Internet.
- Significant progress has been observed in relation to the proliferation of mobile phone usage for years. For example in 2014, in Afghanistan nearly 75 pieces, in Syria nearly 71 pieces, in Iraq and Turkey nearly 95 pieces, in Jordan nearly 148 pieces, in Libya 161 pieces of subscriptions had in average of 100 inhabitants. (By comparison, in Hungary, in 2014 there were 118, meanwhile in Germany, there were 120 subscriptions per 100 inhabitants.) It is a fact that, in some overpopulated countries tens of million mobile phone subscriptions are behind the rates (eg. in Nigeria nearly 139 million, nearly 136 million in Pakistan, Bangladesh more than 120 million subscriptions) are displayed. All these indicate that the mobile communication with its benefits (eg. of wireless, access / subscriber base growth, rapid development capabilities) has become essential and personal mobile communication solution of everyday life through.

Since there are not available documented data on the composition of current European migratory, as an input data, it would be worth to review ICT data in major areas of migration. It is called for IDI index, which indicates a country's ICT development level on a complex way. In the composition of IDI plays role: the access to ICT, the usage of ICT and the ICT skills.

- On the IDI index (166 ranks) list, where Germany is the first, in 2012–2013, Hungary was on the 46th, Turkey on the 58th, Syria on the 112th, and Afghanistan on the 155th place
- On the first third of the list, basically the economically developed countries can be found, in the last third of the list are African and Asian developing countries. The IDI index of the African continent is considered to be the lowest, despite of

the fact that the infrastructure and usage of mobile networks have risen. At the same place a significant gap can be seen in the achievement of the internet. At the end of 2013 less than 10% of the households had Internet access (the average in the developing countries was 28%).

- In the Arab states, a strong fragmentation can be observed. In contrast to the more developed countries (Bahrain, United Arab Emirates, Qatar, Saudi Arabia and Oman) there are the less developed regions, and countries (eg. Syria, Yemen). The mobile network penetration is generally high (100% and more) but in Syria it was only 56% in 2013.⁴

Concerning the role of mobile communication related to the migration we faced with an extremely complex issue. Generally stating, the composition of the current migration pressure affecting Europe is mostly from the younger generation, which is more willing to use developed technical solutions. ("The so-called Y and Z generations [...] are pioneers in the usage of new communication solutions [...] they are much more interested in Internet-based communication, they use and acquire the extended functions naturally and fully use."⁵) The information about the developed world through the ICT solutions – in particular the use of the Internet/smart phones – appears as a special "pull" factor. Even in the undeveloped regions (eg. Africa) too, lots of shops and vendors sell various types of mobile phones, opening the range of information and options (eg. business, political, social, health, and educational links). The possible migrants via these technical platforms get "supporting" information about the economic, social, and political environments of the destination area, or will be able to choose the migration routes, or even the options of border-crossing. The movement of migrants in an foreign geographically area, the planning routes on digital maps or even usage of the digital language translator make indispensable the use of mobile communication devices. As a result of a Hungarian conducted research study in recent times, in connection with the Balkan route, it sets out that "the vast majority of people involved in illegal migration, use of mobile phones or the Internet, and many people use electronic money transfer services".⁶ The use of devices can be divided in four main areas: information gathering of migrants, communication with other groups, the existential (ie. money remittance-receiving), or emergency-type activities.

Lots of relevant examples can be found about the linkage between migration and mobile communication in the media.

- In connection with the current southern mass migration flow, the media clearly indicates that "groups" constantly gives information to the next migrant group

4 Az adatok forrása: *Measuring the Information Society Report 2014*, ITU – International Telecommunication Union, Geneva, Switzerland.

5 DOBÁK I. – KOVÁCS Z.: Új technológiák hatása a hírszerzésre. In: *A nemzetbiztonság általános elmélete*. NKE, 2014, 217.

6 PAP N. – NAGY J. T. – VÉGH A. – LÉPHAFT Á.: A magyarországi muszlim migránsok az információs társadalomban. In: *Infonia, Információs Társadalom folyóirat*, 13. évf. 3–4. sz. 69–77.

via their mobile phones, including information about the routes, possible border crossing points, or even the control of border agencies. As a result, it might change the focal points of migratory pressures on the state borders as well.

- The "21st-Century Migrant's Checklist: Water, Shelter, Smartphone" article (was published in the *New York Times* in August 2015⁷) illustrates the indispensability of mobile phones, and that the charging of mobile devices or the access to information during the migration are a basic need. We find news in media that migrants often ask for help from the media staff or TV satellite trucks in order to charge their smartphones.⁸ It can also happen that the carriers involved in their transportation, sell the charging of smartphones as a service in their car. In another cases, the charities provide the necessary plugs to charge phones or free wireless Internet access. The media also reported that refugees wanted water and to charge their mobile phones.
- Concerning the usage of mobile phones we find some examples for saving lives too. Mainly on the migratory route from Africa on the Mediterranean Sea, it is a common method, that the migrants crossing by ships, indicate the emergency situation to the Italian coast guard by their mobile devices. According the news they hope that after the rescue, the authorities give them a lift to the EU. Often the human traffickers themselves send the immigrants to the Sea with mobile phone, aligned them to start an emergency call to the border enforcement agencies from the middle of the sea. It was also an example of that case when the mobile phone saved the life of migrants who intended to travel to Britain in a refrigerator lorry. "Migrants were rescued from a refrigerated lorry in northern France [...] They were only found because one managed to get a call out to police on his mobile phone and [...] French police managed to track them using a GPS tracking system".⁹ These examples of using mobile phones (and the available information) show that these devices give "indispensable" support to the migrants on their routes.

Besides the "traditional" usage of mobile phones, it important to mention the role of the social networking sites that can help the information-sharing and avoiding the high costs of mobile phone. Moving to distant geographical regions, the migrants often get the main information via different Internet solutions. Therefore, the different

7 BRUNWASSERAUG, M.: *A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone*. www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=0

8 HARTOCOLLIS, A.: *Traveling in Europe's River of Migrants, Refugees in Budapest Use TV Satellite Truck to Recharge Their Phones*. 8. September 2015, www.nytimes.com/interactive/projects/cp/reporters-notebook/migrants/phone-charging-stations

9 DE GRAAF, Mia: *Gang that charged illegal immigrants £4,000 for 'guaranteed arrival in UK' is arrested by French border police*. 21. December 2013, www.dailymail.co.uk/news/article-2527498/People-smuggling-gang-charged-illegal-immigrants-4-000-guaranteed-arrival-UK-cracked-French-border-police.html

social applications have extraordinary importance, which might affect the actions of masses of vulnerable migrants. The information on the social sites (eg. the Facebook with 1.28 billion, the Google+ with 1,6 billion or the Twitter which has more than 645 million registered users¹⁰) by accessing larger groups can directly influence the movement of the masses, or even can have an impact to it. But the information which is placed on these sites could threaten the migrants as well because of the truth and ambiguity of the information. Here must be mentioned the organized human smugglers, who widely use the advertising possibility of the Internet pages, and it may occur, that the internet is the place of first connection between the smuggler and the migrant. The well-intentioned but equivocal or false information also lead to misunderstandings as they provide “pull factors” for the migrants. These could be news in the different social media, statements and resolutions. The usage of personal profiles on the social networking sites, indirectly contribute to identify a person. Some media sources revealed example in Syria, that “Soldiers at government checkpoints, as well as at Islamic State checkpoints, commonly demand Facebook passwords [...] They look at Facebook profiles to determine one’s allegiance in the war.”¹¹

So far, little significance have got those photos, images and digital data which have arrived to Europe on mobile phones or on data storage devices. However, due to the permanent leaving of the place of residence or a country, people often carry themselves the memories and traces of their former life in digital format. Among these, could be some digital traces of conflicts which have occurred around them, and those public disclosures (eg. from the events of armed conflicts) will definitely influence the ex post assessment of these events, or of individual person.

However, the using of ICT equipment does not stop after migrants arrive to the destination country. Arriving to a previously unknown geographical area the migrants find themselves in special situation, where directly appear for example the language barriers, searching social contacts to help their life, finding job opportunities, or the need of connection with family. With the help of ICT the migrants can “easier access to information, [...] keep up to date with events in both the country of origin and the host country, or get information about administrative procedures, job adverts”.¹² Concerning a study in this topic, immigrants pay great attention to the role of mobile phones (eg. often have two devices), which is interpreted as a link between the owner and the developed world. As Ros, A.– González, E.– Marín, A. – Sow, P.: *Migration and information flows: a new lens for the study of contemporary international migration* study (published in 2007) states: “Technology has always played a major role in the history of migration. But in recent years, this relationship has become stronger than

10 List of social networking websites. https://en.wikipedia.org/wiki/List_of_social_networking_websites

11 BRUNWASSERAUG, M.: *A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone*. www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=0

12 www.uoc.edu/in3/dt/eng/ros_gonzalez_marin_sow.pdf

ever. Today, migrants need to use technology to travel, keep in contact, send money home, or get information on host and sending societies.” Answering the question, that how the migrants from the undeveloped countries are able to use modern communication devices, we can get the answer from the above mentioned study. There is a need to connect them to their families (capability of using satellite television broadcasts, remittance services) or access the necessary information (internet use). In the same time, an increasingly demand for advanced technologies could also be observed in the sending areas, because the communication with relatives requires the use of modern (fast, cost-effective) ICT equipment and solutions. The understandable aim of this trend is the more complete information sharing with each other, which is no longer possible without cell phones or using internet telephony capabilities.

Regarding the composition of relevant migration pressure in Europe, it is currently impossible to determine exactly its internal structure, but for example the smartphones are able to promote managing the migration on the sending, on the transit and also on the destination areas. Such examples can be seen in the specific fields of use as mentioned below:

- In the United States there is a program called Lifeline Assistance as a free government cell phone program, which is open to undocumented migrants and provide mobile phones (LG, Motorola or Samsung). Reading the FreeGovernmentCellPhones.net 2013, one of the main aims of the program could be promoting social connections of undocumented migrants (ie. employment, health, family relationships). As the document says: "Has no rule stating that recipients must be a citizen of the United States, but you have to connect to certain programs."¹³
- Another example for the role of mobile phones is in connection with the conflict in Syria. "In Jordan, UNHCR is about to launch a new program giving Syrian refugees custom-designed mobile phone SIM cards through which they can receive mass information messages. Each SIM card will come with a ready-built menu providing key information and contact details of service providers."¹⁴ According to another source "The Office of the United Nations High Commissioner for Refugees has distributed 33,000 SIM cards to Syrian refugees in Jordan and 85,704 solar lanterns that can also be used to charge mobile phones."¹⁵

In different approach, the age of ICT is strongly characterized by the convergence where can be seen the fusion of various information and communication technologies

13 The undocumented immigrant's guide to free government cell phones, 2013, (FreeGovernmentCellPhones.net). www.freegovernmentcellphones.net/undocumented-immigrants-guide-to-free-government-cell-phones.pdf (2015. 09. 10.)

14 www.unhcr.org/cgi-bin/texis/vtx/refdaily?pass=52fc6fbd5&date=2013-11-19&cat=Syria (2015. 10. 10.)

15 <http://anonhq.com/for-syrian-refugees-smartphones-are-more-important-than-food/> or www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=0 (2015. 10. 10.)

and the emergence of new technologies. Therefore the mobile telephony (think about smartphones) on the one hand could be personal communication solutions and on the other hand a community communication solution ensuring exchange of information for mass. Reviewing some scientific researches related to ICT and migration we can find several research directions. We find researches within the framework of social science, or natural science as well. Very interesting research fields are the social life, the mobility, the e-diaspora, ethnic minorities, and so on. There are lots of scientific researches from technical point of view as well, which are based on for example the GIS (geographic information system) data, or the data of mobile operators. The data of mobile phone using obviously appear in the system of mobile phones operators. These data as anonymous data could be a special kind of imprint (in space and time) of the migration. Scientific research of examining these data for the purpose of population movements is not new, its principles and methods evolved in parallel with the emergence of mobile communication systems. One of the direction of the subject can be found in a research study published in July 2015 (Williams-Thomas Dunbar, Eagle Dobra/2015). The basic idea of the examining the data displayed in the cell phone providers systems (for example billing data), based on that the data are able to indicate massive, impersonal population movements within a larger areas (eg. Africa). However, several elements make it more difficult:

- Lack of open data access for scientific research in connection with the international migration.
- The rapid penetration of mobile communication.
- The different infrastructural – development level of network infrastructure in the countries.
- The knowledge of the mobile phone usage rates among the population and the migrants, etc.

Taking everything into account, all of these data could allow mainly estimates. Researches of the topic have been currently in progress, looking for a different measurement methods and solutions. It has wide significance, as mentioned study also calls attention to it – during natural disasters (think for example, flooding, floods, earthquake or other industrial disasters), various emergency situations, or to study the effects on the armed conflict caused population movements.¹⁶ Other studies also highlight the fact that some of the mobile data networks as sources of information could be suitable for research of human mobility, and the movement of human groups. The datasets with their spatiality and temporality elements could be applicable the deduction of valuable conclusions. The results of human mobility research have been applied in many fields, such as in traffic forecasts or tourism. As M. Tiru and R. Ahas

16 <http://anonhq.com/for-syrian-refugees-smartphones-are-more-important-than-food/> or www.ny-times.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=0 (2015. 10. 10.)

states, "Using mobile positioning data in scientific research has several positive aspects as speed of data collection, digital format of data, large sample and high penetration of phones in most of societies."¹⁷

Summarizing, as conclusion can be drawn, that the usage of different ICT tools and solutions is a special element of the phenomenon of migration. Their root causes could be the collection of information, the relationships, and maintaining prosperity in the target area by the migrants. The current migration trends likely will have impacts to the interdisciplinary research of the issue of mobile communication, and new research directions might be formed. In the atmosphere of digital world the "residual" digital data in the systems will certainly allow valuable impersonal analysis, about human activities in the future. The scientists will search the answers for those types of questions that:

- How can the ICT help the support of migrants?
- How the migration flows can forecasted by ICT?
- How will the ICT affect to the immigrants in the developed world?
- How will the ICT help the relationship between migrants on the destination country and their families at the host country?

REFERENCES

- [1] ROS, Adela – GONZÁLEZ, Elisabeth – MARÍN, Antoni – SOW, Papa: *Migration and information flows: a new lens for the study of contemporary international migration*. IN3, Internet Interdisciplinary Institute. www.uoc.edu/in3/dt/eng/ros_gonzalez_marin_sow.pdf, <http://in3wps.uoc.edu/index.php/in3-working-paper-series/article/view/n7-ros-gonzalez-marín-sow/n7-ros-gonzalez-marín-sow>
- [2] ALONSO, Andoni – OIARZABAL, Pedro J.: *Diasporas in the new media age, Identity, Politics, and Community*. University of Nevada Press, 2010.
- [3] DE HAAS, Hein: Migráció és fejlődés elméleti megközelítésben. In TARRÓSY István – GLIED Viktor – KESERŰ Dávid (szerk.): *Új népvándorlás. Migráció a 21. században Afrika és Európa között*. 2. kiadás. Pécs, Publikon Kiadó, 2012, 53–84.
- [4] HAMEL, Jean-Yves: Information and Communication Technologies and Migration. United Nations Development Programme, August 2009, In: *Human Development Research Paper*, 2009/39.
- [5] SCHAPENDONK, Joris: Turbulent Trajectories: African Migrants on Their Way to the European Union. In: *Societies*, 2012, 2(2), 27–41.

17 TIRU, Margus – AHAS, Rein: *Passive Anonymous Mobile Positioning Data for Tourism Statistics*. www.congress.is/11thtourismstatisticsforum/papers/Session3.pdf (2015. 10. 02.)

- [6] DE GRAAF, Mia: *Gang that charged illegal immigrants £4,000 for ,guaranteed arrival in UK' is arrested by French border police.* 21. December 2013. www.dailymail.co.uk/news/article-2527498/People-smuggling-gang-charged-illegal-immigrants-4-000-guaranteed-arrival-UK-cracked-French-border-police.html
- [7] FARRELL, Nicholas: Welcome to Italy: this is what a real immigration crisis looks like. In: *The Spectator*, 20. June 2015. www.spectator.co.uk/features/9560982/the-invasion-of-italy/
- [8] PAP Norbert – NAGY Janka Teodóra – VÉGH Andor – LÉPHAFT Áron: A magyarországi muszlim migránsok az információs társadalomban. In: *Infonia, Információs Társadalom folyóirat*, 13. évf. 3–4. sz. www.infonia.hu/infotars/arch_2013_34.html
- [9] KINGSLEY, Patrick: *People smugglers using Facebook to lure migrants into 'Italy trips'.* 8. May 2015. www.theguardian.com/world/2015/may/08/people-smugglers-using-facebook-to-lure-migrants-into-italy-trips
- [10] COLLARD, Rebecca: *The Christian Science Monitor*. 18. November 2013. UNHCR Refugees daily. www.unhcr.org/cgi-bin/texis/vtx/refdaily?pass=52fc6fbd5&date=2013-11-19&cat=Syria
- [11] PRICE, Rob: *Google Maps is putting Europe's human-traffickers out of business.* Business Insider.uk. <http://uk.businessinsider.com/refugee-crisis-how-syrian-migrants-use-smartphones-avoid-traffickers-2015-9#ixzz3lMkYiLHb>
- [12] TARRÓSY István: Elméleti megfontolások a nemzetközi migrációs tendenciák megértéséhez. In TARRÓSY István – GLIED Viktor – VÖRÖS Zoltán (szerk.): *Migrációs tendenciák napjainkban*. Pécs, IDRResearch Kft. – Publikon Kiadó, 2014.
- [13] WILLIAMS, N. E. – THOMAS, T. A. – DUNBAR, M. – EAGLE, N. – DOBRA, A.: *Measures of Human Mobility Using Mobile Phone Records Enhanced with GIS Data.* PLoS ONE 10(7): e0133630.doi:10.1371/journal.pone.0133630, PLOS ONE, DOI:10.1371/journal.pone. 0133630 July 20, 2015.

SECURITY STRUCTURES

The steps taken for security may come from two directions. In this publication we provide a comprehensive picture of the structure of NATO information facilities and their brief history, as well as the internal structure of the organizations of the Hungarian Defence Forces. A variety of organizations, companies had reached an agreement to share their experiences in this field, so that specific attack methods can not be applied more than once, once the response mechanism has been developed somewhere, in order to develop an effective information security system. To enable the secure exchange of information a Cross-Domain Solutions (CDS) procedure has been developed, which allows each party to use their own protocols to share information with other parties. A uniform system is used which monitors data traffic and enables data sharing between the various elements so that it is inaccessible for third parties. This solution is used for linking military communication systems, but in the civilian sector it's also used by major companies to eliminate industrial espionage.

NATO SOLUTIONS

The association recognizes that the war is not only based on the ground, water and air, but also introduced a new battlefield: the cyberspace. In this area, there are still plenty of undiscovered opportunities: the intention of the attackers is to discover increasingly newer vulnerabilities and to reach their goal by exploiting these.

NATO has incorporated this into their Strategic Concept as a priority, and the recent summits revisited the issue as a point to discuss. Historically NATO has always defended its IT systems, but as long as there was no major threat in this area, defense remained at a basic level. The first time when the topic got on the NATO summit agenda was in Prague 2002, and when it became clear that this is a crucial topic to the alliance's future and further measures are needed to create a stronger defense, it was discussed again at 2006 meeting in Riga. Then came the turning point in the views of the alliance: In 2007, a NATO member, Estonia, suffered a cyber-attack that paralyzed the entire infrastructure.

The same year the defense ministers of the Member States got together and adopted a decision to set up a Cyber Security Policy, which they issued in 2008. The cyber activity at the summer of this year used in the Russian-Georgian conflict highlight-

¹ Associate professor at UNPS.

ed that this area should be rightfully called a battlefield, and should be included in the concept of war and the planning processes of operations. The Lisbon Summit in 2010 was another milestone, as the new strategic concept was created here. It declared the establishment of a new, more detailed cyber-defense policy, which also includes the response plan for its implementation. The document was adopted by the defense ministers in June 2011, and it clarifies the risks and the responses to be given to rapidly evolving technological changes. The defense development process began to incorporate the important elements of the area in April next year. In May the same year, at the Chicago summit the leaders of the alliance states have taken further steps to strengthen cyber-defense: centralizing the networks of the alliance, and expanding and enhancing the NATO Computer Incident Response Capability (NCIRC) has led to improved security. The NATO Communications and Information Agency (NCIA) began its operation in July. In February the same year the development of new policy guidelines begun, which was signed at Wales in September. The latest enhanced guidelines, which include an updated response plan were adopted by delegates from the member states at the Welsh Summit held in September 2014. It identifies cyber-security as one of the main points within the framework of collective defense.

In addition, it states that the alliance complies with international laws in cyberspace, and lays the foundation for cooperation between NATO various industries. The agreement emphasizes the importance of continuous control over this area, processes supporting alliance forces, and involving the analysis of battlefield events in operational planning. It identifies the enhancement of readiness, and performing training, and training exercises as an important task, encourages the cooperation with member states and international organizations. By strengthening such relations a defense system based on information exchange between different sectors and organizations can be created. NATO regards the European Union and the United Nations organization as a major partner. Great emphasis is placed on information flow and processing experience – not only within the alliance – so that recovery from cyber-attacks, prevention and minimization of damage can take place as quickly as possible. Part of the agreement was to develop a response plan that includes the implementation deadlines.

The approach within NATO is that "fortress" of cyber-defense it is made up of four basic elements.

1. Situational awareness

The strategic level of situational awareness implemented by the Allied Command Operations (ACO). This institution has sufficient information to be able to develop long-term plans, which are needed to perceive future threats. Commands subordinate to ACO, such as NATO Allied Joint Force Command Naples (JFC Naples) and the Communication and Information Systems Group (CIS) are responsible for the operational level. Their main task is to analyze the weaknesses of networks and systems – if

they have a backup power source, components of the system are properly ventilated and if the employees are appropriately trained. The tactical level is provided by the NATO Communications and Information Agency. It usually uses open-source information provided by software development or anti-virus development companies. These companies often offer a configurations and upgrades suitable for the tactical level. The short term the goal is to apply the widest possible range of products in combination, providing sufficient information for governing bodies to make the appropriate decisions.

2. Planning

In the Military it's very important to be prepared, so that potential outbreak of conflicts is does not leave the Alliance unprepared. Cybersecurity issues play an important role in all plans and none of them could be effective without adequate situational awareness. The Supreme Headquarters Allied Powers Europe (SHAPE) is responsible for drawing up strategic plans, according to which lower level commands are formed by the ACO.

3. Exercises

Exercises are usually designed on the basis of the above scenarios. These are used to assess the preparedness of the troops and determine those areas that still need improvement. There are two kinds of exercises are organized for cyber-security personnel. One is organized by ACT jointly with subordinate commands. These involve larger scale, extensive simulations that train personnel to perform their tasks within challenging circumstances, in cooperation with other NATO organizations. Another group of exercises only takes place in cyberspace. In these there's more emphasis on tactical level tasks. Such is the annually held Cyber Coalition exercise, which our country helped to organize through the National Security Authority for many years, but this year for the first time experts of the Ministry of Defense also play a role in in the simulations, based on 2013 observer experience.

4. Continuity

Measures taken in case of catastrophes are to be included in continuity plans. Scenarios are elaborated on how to insure the operation of the most important lines of communication when the computer systems cannot operate, or can only perform limited operation.

DOMESTIC TASKS

Organizations in the spirit of collective defense providing cyber-security consider the implementation of network security as the task of individual NATO states. The alliance only imposes standards or guidelines on the member states, so that they are always up to date. NATO is responsible for protecting its own networks. It's the responsibility of the NATO Communications and Information Agency to establish and maintain most parts of cyber security systems, but works closely with the Strategic Command, particularly the Allied Command Operations, so that NATO's cyber-defense is continuously up-to-date and impenetrable. Thanks to the NCIA, the NATO Computer Incident Response Capability (NCIRC) has reached full readiness last year, which is responsible for the security of 51 alliance installations, became part of the process of defense planning, and played a role in the organization and implementation of the yearly Cyber Coalition exercise.

The NCIRC Technical Centre (Technical Centre) is located in Mons, Belgium, this institution is responsible for technical support of cyber-defense within NATO, so it plays a key role in responding to cyber-attacks. Its' main tasks are to respond to and report incidents, and to provide information and experience on attacks to end-users and organizations monitoring system-security. The most important role in the field of research played by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), which was set up after the 2007 attack paralyzed Estonia in 2008. As a result of the attack significant investments have been made in the country to develop cyber-defense, so the facility opened its doors in the most appropriate place, the Estonian capital Tallinn. The goal of the center is to preserve the cooperation, information exchange within the nations of the alliance and to increase capabilities in this field. It tries to reach its' goals by organizing joint exercises, legal and professional conferences and various trainings. To support these they've gathered a group of experts from various NATO member states, including Hungary. Their research results provide the basis of trainings, so that the attendees can learn from an authentic source.

Since NATO does not provide the cyber-defense of individual member states, it also became the task of Hungarian Defense Forces to create their own defense system. In Hungary the National Security Authority (NSA) that operates as part of the Ministry of Interior and the Ministry of Defense is responsible for the national level of military cyber-security. The responsibility of the Ministry is to create the cyber-defense installations of organizations, to control their operation through laws, and to operate the Military National Security Service. While the NSA accredits and oversees the operations of various organizations. The task of the General Staff is planning on the level of the Hungarian Defense Forces, a specific command of this is the Communication and IT and Cyber-Defense Command.

Among the four Divisions of commands the IT and Cyber-Security Division are responsible for developing communication, IT cyber-security plans, planning and

controlling peace and crisis time technical operations, and the management of the systems of organizations directly subordinate to the General Staff. The commander of corps not directly subordinate to the General Staff is a mid-level commanding organization the Joint Force Command (JFC), who has a separate command for providing technical operations, so the J6 command is responsible for the topic of IT and cyber-security. They supervise and assist each signal corps specialist team's activities. Some military organizations differ in the number of security staff and interdependence, this usually depends on the amount of classified data generated and to be processed. Every unit contains a security chief appointed by the commander, who is responsible for classified data management and for meeting the required conditions. Their responsibility is to decide what kind of subordinates are required for the secure usage of information. The system-security management is responsible for any information systems the organization might have. If classified information is distributed electronically to or from other units, this can only be done using cryptography, and a cryptographic management should be established. In addition a security manager should manage the resulting classified information within an organization. In addition, the security manager can initiate the creation of a local security management if a large amount of classified information is handled by the organization.

SUMMARY

In the world of IT the issue of security is constantly changing and increasingly newer trends dictate the direction of change. Keeping track of this constantly changing challenge is hard even for IT security specialists, not to mention average end-users.

It is especially important that not only should the software be always up to date, but also that the users follow the kind of challenges they can encounter on the web and how they can overcome them, and if they discover a new threat, they know who to contact and where they can share their experience. The preparedness of personnel in leading positions in this area is crucial. The application of appropriate security measures is especially important in the military, and also to be familiar with not only our own country's system but also the hierarchy formed by allied forces including their installations and the devices managing them.

REFERENCES

- [1] BREEDLOVE, Phil: *Attacks from Cyberspace... NATO's newest and potentially biggest threat*. www.aco.nato.int/saceur2013/blog/attacks-from-cyberspace-natos-newest-and-potentially-biggest-threat.aspx (2014. 10. 05.)
- [2] FAISAL, Khawaja: *Global State of Information Security & Standards*. PITB – Information Security Conference, 2013. 03. 12. www.youtube.com/watch?v=ZvukDyve1Ds; www.tempest.hu/index.php?option=com_content&view=article&id=65:mi-is-az-a-tempest-&catid=11:cikk&Itemid=1 (2014. 09. 30.)
- [3] www.nbf.hu/tempestmer.html (2014. 10. 10.)
- [4] www.crossdomainsolutions.com/cyber-crime/ (2014. 10. 17.)
- [5] KERTI András: *Az információbiztonsági kockázatkezelés oktatásának buktatói*. Budapest, NKE, Kommunikáció 2013, 53–60.
- [6] FEKETE Károly: The Main Technical Characteristics of the Insular Telecommunication Network for Purpose of Government of the Hungarian Defense Forces. In: *Bolyai Szemle*, 2015/1. 70–77.
- [7] KERTI András – PÁNDI Balázs – RAJNAI Zoltán: Structure of the command and information system. In: *Hadmérnök*, 2009, 4. évf. 3. sz. 303–309.
- [8] KERTI András – PÁNDI Erik – TÖREKI Ákos: *A vezetési és információs rendszerek elméleti megközelítése*. Budapest, ZMNE, Kommunikáció 2010, 39–49.
- [9] MATHER, Jim: *Warning: Information is Everywhere*. www.act.nato.int/article-2014-1-13 (2014. 04. 06.)
- [10] Microsoft Digital Crimes Unit & IDC & NUS: *The Link Between Pirated Software and Cybersecurity Breaches*. www.play-it-safe.net/ (2014. 11. 10.)
- [11] FEKETE Károly: Several considerations of disaster recovery communications. In: *Hadmérnök*, 2014, 9. évf. 3. sz. 311–317.
- [12] MURPHY, Kate: Web Photos That Reveal Secrets, Like Where You Live. In: *The New York Times*, 2010. 08. 11. www.nytimes.com/2010/08/12/technology/personaltech/12basics.html
- [13] WordPress: *SaferInternet*. <https://saferinternet.hu> (2014. 10. 10.)
- [14] RIZWAN, Ali: On cyber defence. In: *The Three Swords Magazine*, 2014/26.

AZ INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

Az állami és önkormányzati szervezetek egyre nagyobb mértékben támaszkodnak informatikai és infokommunikációs megoldásokra közfeladataik elvégzése során. A kormány felismerte az információs rendszerek és a bennük kezelt adatok biztonságától való függés kockázatait. Az elektronikus információ kockázatarányos védelme érdekében kidolgozták a 2013. évi L. törvényt és végrehajtási rendeleteit (a továbbiakban: Ibtv.). Az Ibtv. a szervezeti, a fizikai és a logikai biztonság területén is elvárásokat fogalmaz meg a szervezetek számára, biztonsági szintenkénti bontásban. Az Ibtv. 4. szintjének teljesítését elősegíti a követelményeknek az *információbiztonsági irányítási rendszer (IBIR)* keretében történő megvalósítása.

Az MSZ ISO/IEC 27001:2014 szabvány világszerte elismert módon teszi lehetővé információbiztonsági irányítási rendszerek bevezetését minden szervezet számára. A szabvány és a jogszabály biztonsági követelményeinek teljesítése fizikai, logikai, szervezeti és életciklushoz kapcsolódó integrált intézkedések kialakítását igényli irányítási, adminisztratív és technológiai szinten egyaránt. Ugyanakkor az elsősorban a szabványok és jogszabályok alapján létrehozott irányítási rendszerek és folyamatok sok esetben elszakadnak a mindennapi feladatok végrehajtásától, akár olyannyira, hogy esetenként már akadályozzák is a kitűzött célok elérését, más esetekben pedig a kialakított szabályozás nem felel meg minden tekintetben az irányítási rendszer követelményeinek. Nem megfelelő az IBIR tehát, ha a szabályozás nem betartható, illetve az eljárásrendek nem végrehajthatók, továbbá akkor sem, ha betartható, de nem csökkenti megfelelő mértékben a kockázatot.

Jelen tanulmány arra keresi a választ, hogy milyen szakmai okokra vezethetők vissza az irányítási rendszer bevezetésének és végrehajtásának nehézségei, ez miként kerülhető el az Ibtv. követelményeinek teljesítése során, nemzetközileg bevált gyakorlatok segítségével. Az okok feltárása lehetőséget nyújt az állami és önkormányzati szervezetek számára, hogy megfelelő módon, betartható szabályozásokat, végrehajtható eljárásrendeket és működő információbiztonsági irányítási rendszert vezessenek be.

Az információs társadalom kialakulásával felgyorsult az információcsere, és a műszaki fejlődés megteremtette ennek infrastrukturális feltételeit. Az ipar, a kereskedelem és a közszolgáltatások működése is elképzelhetetlen infokommunikációs szolgáltatások nélkül. Az információs rendszerek és a bennük kezelt információ védelmét az információbiztonsági menedzsmenttevékenység képes biztosítani egy szervezetben.

1 Tanársegéd, Óbudai Egyetem, PhD-hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola (dombora.sandor@kvk.uni-obuda.hu).

2 Címzetes főiskolai docens, PhD-hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola (horvath.gergely.krisztian@bgf.hu).

A hazai szakirodalomban (például Vasvári György: *Vállalati biztonságirányítás – Informatikai biztonságmenedzsment* című könyvében) a biztonságot egy kedvező állapotként definiálják, amelynek megváltozása nem valószínű, de nem is lehetetlen. Információbiztonság tekintetében biztonságos egy információs rendszer, ha a rá vonatkozó funkcionális és nem funkcionális követelményeket az elvárt minőségben teljesíti, vagy ha nem teljesíti teljes mértékben, akkor legfeljebb a kívánatostól előre meghatározott mértékben tér el tőle. A nemzetközi bevált gyakorlatok szerint (Cobit 5 for Information Security, ISACA³) az információbiztonság az alapelveinek összessége: azaz a bizalmasság, sértetlenség (hiteles és nem megváltoztatott) és rendelkezésre állás (időben és funkcionalitásban) együttes megléte.

Az információbiztonsági követelmények az egyes szervezetek esetében más és más szempontból válnak fontossá. Végigtekintve az iparágakon, az információbiztonság más-más jellemzői kerülnek előtérbe. A közigazgatásban a legnagyobb kihívást a személyes adatok, a nemzeti adatvagyon és a nemzeti minősített adatok védelme, az ipari termelésben a gyártás támogatása aktuális információkkal és az ipari kémkedés elhárítása, a tervezésben az információ előállítása és védelme, a kereskedelemben az árazási, értékesítési, beszerzési és logisztikai információk biztosítása és védelme, banki környezetben pedig a banktitkok megőrzése, a számla, a bankkártya és a banki tranzakciók adatainak védelme, az online banki műveletek biztonságának garantálása jelenti.

Az ipari termelési folyamat során szükséges kritikus tevékenységek a gyártás előkészítése, tervezésére és a legyártott termékek minőségbiztosítása. Mindkét esetben elengedhetetlen a támogató rendszerek működése, az általuk biztosított információ rendelkezésre állása. A gyártósorokon a megrendeléseknek megfelelő termékeket állítják elő. Mivel ugyanazokon a gyártósorokon különböző termékek előállítása folyik, a gyártástervezésnél fontos szerepet játszik a termékek gyártásának sorrendje, a gyártandó termékek mennyiségének meghatározása és a minimális mennyiség, amelyet egy termékből a gyártás során elő kell állítani a gazdaságosság megteremtéséhez. A gyártási folyamatok működésének biztosításához elengedhetetlen a termékek gyártásához szükséges információk eljuttatása a gyártósori berendezésekhez. A gyártósori infokommunikációs szolgáltatások leállása termelés kiesést okoz, ezáltal csökken az előállított termékek mennyisége, és gazdasági kár következik be. A másik fontos szempont a gyártott termékek minőségének biztosítása. Ennek érdekében a gyártás utolsó fázisában tesztelik az elkészült termékeket. A tesztelés lehet manuális vagy automatizált. A tesztelési eredmények gyűjtése, a kész termékek minőségi paramétereinek tárolása fontos szerepet játszik a gyártási technológiák fejlesztésében és a legyártott termékek továbbfejlesztésében. Az így összegyűjtött információból meghatározható:

- a hibásan gyártott termékek aránya;
- az egyedi termékek minőségi mutatói;
- a gyártósor és technológia alkalmassága az egyes termékek gyártásához.

3 Information Systems Audit and Control Association.

Az így összegyűjtött gyártástervezési és minőségbiztosítási adatok nemcsak a termék gyártójának jelentenek hasznos információt, hanem a konkurencia számára is. Mivel sok termék gyártása bérgyártás keretében zajlik, fontos megemlíteni, hogy egy gyártósoron több gyártó termékeit is előállíthatják. A bérgyártóknak kiemelt figyelmet kell fordítaniuk arra, hogy az előállított termékekhez köthető információ csak az adott termék megrendelőjéhez juthasson el.

A tervezési munkák végrehajtása általában számítógéppel támogatott folyamat. A munka során értékes információk keletkeznek, amelyek lehetnek eredeti ötletek, megvalósítási tanulmányok, kivitelezéshez szükséges számítások stb. Ezen információk meghatározzák a végtermék megjelenését, alakját, minőségét, használhatóságát. Az így keletkezett adatok sok esetben üzleti titoknak minősülnek, mivel továbbfejleszthetők és általában a konkurencia is dolgozik hasonló terveken.

Az információfeldolgozás és információcsere felgyorsulásával, az e-kereskedelem elterjedésével fontossá vált az árukészletek mennyiségének azonnali lekérdezhetősége az áruk körforgásának optimalizálása érdekében, a beszerzési árak elérhetősége, a pénztárak árazási információval való ellátása, a beszerzett és eladott áruk mennyiségének folyamatos nyilvántartása. A bankkártya-tranzakciók és a hozzájuk kapcsolódó adatok védelme fontos szerepet játszik, amelyet a PCI (Payment Card Industry) DSS (Data Security Standard) szabvány ír elő, és kötelező minden bankkártya-információt feldolgozó szervezetre nézve.

Banki környezetben nemcsak személyes adatok fordulnak elő, hanem személyekhez köthető bizalmas információk is. A banki működést szabályozó jogszabályok kiterjednek a bankok által kezelt adatok információbiztonságára. Ezek részben üzleti és ügyviteli síkon határozzák meg az általuk kezelt információk biztonsági paramétereit, részben pedig informatikai rendszerekre érvényes szabályozással. Ugyanakkor a bankbiztonsági követelményeknek való megfelelés szükségessé teszi az információbiztonság teljes körű megvalósítását mind az írott információ, mind pedig az informatikai rendszerekben fellelhető adatok szempontjából.

Mint azt láthatjuk, az információ bizalmasságának, sértetlenségének és rendelkezésre állásának hiányában a szervezetek, függetlenül attól, hogy melyik iparágban végzik a tevékenységüket, nem képesek elérni a céljaikat.

INFORMÁCIÓBIZTONSÁG AZ ÁLLAMI ÉS ÖNKORMÁNYZATI SZEKTORBAN

Állami szervek felelősek számos kritikus fontosságú, legmagasabb biztonsági szintet igénylő tevékenység végzéséért. Idetartozik (a teljesség igénye nélkül) a személyes okmányok igénylése és előállítása, az egészségbiztosítási szolgáltatások nyújtása, a nyugdíjbiztosítási és -folyósítási szolgáltatások biztosítása, a bűnüldözés és a bűnmegelőzés, valamint a közoktatással, a honvédelemmel és a nemzetbiztonsággal kapcsolatos tevé-

kenységek. E szolgáltatások nyújtása során az állami intézmények nagy mennyiségű személyes és kiemelten védett adatot kezelnek, amelynek során kiemelt szerepet játszik az adatok bizalmasságának és sértetlenségének megőrzése és rendelkezésre állásuk biztosítása. Az Ibtv. megjelenését megelőzően a szerzők tapasztalatai szerint a biztonság elvárt szintjének meghatározását az állami és önkormányzati szektor vezetői részben nem ismerték fel, részben a szakirányítást végző szervek nem biztosították a szükséges emberi és anyagi erőforrásokat.

A fenti cél megvalósításnak érdekében Magyarország Országgyűlése megalkotta az állami és önkormányzati szervezetekre vonatkozó a 2013. évi L. törvényt és annak végrehajtási rendeleteit. A védelmi intézkedéseket tartalmazó végrehajtási rendelete a NIST SP 800-53 szabványra épül, gyakorlatilag annak kivonatolt magyar változata. Végrehajtási rendeletei:

- korábban a 77/2013. (XII. 19.) NFM rendelet, majd a helyette kiadott 41/2015. (VII. 15.) BM rendelet (Ibtv. vhr.) részleteiben kitér az informatikai rendszerek biztonsági osztályokba sorolására és az egyes osztályok esetében megvalósítandó védelmi intézkedésekre;
- a 26/2013. (X. 21.) KIM rendelet, amely az információbiztonsági szerepkörökkel rendelkező személyek oktatását írja elő;
- a 42/2015. (VII. 15.) BM rendelet, amely a jogszabály hatálya alá tartozó szervezetek hatósági nyilvántartásba vételét írja elő;
- a 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok feladatait és hatáskörét szabályozza, valamint a zárt célú elektronikus információs rendszerek meghatározását támogatja.

A minél jobb információbiztonsági környezetek kialakításának érdekében a jogalkotók és a jogszabály végrehajtását felügyelő szerv, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), amely 2015. október 1-től a Nemzeti Kibervédelmi Intézet részévé vált, folyamatosan nyomon követi a jogszabályok alkalmazásának módját, betarthatóságát, és szükség esetén javaslatot tesz ezek módosítására, használhatóbbá tételére, hozzájárulva ezáltal az információvédelem megvalósításához.

Az Ibtv.-t legutóbb 2015 első felében vizsgálták felül, és több jelentős módosításon esett át. A szervezetek biztonsági szintbe sorolásának és a rendszerek biztonsági osztályba sorolásának változásával az elektronikus információs rendszert üzemeltető szervezetekkel szembeni elvárások szigorodtak, és az új rendszerek bevezetésére vonatkozó követelmények teljesítésének halasztott teljesítési lehetősége megszűnt, azokat már az éles induláskor teljesíteni kell.

Az új végrehajtási rendelet, a 41/2015. (VII. 15.) BM rendelet felépítése több szempontból is szakított az eredeti NIST-szabvány struktúráját követő felépítéssel és logikával. A fejezetek között átcsoportosítottak egyes kontrollokat, illetve több menedzsment jellegű követelmény ki is került belőle: az informatikai biztonsági politika, az informatikai biztonsági stratégia, a szervezetszintű architektúra, a kockázatkezelési stratégia, a pénzügyi erőforrások biztosítása már nem követelmény.

Az elmúlt években a jogszabályok kereteinek megfelelően felerősödött az állami és önkormányzati szervek információbiztonsági átvilágítása, hiányosságai meghatározása, és tervezetek készültek a feltárt gyenge pontok kockázatainak megszüntetésére vagy csökkentésére. Az információbiztonsági felmérések rámutattak a legfőbb elmaradásokra, amelyek a szerzők tapasztalatai alapján többek között a következő intézkedésekkel kezelhetők:

- az intézkedések információbiztonsági programként való megvalósításával;
- a biztonságtudatosság növelésével;
- szabályzatok létrehozásával;
- eljárásrendek kialakításával;
- az ügyviteli és informatikai folyamatok végrehajtását támogató megoldások bevezetésével;
- rendszerfelügyeleti megoldások bevezetésével;
- konfigurációkezelési megoldások bevezetésével;
- formalizált változáskezelés bevezetésével.

Az Ibtv. vhr. strukturálja és részletezi az Ibtv. követelményeit. Az egyes követelménypontokban meghatározott elvárások szerteágazóak, és egy ponton belül is több kontrolltevékenységet érintő elvárások fogalmazódnak meg, ami nehezíti a követelmények értelmezését és betartását, és esetenként az érthetőséget is gátolja.

A következő fejezetekben bemutatjuk, hogy az egyes követelmények alapját szolgáló NIST-kontroll-leírások, az *MSZ ISO/IEC 27001:2014* és a *Cobit 5 for Information Security* szabványok hogyan segíthetik elő a követelmények eredményes és hatékony teljesítését, és végső soron a szervezetek közfeladatainak elvárt minőségben való végrehajtását.

INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZEREK

A követelmények teljesítésének megtervezéséhez, megszervezéséhez és működtetéséhez a megoldást nem egy jogszabályban kell keresnünk, ez az információbiztonsági felelős szakirányítási feladata, amelynek végrehajtásában leginkább a biztonságmenedzsment vonatkozó, nemzetközileg bevált gyakorlatai (*Cobit 5 for Information Security* és *ISO/IEC 27000* szabványcsalád) adnak iránymutatást.

Az információbiztonság-menedzsment területén egyes országok és szakmai szervezetek kialakították a saját bevált gyakorlataikat. Jelen tanulmány keretében a szerzők három nemzetközi módszertant ismertetve mutatják be, hogy a hazai tapasztalatok alapján milyen megközelítést javasolnak az állami és önkormányzati szervek információbiztonsági felelősei részére.

A NIST⁴ egy egyesült államokbeli központi kormányzati szervezet, amelynek nincsenek hatósági jogkörei. A szövetségi elektronikus információs rendszerek védelmé érdekében dolgoznak ki és tartanak naprakészen az információbiztonság lényeges területeire vonatkozó ajánlásokat az „SP 800” azonosítóval kezdődő számozású kiadványokkal. Az SP 800-53 4. kiadása az adatbiztonság és adatvédelem megvalósítása érdekében összeállított, szövetségi elektronikus információs rendszerek esetében alkalmazandó kontrollok részletes katalógusa, amely összefüggéseken keresztül mutatja be a szintenként meghatározott, minimálisan szükséges kontrollokra vonatkozó elvárásokat.

A Cobit⁵ az informatikai irányítás világszerte ismert keretrendszere, amely rendszerbe foglalja az információ, az információk technológia és az ezzel kapcsolatos kockázatok kontrollálására alkalmas jó gyakorlatokat. Az 5. kiadásában integráltan használja fel az informatikai irányítás, az informatikai ellenőrzés, az informatikai kockázatkezelés és az információbiztonság-menedzsment jó gyakorlatait, ugyanakkor adaptálja a korszerű vállalatirányítási módszereket is. Az üzleti célkitűzések elsődlegességét hangsúlyozza az informatikai, illetve információbiztonsági célok megfogalmazása során.

Maga a Cobit keretrendszer egy egyszerű és pragmatikus alaptételből indul ki: a szervezeti célkitűzések teljesítéséhez szükséges információk biztosítása érdekében az informatikai erőforrásokat természetesen üleg összetartozó folyamatokká kell szervezni. A Cobit 4.1⁶ alapvetően az informatikai szolgáltatással foglalkozik, és csak az ahhoz szükséges mértékben tér ki az üzleti/ügyviteli, számviteli és döntés-előkészítési folyamatok vizsgálatára. Az új verzió, a Cobit 5 már az irányítási folyamatokat is külön területként tartalmazza.⁷

A folyamatokat öt területre csoportosítja a modell:⁸

- Értékel, irányít és figyelemmel kísér.
- Illeszt, tervez és szervez.
- Épít, beszerez és megvalósít.
- Nyújt, szolgáltat és támogat.
- Figyelemmel kísér, értékel és felmér.

Ez a szerkezet az információ és a feldolgozásához kapcsolódó technológia minden területére kiterjed. Kiegészítő kötetei közül a következő három segíti leginkább egy információbiztonsági felelős munkáját:

- Cobit 5 for Information Security: a Cobit 5 információbiztonsági területét mutatja be, útmutatóul szolgál bevált információbiztonsági gyakorlatok alkalmazásához, összhangban a keretrendszer többi elemével. A logikai, a fizikai és a humán

4 National Institute of Standards and Technology.

5 Control Objective for Information and related Technology.

6 Cobit 4.1 Excerpt, ISACA, 2007. www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf (2015. 10. 16.)

7 Cobit 5 Introduction, ISACA. www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf (2015. 10. 16.)

8 A szerzők fordítása.

biztonság mellett a megvalósítást segítő kapcsolódó módszerek és eljárások bemutatásával átfogó, ún. holisztikus modellben kezeli a biztonságot.

- Cobit 5 for Assurance: az informatikai belső és külső ellenőrzési szakemberek számára készült útmutató. Csak angol nyelven érhető el. Egy korábbi kiadvány, a Cobit 3 Auditálási útmutató férhető hozzá magyarul.
- Cobit 5 for Risk: az informatikai kockázatkezelési szakemberek számára kíván útmutatást adni a kockázatfelmérési, -értékelési és -kezelési feladataik Cobit-ke-retrendszerbe illeszkedő végrehajtásához.

Az MSZ ISO/IEC 27001:2014 szabvány elődei (előzőleg: BS 7799-2:2002) 2002 óta teszik lehetővé információbiztonsági irányítási rendszerek (ISMS) kialakítását, megvalósítását, működtetését, figyelemmel kísérését, átvizsgálását, fenntartását és fejlesztését. Ezenfelül a szervezet információbiztonsági irányítási rendszere külső szakértő általi ellenőrzésének követelményeit tartalmazza, és a tanúsíthatóságot teszi lehetővé. A szabványt alkalmazó szervezeteket először a Nagy-Britanniában, majd világszerte az információbiztonság kockázatarányos kezelésében érték el kiemelkedő eredményeket.

Az ISO/IEC 27002:2013 (előzőleg: ISO 17799:2005) az információbiztonság menedzsmentjének gyakorlati kódexe. A korábbi informatikai biztonsági ajánlásoktól eltérően a biztonsági követelményeket és intézkedéseket a szervezet üzleti céljaiból és stratégiájából vezeti le egy szervezeti szintű, informatikai biztonságmenedzsment központú szemléletben. Az ISO/IEC 27002:2013, a minőségbiztosításra vonatkozó ISO 9000 szabványokhoz hasonlóan, a teljes körű informatikai biztonság megteremtéséhez szükséges szervezési, szabályozási szempontrendszert adja meg.

INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZEREK MŰKÖDŐKÉPESSÉGE

Az információbiztonsági irányítási rendszerek bevezetése során Alan Calder: *Nine Steps to Success – An ISO 27001 Implementation Overview* című műve alapján összefoglalhatók azok a tevékenységek, amelyeknek a megfelelő végrehajtása növeli az IBIR-bevezetési projektek sikerét.

Általában a komplex szervezeti változtatási projektek, mint az IBIR-bevezetés sikere nagyban függ attól, hogy a sikert akadályozó tényezőket időben felismeri-e a projektvezető, illetve a projektszponzor, és megteszik-e a szükséges lépéseket.

- *A kockázatok feltárása:* Kockázatcsökkentési lehetőség a kulcs emberekkel való interjúk vagy a fókuszcsoport körében végzett problémafeltárás. Fontos, hogy nemcsak a projekt kezdetén kell a kockázatokat kezelni, hanem a projekt végrehajtása során is.
- *Az érdekelt felek céljainak elemzése:* A projekt elején fel kell tární a projektre hatással lévő személyek elvárásait és azok prioritását.

- *Felső vezetői támogatás:* Fel kell kelteni a felső vezetés figyelmét, és a projekt során fenn is kell azt tartani. A lényeges kockázatok üzleti nyelven való bemutatása elősegíti a vezetők figyelmének megszerzését. A figyelem fenntartását a változtatások megvalósulásának döntési pontjaihoz kapcsolódó vezetői tájékoztatók segítik.
- *Szervezeti változtatásmenedzsment:* Egy IBIR-projektre általában úgy tekintenek a szervezet munkatársai, hogy biztosan változást fog hozni, de nem tudják pontosan, hogy mit. Minden szervezetben vannak néhányan, akik értik, hogy miért szükséges a biztonság, és támogatják a változást, ugyanakkor a többség passzívan szemléli vagy ellenáll, nem látja szükségesnek. Minden szervezetben van néhány olyan ember is, aki aktívan tesz azért, hogy zátonyra futtassa a projektet.
- *Tapasztalt projektvezető:* A tapasztalt IBIR-projektvezető inkább menedzser, mint műszaki szakember. Ő az a személy, akihez bárki fordulhat a projekttel kapcsolatos kérdésekben.
- *Belső kommunikáció:* Szervezeti változtatási projektekben kulcsfontosságú, hogy minél előbb adjunk tájékoztatást, és gyakran informáljuk az érintetteket a projekt előrehaladásáról (pl. belső honlap, rendszeres belső hírlevél). Közérthető nyelven kell megfogalmazni, hogy miért fontos az információbiztonság, és miért megfelelő módja a biztonság megteremtésének egy IBIR bevezetése. Be kell mutatni a szervezet jövőképét az IBIR bevezetése esetén, valamint annak szervezetre gyakorolt pozitív hatását.
- *A tudás megszerzése a szervezet számára:* A külső szakértők bevonását célszerű korlátozni, inkább az IBIR működését elősegítő tudást és képességeket kell beépíteni a szervezetbe. Ezt a tudást a bevezetési projekt során érdemes megszerezni a projektben való aktív részvétellel. A projekt elején javasolt kijelölni az információbiztonsági felelőst, aki aktívan részt vesz az IBIR bevezetésében. A speciális biztonságtechnikai területeken célszerű külső szakértőket igénybe venni rugalmasan alkalmazható keretszerződéssel.
- *Minden érintett bevonása:* Minden érintett szervezeti egységet és kulcsszereplőt aktívan be kell vonni a projektbe, hogy vegyenek részt a készülő anyagok elkészítésében és véleményezésében. Ez biztosítja, hogy minden lényeges szempontot időben figyelembe vegyenek, és a szervezet munkatársai magukénak érezzék az elkészült rendszert, továbbá megelőzi, hogy az egyébként ellenállást tanúsító munkatársak akadályozzák vagy ellehetetlenítsék a projekt megvalósulását.
- *Mérés, mutatószámok:* Azok a tevékenységek, amelyeket nem mérünk objektív mutatószámokkal, nehezen irányíthatóak, ezért megvan a kockázata annak, hogy nem vesszük észre időben a céloktól való eltérést. Törekedni kell arra, hogy a kulcskontrollok működésének mérhetősége megvalósuljon cél és eredménymutatók alkalmazásával.
- *Tesztelés:* A tesztelés kulcsfontosságú feladat. Elvégzése visszajelzést nyújt az előkészített változások által bevezetendő folyamatok működőképességéről. Tesztelés a folyamatok alapos ellenőrzése, amely minden részletre kiterjed. Addig kell tesztelni a folyamatokat, amíg azok minden elvárást kielégítően nem működnek.

AZ INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZERKÖVETELMÉNYEK TELJESÍTÉSE

Az információbiztonságra vonatkozó követelmények előírása az első lépés a biztonság megteremtésében, amely megadja egy szervezet számára a minimálisan teljesítendő, kötelező feltételeket. A követelmények forrásai részben jogszabályi, hatósági vagy szerződéses követelmények (megfelelőségi követelmények), részben a szervezeti célok megvalósításához szükséges tevékenységek – a megfelelőségi követelmények teljesítését követően – a szervezet kockázatértékelése szerint fennmaradó kockázatainak az elvárt szintre való csökkentéséhez szükséges vezetői elvárások. A védelmi intézkedéseket tehát a megfelelőségi követelmények és a szervezet vezetőinek elvárásai alapján határozzák meg.

Jelen esetben az Ibtv. vhr. írja elő a részletes követelményeket. Tapasztalataink alapján az egyes követelmények alapjául szolgáló NIST-kontroll-leírások nagyban segítik a követelmények pontos értelmezését. Erre vonatkozóan kutatásunk során elemzéseket végeztünk. Az elemzés kiindulópontja a NIST SP 800-53 rev 4. H mellékletében található ISO/IEC 27001:2013 és NIST SP 800-53 rev 4. összerendelés volt, amelyhez az Ibtv. vhr. követelményeit illesztettük. Az 1. táblázat egy kiemelés az elemzésből.

1. táblázat: Ibtv. vhr., ISO/IEC 27001:2013 és NIST SP 800-53 összerendelés

Ibtv. vhr. követelmény-azonosító	NIST-kontroll-azonosító	ISO/IEC 27001:2013 kontrollazonosító
3.2.1.2	PE-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
3.2.1.3	PE-2	A.11.1.2*
3.2.1.4, 3.2.1.4.2	PE-3	A.11.1.1, A.11.1.2, A.11.1.3
3.2.1.5	PE-4	A.11.1.2, A.11.2.3
3.2.1.6	PE-5	A.11.1.2, A.11.1.3

Az Ibtv. 4. §-a előírja, hogy más, a szervezet által alkalmazott szabványokat is figyelembe vehet a hatóság egy szervezet információbiztonságának értékelésekor. „Az elektronikus információs rendszerekre és eszközökre, szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat a hatóság az eljárása során figyelembe veszi.”⁹ Ennek gyakorlatban való alkalmazásáról még nem ismertek tapasztalatok.

Kutatásunk során arra az eredményre jutottunk, hogy az Ibtv. által előírt követelmények egy informatikai szolgáltatásokat is üzemeltető szervezetnél (4. biztonsági

⁹ Ibtv. 4. §

szint) túlmutatnak azon, amelyet egy MSZ ISO/IEC 27001:2014 tanúsításnál a tanúsító auditorok elvárnak. Így az IBIR-bevezetés esetén egy ilyen szervezetnek 46 darab 4. szintű (pl. 3.3.10.11) követelményt kell még megvalósítani, amelyek további elemi követelményekre bonthatók.

Megvizsgáltuk továbbá azt is, hogy egy olyan szervezet esetén, ahol az Ibtv.-nek való megfelelésen túl nem cél az MSZ ISO/IEC 27001:2014 tanúsítás megszerzése, vannak-e olyan követelmények, amelyeket nem ír elő a jogszabály. Találtunk nyolc ilyen védelmi intézkedést: A.11.1.5, A.12.3.1, A.12.7.1, A.14.2.6, A.14.2.9, A.14.3.1, A.18.1.3, A.18.2.1. Ezenfelül vannak olyan védelmi intézkedések is, amelyeket csak az 5. biztonsági szinten kell megvalósítani. Ezek szükségességéről az adott állami vagy önkormányzati szervezetnek a kockázatelemzése során kell döntést hoznia.

Az MSZ ISO/IEC 27001 szabvány meghatározza azokat a követelményeket, amelyek teljesítése elősegíti az információbiztonság strukturált megvalósítását. Az IBIR kialakítása a szabvány alapján úgymond egyszerű feladat egy tanácsadó cég vagy tapasztalt információbiztonsági felelős számára. Ugyanakkor a szabvány és az Ibtv. végrehajtási rendeleteinek együttes megvalósítása igényli a követelmények együttes teljesítését, amelyet hatékonyan egy összerendelő táblázat segítségével lehet megvalósítani.

Az adott szervezet számára az információbiztonság megfelelő szintű kiépítését még nagymértékben befolyásolják a szervezetek sajátosságai. Az IBIR kialakítása során figyelembe kell venni a szervezet profilját, információbiztonsági szükségleteit. A szabvány és a jogszabályok által megkövetelt kockázatarányos védelem kialakítása nem mindig egyszerű feladat, hiszen előfordulhat, hogy a kockázatok besorolása okozza a legnagyobb problémát, amely információvédelmi hiányosságok kialakulásához vezethet. Például egy nagyon nagy kárértékkel rendelkező veszélyforráshoz közepes kockázat társulhat, mivel annak előfordulása nagyon ritka, szinte sohasem következik be. Előfordulhat olyan eset is, amikor a kockázatot már egy meglévő védelmi intézkedés csökkenti, és emiatt sorolják alacsonyabb kategóriába. Elképzelhető az is, hogy az MSZ ISO/IEC 27001:2014 tanúsítvánnyal rendelkező szervezetek információbiztonsága mégsem működik jól a gyakorlatban. Ez adott esetben szemmel látható, de az is lehetséges, hogy évekig nem észlelik az adatok szivárgását, mivel a biztonsági rendszer kialakításakor kimarad egy-egy monitoringkontroll megfelelő kiépítése.

A Cobitban meghatározott információbiztonsági programmenedzsment-alapú bevezetés úgy épül fel, hogy az információbiztonsági politika és stratégia által lefektetett információbiztonsági architektúra kialakítására, továbbfejlesztésére részletes tervet kell kidolgozni. A tervben szereplő, napi rutinon túlmutató feladatokat projektekbe kell szervezni, és azokat programmá rendezni. Ezt követően – az információbiztonsági irányítási keretrendszer alapján – a programot le kell bontani az egyes szervezeti egységek, akár a szervezeti egységek munkatársainak szintjére. Pontosan meg kell határozni, hogy kinek mi ezzel kapcsolatban a feladata, és azt hogyan tudja eredményesen teljesíteni.

Az ISACA az alábbiakon keresztül határozza meg az információbiztonsági program kidolgozási és megvalósítási tevékenységeit:

- Az információbiztonsági program információbiztonsági stratégiához való illesztése.
- Az információbiztonsági programnak a szervezet alap- és támogató folyamataihoz való illesztése.
- Az információbiztonsági program végrehajtásához szükséges erőforrások azonosítása és biztosítása.
- Az információbiztonsági program végrehajtását támogató információbiztonsági architektúra kialakítása és fenntartása.
- Az információbiztonsági szabályozások kialakítása és karbantartása az információbiztonsági politikának megfelelően.
- A biztonság tudatos szervezeti kultúra kialakítása érdekében információbiztonság-tudatosítási program létrehozása, valamint képzések kialakítása és karbantartása.
- Az információbiztonságból fakadó követelmények beépítése a szervezet folyamataiba.
- A külső partnerekkel kötendő szerződésekbe az információbiztonsági követelmények beépítése.
- Az információbiztonsági program eredményességének és hatékonyságának számszerűsített értékelése.

ÖSSZEFOGLALÁS

Magyarországon 2013 előtt az állami és önkormányzati szektorban az elektronikus információs rendszerek és az általuk kezelt információ védelme nem volt központilag átfogóan szabályozott. Ahol szabályozott volt, ott sem felügyelték szorosan a szabályozás betartását és nem szankcionálták a be nem tartását. A 2013. L. törvény teremtette meg azt az előremutató, nemzetközileg bevált gyakorlatokon alapuló jogszabályi környezetet, amely az állami és önkormányzati szervezetek biztonsági szintjének növelését teszi lehetővé. A törvény 2015. júliusi módosítása és a 2015. október 1-jén megalakult Nemzeti Kiberbiztonsági Intézet megteremti a követelmények teljesítését figyelemmel kíséző intézményrendszert, továbbá a szankcionálás feltételeit az előírások be nem tartása esetén.

Az állami és önkormányzati szektorban az Ibtv. követelményeinek teljesítése magas szakmai felkészültséget igényel a helyi információbiztonsági felelősök részéről. A szerzők a követelmények elemzése és a nemzetközileg bevált gyakorlatok alapján azt állapították meg, hogy az információbiztonság eredményes megvalósításához az állami és önkormányzati szervezeteknél dolgozó információbiztonsági felelősök jól alkalmazhatják a kapcsolódó nemzetközileg bevált gyakorlatokat. A NIST SP 800-53 rev 4. szabvány az Ibtv. követelményeinek pontosítását segíti, mivel egyszerűen megfeleltethetőek egymásnak; az MSZ ISO/IEC 27001:2014 szabvány keretbe foglalja a követelményeket és elősegíti a biztonság fenntartását, a Cobit információbiztonsági program

menedzsmentmodellje pedig a napi feladatokon túlmutató tevékenységek projektekbe, majd információbiztonsági programba szervezésével az információbiztonsági célok kiszámítható elérését segíti elő.

A cikkben bemutatott lépéseket követve tehát az ismertetett nemzetközileg bevált gyakorlatok felhasználásával a magyar állami és önkormányzati szervek információbiztonsági felelősei eredményesebb és hatékonyabb módon képesek megteremteni az elektronikus információs rendszereik és az azok által kezelt adatok védelmét.

IRODALOMJEGYZÉK

- [1] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- [2] 1491/2013. (VII. 29.) Korm. határozat a Nemzeti Elektronikus Információbiztonsági Hatóság és a Nemzeti Biztonsági Felügyelet, mint szakhatóság kialakításához szükséges személyi és tárgyi feltételek biztosításáról
- [3] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- [4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- [5] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
- [6] 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról
- [7] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- [8] 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- [9] 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről

- [10] 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről
- [11] CALDER, Alan: *Nine Steps to Success – An ISO 27001 Implementation Overview*. IT Governance, 2005, UK.
- [12] ISACA: Cobit 3 Auditálási Útmutató, ISACA Hungary Chapter, 2000.
- [13] ISACA: COBIT 4.1 Excerpt, ISACA, 2007. www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf, 2014. 09. 12.
- [14] Cobit 5 for Assurance Preview, ISACA, 2013.
- [15] ISACA: Cobit 5 for Information Security Introduction, 2012. www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf (2015. 05. 11.)
- [16] ISACA: Cobit 5 Introduction. www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf (2015.05. 11.)
- [17] ISACA: Cobit 5 for Risk Preview, 2013. www.isaca.org/cobit/documents/cobit-5-for-risk-preview_res_eng_0913.pdf (2015. 10. 16.)
- [18] MICHELBERGER Pál – LÁBODI Csaba: Vállalati információbiztonság szervezése. In NAGY Imre Zoltán (szerk.): *Vállalkozásfejlesztés a XXI. században*. II. kötet, Óbudai Egyetem.
- [19] MSZ ISO/IEC 27001:2006; Informatika. Biztonságtechnika. Az információbiztonság irányítás rendszerei. Követelmények.
- [20] MSZ ISO/IEC 27001:2014; Informatika. Biztonságtechnika. Az információbiztonság irányítás rendszerei. Követelmények.
- [21] NIST SP 800-53 rev 4. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (2015. 01. 30.)
- [22] A Survey of IT and Security Professionals: The Impact of Mobile Devices on Information Security, Dimensional Research, 2014, 5–6. www.checkpoint.com/downloads/product-related/report/check-point-capsule-2014-mobile-security-survey-report.pdf (2015. 03. 04.)
- [23] PCI DSS. www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss (2015. 09. 10.)
- [24] Symantec: Internet Security Threat Report. Vol. 20. 2015, 21–22. www.symantec.com/security_response/publications/threatreport.jsp (2015. 05. 05.)
- [25] VASVÁRI György: *Vállalati biztonságirányítás. Informatikai biztonságmenedzsment*. Info-Szakkönyv Bt., 2007.

SZÁLFELÜGYELET „PARANCSSZÓRA” – A BIZTONSÁG MINDENK FELETT

A fizikai hálózat biztonsága mindennél előbbre való, de emellett fontos, hogy kevés energia és élő erő felhasználásával valósuljon meg a biztonság érzete. De hogyan érhetjük el mindezt? Az előadás betekintést nyújt a szálmonitorozási praktikákba, és egy olyan rugalmas, skálázható megoldásról tesz említést, amely megoldást választva viszonylag kis költségkerettel is eredményeket lehet elérni, ha vannak kritikus és kiemelten a biztonság megteremtésére hivatott hálózati szakaszok, amelyeket folyamatosan vizsgálni kell. Ugyanakkor fontos a későbbi bővítés, sőt esetleg a komplett RFTS-rendszer kiépítése is.

Gyakorlatilag minden cégvezető álma évek óta a kiemelt biztonsággal rendelkező és könnyen üzemeltethető optikai hálózat megteremtése kis ráfordítással, úgy, hogy biztos lehessen benne: nem lesz probléma az optikai hálózatával, legyen szó kábelrongálásról, kábel- vagy adatlopásról, esetleg egyszerűen a szálak öregedéséről.

MIÉRT FONTOS A MONITOROZÁS?

Az optikai hálózatok a XXI. században már rengeteg adatot szállítanak, folyamatosan gyorsul a világ, egyre több mozgóképtartalmat használunk, és egyre több alkalmazás-orientált program fut eszközeinken, mondhatni, a hálózaton futó megoldások szerves részét képezik munkahelyi vagy akár magánéletünknek is. De mi történik, ha mindennek a fundamentuma, az alap nem képes többé ezen kihívásoknak megfelelni, hibákat okoz az adatátvitelben, vagy akár egyik napról a másikra összeomlik? Gondoljunk bele, hogy mi mindenre használjuk odahaza a vizet, amely az életünk elemi szükséglete, az egyik legfontosabb közmű. Ha ezt tekintjük a fizikai hálózatnak, akkor efelett sok olyan alkalmazás van, amit nap mint nap többször is használunk otthon. Legyen az a mosás, a mosogatás, a főzés, a fürdés, a mellékhelyiség használata, de ha csak nem tudunk fogat mosni, az is komoly problémát jelent számunkra. Vagyis a víz fizikai megléte nélkül nem érnek semmit a rajta futó alkalmazások. Ugyanez természetesen vonatkozik az optikai hálózatunkra is: ha azzal baj van, akkor nem működnek a felette futó alkalmazások. Összességében tehát elmondhatjuk, hogy az optikai hálózatunk fizikai közegének biztonságos megléte a legfontosabb dolog minden ilyen hálózattal rendelkező cég számára. Tudjuk, hogy van, és ezzel lezárjuk a kérdést, hasonlóan ah-

¹ Ügyvezető igazgató, EQUICOM Méréstechnikai Kft.

hoz, amelyen természetesnek vesszük az otthoni vízellátást. Ha baj van, csak akkor ismerjük fel a fontosságát, és igyekszünk mielőbb visszanyerni kényelmünk feltételét.

További kritikus kérdések, amelyek a monitorozás szükségességét támasztják alá:

- az optikai hálózatnak nincs fizikai védelme, a biztonságos zónán kívül esik;
- az optikai kábelek 75 százaléka szabadon hozzáférhető;
- az adat, amelyet az optikai szál folyamatosan szállít, nincs biztonságban, azt „megcsapolhatják”;
- évről évre növekszik az internettámadások száma;
- könnyű a helyzetjelentés a hálózatról a vezetőség felé, preventív mérések végezhetőek a szálak állapotáról.

ALKALMAZÁSI TERÜLETEK

Számos területen hasznát vehetjük a monitorozásnak, de természetesen vannak ezen belül is olyan esetek, ahol nagy segítséget jelenthet egy szálfelügyeleti megoldás.

- *Kritikus linkek:* a mai hálózati topológiák redundánsak, de mi van például az üvegnyakakkal, a kulcsfontosságú útvonalakkal?
- *Kiemelt ügyfelek:* minden ügyfél azonos, de mi van azokkal a prioritást élvező ügyfelekkel, mint például a bankok, a közigazgatási, kormányzati szektor szereplői, a sportesemények szervezői?
- *Hibaelhárítás:* a hálózati eszközök felügyelete megold mindent, de a rossz BERT-értéket okozhatja fizikai szintű hálózati probléma is, amelynek a helye is ismeretlen marad.
- *Tenger alatti kábelek:* ez kevésbé érdekel bennünket.
- *Biztonság:* az optikai hálózatok nem immunisak a lehallgatásra.

A kriptográfia (titkosítás) csak félmegoldás, mert:

- nem szerzünk tudomást a támadásról, így az adatok kiszivárognak;
- adatot nemcsak kinyerni lehet, tehát a kriptográfia ellenére megtagadható vagy módosítható a kommunikáció;
- a kriptográfia nem fizikai szintű védelem.

Jelen esetben talán a biztonság a legfontosabb, és ezt emelném ki. Ahogy fentebb említettem, folyamatosan növekszik az internettámadások száma, amely évente akár a 10–15 százalékot is elérheti, ráadásul az elmúlt években történt támadások 35 százaléka az EU-t érintette, és ezek nagyon sok esetben észrevétlenek maradnak.

Szintén fontos hangsúlyozni, hogy az optikai hálózatot le lehet hallgatni, az adatot meg lehet szerezni egy egészen olcsó megoldással, amely kicsatolja a fényt az optikai szálból, és egy demoduláció után akár rendelkezésre is áll a hálózaton lévő adat, így azt ellopni, de manipulálni is lehet, s ez még nemzetbiztonsági problémát is okozhat. Mi-

vel a beavatkozás a berendezések számára láthatatlan, ezért a fizikai közeg paramétereit kell vizsgálni, hiszen szerencsére az adat kicsatolása csillapításnövekedéssel jár együtt, amit figyelni lehet. Az adatokat persze lehet titkosítani, de ez egyrészt költségesebb megoldás a szálfelügyelet használatához képest, másrészt ennek révén nem szerzünk tudomást a támadásról, és ha sikerült megfejteni a titkosítást, akkor nem értünk el semmit sem.

A KÖLTSÉGEK TERVEZÉSE

Vannak olyan esetek, amikor „a pénz nem számít” elve alapján egy kritikus vagy nemzetbiztonsági érdekeket is érintő hálózatot kell felügyelni, több okból fakadóan is. Természetesen ilyenből nem sok létezik, ezért érdemes a tervezéskor szemügyre venni, hogy egy egyszeri beruházás hosszabb távon milyen előnyöket jelent egy optikai hálózat monitorozása során, milyen kérdésekre kapunk válaszokat, amiket még nem tudunk a hálózatunkról, illetve mennyiben segíti és csökkenti az üzemeltetést egy rendszer telepítése. Tudjuk-e, hogy évente hány kábelrongálás történik, és annak milyen hozadéka jelentkezik a költségek terén? Mennyi idő alatt és hány ember azonosítja a probléma okát és helyét? Vannak preventív megoldások idegen támadások esetére? Milyen statisztikai adatok vannak arra vonatkozóan, hogy egy hiba esetén a hálózat fizikai közege sérült, vagy éppen a berendezéssel volt-e probléma? Mekkora egy átlagos hibajavítási időtartam, és ez milyen költségeket tartalmaz? Mindig végzünk periodikus ellenőrző méréseket az optikai szálakon, hogy lássuk azok öregedését, a megelőző karbantartás miatt? A cég szakemberei használnak műszereket, valamint megfelelő számú technikust áll készenlétben?

Ha a fentieket sorra vesszük, és összevetjük azzal a ténnyel, hogy egy monitorozórendszer használatának segítségével a hibahelyet két percen belül meghatározhatjuk, a problémát akár fél óra alatt elháríthatjuk és a kiesési időt drasztikusan csökkenthetjük, akkor kiderül, hogy az egyszeri beruházás hosszabb távon megtérül az üzemeltetési költségek okán, valamint a megoldás számos olyan előnnyel jár, amelyeknek hála végre nyugodtabb lesz a mindennapi munka.

A TÁVOLRÓL VEZÉRELT KÖZPONTI MÉRÉSEK ELŐNYEI

A centralizált méréseknek sok olyan előnyét lehet felsorolni, amelyek segítséget adnak számunka a mindennapokban. Egy ilyen mérés esetén azonnal megkapjuk a hiba jellegét, és azt nem a terepen, egy mérés után kell megérteni, amikor nincs időnk, és inkább cselekedni kellene. Ezt az átlagos „megértési” időt tudjuk ezáltal nagymértékben csökkenteni. Minden központosított mérés automatizált, és a szerverre való mentések is könnyen megoldhatók. Óriási segítség lehet az üzemeltető számára, hogy az

archivált mérési adatokhoz hozzáférhet, valamint a mérések majdnem minden esetben egyúttal preventív célt szolgálnak, vagyis a hiba megelőzésén van a hangsúly, nem csak a felmerülő hibát kell azonnal orvosolni a terepen. Ezzel gyakorlatilag a kezünkben lehetnek a hálózatunk napi szintű paraméterei, és nem ér meglepetés, ha azt látjuk, hogy egy-egy optikai szakaszunk öregszik és idővel baj lesz, hanem még idejében fel is tudunk készülni annak a szakasznak a terv szerinti cseréjére. Egy szálfelügyeleti megoldást könnyedén át lehet emelni meglévő menedzsmentmegoldásokhoz (NMS, GIS, OSS stb.), ha rendelkezik nyílt architektúrával, és az interfész adott erre a feladatra.

A hálózatmenedzsmentet és -monitorozást sokan összetévesztik, pedig két élesen elkülönítendő területről van szó. A menedzsmentet sokszor az infrastruktúra-rendszer önmagában támogatja, vagy külön NMS-rendszerrel oldják azt meg. A monitorozórendszer ezzel szemben céleszköz, amelyet nem forgalomtovábbításra terveztek. Ettől függetlenül persze kizárólag a felügyelettel, a forgalomanalízissel, a biztonsági resek okozta károk csökkentésével, a riasztásokkal és az automatizált folyamatokkal foglalkozik, viszont eredményeit integrálni lehet meglévő rendszerekbe ahhoz, hogy a hibaelhárítást és a diszpécseri NOC-feladatokat még hatékonyabban lehessen ellátni.

A MEGOLDÁS

A hálózatmonitorozó megoldások folyamatos felügyeletet garantálnak az optikai infrastruktúra és az ügyfél védelmével, a valós idejű és akár a sötét, akár az élő szálás hálózatok ellenőrzésével, a hibahelyek lokalizálásával és a proaktív szálfelügyeleti megoldással. Az EXFO NQMSfiber (www.equicom.hu/nqms) szálmonitorozási rendszere a távoli tesztegységekkel (RTU²) ideális megoldás a hálózat komplex felügyeletére. Az NQMSfiber egy összetett funkciókkal (mint például riasztásmenedzsment és naplózás, hibajegykezelés, valamint a teljes hálózat állapotának megjelenítése sematikus ábrán) rendelkező rendszer. A teljes megoldással lehetővé válik a hálózat működésének és állapotának nyomon követése, akár a létező menedzsmentrendszerrel együttesen. Továbbá az NQMSfiber alkalmazás képes GIS-alapú hibahely lokalizálására. A legfontosabb része ennek a rendszernek azonban az, hogy minden elemében skálázható, és a fent említett NQMSfiber már csak akkor szükséges, ha egybe szeretnénk fogni az önmagukban is működőképes, kihelyezett mérőegységeket, s ezáltal válik valóban praktikus és költséghatékony szálfelügyeleti megoldássá.

Ezért mindenekelőtt a legfontosabb kérdés: egy monitorozóegység beruházásában gondolkodik, de egyelőre még nem teljes kiépítésű kliensszerver felügyeleti és monitorozórendszerre van szüksége? Az EXFO Fiber Guardian egy távoli elérésű, stand-alone, önállóan is működni képes RTU-eszköz, amely képes a kritikus optikai szálszakaszok

2 Remote Test Unit.

monitorozására, felügyeletére, RFTS³-rendszer kiépítése nélkül. Ezeket az önálló egységeket is közvetlen webes eléréssel lehet konfigurálni, s riasztás esetén akár SMS, akár e-mail, akár SNMP-üzenetek formájában a tudtunkra adja a hiba helyét és paramétereit. A későbbiekben, amennyiben szükséges, a Fiber Guardian és az NQMSfiber migrációja egyszerűen és gyorsan, minimális konfigurálással megvalósítható, anélkül hogy a tesztegységeket cserélni kellene, így az összes mérőegységet egy képernyőn és interfészen láthatjuk, és centralizált módon adhatják ki a diszpécsernek a hibát az éppen ügyeletben lévő kollégáknak, valamint teljes képet kaphatunk az egész hálózatról, statisztikai riportokhoz is.

A rendszer előnyei:

- automatikus felügyelet egyetlen kattintással;
- webalapú EMS⁴ és RTU;
- az optikai szálak napi 24 órás felügyelete, hibák lokalizációja és nyomon követése;
- egyedi RFTS-módszer a referenciaadat-menedzsmenthez;
- széles körű monitorozó és jegyzőkönyvező funkciók;
- GIS-alapú térképes hibahely-lokalizáció (opcionális);
- könnyedén bővíthető, rugalmas infrastruktúra;
- a link teljes csillapításának mérése 1625 vagy akár 1650 nm hullámhosszon;
- aktív és sötét szálak felügyelet, valamint In-Band és Out-of-Band CWDM monitorozás;
- tanulási fázis csak a valós események riasztásához;
- proaktív mérések a preventív üzemeltetéshez és karbantartáshoz;
- rövidebb és hosszabb optikai linkek vizsgálata nagy felbontással és széles dinamikatartománnyal;
- automatikus hibadetektálás és helymeghatározás, egy korábbi és a jelenlegi OTDR-görbe összehasonlítása alapján;
- bármelyik hálózatfelügyeleti rendszer számára hozzáférést biztosít egy részletesen dokumentált webszolgáltatási architektúra alapján.

KONKLÚZIÓ

Összefoglalásul elmondható, hogy a szakma egyéb területein is minden esetben a költséghatékonyság az elsődleges, és a legtöbb esetben a beruházások ezen irányelv mentén születnek. A szálfelügyeletnél sincs ez másképp: egy ilyen beruházás hosszabb távon komoly költségcsökkenést eredményezhet. A berendezésekhez használt felügyelet nem mondja meg a hiba helyét, ezért nagy segítség lehet a piac legjobb paramétereivel ren-

3 Remote File Transfer System.

4 Element Management System.

delkező OTDR-t használni szálmonitorozási alkalmazásra is. Ahogy a cím is előrevetíti: a biztonság sok esetben mindent megelőz, ez a legfontosabb szempont, mivel meg kell védeni az adatokat a betolakodók előtt. Ha pedig egyre több szigetmegoldást használunk, akkor a skálázható megoldással és a nyílt architektúrájú interfész segítségével könnyedén és egyszerűen megvalósítható a menedzsmentintegráció vagy a különálló megoldások központi szerverre történő összegyűjtése.

AZ EQUICOM-RÓL

Az EQUICOM Méréstechnikai Kft. idén 15 éves, és a kezdetektől telekommunikációs, informatikai és kábeltelevíziós méréstechnikai megoldásokkal foglalkozik. Világviszonylatban is vezető pozíciót elfoglaló beszállítói innovatív megoldásokat kínálnak az adatátviteli és kommunikációs hálózatok létesítési és üzemeltetési méréséhez, analíziséhez és monitorozásához. Ez az egyedülállóan széles termékkála, a beszállítókkal kialakított hosszú távú jó kapcsolat, valamint a technológiaközpontú szemlélet biztosítja az ügyfelek maradéktalan elégedettségét.

SMART DUST – A VÉDELMI ELEKTRONIKA, INFORMATIKA ÉS KOMMUNIKÁCIÓ LEGÚJABB TERÜLETE

Ma már elképzelhetetlen bármilyen védelmi elektronika hatékony informatikai támogatás nélkül. Az IT (információs technika) rohamos fejlődése pedig soha nem látott új távlatokat, a legmerészebb innovatív elképzelések alapjait teremtette meg, amelyek természetesen a katonai fejlesztésekben is szükségszerűen megjelentek. Az Egyesült Államok hadseregében már ma is több ezer robotot vetnek be, a távirányítású repülőgépektől az aknamentesítőkön át a *Csillagok háborújából* ismert birodalmi lépegetőkre hasonlító szállítóeszközökig.

A nem túl távoli jövőben még furább szerkezetek tűnnek majd fel a harcokban: például a képlékeny robot, amely képes átréselődni a falon lévő repedésen, az ellenséget felderítő „okos por”, valamint az emberi testbe hatoló, sejt méretű szerkezet, amely belső sérüléseket okoz. Lesz-e így „tisztá háború”?

ELŐZMÉNYEK

Amikor az NKE KMDI (a Nemzeti Közszerológiai Egyetem Katonai Műszaki Doktori Iskolája) leendő hallgatójaként a harmadik (védelmi elektronika, informatika és kommunikáció) kutatási területre jelentkeztem, nem is gondoltam át, milyen összetett és szerteágazó, számomra és társaim számára is új ismereteket nyújtó tudományterületet választottam, amelynek nemcsak jelentős múltja és jelene, de egyúttal fantasztikus jövője is van.

Számomra – mint informatikus szakember – az első komoly feladat a védelmi elektronika területén fennálló tudáshiányom pótlása volt. Hamar rá kellett jönnöm azonban, hogy a másik két témakörben is sok fontos ismeretet kell még elsajátítanom. Elég gyorsan, már a tanulmányaim elején pontosan és világosan láttam, mennyire logikusan felépített területe ez a katonai műszaki tudományoknak. A felállított logikai sorrend (védelmi elektronika, informatika és kommunikáció) egyenes irányú, s az egyik legfontosabb katonai (stratégiai, védelmi, hadászati) terület.

Ma már elképzelhetetlen bármilyen védelmi elektronika hatékony informatikai támogatás nélkül. Az IT rohamos fejlődése pedig soha nem látott új távlatokat, a

1 NKE, Katonai Műszaki Doktori Iskola (lnyari@t-online.hu).

legmerészebb innovatív elképzelések alapjait teremtette meg, amelyek természetesen a katonai fejlesztésekben is szükségszerűen megjelentek. Az 1970-es évek elején az Egyesült Államokban összegyűlt egy maroknyi tudós, mérnök, védelmi szállító és az amerikai légierő néhány tisztje, hogy megalakítsanak egy szakmai csoportot. Céljuk az volt, hogy kidolgozzák, miként lehet olyan gépezeteket építeni, amelyek emberi beavatkozás nélkül is képesek működni, valamint az, hogy kitalálják, hogyan lehet meggyőzni a vonakodó Pentagont arról, milyen komoly előnyökkel is járhat a robotok felhasználása a harctéren. Az azóta eltelt évtizedek alatt hatalmas új iparág született, az Association for Unmanned Systems International pedig jelentős nemzetközi szervezeté nőtte ki magát. A harci és a legkülönbözőbb robotok hasznáról ma már nem kell se a katonaságot, se a civilek nagy részét győzködni.

INFOKOMMUNIKÁCIÓS FEJLŐDÉS

Az információtechnológiai fejlődés jóvoltából egyre nagyobb számú és több típusú eszköz és információs csatorna válik alkalmassá az okos hálózatokban történő világméretű kommunikációra. Az intelligens hálózatok elemei – szenzor, mérő, szolgáltató központ, frontpage – közötti kommunikáció lényege az egyes elemek közötti biztonságos kétirányú információszolgáltatás megteremtése, a valós idejű adatszolgáltatás biztosítása. A mobileszközökről nyomon követhető folyamatok már lakossági és ipari szinten is elérhetővé váltak. Az energiaszolgáltatások mérésére és optimalizálására létrehozott applikációk pedig könnyű kezelhetőséget kínálnak minden felhasználónak.

Az infokommunikációs eszközök használata természetesen nem csupán az energiaszektor kiváltsága. Alkalmazásuk jelentős támogatást nyújthat minden smart grid² megoldással bíró ágazatban, legyen az oktatás, egészségügy vagy akár turizmus. A bennük rejlő potenciál – akárcsak a smart grid hálózatok által hordozott lehetőségek – egy olyan új területet nyitott meg globális szinten, amely jelentős mértékben alakíthatja mind a hétköznapi felhasználói, mind a vállalati – ipari vagy akár mezőgazdasági – területen is a működés folyamatait. Az eszközök fejlődésében ma már elérhető a 3D-s technológia, nemcsak a nyomtatásban, de a virtuális 3D világában történő együttműködésben is (virtuális labor).

A 3D-s egerek, mobiltelefonok, laptopok, szemüvegek, a mozgás- és érzékelés új alapokra helyezése világosan mutatja az utat az okos hálózatok egyre magasabb szintű kiépítése felé. A cél az „élhetőbb bolygónk”, bízunk benne, hogy a témérdek és folyamatosan bővülő high-tech-megoldások kívánta árammennyiség előteremtéséhez már megújuló energiaforrásokat veszünk majd igénybe.

2 Okos hálózatok.

MEGJELENTEK A DRÓNOK – LESZ-E „TISZTA HÁBORÚ”?

Természetesen – vagy sajnos –, mint minden új fejlesztésnek, ennek is lehetnek negatívumai, vadhajtásai. Az Egyesült Államok hadseregében már ma is több ezer robotot vetnek be, a távirányítású repülőgépektől az aknamentesítőkön át a *Csillagok háborújából* ismert birodalmi lépegetőkre hasonlító szállítóeszközökig.

A legegyszerűbb megfogalmazásban a robotok olyan gépek, amelyek az „érzékelni, gondolkodni, cselekedni” vezérelve alapján működnek, azaz érzékelőikkel adatokat gyűjtenek a külvilágról. Ezen adatok feldolgozásuk után további számítógépes processzorokhoz, esetleg egy mesterségesintelligencia-programba továbbítódnak, amelyek az információk felhasználásával és kiértékelésével hozzák a megfelelő döntéseket. Végül az effektoroknak nevezett mechanikus rendszerek végrehajtanak valamilyen fizikai akciót a környezetükben.

Az amerikai hadsereg jelentős tőkével támogatja a robotikai kutatásokat, [1] mert a robotokkal emberéletek kímélhetők meg, és bizonyos feladatok ellátására alkalmasabbak, mint az emberek. A jelenlegi robotok zöme emberi távirányítással működik, de erőteljesen fejlesztik a mesterséges intelligenciával rendelkező robotokat is.

Újabb lépésként megjelentek a pilóta nélküli légijármű-rendszerek, -eszközök (UAS, UAV), közkezdveltebb néven a drónok. Napjainkban a drónok fejlesztésének és dinamikus térhódításának periódusát éljük. A kutatók beszámolóí szerint a fejlődés léptékét csak a '70-es évek PC-forradalmához lehet hasonlítani. A kezdeti katonai, rendvédelmi felhasználási területeket messze meghaladva terjednek a civil szférában is, például az árvízvédelem vagy a légi fotós technika területén is egyre elterjedtebbek. A felhasználásuknak szinte csak a fejlesztők fantáziája szabhat határt.

A jövőkutatók szerint körülbelül 20 év múlva igaz lesz a megállapítás, miszerint: „egy szabványos méretű joghurtos pohárban annyi intelligencia elfér, mint az összes európai ember fejében”. Ezzel a mondattal kezdte felszólalását Ian Pearson Londonban, a *Global Security Summit* konferencián és kiállításon, amelyet 2012. október 11–12-én rendeztek meg. Előadása, amelyet gondolatébresztőnek szánt, meghökkentő volt, egyik figyelmeztetése szerint például a zombik átveszik bolygónk irányítását, de említésre méltó a retinaméretű iPad-ekről szóló prognózisa is.

NAGY UGRÁS: AZ IT-TECHNOLÓGIA FEJLŐDÉSE

Néhány évtized alatt – szűk ötven évről beszélünk – minden paraméterében fantasztikus fejlődésen ment át az informatikai, és vele párhuzamosan természetesen a kommunikációs technológia is. Ma már szinte mindenki az 5+ generációs IT-berendezések sorát alkalmazza nap mint nap. A teremméretű, 1012 mm-es, nagy számítógépek³

3 IBM 360, ESZ-R-40, -60 stb.

tudását meghaladó, a 3–10 mm-es tartományban is működő nanotechnológiai fejlesztésekkel is komolyan kell számolnunk.

Az előadásom témája az ebben a nagyságrendben kifejlesztett és ma már széles körben alkalmazott smart dust, azaz az „okos por”. [2] Globalizált világunk számos nagyhírű egyeteme (Berkeley, Stanford, Brown stb.) és cége (Intel, Philips, Shell, HP stb.) is hihetetlen lendülettel fordult ehhez a témához és kezdett neki az új és újabb fejlesztéseknek.

„OKOS POR” – SMART DUST

Pearson arra figyelmeztetett, hogy a folyamatos miniaturizálás az egyik legnagyobb fenyegetés a következő 5–10 évben. Az egyik ilyen fejlesztés az úgynevezett „okos por” (smart dust), amely vezeték nélküli kommunikációra képes mikro-elektromechanikai rendszereket takar. Gondoljunk csak bele, mekkora a különbség a '90-es évek technológiája és a mai iPhone 5 között! Néhány generációnyi iPhone után az Apple is használni fogja ezt a technológiát. „Merre halad az okos por?” – tette fel a kérdést a jövőkutató. Amikor elkezdték a fejlesztéseket, az okos por 1–2 cm átmérőjű volt, ma 50 mikron körül tartunk. De mire is lehet használni?

A miniatűr mobileszközökkel is nyomon követhető folyamatok már lakossági és ipari szinten is elérhetővé váltak, az energiaszolgáltatások mérésére és optimalizálására létrehozott applikációk pedig könnyű kezelhetőséget kínálnak minden felhasználónak. Az infokommunikációs eszközök használata természetesen nem csupán az energiaszektor kiváltsága. Alkalmazásuk jelentős támogatást nyújthat minden smart grid megoldással bíró ágazatban, legyen az oktatás, egészségügy vagy akár turizmus.

Természetesen a legnagyobb üzleti vállalkozások sorából a katonai fejlesztésekre specializálódott cégek is kiveszik a részüket. Az új és újabb eszközök harctéri alkalmazása gyökeresen megváltoztathatja az információs tér fogalmát, az információs fölény elérésének feltételeit. Az NSA egyik prezentációjában az a mondat szerepel, hogy a következő nagy konfliktus az interneten fog elkezdődni. A fegyverkezés pedig ennek szelvében zajlik. Az amerikai titkosszolgálatok titkos költségvetésében 2013-ban több mint egymilliárd dollárt különítettek el a számítógépes hálózatok elleni hadműveletek kategóriájában a támadási potenciál erősítésére. A „hálózati” és robotkatonákkal együtt kialakított hálózatközpontú hadviselés információs hálózatának meghatározó elemeit képezhetik a mikro/nano [3] méretű, de annál nagyobb tudású berendezések. Az amerikai hadsereg olyan módszerek kifejlesztésén is dolgozik, amelyekkel a katonák a gondolataikkal irányíthatnák a csatatéren őket helyettesítő android robotokat.

Nem mehetünk el szó nélkül a „civil” alkalmazások új lehetőségei mellett sem. A beültethető fejlesztések közül talán az okos por klinikai alkalmazása a legmegdöbbentőbb. A homokszemcsénél is apróbb, saját antennával ellátott okos porszemek hálózatba rendeződnek a testben, és egy egész sor összetett folyamat elvégzésére képesek.

Talán egy nanohadseregként lehetne jellemezni őket, amely például a rákos sejtek ellen indulhat csatába, vagy csillapítja a fájdalmat, és persze képes a gazda személyes adatainak titkosított tárolására.

Az okos por segítségével az orvosok egy napon képesek lesznek a beteg felnyitása nélkül dolgozni a testben, az információk pedig egészen addig titkosak maradnak, míg a gazda hozzáférhetővé nem teszi saját nanohálózatán keresztül. Egy még inkább futurisztikus ötlet: a levegőbe szórják az okos port úgy, hogy azt beszívva csatlakozik idegrendszerünkhöz, és amikor a bankautomata előtt arra gondolunk, mi is a PIN-kódunk, az okos por már elfogta a gondolatot, továbbította azt, s már föl is törték bankszámlánkat.

Lehet, hogy ezek a gondolatok túl fantáziadúsnak tűnnek, de elméletileg mindez már lehetséges. Az apró intelligens részecskék fenyegetése valamely szervezet biztonsága ellen egyelőre még jelentéktelen. De hogy ez ne is fordulhasson elő, ahhoz először is el kell képzelnünk, mekkora fenyegetettséget jelenthet mindenki számára ez a technológia. Gyakorlatilag minden netfelhasználó célponttá válhat. A Facebookon zajló chatbeszélgetések feltörhetőek és kimásolhatók, például az olyan programok segítségével, mint a Quantumdisk.

Egyesek pozitívként tekintenek erre az irányra, a bűnüldözés hatékonyságát, a választási csalások kiküszöbölését, az orvosi információkezelés forradalmasítását és a gyerekek biztonságát tartva szem előtt. Megint mások a szingularitás felé tett első végzetes lépést sejtik benne, amikor az emberiség jövőjének irányítását a mesterséges intelligenciára alapozott szoftvereknek adják át. Sokan – talán nem is ok nélkül – egy orwelli társadalom kialakulását látják a folyamatban, amelynek élén Nagy Testvér mindent tud, mindent lát és mindent irányít. Egyes szakemberek szerint egy ilyen vagy ehhez hasonló azonosító kiterjesztése a társadalom minden részére elkerülhetetlen következményekkel járhat.

ÖSSZEFOGLALÁS

A titkosszolgálatok ma már nemcsak kémkednek, hanem meg akarják szerezni a világháló fölötti ellenőrzést is, és digitális háborúra készülnek. A titkosszolgálatok kiadták a „plausible deniability” irányelvet, amely azt jelenti, hogy a támadásokat úgy kell végrehajtani, hogy letagadhatók legyenek, és az akciókat ne lehessen bizonyítani sem.

Az agy közvetlen összekapcsolása a számítógéppel a tudományos fantasztikum álma (vagy rémálma). Az Intel szerint a gyakorlatban is alkalmazható számítógépagy-interfészek 2020-ra kerülhetnek piacra. A Brown Egyetem BrainGate (agykapu) nevű csapata vezeti az ilyen irányú kutatásokat. Weboldaluk szerint a csecsemőknek való aszpirin tabletta méretével megegyező, agyba ültetett elektródák segítségével a BrainGate csapat bebizonyította, hogy képesek valós időben dekódolni a neuronok jeleit, és ezekkel külső eszközöket irányítani.

A kényes adatok továbbítására pedig akár idegenek mobiltelefonjai is felhasználhatók átmenetileg. Ebben az információk megszerzésére irányuló gerillaháborúban gyakorlatilag alig lehet megkülönböztetni egymástól a polgári és a katonai célpontokat. Azt remélem, az új technológiák a fejlődés helyes irányába mutatnak, az ellenőrzött biztonságot és a békefenntartást szolgálják majd.

IRODALOMJEGYZÉK

- [1] MOLNÁR Berta: A következő ipari forradalom a robotoké lesz. In: *PC Word*, 2014. augusztus 15.
- [2] BALOG Károly: *Wireless Data Communications in the 21st Century*. Issue of "Robot warfare" international conference presentations, ZMNE, 2001.
- [3] MALLÁSZ Judit: Emberközpontú robotika – mi lesz a jövő? In: *Robottrend*, 2015/2.
- [4] www.darpa.mil/work-with-us/opportunities/Military_Services/Military_Services/Military_Services (2015. 10. 03.)
- [5] www.darpa.mil/about-us/timeline/darpas-stealth-revolution (2015. 10. 03.)
- [6] www.nanotechnology.hu/magyarul/Nanotech-BLP.html (2015. 10. 11.)

NYÍLT FORRÁSKÓDÚ KIBERBIZTONSÁGI SZOFTVEREK ALKALMAZÁSA KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME SORÁN

A kritikus információs infrastruktúrák védelme minden nemzet számára kiemelkedő fontosságú feladat, azonban az erőforrások szűkössége megkívánja a költséghatékony védekezés kialakítását. Ebben nyújthat segítséget a nyílt forráskódú szoftverek alkalmazása. Tanulmányomban bemutatom a nyílt forráskódú szoftverek felhasználása során fontos licenceket, majd összehasonlításom a nyílt és a zárt forráskódú szoftverek tulajdonságait. Röviden ismertetem a Magyarország létfontosságú rendszereinek és rendszerlemeinek védelmével kapcsolatos jogszabályi környezetet, és az előírt logikai védelmi intézkedések elvégzéséhez bemutatok néhány szabad forráskódú szoftvert is.

Rendkívül nagy felelősség hárul a létfontosságú rendszereket üzemeltető szervezetre, hiszen a társadalom számára alapvető fontosságú szolgáltatások zavartalan biztosításáról kell gondoskodniuk, s e feladathoz sokszor nem áll rendelkezésükre a megfelelő mennyiségű anyagi erőforrás. A magas szintű és emellett költséghatékony védelem kialakításához jól használható eszközök lehetnek a nyílt forráskódú kiberbiztonsági szoftverek, amelyek egyre nagyobb teret nyernek a védelem területén.

NYÍLT FORRÁSKÓDÚ SZOFTVEREK

A szabad szoftver (angolul „free software”) nem a szoftver árára utal, hanem arra, hogy mit tehetünk meg vele. A felhasználónak a következő négy alapvető jogát jelenti: [8]

- a program futtatásának lehetősége bármilyen céllal;
- a program működésének tanulmányozása és a működés módosítása (ehhez a forráskód is szükséges);
- másolatok közzététele;
- a program tökéletesítése és a tökéletesített változat közzététele.

Számunkra talán az első pont a legfontosabb, hiszen ez azt jelenti, hogy a szabad szoftvereket a licencfeltételek megsértése nélkül használhatjuk rendszereink védelmére, függetlenül attól, hogy a rendszer milyen célt szolgál, üzleti vagy magánfelhasználásra

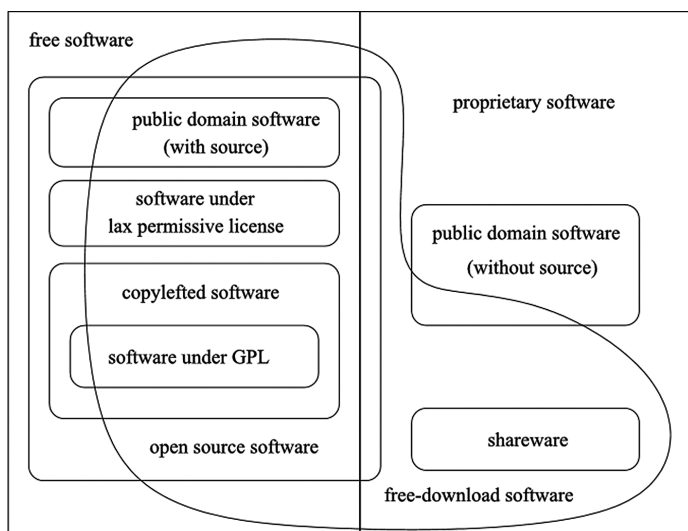
¹ Hálózati és hálózatbiztonsági tanácsadó (repa@ahol.com).

készült-e. A következőkben mi inkább a nyílt forráskódú szoftver elnevezést alkalmazzuk, amely szintén elterjedt a szabad szoftverek azonosítására.² Az Open Source Initiative szervezet felmérése szerint a legelterjedtebb licenctípusok szabad szoftverek esetén a következők (2006-os adatok alapján):³

- Apache License 2.0;
- BSD 3-Clause „New” or „Revised” license;
- BSD 2-Clause „Simplified” or „FreeBSD” license;
- GNU General Public License (GPL);
- GNU Library or „Lesser” General Public License (LGPL);
- MIT license;
- Mozilla Public License 2.0;
- Common Development and Distribution License;
- Eclipse Public License.

A különböző licenctípusok között alapvetően kétfélet különböztethetünk meg:

- *Copyleft*: a módosított szoftvert csak azonos licenfeltételekkel szabad terjeszteni, mint az eredeti szoftvert.
- *Permissive*: megengedő, azaz a módosítás után más licenc is alkalmazható, akár zárt forráskódú programként is terjeszthető az új (módosítás utáni) szoftver.



1. ábra: Különböző licenctípusok⁴

² A Free Software Foundation a *szabad szoftver* (free software), míg az Open Source Initiative a *nyílt forráskódú* (open source) elnevezést alkalmazza.

³ *Open Source Initiative: Licenses & Standards*. <http://opensource.org/licenses> (2015. 10. 30.)

⁴ Forrás: *GNU: Categories of free and nonfree software*. www.gnu.org/philosophy/categories.html (2015. 10. 30.)

A copyleft licencre a legismertebb példa a GPL alatt terjesztett Linux, míg a megengedőre (permissive) az Apache licenc alatt terjesztett Apache webservert és a BSD licenc alatt terjesztett FreeBSD. A különböző licencfajták összefüggését mutatja be az 1. ábra, amelyen a feliratokat az egyértelmű azonosíthatóság érdekében nem fordítottam le. Nem volt cél a szabad forráskódú szoftverek licencléhetőségeinek teljes körű bemutatása, csak a számunkra legfontosabb információk ismertetése. Részletesebb információkért javasolt a megadott referenciák tanulmányozása.

A NYÍLT FORRÁSKÓDÚ SZOFTVEREK ELŐNYEI ÉS HÁTRÁNYAI

A következőkben részletesen megvizsgáljuk, hogy milyen előnyei és hátrányai lehetnek a nyílt forráskódú biztonsági szoftverek alkalmazásának. Greiner és társai már 2003-ban arra a következtetésre jutottak, hogy a nyílt forráskódú szoftverek gyors térnyerése elsődlegesen az alacsony költségeknek köszönhető. A kutatók véleménye szerint a nyílt forráskódú szoftvereket fejlesztők magas kompetenciákkal rendelkeznek, és a zárt forráskódú szoftvereknél is magasabb biztonság érhető el a szabad szoftverek alkalmazásával. [2]

Cowan nem próbálja eldönteni, hogy a zárt vagy a nyílt forráskódú szoftver-e a biztonságosabb, ellenben az a véleménye, hogy a szabad szoftverek lényegesen több eszközt adnak mind a támadó, mind pedig a védekező kezébe. Ugyanakkor sok biztonságnövelő technika tud segíteni a védekezőnek a biztonság növelésében, amelyek közé a szoftverauditáló, a sérülékenységmérés-kló, a viselkedésmenedzsment-eszközök és az integrált rendszereket sorolja. [1]

Schryen és Rich 17 különböző nyílt és zárt forráskódú szoftver empirikus vizsgálatát végezte el, amelyek közt egyaránt megtalálható kliens- és szerveralkalmazás, valamint operációs rendszer is. A kutatók vizsgálták a nyilvánosságra került sebezhetőségeket, azok súlyosságát és a hibajavítások számát. Kutatásuk eredménye alapján nem található számottevő különbség a sebezhetőségek súlyosságában, valamint a hibajavítások kiadásában a zárt és a nyílt forráskódú szoftverek közt. Fontos megállapításuk azonban, hogy a nyílt forráskódú szoftverfejlesztés segít megelőzni a hibajavítások kiadásával kapcsolatos „extrém rossz” viselkedést. [6]

Lawton a következő területeket azonosítja az előnyök és a hátrányok meghatározásához: [3]

- *Költségek:* az egyik legfőbb előnye a nyílt forrású biztonsági eszközöknek a jelentősen alacsonyabb költség.
- *Minőség:* Ezen a területen Lawton sem tud egyöntetű véleményeket felmutatni, leginkább Schryen és Rich megállapításaihoz hasonló következtetésre jut, miszerint a forráskód nyíltsága nincs hatással a minőségre.
- *Támogatás:* A nyílt forráskódú szoftverek nem rendelkeznek gyártói, telefonos vagy egyéb támogatással.

- *A forráskód elérhetősége:* A forráskód elérhetősége segíti a hackerek tevékenységét, azonban lehetővé teszi a felhasználónak a kód testre szabását is.

Nagyon fontos megállapítása, hogy a szabad szoftverként elérhető biztonsági alkalmazások fejlesztői elsődlegesen a funkcionalitásra fókuszálnak, és elhanyagolják a kezelhetőséget, a nehezen kezelhető szoftverek pedig hátráltatják a széles körű alkalmazást. Ugyanakkor egyre több megoldás és támogató szolgáltatás jelenik meg ezekhez az eszközökhöz, s ez megkönnyíti alkalmazásukat.

A SANS Institute kiadványa a következő *kockázatokat* azonosítja a nyílt forrású szoftverek alkalmazásával kapcsolatban: [4]

- Aprólékos értékelés hiánya: a legtöbb vállalkozás egy szoftver vásárlása előtt komoly döntés-előkészítő munkát végez, megvizsgálja a lehetséges szoftvereket, azok tulajdonságait, költségeit, kockázatait. Ezt az előkészítést azonban a szabad szoftverek esetében általában nem hajtják végre.
- Hamis forráskód: a nyílt forráskódú szoftvereket bárki letöltheti, és rosszindulatú kódot helyezhet el bennük, majd terjesztheti a programot. Növelheti a kártékony kóddal ellátott program terjesztésének hatékonyságát, ha a lehetséges felhasználók számára vonzó, valós funkciókkal is kiegészíti azt.
- Anyagi támogatás hiánya: sok esetben a nyílt forráskódú szoftverek fejlesztőinek nem áll rendelkezésére elegendő erőforrás, hogy a szoftvert megfelelő minőségben készíthessék el.

A SANS Institute a *kockázatok mérséklésére* a következő eszközöket ajánlja:

- Biztonságpolitika: nagyon fontos, hogy a szervezet rendelkezzen egy jól kidolgozott biztonságpolitikával, amely részletesen tartalmazza a nyílt forráskódú szoftverek alkalmazásával kapcsolatos teendőket is.
- Értékelés: Alkalmazásuk előtt a szoftvereket alaposan meg kell vizsgálni és ki kell értékelni.
- Kerülni kell az ad hoc telepítéseket: ugyanolyan formális installációs eljárásokat kell alkalmazni, mint az egyéb szoftverek esetében.
- Csak megbízható forrásból szabad letölteni a szoftvert.
- Amennyiben lehetséges, úgy kerüljük a már lefordított bináris kódok alkalmazását, és a forráskódból magunk állítsuk elő a futtatható programot!
- Sérülékenységhatárokat kell alkalmazni a sebezhetőségek megtalálására.
- A nem szükséges szolgáltatásokat le kell tiltani, ugyanúgy, mint más alkalmazások esetében.
- Mélységi védekezés: a nyílt forráskódú szoftverek alkalmazásánál is alkalmazni kell a mélységi védekezés stratégiáját.
- Karbantartás: ugyanúgy fontos a karbantartás, a javítások és frissítések telepítése, mint más szoftverek esetében.
- Képzés és dokumentálás: a zárt forráskódú szoftverekhez hasonlóan kell végezni.
- Üzletmenet-folytonossági (BCP) és katasztrófaterv (DRP): részletesen foglalkozni kell a nyílt forráskódú szoftverekkel is a BCP és a DRP kialakítása során.

Fontos megfigyelni, hogy az ajánlott eszközök csak kismértékben térnek el a zárt forráskódú szoftverek alkalmazása során is ajánlott módszerektől. Kijelenthető tehát, hogy a szoftver minőségére nincs egyértelmű hatása a forráskód nyíltságának. Vannak azonban más fontos szempontok, amelyek általában jellemzik a nyílt és a zárt forráskódú szoftvereket, ezért elengedhetetlen a figyelembevételük. Ezeket az 1. táblázat sorolja fel.⁵

1. táblázat: A zárt és a nyílt forráskódú szoftverek jellemzői⁶

Zárt forráskódú szoftver	Nyílt forráskódú szoftver
Magasabb egyszeri beruházási költség	Várhatóan alacsony beruházási költség
Magas szoftverkövetési díj (licenccdíj)	Esetlegesen nehezebb frissítés, telepítés
Alacsonyabb üzemeltetési költség	Várhatóan magasabb üzemeltetési költség
Gyártófüggés kialakulása (vendor lock-in)	Gyártófüggetlenség (részbeni függés a fejlesztőktől)
Fejlesztés megszűnése általában csak bejelentés után	Fejlesztés esetleges váratlan megszűnése
Gyártói támogatás beszerezhető	Csak néhány gyártó nyújt támogatási szolgáltatást, esetleg független szervezetektől beszerezhető
Alacsonyabb közösségi támogatás	Magas közösségi támogatás
A biztonsági célú kódelemzés általában kizárt	Biztonsági célú kódelemzés végezhető
Nem testre szabható, módosítható	Tetszőlegesen módosítható
A forráskódhoz általában nem fér hozzá a támadó	A forráskódot megismerheti a támadó
Esetlegesen korlátozott jótállás kapható	Jótállás nincs

A magasabb egyszeri beruházási költség egyértelműen a licenccdíj költségeiből adódik, ugyanakkor sok járulékos költsége is van egy szoftver bevezetésének,⁷ így a szabad szoftver bevezetési költségei sem tekinthetők nullának. Szinte az összes zárt forráskódú szoftver esetén van valamilyen szoftverkövetési licenccdíj. Ez lehet állandó éves díj (előfizetési díj), vagy csak a növelt funkcionalitásért fizetendő plusz díj (frissítési díj, upgrade-díj), de olyan megoldás is lehetséges, hogy a biztonsági frissítések is csak díj ellenében tölthetők le a termékhez. A nyílt forráskódú szoftverek esetében licenccdíjjal nem kell számolni,

⁵ A táblázatban megfogalmazottak természetesen nem minden egyes szoftver esetén teljesülnek.

⁶ Forrás: saját összeállítás.

⁷ Ilyenek lehetnek: tesztek, személyre szabás, telepítés, kiegészítő szoftverek, hardvereszközök stb.

és ha a fejlesztés még folyik, a frissítés megoldható. Ugyanakkor előfordulhat, hogy a frissítési folyamat nincs megfelelően dokumentálva, s ez növeli a költségeket.

Rengeteg egymásnak ellentmondó tanulmány vizsgálta a kétféle forráskódú szoftver alkalmazása során felmerülő teljes birtoklási költségeket.⁸ [7] Amint Lawton is megállapította, a legtöbb szabad szoftver fejlesztése során előnyt élvez a funkcionalitás a menedzselhetőséggel szemben, [3] s ez nagyobb szakértelmet és magasabb humán-erőforrás-ráfordítást kíván meg az üzemeltetés során. Ez a megállapítás azonban nem minden alkalmazás esetén igaz vagy releváns, így semmiképpen nem jelenthető ki általános igazsággént.

Napjainkban egyre fontosabb szemponttá lép elő a beszállítóktól való függetlenség biztosítása. A zárt forráskódú szoftverek alkalmazása esetén a felhasználó kiszolgáltatott a program szállítójának, azonban bizonyos esetekben ennek a függésnek a csökkentésére is van lehetőség a forráskód letétbe helyezésével.⁹ Így, ha a gyártó vállalkozás valamilyen oknál fogva felhagy a szoftvertermék további fejlesztésével és támogatásával, a felhasználó gondoskodhat a további fejlesztésekről. Figyelembe kell venni azonban, hogy már egy kisebb szoftver megértése és továbbfejlesztése is hatalmas feladat lehet, amely sokszorosan meghaladhatja a felhasználó szervezet képességeit. Nyílt forráskódú szoftverek esetén is kiszolgáltatott a felhasználó, azonban a fejlesztőknek. Ez a kiszolgáltatottság ugyanakkor lényegesen kisebb (vagy kisebb erőráfordítással orvosolható), mint a zárt forráskódú termékek esetén.

Amennyiben a szoftvertermék gyártója nem kerül valamilyen, a működését ellehetetlenítő helyzetbe, akkor a szoftverek fejlesztésének vagy támogatásának megszűnését általában előzetesen bejelenti, ezzel időt biztosítva az átállásra. A nyílt forráskódú termékek esetében azonban rendszeresen előfordul, hogy a fejlesztés hirtelen félbeszakad, így az ebből eredő kockázatok csökkentésére nagyon fontos a szabad forráskódú szoftver körültekintő kiválasztása.

Zárt forráskódú szoftverek esetén általában a vásárlást követő hosszabb-rövidebb időszakban a szállító díjmentes támogató szolgáltatást nyújt, amely díj ellenében további időszakra is megrendelhető. A szabad szoftverek esetében támogatási szerződés megkötésére sokszor nincs lehetőség. Egyre népszerűbb a nyílt forráskódú szoftverek esetében az a gyakorlat, hogy a szoftver bárki által szabadon hozzáférhető, és a fejlesztőkkel támogatási szerződés köthető.¹⁰ Mind szélesebb körben terjed az a megoldás is, hogy a szoftvernek létezik egy szabad szoftverként hozzáférhető, korlátozott funkcionalitású verziója,¹¹ de megvásárolható vagy előfizethető egy fejlettebb változat is a programból, amelyhez már támogatási szerződés is jár. Amennyiben nincs szükség gyártói támogatásra, úgy általában minden szoftverhez beszerezhető nem gyártói támogatás, azonban előfordulhatnak olyan esetek is, amikor ez nem elégséges a felmerülő problémák megoldásához.

8 Total Cost of Ownership, TCO.

9 Mezrich, Jonathan L.: *Source Code Escrow: An Exercise in Futility?* Milwaukee, 2001, 117–131.

10 Jól ismert példa ennek az üzleti modellnek az alkalmazására a Red Hat, Inc.

11 Általában *community edition* néven.

A legtöbb szabad szoftver széles körű közösségi támogatással, fórumokkal, levelezőlistákkal, blogokkal rendelkezik, azonban a zárt forráskódú szoftvereknél ez általában csak a nagyobb penetrációjú termékekről mondható el. Egyre fontosabb annak megállapítása, hogy egy szoftver rendelkezik-e beépített hátsó ajtóval, vagy a készítése során betartották-e a szoftverkészítési ajánlásokat, illetve milyen minőségű programozói munkát végeztek. Míg a nyílt forráskódú szoftverek biztonsági célú kódelemzése tetszőlegesen elvégezhető, addig a zárt forráskódúak esetén csak igen korlátozottan van erre lehetőség. Erre példa a Microsoft vállalat, amely 2003 óta lehetővé teszi a forráskód biztonsági célú vizsgálatát kormányzatok számára,¹² majd különböző partnereinek is engedélyezte ezt,¹³ végül pedig 2015-ben átláthatósági központot nyitott Brüsszelben.¹⁴ Néhány más kivételtől eltekintve azonban ezt a lehetőséget más gyártók nem biztosítják.

A zárt forráskódú szoftverek csak nagyon kis mértékben tesztre szabhatóak, és ehhez a munkához általában valamilyen szabványos interfész áll rendelkezésre, míg nyílt forráskód alkalmazása esetén tetszőleges módosítások végezhetőek a programon. Ezáltal a szoftver új funkcionalitással is szabadon ellátható. Figyelni kell azonban arra, hogy ha a forráskódot valamilyen okból módosították, úgy a program újabb verziójának megjelenésével ezeket a változtatásokat nem lehet egyszerű eszközökkel átemelni az újabb variánsba.

Nagyon sokszor elhangzik érvként, hogy a nyílt forráskódú szoftvereket a támadó tetszőlegesen kielemezheti, majd vizsgálatának eredményeit felhasználva hatékonyabb támadást vihet véghez. Erre általában az az ellenérv, hogy cserébe nagyon csekély a hibák valószínűsége, hiszen a forráskódot sokan látták, és a feltárt hibákat kijavították. A 2014 áprilisában nyilvánosságra hozott Heartbleed hiba azonban ezt a kijelentést más megvilágításba helyezi.¹⁵ A titkosításért felelős, BSD licenc alapján terjesztett, OpenSSL-ben talált hiba – az OpenSSL széles körű felhasználása miatt – olyan gyártók termékeit is támadhatóvá tette, mint a legismertebb hálózateszköz-gyártó, a Cisco Systems, Inc.¹⁶ Mindemellett annak figyelembevétele is szükséges, hogy számtalan biztonsági szakember foglalkozik a nyílt forráskódú szoftverek vizsgálatával. Ráadásul ennek a hibának a felfedezése rávilágított arra is, hogy sok alapvető fontosságú szabad szoftver készítése alulfinanszírozott, és ezzel elősegítette a jövőbeni finanszírozás megoldását is.¹⁷

12 *A Matter of National Security: Microsoft Government Security Program Provides National Governments with Access to Windows Source Code.* <http://news.microsoft.com/2003/01/14/a-matter-of-national-security-microsoft-government-security-program-provides-national-governments-with-access-to-windows-source-code/> (2015. 10. 30.)

13 *Shared Source Initiative.* www.microsoft.com/en-us/sharedsource/default.aspx (2015. 10. 30.)

14 *The Microsoft Transparency Center in Brussels.* <https://blogs.microsoft.com/eupolicy/transparency-center/> (2015. 10. 30.)

15 *The Heartbleed Bug.* <http://heartbleed.com/> (2015. 10. 30.)

16 *OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products.* <http://tools.cisco.com/security/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed> (2015. 10. 30.)

17 ROMAN, Jeffrey: *OpenSSL Gets Funding After Heartbleed.* www.bankinfosecurity.com/openssl-gets-funding-after-heartbleed-a-6893/op-1 (2015. 10. 30.)

A szabad szoftverek licencfeltételei egyértelműen elhárítanak minden felelősséget. Emellett a legtöbb gyártó olyan szigorú korlátozásokat szab meg szoftvere licencszerződésében, amelyek csak nagyon korlátozott jótállási felelősséget nyújtanak. A 2. táblázat tartalmaz néhány megvásárolható szoftverterméket, amelyek nyílt forráskódú szoftvereken alapulnak, s elismert gyártók biztonsági megoldásai is megtalálhatók benne. Általában a gyártók kibővített funkcionalitással, biztonsági fejlesztésekkel látják el a nyílt forráskódú programot, és azt árusítják.

2. táblázat: Néhány szabad szoftveren alapuló termék¹⁸

Gyártó és terméke	Nyílt forráskódú alap	Típus
Sophos Email Appliance ¹⁹	FreeBSD	Biztonsági
McAfee SecurOS ²⁰	FreeBSD	Biztonsági
Juniper JunOS ²¹	FreeBSD	Hálózati eszköz
Check Point IPSO ²²	FreeBSD	Biztonsági
Cisco IronPort ²³	FreeBSD	Biztonsági
Cisco Secure ACS ²⁴	Linux	Biztonsági
Check Point SecurePlatform ²⁵	Linux	Biztonsági
VMware ESX Server ²⁶	Linux	Virtualizációs rendszer
Genua genugate ²⁷	OpenBSD	Biztonsági
Fox-IT DataDiode	OpenBSD	Biztonsági

¹⁸ Forrás: saját összeállítás.

¹⁹ *Sophos Email Appliance: overview*. www.sophos.com/en-us/support/knowledgebase/14384.aspx (2015. 10. 30.)

²⁰ *Welcome to FreeBSD!* www.freebsd.org/doc/handbook/nutshell.html (2015. 10. 30.)

²¹ *Downgrading Junos OS from Upgraded FreeBSD*. www.juniper.net/techpubs/en_US/junos15.1/topics/task/installation/junos-os-downgrading-kernel-freebsd10.html (2015. 10. 30.)

²² *Release Notes and Getting Started Guide IPSO 6.2*. <http://downloads.checkpoint.com/dc/download.htm?ID=10292> (2015. 10. 30.)

²³ *IronPort: Demonstrating the Cisco Commitment to Open Source*. www.cisco.com/web/about/doing_business/open_source/stories/ironport.html (2015. 10. 30.)

²⁴ *Introducing ACS*. www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-2/user/guide/acsguide/intro.html (2015. 10. 30.)

²⁵ *Introduction to SecurePlatform*. www.checkpoint.com/services/education/training/courses/samples/cpsa1_r65_sample.pdf (2015. 10. 30.)

²⁶ *VMware ESX*. https://en.wikipedia.org/wiki/VMware_ESX (2015. 10. 30.)

²⁷ *Products for OpenBSD*. www.openbsd.org/products.html (2015. 10. 30.)

A LÉTFONTOSSÁGÚ INFORMÁCIÓS INFRASTRUKTÚRÁK, VALAMINT A VÉDELMEKRE ALKALMAZHATÓ NYÍLT FORRÁSKÓDÚ KIBERBIZTONSÁGI SZOFTVEREK

A modern társadalmak működéséhez elengedhetetlen szükség van különböző infrastruktúrák szolgáltatásaira, amelyek folyamatosan biztosítják az emberek életének és a gazdaság működésének feltételeit. Ilyen infrastruktúra lehet például az energiaellátás, az infokommunikáció, a közlekedés, de a pénzügyi rendszer is. Könnyen belátható, hogy a felsoroltak közül bármelyik elégtelen működése komoly károkat okoz a társadalom számára, így ezen infrastruktúrák kielégítő működése kritikus fontosságú. Magyarországon jelenleg a többször módosított 2012. évi CLXVI. törvény²⁸ (Lrtv.) foglalkozik a létfontosságú rendszerek és rendszerelemek²⁹ kijelölésével és védelmével.

Az Lrtv. mellékletében meghatározott tíz létfontosságú ágazat a következő:

- energia,
- közlekedés,
- agrárgazdaság,
- egészségügy,
- pénzügy,
- ipar,
- infokommunikációs technológiák,
- víz,
- jogrend – kormányzat,
- közbiztonság, -védelem.

A kritikus infrastruktúrák egyik legfontosabb tulajdonsága az egymástól való kölcsönös függés, az interdependencia. [5] Az egyes infrastruktúrák és az egyes infrastruktúraelemek kölcsönösen egymásra utaltak, például csak korlátozott ideig tartható fenn a telekommunikáció a villamosenergia-ellátás kiesése esetén amellet, hogy csak nagy nehézségek árán biztosítható a villamosenergia-ellátás az infokommunikációs technológiák nem megfelelő működésekor. Ezek alapján kiemelkedő fontosságú a kritikus információs infrastruktúrák megfelelő védelméről gondoskodni. A létfontosságú információs infrastruktúrák³⁰ kibervédelme során ellátandó konkrét feladatokat 2015. július 17-től a 41/2015. BM rendelet határozza meg.³¹ A következőkben a rendeletben

28 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

29 Másként: kritikus infrastruktúrák.

30 Más elektronikus információs rendszerek mellett.

31 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

található védelmi intézkedések katalógusában előírt feladatok megvalósításához mutatunk be néhány nyílt forráskódú szoftvert.

1. Előírt intézkedés:

3.3.11.4.1.1. Az érintett szervezet az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat.

Magyarázat: A hálózat kapcsolódási pontjait vírusvédelemmel kell ellátni.

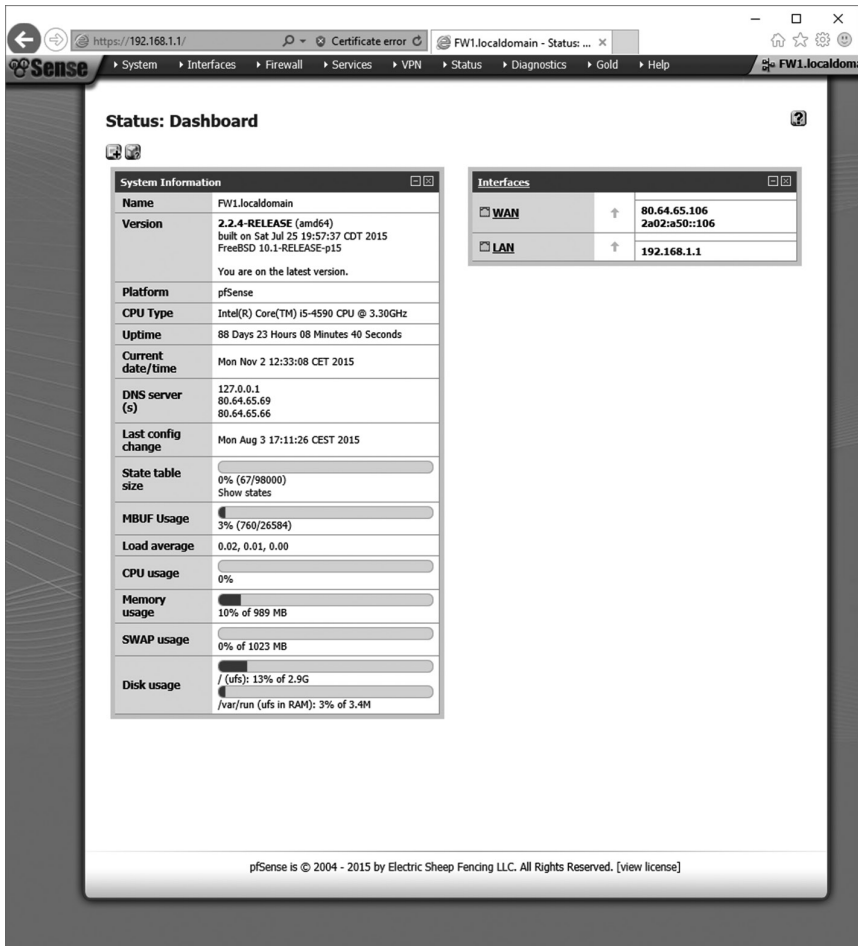
Lehetséges megoldás: A pfSense alkalmazása HAVP-csomaggal kiegészítve.

A pfSense³² egy FreeBSD rendszeren alapuló tűzfalcsomag, amelynek fejlesztését 2004-ben kezdték meg.³³ A programnak nagy előnye a könnyű menedzselhetőség, amelyhez internetböngészővel elérhető grafikus felület áll rendelkezésre (2. ábra). Fontos, hogy a rendszert virtualizált környezetben is lehet telepíteni, így futtatásához nincs szükség külön számítógépre, sőt az egyes virtuális gépek közti forgalom figyelése és szabályozása is megvalósítható a szerveren belül. Támogatja a redundáns működést, így a magas rendelkezésre állást követelő alkalmazások esetében is használható. Moduláris felépítésű, több kiegészítőcsomag elérhető hozzá, de nyílt forráskódú eszköz lévén akár saját csomag is fejleszthető. A HAVP³⁴-csomaggal kiegészítve képes a http-forgalomban megtalálni és kiszűrni a vírusokat. SslBump alkalmazása esetén akár a https-forgalmat is képes vizsgálni.

32 *PfSense*. www.pfsense.org/ (2015. 10. 30.)

33 A BSD-rendszerek csomagszűrő eszköze a „Packet Filter” (pf), amely rendkívül sokrétű csomagmanipulációra nyújt lehetőséget.

34 HTTP Antivirus Proxy ClamAV víruskeresővel.



2. ábra: PfSense webfelület³⁵

2. Előírt intézkedés:

3.3.11.5.1.1. és 3.3.11.5.1.2. Az érintett szervezet felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat; azonosítja az elektronikus információs rendszer jogosulatlan használatát.

Magyarázat: A hálózatot behatolásdetektáló, esetleg behatolásmegelőző eszközzel kell védeni.³⁶

³⁵ Forrás: saját szerkesztés.

³⁶ Intrusion Detection System (IDS), Intrusion Prevention System (IPS).

Lehetséges megoldás: A SNORT³⁷ vagy a Suricata³⁸ alkalmazása. Mindkét szoftver elérhető pfSense csomagként is, így nincs szükség külön eszköz telepítésére és karbantartására. A SNORT egy hálózatalapú behatolásdetektáló és -megelőző eszköz, amelynek fejlesztése 1998-ban kezdődött meg. Jelenleg a Cisco Systems, Inc. egyik leányvállalata fejleszti. A Suricata szintén hálózatalapú IDS/IPS. Első stabil verziója 2010-ben jelent meg. Fejlesztését az Open Information Security Foundation végzi.

3. Előírt intézkedés:

3.3.11.8.1. Az érintett szervezet sértetlenség-ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.

Magyarázat: Állományintegritás-ellenőrző eszközt kell használni a számítógépeken.

Lehetséges megoldás: Az OSSEC³⁹ hosztalapú behatolás-ellenőrző eszköz alkalmazása. Futtatható Linux, MacOS, Solaris, HP-UX, AIX, Windows és más rendszereken. Logelemzésre, állományintegritás-ellenőrzésre, policyfigyelésre, rootkitdetektálásra, valós idejű riasztásra és ellenlépések megtételére képes. Teljesíti a bankkártya-elfogadók adatvédelmi szabványát.⁴⁰ 2004 óta elérhető eszköz, amelynek fejlesztését jelenleg a Trend Micro Inc. felügyeli.

4. Előírt intézkedés:

3.3.11.9.1.1. Az érintett szervezet kéretlen üzenetek – úgynevezett levélszemét – elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében.

Magyarázat: SPAM-szűrő eszköz használata szükséges a levelezőkiszolgálón vagy tűzfalon.

Lehetséges megoldás: A SpamAssassin⁴¹ alkalmazása a levelezőrendszerhez kapcsolva vagy SMTP-proxyként alkalmazva. Egyszerűen konfigurálható, API-k alkalmazásával bővíthető, szinte minden elterjedt SMTP-rendszerhez könnyen illeszthető megoldás. Sokszor használják ClamAV víruskeresővel kiegészítve, de elérhető pfSense csomag formátumban is. A nem kívánt e-mailek azonosítására több technikát alkalmaz, amelyek eredményeit pontozási rendszerrel összesíti, könnyen tanítható. Első nyilvános verziója 2001-ben jelent meg. Jelenleg az Apache Software Foundation felügyeli a fejlesztését.

37 SNORT. <https://snort.org/> (2015. 10. 30.)

38 Suricata. <http://suricata-ids.org/> (2015. 10. 30.)

39 Open Source SECURITY (OSSEC). www.ossec.net/ (2015. 10. 30.)

40 Payment Card Industry Data Security Standard (PCI DSS).

41 ApacheSpamAssassin. <http://spamassassin.apache.org/> (2015. 10. 30.)

5. Előírt intézkedés:

3.3.13.8.1. és 3.3.13.8.2. Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét. Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

Magyarázat: Virtuális magánhálózat, VPN segítségével kialakított, titkosított kapcsolaton keresztül kell az adatokat továbbítani, fizikai védelem hiányában.

Lehetséges megoldás: Az OpenVPN⁴² alkalmazása SSL VPN-ek kialakításához. Az OpenSSL-re épülve, többféle korszerű titkosítási protokollt is támogat, mint például: AES-CBC, CAMELLIA-CBC, RSA, ECDH. Alkalmas telephelyek közti,⁴³ de egyszerű távoli hozzáférésre szolgáló⁴⁴ VPN kialakítására is. Támogatja a terheléelosztást, de a redundáns működést is. Futtatható Linux, Windows XP/Vista/7 és újabb, OpenBSD, FreeBSD, NetBSD, Mac OS X és Solaris rendszereken.

Természetesen a lehetséges szoftverek bemutatása nem lehet teljes körű, így csak néhány, az intézkedési katalógus által előírt feladathoz mutattam be szabadon hozzáférhető forráskódú eszközt, ugyanakkor szinte mindegyik teljesítéséhez található (akár több) megbízható és széles körben elismert termék.

ÖSSZEGZÉS

A szabad forráskódú biztonsági szoftverek hatékony eszközök a kritikus információs infrastruktúrák védelmére. Fontos, hogy alkalmazásuk során betartsák ugyanazokat a szabályokat, mint más szoftverek használatakor. Elengedhetetlen továbbá, hogy csak megbízható forrásból szabad letölteni őket, azt követően pedig az állomány integritásának ellenőrzése is elvégzendő feladat. Amennyiben lehetséges, a forráskódból a futtatható bináris előállítását is ajánlott saját hatáskörben elvégezni. Szinte minden kibervédelmi feladatra készült megbízható, szabad szoftver, így ezek alkalmazhatóságát minden esetben célszerű megvizsgálni, hiszen segítségükkel sokszor költséghatékonyabb, valamint az infrastruktúrához jobban igazodó védelem alakítható ki, mint zárt forráskódú alternatíváikkal.

42 OpenVPN. <https://openvpn.net/> (2015. 10. 30.)

43 Site-to-site VPN.

44 Remote access VPN.

IRODALOMJEGYZÉK

- [1] COWAN, Crispin: Software security for open-source systems. In: *IEEE Security & Privacy*, 2003, Vol. 1. No. 1. 38–45.
- [2] GREINER, Sašo et al.: *Security issues in information systems based on open-source technologies*. Proc. The IEEE Region 8 EUROCON 2003, Computer as a Tool, Ljubljana, 2003, Vol. 2. 12–15.
- [3] LAWTON, George: *Open source security: opportunity or oxymoron?* IEEE Computer, Los Alamitos, 2002, Vol. 35. No. 3. 18–21.
- [4] SREENIVASA, Rao Vadalasetty: *Security concerns in using open source software for enterprise requirements*. Fredericksburg, SANS Institute, 2003.
- [5] RÉPÁS Sándor – RAJNAI Zoltán: SCADA Rendszerek, mint Kritikus Információs Infrastruktúrák Biztonsága. In: *Hírvillám/Signal Badge*, Budapest, 2015, Vol. 6. No. 1. 139–151.
- [6] SCHRYEN, Guido – RICH, Eliot: *Increasing software security through open source or closed source development? Empirics suggest that we have asked the wrong question*. Proc. 43rd Hawaii International Conference on System Sciences (HICSS), Honolulu, 2010, 1–10.
- [7] VEN, Kris et al: Should You Adopt Open Source Software? In: *IEEE Software*, Los Alamitos, 2008, Vol. 25. No. 3. 54–59.
- [8] GNU: *Mi a Szabad Szoftver?* www.gnu.org/philosophy/free-sw.html (2015. 10. 30.)



PC vezérelt Real-Time
Spektrum Analizátor

- Univerzális alkalmazási terület
R&D, gyártás, monitoring
- Széleskörű fejlesztői környezet
MATLAB®, LabVIEW®, C/C++
- Kiváló ár-érték arány
- Flexibilis telepítési lehetőségek
- RBW: 100MHz
- Frekvencia tartomány:
100kHz – 8/18/28GHz



Próbálja ki demo készülékünket!

IDA2: Gyanús és zavaró jelek detektálására, azonosítására és lokalizálására!

- Extra gyors söprési sebesség: 12 GHz/s
- Kényelmes interferenciakeresés
- Könnyű (<3kg) és stapabíró kivitel
- IQ Analizátor
- Frekvencia tartomány: 9kHz- 6GHz

 **narda**
Test Solutions
Communications Company

ELSINCO
Electronic Measurement Technology

www.elsinco.hu

**HTEST**

Your partner for electronic test & measurement solutions.

**KEYSIGHT
TECHNOLOGIES****COMTEST****HAEFELY
HIPOTRONICS****ADLINK
TECHNOLOGY INC.**

H TEST group is a leading supplier of test & measurement instruments and systems for industry, education and telecommunications. We are currently operating in the Czech republic, Slovakia, Austria and Hungary. Our company was established in summer 1999 in Prague, Czech republic and starting 1st September 1999 we were appointed as an authorized distributor of Agilent Technologies test and measurement products for Czech republic. In 2001 we have opened subsidiary sales office at Slovakia. In May 2010, our subsidiary company x.test GmbH started its business in Wien, Austria.

And finally, in July 2013 our last subsidiary company H TEST Hungary Kft. was found in Győr, Hungary. We are offering instruments and systems for measurement of electrical and non-electrical quantities. We are supplying wide variety of test instruments, test solutions and accessories from renowned manufactures such as: Amplifier Research, Haefely Hipotronics EMC, EMSCAN, Pasternack enterprises, Keysight Technologies, Adlink Technologies, etc.



H TEST Hungary Kft.
 Gesztenyefa u. 4.; 1.em/No.3;
 H-9027 Győr, Hungary
 Phone: +36 203 137 079
 +36 96 999 262
 Fax: +36 96 999 263
 E-mail: info@htest.hu
www.htest.hu



Konferencia-előadások

SZARVÁK Anikó

A MISSING THING OF SAFER CYBERWORLD



About

- Anikó Szarvák, niko@paraweb.hu
- Information security expert
- 10+ years in information security, IT security
- BSC & MSC @ ZMNE
 - Information security
 - Infocommunication
- CHFI @ EC-Council
- CISSP @ ISC²
- Co-founder @

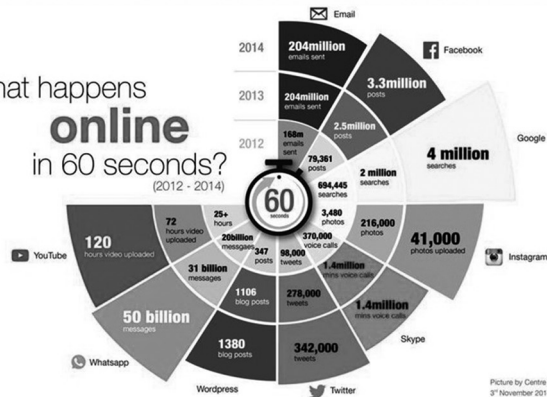


2015. 11. 11.

2

Exponentially....

What happens
online
in 60 seconds?
(2012 - 2014)

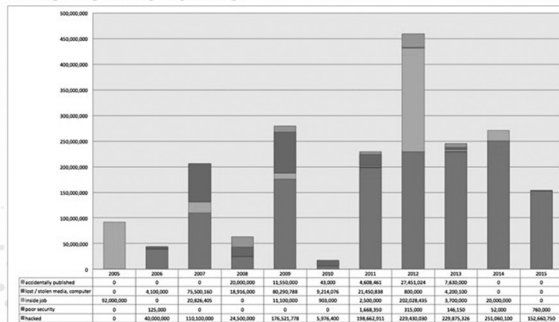


Pictures by Centre for Learning and Teaching
3rd November 2014

2015. 11. 11.

5

... so the attacks



World's Biggest Data Breaches, source:

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

2015. 11. 11.

6

What is common?

TOP	2007	2010	2013
1	<u>Cross Site Scripting (XSS)</u>	<u>Injection</u>	<u>Injection</u>
2	<u>Injection</u>	<u>Cross Site Scripting (XSS)</u>	<u>Broken Authentication and Session Management</u>
3	Malicious File Execution	<u>Broken Authentication and Session Management</u>	<u>Cross Site Scripting (XSS)</u>
4	<u>Insecure Direct Object Reference</u>	<u>Insecure Direct Object References</u>	<u>Insecure Direct Object References</u>
5	<u>Cross Site Request Forgery (CSRF)</u>	<u>Cross Site Request Forgery (CSRF)</u>	Security misconfiguration
6	Information Leakage and Improper Error Handling	Security misconfiguration	Sensitive Data Exposure
7	<u>Broken Authentication and Session Management</u>	Insecure Cryptographic Storage	Missing Function Level Access Control
8	Insecure Cryptographic Storage	Failure to Restrict URL Access	<u>Cross Site Request Forgery (CSRF)</u>
9	Insecure Communication	Insufficient Transport Layer Protection	Using Components with Known Vulnerabilities
10	Failure to Restrict URL Access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards

OWASP top 10 by years 2007, 2010 and 2013,
Source: <http://www.owasp.org>

2015. 11. 11.

7

It is your company.

An organization with

- Computers
 - With databases and
 - Networks and
 - Electronically stored information.
- People
 - Who are Managers,
 - Administrators and
 - Users.

Call it information system.

2015. 11. 11.

8

ITS your choice.

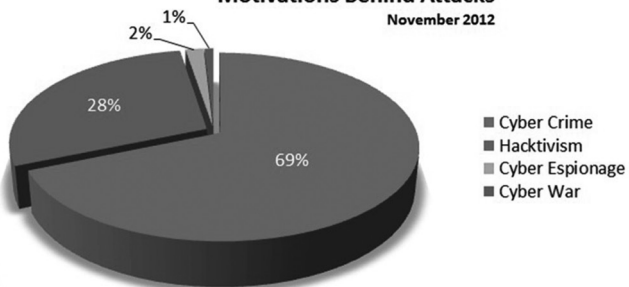


2015. 11. 11.

9

Attacker's choice @2012

Motivations Behind Attacks
November 2012



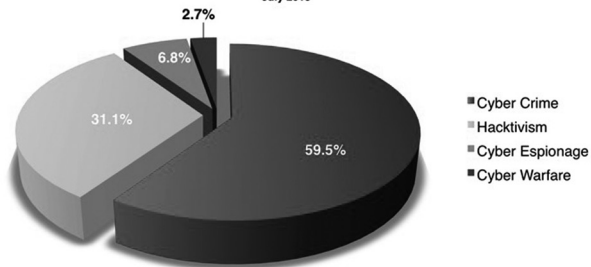
Hackmageddon statistics, Motivation behind Attacks,
November 2012, source:
<http://www.hackmageddon.com/2012/12/09/november-2012-cyber-attacks-statistics/>

2015. 11. 11.

10

Attacker's choice @2015

Motivations Behind Attacks
July 2015

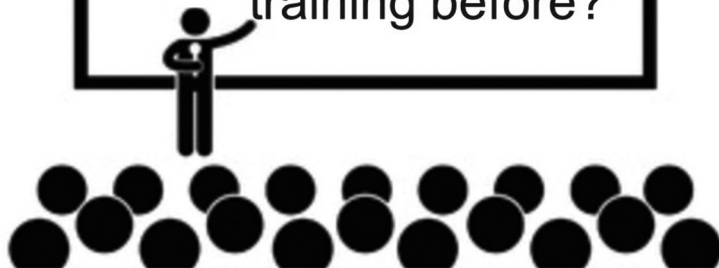


Hackmageddon statistics, Motivation behind Attacks, July 2015, source:
<http://www.hackmageddon.com/2015/08/10/july-2015-cyber-attacks-statistics/>

2015. 11. 11.

11

Have you held
awareness
training before?



2015. 11. 11.

12



BÓDOGH Attila

MESTERSÉGES INTELLIGENCIA ÉS A BIGDATA-ELEMZÉSEK ALKALMAZÁSI LEHETŐSÉGEI A RENDVÉDELEMBEN

SCI-Network

VoiceAnalytics

Xdroid
Intelligent Innovative Informatics

Mesterséges intelligencia és big data
elemzések alkalmazási lehetőségei a
rendvédelemben



Bódogh Attila ügyvezető
Xdroid Kft.
+36 30 210 35 60
attila.bodogh@xdroid.com
www.xdroid.com

SCI-Network

Xdroid
Intelligent Innovative Informatics

SCI-Network zRt. kapcsolata a Xdroid Kft-vel

- **SCI-Network: általános rendszerintegrátor**
- Széles ügyfélbázis, kiterjedt piaci kapcsolatok
- Professzionális hang/adat megoldások szállítója
- Jelentős szakember gárda, amely képes különféle rendszerekben új fejlesztéseket integrálni
- **Xdroid Kft: innovatív megoldások fejlesztése**
- Komoly szellemi tőke, kutatás/fejlesztési kapacitás
- Kapcsolat egyetemi tudáscentrumokkal
- Kész termékek, prototípusok
- **Együttes fejlesztések, felhasználói illesztések, új K+F+I projektek**

www.xdroid.com

Rólunk



Magyar szoftverfejlesztő cég



Hang, szöveg és adatbányászati megoldásokkal foglalkozunk

VoiceAnalytics

Hang és érzelelemzés

MORPHORANK

leverage your business

Big data előrejelzések

www.xdroid.com



A VoiceAnalytics egy teljesítmény és minőségmenedzsment eszköz ügyélszolgálatok számára.

Hogyan működik?

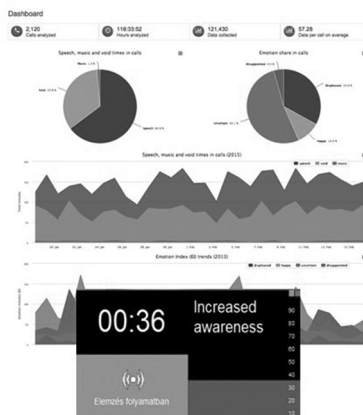
Elemzi az ügyfelekkel folytatott interakciókat.

- Technikai (hívás hossz, időpont, operátor, stb.)
- Tartalmi (szavak és szókapcsolatok, témakörök)
- Érzelmi (dühös, csalódott, bizonytalan, elégedett)
- Produktivítás (beszéd/csend/zene/egymásrbeszélés)
- Beszédminőség(artikuláció minősége, intonáció, beszédtempó, hangerő, dominancia, stb.)
- Ügyfél és forgalmi adatok (szerződés, termék, pénzügyi adatok)
- Személyes és elektronikus csatornák is



Felhasználási területek

- Protokoll szűrés (megfelelő vagy nem megfelelő szavak, kifejezések vizsgálata)
- Véletlenszerű visszahallgatások kiváltása célzott módszerekkel
- Minőségi benchmarkok felállítása és kontrollja (pl. érzelmi alapú ügyfélelégedettség)
- Automatizált különbség elemzések
- Operátori értékelések támogatása minőségi mutatókkal
- Ügyfélmegtartás támogatása
- Értékesítés (bizonytalan ügyfelek azonosítása)
- Valós idejű előrejelzések (pl. sales beszélgetés első 30 másodperce alapján a kimenetet)



Case study: biztosítási csalások felderítése hangelemzés segítségével

- Hazai biztosítótársaság, számos kárbejelentés
- A bejelentések egy része nem valós

Feladat: hangelemzéssel támogatni a biztosítási csalások felderítését, csökkenteni az indokolatlan kárkifizetések számát

Módszer: Hatékony jellemzőkinyerési módszerek és mesterséges intelligencia alapú gépi tanuló algoritmusok használatával rangsoroljuk a beérkezett kárbejelentéseket.

Input: Kárbejelentési beszélgetések + bejelölések

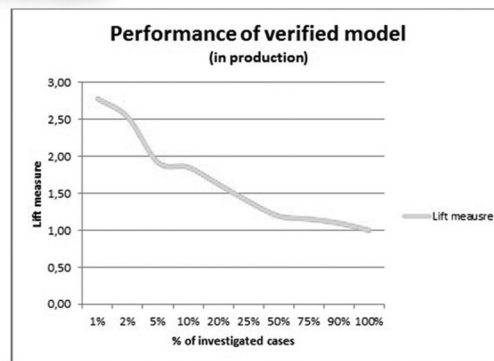
Case study: biztosítási csalások felderítése hangelemzés segítségével



Mérési módszer

A lista első 10%-ban mennyivel több felderített csalási
eseményt tudott a rendszer elhelyezni a lista átlagához
képest?

Eredmények



Az eredmények alapján megközelítőleg 2-3 szoros
hatékonyságnövekedés mérhető az első 5%-10%-ban.

Előrejelző modellek alkalmazhatósága a rendvédelemben

- Nyomozati munka támogatása az összegyűjtött hangfelvételek elemzésével és kereshetővé tételével
- Szövegbányászati módszerekkel társadalmilag veszélyes bejegyzések figyelése blogokon és közösségi oldalakon
- Közterületi kamerák segítségével célszemély menekülési útjának követése alak-és arcfelismerő algoritmusokkal

Köszönöm a figyelmet!

Kérdések?



DOMBORA Sándor - HORVÁTH Gergely Krisztián

AZ INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA



Kommunikáció 2015
Nemzetközi tudományos-szakmai konferencia

**INFORMÁCIÓBIZTONSÁG
INTEGRÁLT
MEGVALÓSÍTÁSA**
MSZ ISO/IEC 27001:2014, ÉS IBTV.
(NIST SP 800-53 REV 4) ALAPON

Dombora Sándor, Horváth Gergely Krisztián
Biztonságtudományi Doktori Iskola



Információbiztonság Integrált megvalósítása

- Miért szükséges az integrált megvalósítás?
 - Jogszabályi megfelelés
 - Jogszabály értelmezés
 - ISO 27001 tanúsítás
 - Azonos célok → nagyobb biztonság



Jogszabály módosítás 2015

2013. évi L. tv. (2013)

77/2013. (XII.19.) NFM

26/2013. (X.21.) KIM

73/2013. (XII. 4.) NFM

301/2013. (VII. 29.) Korm.

2013. évi L. tv. (2015)

41/2015. (VII.15.) BM

26/2013. (X.21.) KIM

42/2015. (VII.15.) BM

187/2015. (VII.13.) Korm.



3

INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

Információbiztonság hiányosságok kezelési módjai

- intézkedések információbiztonsági programként való megvalósításával
- biztonság tudatosság növelésével
- szabályzatok létrehozásával
- eljárásrendek kialakításával
- ügyviteli és informatikai folyamatok végrehajtását támogató megoldások bevezetésével
- rendszerfelügyeleti megoldások bevezetésével
- konfigurációkezelési megoldások bevezetésével
- formalizált változáskezelés bevezetésével
- stb.



4

INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

Ibtv. vhr., ISO/IEC 27001:2013 és NIST SP 800-53 összerendelés (részlet)

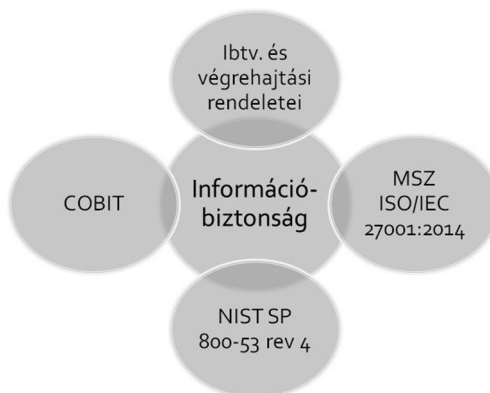
Ibtv. vhr. követelmény-azonosító	NIST kontroll azonosító	ISO/IEC 27001:2013 kontroll azonosító
3.2.1.2	PE-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
3.2.1.3	PE-2	A.11.1.2*
3.2.1.4, 3.2.1.4.2	PE-3	A.11.1.1, A.11.1.2, A.11.1.3
3.2.1.5.	PE-4	A.11.1.2, A.11.2.3
3.2.1.6.	PE-5	A.11.1.2, A.11.1.3



5

INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

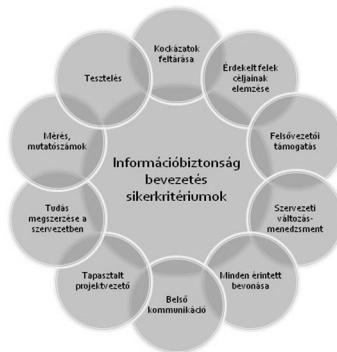
Információbiztonságot támogató jogszabályok, szabványok, ajánlások



6

INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

Információbiztonság bevezetési projektetek sikerének feltételei



7

INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

Köszönöm a figyelmet!

Dombora Sándor

dombora.sandor@kvk.uni-obuda.hu

Horváth Gergely Krisztián

horvath.gergely.krisztian@bqf.hu



8

INFORMÁCIÓBIZTONSÁG INTEGRÁLT MEGVALÓSÍTÁSA

KOLOZS Csaba

SZÁLFELÜGYELET „PARANCSSZÓRA” – A BIZTONSÁG MINDENK FELETT



equicom
ICT MÉRÉSTECHNIKA

Szálfelügyelet
"parancsszóra,"
A biztonság mindenek felett

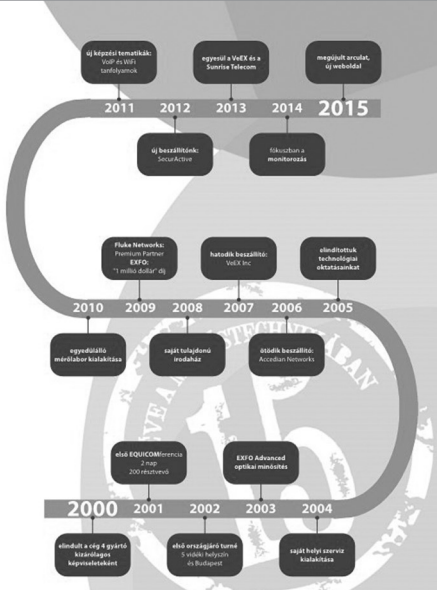
Kolozs Csaba
| ügyvezető, szolgáltatói hálózatok |
| +36 20 9728 895 |
| kolozs.csaba@equicom.hu |





az EQUICOM-ról

- Kizárólag ICT mérés technikai megoldásokra szakosodva
- Több mint 15 éves szakmai múlt
- Világviszonylatban vezető beszállítók kizárólagos magyarországi képviselői
- Piaci jelenlét: szolgáltatók és vállalati szegmens
- Közvetlen kapcsolat a felhasználó és a gyártó között
- Szakértelem, tanácsadás, támogatás, szakmai oktatások (9 tematikus EOK tanfolyam)



2015
új képzési tematikák: VoIP és SD-WAN tanfolyamok
egyesül a VeEX és a Sunrise Telecom
megújított arculat, új weboldal

2014
új beszállítók: SecuActive
fokozott a membership

2013
Fluke Networks: Precision Partner
EXFO: "1 millió dollar" díj

2012
új beszállítók: hálózati beszállító: VeEX Inc.
előadottak technológiai előadásokat

2011
szál felügyeleti megoldások kutatása

2010
szál felügyeleti megoldások kutatása

2009
szál felügyeleti megoldások kutatása

2008
szál felügyeleti megoldások kutatása

2007
szál felügyeleti megoldások kutatása

2006
szál felügyeleti megoldások kutatása

2005
szál felügyeleti megoldások kutatása

2004
szál felügyeleti megoldások kutatása

2003
szál felügyeleti megoldások kutatása

2002
szál felügyeleti megoldások kutatása

2001
szál felügyeleti megoldások kutatása

2000
szál felügyeleti megoldások kutatása

EQUICOM Mérés Technikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

„Ars Poetica”

*"Ami számítható, azt
számítsd ki, ami mérhető, azt
mérd meg, és ami nem
mérhető, azt tedd
mérhetővé!"*



EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

Miért fontos a monitorozás?

- A fizikai szint, mint egy alap közmű... ha nem adott a hibamentes fizikai közeg, akkor semmit sem érnek az alkalmazások
- Nincs fizikai védelem, biztonságos zónán kívül esik
- „az optikai kábelek 75%-a szabadon hozzáférhető - John Pescatore /Gartner/”
- Nemzetbiztonsági kockázatok... az adat nem biztonságban optikai szálon sem
- Internet támadások 10-15%-os növekedés
- Menedzselhetőség, prevenció gyors dokumentálás, riport a vezetőség felé
- Szenzor központi adatmentések



EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

Kritikus linkek

Minden modern hálózati topológia
rendelkezik kerülő útvonallal.



igaz?

igen, de...

Szűk keresztmetszetek, „üvegnyak”
Kiemelten fontos szakaszok

Kiemelt ügyfelek (VIP)

Minden ügyfél egyforma



igaz?

igen, de...

Kritikus érzékenyséű területek: bank, közigazgatás,
közszolgáltatás, kormányzat, sport események, stb.
SLA alapú számlázás

Hibaelhárítás

A hálózati berendezések
saját felügyelete elegendő



igaz?

sajnos nem...

A berendezések csak bit hiba arány romlást észlel
Layer 2/3 szinten, viszont ha fizikai hálózati probléma
lép fel, akkor annak helye ismeretlen marad

Kiemelt ügyfelek (VIP)

Rosszindulatú rongálások és
halászok által okozott károk,
c-OTDR-t igényelnek



igaz?

igen, sajnos igaz, de...

Szerencsére a Magyar Tengeren ez kevésbé kritikus,
max. ha hosszában 77 km-en tervezne valaki optikai
kábelt építeni. 😊

Biztonság

Száloptikai rendszerek
immunisak a lehallgatásra,
azokat nem lehet lecsapolni

igaz?

sajnos NEM !!! ... de

Elérhető megoldások léteznek erre...



Biztonság??? – a helyzet nem javul

- 10-15%-os növekedés a támadó forgalomban
- Hálózati támadások 35%-a EU-n belüli
- Még mindig sok esetben észrevétlenek maradnak a támadások

Home » Internet

News

**Internet attacks from China and US
increased in first quarter of 2012, report
says**

Most attacks are aimed at Port 445, which is favored by the Conficker worm, according to Akamai

Topic: Security

Follow: rss |

**Most cyber attacks fly under our
radar: Aussie spy chief**

Summary: Five thousand cyber attacks have been reported to Australia's CERT this year, but the director-general of ASIO says that it's just the tip of the iceberg.



Biztonság??? – elérhető megoldások

- Optikai ún. Clip-on eszköz (~\$1.000)
 - Alacsony beiktatásos csillapítás (<3dB)
- Érzékeny optikai detektor
 - Max. 1% fényvesztés -> 100% adatlopás
- Adatot nem csak kivenni lehet: DoS Attack, manipuláció, stb.
- Adatátviteli eszközök számára láthatatlan
- Adatok titkosítása fél megoldás (és sokkal költségesebb)
- Ettől még nem szerzünk tudomást a támadásról



EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

MEGOLDÁS: Optikai szálmonitorozás + kriptográfia

Biztonság



Kritikus linkek



Kiemelt ügyfelek (VIP)

Tenger alatti kábelek



Hibaelhárítás

EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

Mindig első a Capex az Opex ellenében?

- Hány kábel rongálás és vágás történik egy év alatt?
- Mennyi idő alatt sikerül beazonosítani a probléma okát és helyét?
- Az idegen támadásra milyen prevenció létezik?
- Mekkora százalékban fizikai és/vagy berendezés szintű a hiba forrása?
- Mekkora az átlagos ideje egy javításnak, ami után visszatérhetünk az újbóli normál működésre? Utazási idő, autó és személyi költségek számítása...
- Mindig elvégezzük fél évente vagy évente a preventív méréseket?
- Megfelelő számú mérő technikus dolgozik a cégnél, aki fel van szerelve mérőműszerekkel?

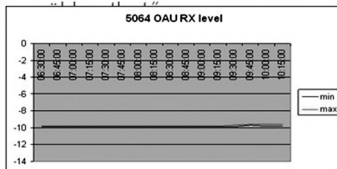


EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

Monitorozással vagy nélküle?

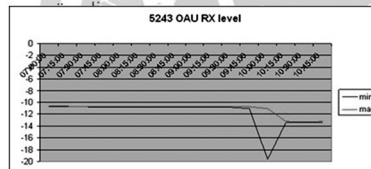
Monitorozó rendszerrel

- Riasztás érkezése azonnal és hibahely meghatározás 2 percen belül!
- Hibaelhárítók fél órán belül úton vannak
- Átlagos kiesési idő több órával



Monitorozó rendszer nélkül

- Döntést egy szűk körű, Berendezés vagy hálózati hiba?
- Hibahely meghatározása több óra is lehet
- A hibaelhárítási időt több órával



EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

Távoli és centralizált OTDR mérések előnyei

*MTTU = Átlagos idő, hogy megértsük
*TTU = Ideje, hogy megértsük

3rd party
beszerzések
átemelése
(OSS, NMS)

SLA
menedzsment

Optikai
határok

Preventív
inkább, mint
utólagos

Archív
adatokhoz
történelmi
hozzáférés

"TTU"
késleltetések
elhagyása

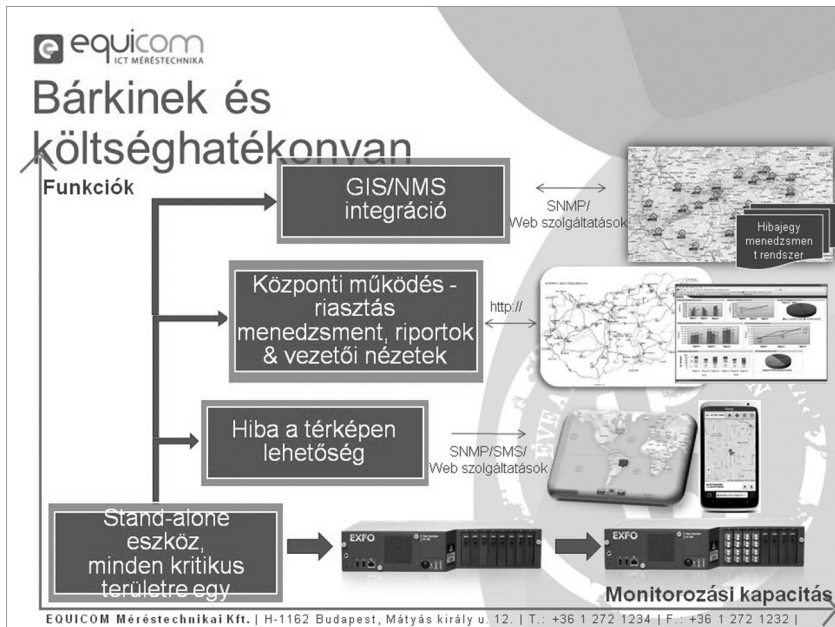
MTTU
csökkentése

EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

A sikeres recept egy formája

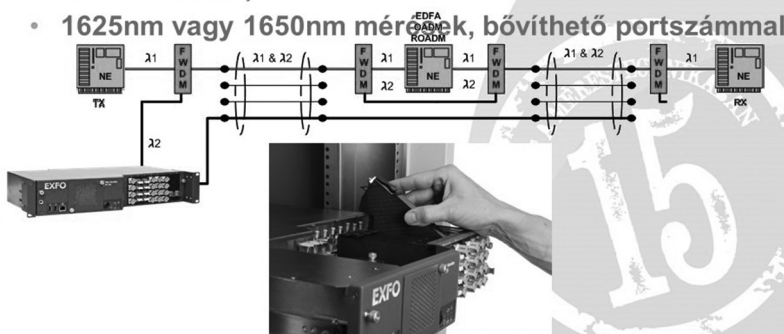


EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |



Aktív- és sötétszálás monitorozás

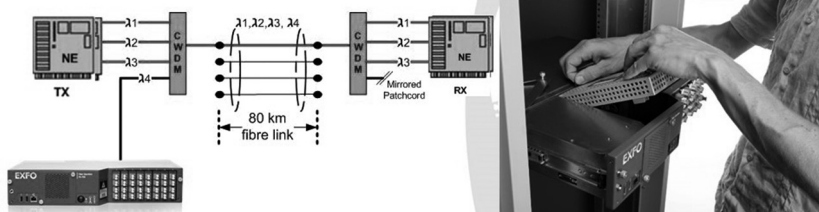
- Mérések egyedi szekvenciában
- Igény szerinti prioritást élvező port (kritikus összeköttetés)
- 1625nm vagy 1650nm mérők, bővíthető portszámmal



EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

„In- és Out of Band” CWDM monitorozás

- **In-Band:**
 - CWDM dedikált hullámhossz szükséges
 - Extra izoláció szükséges az OTDR csatorna körül
- **Out-of-Band:**
 - Érzékenyebb a makro hajlításokra
 - Bonyolultabb, költségesebb, extra csillapítás a WDM szűrő miatt



EQUICOM Méréstechnikai Kft. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |

Szakmai segédanyagok

Tesztelje saját hálózatát! ➔ info@equicom.hu

- Kérje személyes

u

Szakmai cikkeink ➔ info@equicom.hu

u

Hírleveleink:

- <http://www.equicom.hu/hirlevelek>

Monitorozásokról szóló szakmai

cikkeink: <http://www.equicom.hu/?q=webpage/szakmai>

EXFO szálonmonitorozó megoldásaink:

- http://www.equicom.hu/exfo_optikai_szalfelugyel
- Fiber Guardian: <http://www.equicom.hu/fg720>
- Node iOLM: <http://www.equicom.hu/fg750>

EQUPCON MÉRÉSTECHNIKAI KFT. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |



Összefoglalás, rövid konklúzió

**Capex
vs.
Opex**

Gondolkodjunk „költség” hatékonyan.

A monitorozó beruházás hosszabb távon költséget csökkent.

**OTDR
mérés**

A berendezés felügyelet nem mondja meg a hiba helyét.

A piac legjobb OTDR-e monitorozási alkalmazásra is.

**Kulcs
App**

A BIZTONSÁG mindenképp felett.

Védjük meg adatainkat a betolakodók elől.

**A
Termék**

Nyílt architektúrájú interfész.

Skálázható platform, egyszerű menedzsment integráció.

EQUPCON MÉRÉSTECHNIKAI KFT. | H-1162 Budapest, Mátyás király u. 12. | T.: +36 1 272 1234 | F.: +36 1 272 1232 |



equicom
ICT MÉRÉSTECHNIKA

Köszönöm a
figyelmüket!

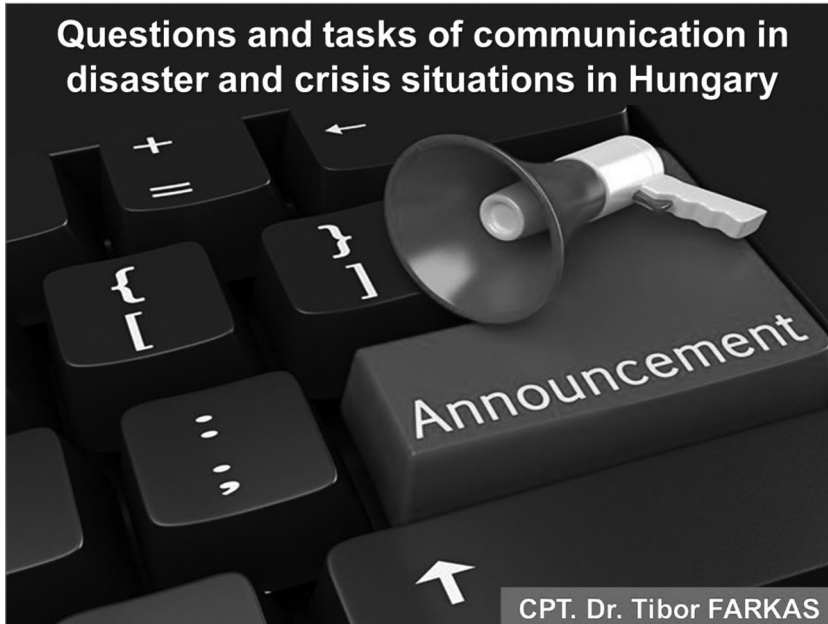
Kolozs Csaba
| ügyvezető, szolgáltatói hálózatok |
| +36 20 9728 895 |
| kolozs.csaba@equicom.hu |

EQUICOM Méréstechnikai Kft.
| H-1162 Budapest, Mátyás király u. 12. |
| T.: +36 1 272 1234 |
| F.: +36 1 272 1232 |
| www.equicom.hu |



FARKAS Tibor

QUESTIONS AND TASKS OF COMMUNICATION IN DISASTER AND CRISIS SITUATIONS IN HUNGARY



„Communication 2015” International Scientific Conference

- **CPT. Dr. Tibor FARKAS (PhD),**
National University of Public
Service /Hungary/
 - Faculty of Military Sciences and
Officers Training
 - CIS (Signal) Department
 - Associate professor
 - Deputy chief of Department



„This presentation was supported by the
János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

- **Definitions**
- **Support of CIS (Tasks)**
- **Information needs in crisis situations**



Bf „This presentation was supported by the
János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

- **Signals**

develops, tests, provides, and manages communications and information systems (CIS) support for the command and control (C2) of leadership (commander)

(military)

Signal support includes **Network Operations** (information assurance, information management, and network management) and **management of the electromagnetic spectrum**



Bf „This presentation was supported by the
János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

- **Communication experts**

Signal forces plan, install, operate, and maintain voice and data communications networks that employ single and multi-channel satellite, tropospheric scatter, and other related systems

Integrate tactical, strategic and sustaining base communications, information processing and management systems



„This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

- **Support of cmd's (civilian leaders) C2 process**

- To give informations
 - enough;
 - reliable;
 - in time
- Get (collect) infos;
- Protect infos;
- Exchange infos



„This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

„Communication 2015” International Scientific Conference



By „This presentation was supported by the
János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”



„Communication 2015” International Scientific Conference

- Plane crash
- Sk. An-24
- 19. Jan. 2006., Hejce
- KFOR- Slovakia
- 1/43 survivor
- Between the mountains
- No roads, ...
- No communication
- Different organizations
- Foreign forces



„This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

„Communication 2015” International Scientific Conference

- Storm
- National holiday
- 20. Aug. 2006., Bp.
- fireworks
- 4 dead/300 wounded
- 1-1,5 million people
- No public informations
- No communication
- No information between the executives



„This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

„Communication 2015” International Scientific Conference

- **Flooding**
- **..., 2010, 2013**
- **woundeds**
- **damages**
- **Everywhere in the country**
- **No public informations**
- **No communication**
- **No information between the executives**



"This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences."

„Communication 2015” International Scientific Conference

- **Red Sludge industrial disaster**
- **04. October. 2010**
- **Woundeds/ 10 deads**
- **damages**
- **40 km²**
- **Information needs**
- **No information between the executives**
- **Comm. links down**



"This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences."

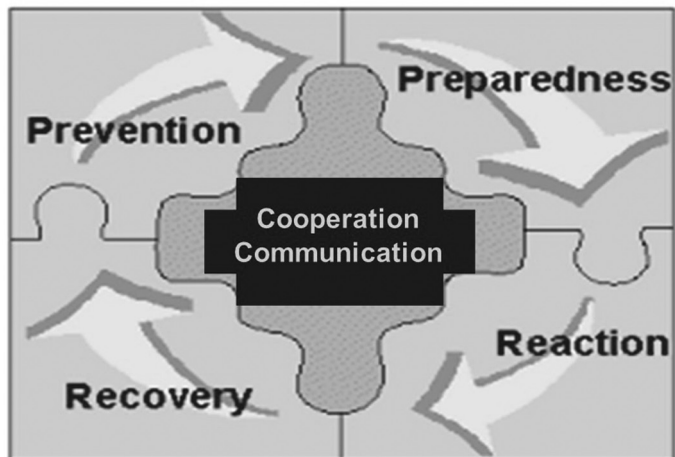
„Communication 2015” International Scientific Conference

- Hungarian migrant crisis
- Transit country
- Thousands of people
- Hundreds of km's
- Information needs
- Many cooperatives
- Huge comm. needs



„This presentation was supported by the
János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

„Communication 2015” International Scientific Conference



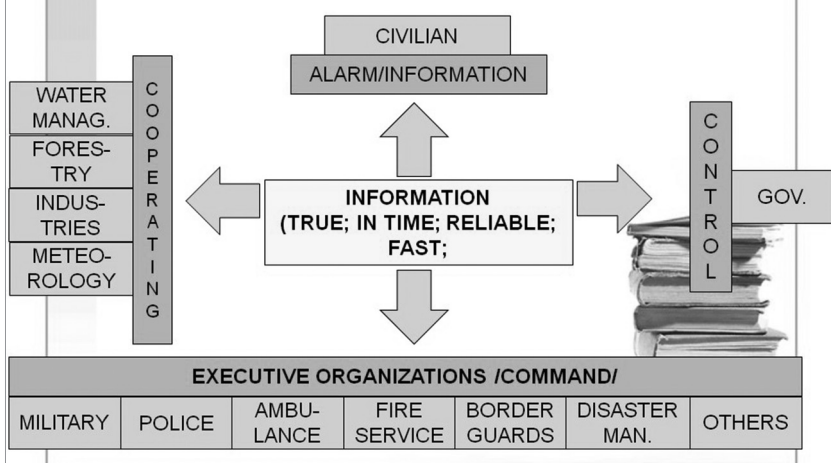
„This presentation was supported by the
János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”

• General problems:

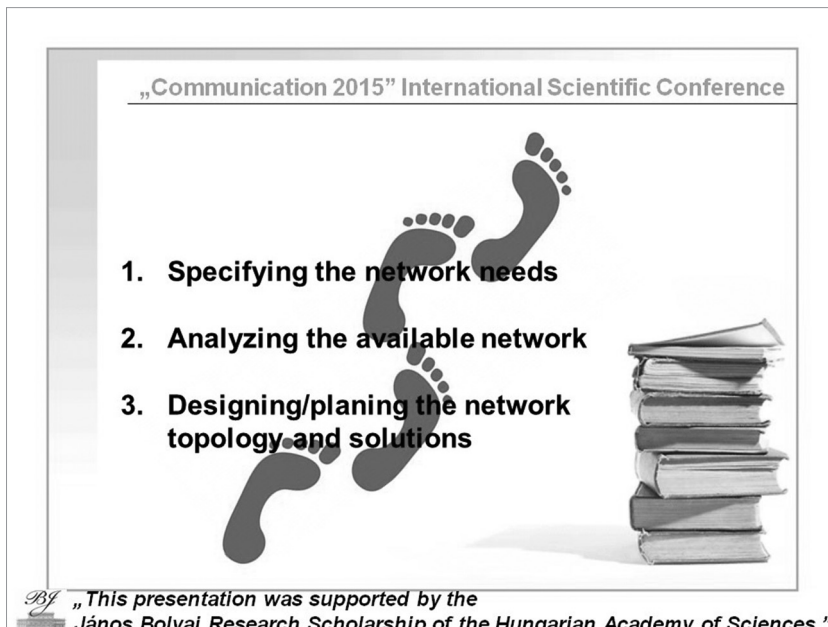
- Places
 - Difficult to reach;
 - Large extent;
- Different organizations;
- Information needs;
- No communication lines;
- No informing system;
- No information database
 - Temp. Accommodation;
 - Hospitals (free places)
 - ...



„This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”



„This presentation was supported by the János Bolvai Research Scholarship of the Hungarian Academy of Sciences.”





Questions and tasks of communication in disaster and crisis situations in Hungary

CPT. Dr. Tibor FARKAS (PhD)

„Communication 2015” International Scientific Conference
11.11.2015. Budapest



„This presentation was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.”

TRENCSÁNSZKY Imre

JUNIPER SRX-EK A KATASZTRÓFAVÉDELEMBEN, AVAGY A TÚZFAL A VÍZ ELLEN IS VÉD



**Juniper SRX-ek a
katasztrófavédelemben,
avagy a tűzfal a víz ellen is véd**

Trencsánszky Imre
Vezetéknélküli üzletág, Vezető hálózati mérnök
2015.11.11. Budapest

SCI-NETWORK
Távközlési és Hálózatintegrációs zRt. • 1142 Budapest, Erzsébet királyné útja 125. • telefon: 06 1 467-7030

A FETIVIZIG zártcélú adatkommunikációs hálózatának jellemzői

- Közcélú szolgáltatóktól független, katasztrófa helyzetben is működőképes, autonóm hálózat
- Áramkörkapcsolt hang (E1-es telefonközpontok), IP alapú adat és ipari automatizálási forgalom (zsilip, szivattyúvezérlés, vízmérő leolvasás stb) biztosítása Nyiregyháza és hazai telephelyek valamint romániai és ukrainai társszervek között
- Az egyes állomások távfelügyelték és szünetmentes áramforrásokkal felszereltek
- Saját tulajdonú adótorony és mikrohullámú gerinc hálózat
- Az üzemeltetés teljes mértékben a FETIVIZIG kezében van, nincs szükség külső szolgáltatóra/ szolgáltatásra

SCI-NETWORK

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

A FETIVIZIG régi hálózatának jellemzői

SzSzB. megyében, 10 telephelyen, 2001-től megvalósított L2-es hálózat

- A meglévő E1-es mikró kapcsolatok által kiszolgált $n \times 2$ Mbps-es hálózat elavult és rugalmatlan
- Az adatkapcsolat a 2Mbps-es, áramkörkapcsolt E1-es vonalakon $n \times 64$ kbps-es dinamikus csatornába volt multiplexálva (Nortel Passport berendezéseken keresztül)
- Feladata a telephelyek meglévő ISDN telefonközpontok forgalmának a biztosítása Nyiregyháza és egymás felé
- Telephelyenként a 2 Mbps átviteli sebesség

SCI-NetWork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

Megvalósítandó feladatok az új hálózatban

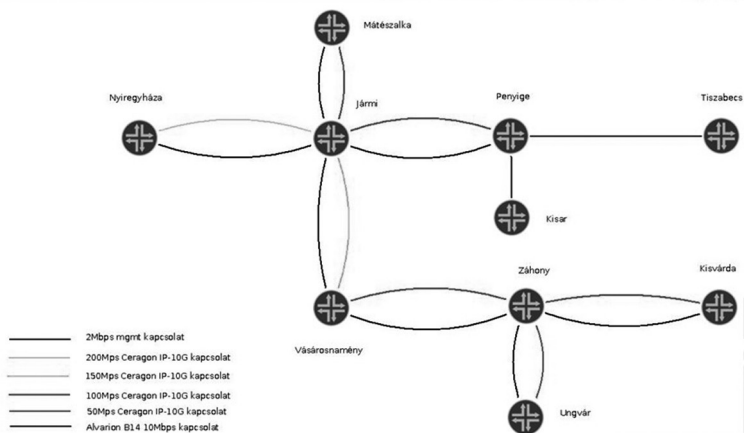
SzSzB. megyében, 10 telephelyen, 2015-től megvalósított L3-as hálózat

- Csomagkapcsolt, IP alapú hálózat kialakítása
- Nagyforgalmú szakaszmérnökségeken 100 Mbps –re bővítés (védelmi központokon 10 Mbps)
- VoIP bevezetése az új telephelyeken
- QoS támogatás
- Meglévő ISDN telefonközpontok forgalmának kezelése a régi telephelyeken
- Dinamikus routing kialakítása

SCI-NetWork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

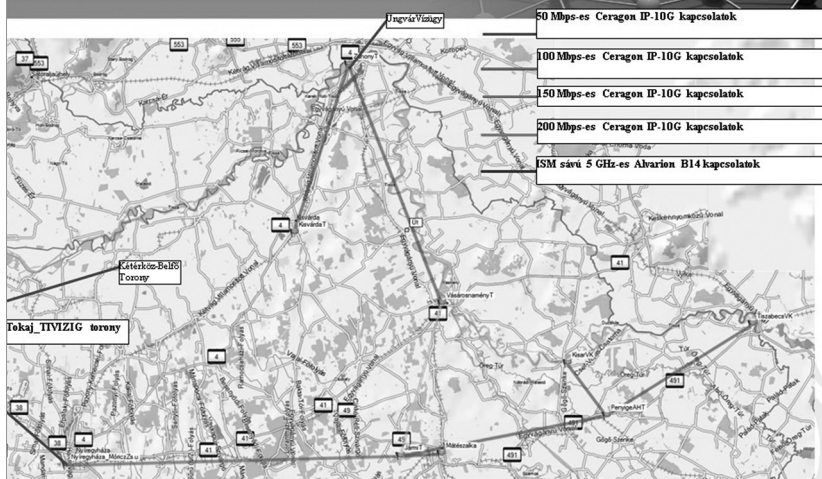
Új hálózati topológia



SCI-NETwork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

A FETIVIZIG ÚJ MIKROHULLÁMÚ HÁLÓZATA



SCI-NETwork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

Eszközválasztás

Az eszközzel szemben támasztott követelmények

- Telephelyi switching, VLAN
- Statikus, dinamikus routing támogatás
- QoS támogatás (hang prioritizálás)
- Tűzfal funkciók (UTM opció)
- VPN támogatás (pl. ADSL tartalékolt útvonal kiszolgálása)
- E1 és BRI kapcsolatok fogadásának lehetősége
- Telephelyenként 8 port biztosítása elegendő

SCI-NETWork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

Eszközválasztás

- A kialakított feltételrendszer klasszikus hálózati topológiával 3 eszközt jelentene: router, tűzfal, switch
- Az SRX család költséghatékonyabb megoldás más gyártókkal szemben, mivel egy eszközben képes nyújtani a szükséges funkciókat
- Eszköz konfigurációk összehasonlítása:

Gyártó	Juniper	C gyártó
Eszköz	SRX220	ASA-5506-K9
Eszköz	-	1921/K9
Eszköz	-	C2960CX-8TC-L
Bekerülés	100 %	149 %

SCI-NETWork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

A Juniper SRX termékcsaládot választottuk

- SRX100 és 210-es eszközöket alkalmaztunk
- A 210-es modellnél 2 db Gbps-es és 6 db 100 Mbps-es port van, 100-as modellnél 8 db 100 Mbps-es port
- A 210-es változat 1 db bővítő kártyahely van (SFP, E1, BRI, ADSL opciókkal)
- QoS és VPN támogatás
- Teljes értékű switching és routing funkciók
- Aggregált throughput kapacitás : 700-850 Mbps
- Minden követelményt egy eszköz képes biztosítani



SCI-NetWork Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

Köszönöm a figyelmet!

timre@scinetwork.hu

SCI-NETWork

Telecommunications & Networking, Inc. • 1142 Budapest, Erzsébet királyné útja 125. • phone: +36 1 467-7030

NÉMETH József Lajos

THE NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence

Dr. Jozsef Lajos NEMETH, PhD

National University of Public Service, Budapest, Hungary

CONTENT

Introduction, origins

The NATO's Strategic Communication

**History, mission, structure, activities,
events, publications**

Conclusion

MOTTO

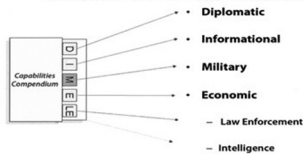
"Since wars begin in the minds of men, it is in the minds of men that the defences of peace must be constructed."

Preamble to the Constitution of UNESCO (1946)

Source:
<http://unesdoc.unesco.org/images/0022/002269/226924e.pdf#page=8>, date of download: 15 October 2015, p.5.

WHAT IS STRATEGIC COMMUNICATION? ORIGINS AND FEATURES

After 9/11 United States felt misunderstood politically and socially by other nations and ethnic and religious groups with which it had not maintained an open flow of information.



**PRACTICE OF (SOFT)
POWER
„MASS vs. PUBLIC”
PUBLIC DIPLOMACY**

Source:
<http://static1.squarespace.com/static/55324e45e4b0c396560ea1f1/55324e8de4b0323bd7301fa5a/55325292e4b0323bd731875b/1429381288890/orchestraTemplate24Jun08.jpg?format=original>, date of download: 15 October 2015

The NATO's Strategic Communication I.

„Strategic communication is an integral part of the efforts to achieve the Alliance's political and military objectives, thus it is increasingly important that the Alliance communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions”.

(Source: NATO STRATCOM COE, <http://www.stratcomcoe.org/about-us>, date of download: 15 October 2015)

A word cloud shaped like a compass rose, centered around a four-pointed star. The words are arranged in four quadrants:

- Top Quadrant:** EXCELLENCE, solutions, emerging, politics, expertise, goals, communication, respect, ambition, change, growth, progress, innovation, technology, knowledge, science, digital, media, networks, virtual, global, mission, NATO, STRATCOM, alternative, strategies, diplomacy, capabilities, culture, CENTRE, solutions of, growth, progress, innovation, technology, knowledge, science, digital, media, networks, virtual, global, mission, NATO, STRATCOM, alternative, strategies, diplomacy, capabilities, culture, CENTRE, solutions of.
- Right Quadrant:** LATVIA, RIGA, evolution, future, respect, ambition, change, growth, progress, innovation, technology, knowledge, science, digital, media, networks, virtual, global, mission, NATO, STRATCOM, alternative, strategies, diplomacy, capabilities, culture, CENTRE, solutions of.
- Bottom Quadrant:** CENTRE, solutions of, growth, progress, innovation, technology, knowledge, science, digital, media, networks, virtual, global, mission, NATO, STRATCOM, alternative, strategies, diplomacy, capabilities, culture, CENTRE, solutions of.
- Left Quadrant:** STRATCOM, NATO, mission, virtual, global, networks, digital, media, knowledge, science, emerging, solutions, EXCELLENCE, solutions, emerging, politics, expertise, goals, communication, respect, ambition, change, growth, progress, innovation, technology, knowledge, science, digital, media, networks, virtual, global, mission, NATO, STRATCOM, alternative, strategies, diplomacy, capabilities, culture, CENTRE, solutions of.

The NATO Strategic Communications Centre of Excellence HISTORY

- January 2014 - NATO StratCom COE became functional (based in Riga, Latvia)
- 01 July 2014 - seven member states – Estonia, Germany, Italy, Latvia, Lithuania, Poland, and the United Kingdom – signed memorandums of understanding on the establishment of the StratCom COE.
- 01 September 2014 - The centre received NATO accreditation

2014 Wales NATO Summit Declaration:

“...the establishment of the StratCom COE as a meaningful contribution to NATO’s efforts...” in the area of strategic communications.

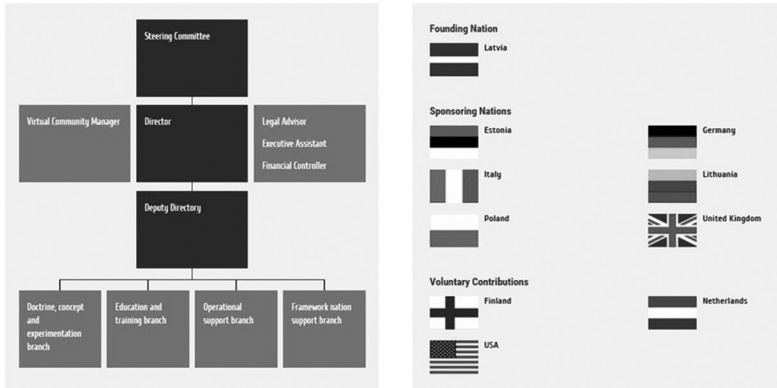
(Source: http://www.nato.int/cps/en/natohq/official_texts_112984.htm, date of download: 15 October 2015)

The NATO Strategic Communications Centre of Excellence MISSION

The mission of the NATO StratCom COE
is to contribute to the Alliance’s communication processes
**in order to ensure that it communicates
in an appropriate, timely, accurate and responsive
manner**
on its evolving roles, objectives and missions.

(Source: NATO STRATCOM COE, <http://www.stratcomcoe.org/about-us>, date of download: 15 October 2015)

The NATO Strategic Communications Centre of Excellence STRUCTURE AND MEMBERS in 2015



(Source: NATO STRATCOM COE, <http://www.stratcomcoe.org/structure>, date of download: 15 October 2015)

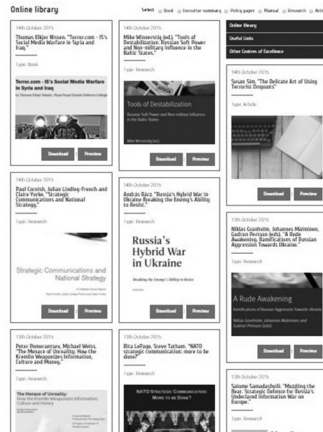
The NATO Strategic Communications Centre of Excellence ACTIVITIES IN 2015

- Support the development of a NATO Military Committee Strategic Communications policy and doctrine,
- Research how to identify the early signals of a hybrid warfare scenario,
- Develop Academic Magazine "Defence Strategic Communications",
- Study Russia's Information Campaign against Ukraine,
- Research how NATO and its members could protect themselves from subversive leverage,
- Research 10 years of ISAF Strategic Communications efforts to extract best practices and lessons learned,
- Analyse the implementation of the NATO Strategic Communications policy throughout the NATO Command Structure,
- Research the implementation of Strategic Communications within Allied nations,
- Research ISIL information campaign and its influence on NATO countries' societies,
- Develop Strategic Communications online course "Strategic Communications for beginners", courses for senior officials, basic and advanced courses for international staff officers,
- Support NATO StratCom training and education, including exercises education,
- Study how social media is being used as a weapon in hybrid warfare.

(Source: NATO STRATCOM COE, <http://www.stratcomcoe.org/about-us>, date of download: 15 October 2015)

The NATO Strategic Communications Centre of Excellence PUBLICATIONS (on-line library)

- Thomas Elkjer Nissen. "Terror.com - IS's Social Media Warfare in Syria and Iraq.,,"
- Mike Winnerstig (ed.). "Tools of Destabilization. Russian Soft Power and Non-military Influence in the Baltic States."
- Susan Sim. "The Delicate Art of Using Terrorist Dropouts"
- Paul Cornish, Julian Lindley-French and Claire Yorke. "Strategic Communications and National Strategy.,,"
- András Rácz. "Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist."
- Rita LePage, Steve Tatham. "NATO strategic communication: more to be done?"



(Source: NATO STRATCOM COE, http://www.stratcomcoe.org/online_library/, date of download: 15 October 2015)

The NATO Strategic Communications Centre of Excellence EVENTS

☐ eCourses ☐ Trainings ☐ Workshops ☐ Conferences

23rd October 2015

Seminar on Strategic Communications for Senior Officials

22nd - 25th July 2015

StratCom seminar for Georgian civil servants

19th February 2015

Coordination meeting for Ukrainian, Georgian and Moldovan wider security sector

27th September 2015

Centre organises seminar "The DAESH information campaign and its influence on NATO countries' societies"

2nd June 2015

Centre organises seminar "The DAESH information campaign and its influence on NATO countries' societies"

17th April 2015

Workshops about hybrid warfare and its challenges for NATO countries

20th August 2015

Centre will mark the inauguration of its new premises with a high level conference

20th - 21st August 2015

"The Riga StratCom Dialogue: Perception Matters"

16th July 2015

Presentation of preliminary results of the study on internet trolling

(Source: NATO STRATCOM COE, <http://www.stratcomcoe.org/events/>, date of download: 15 October 2015)

CONCLUSION

NATO Strategic Communications Centre of Excellence is an important player and contributor for related activities.

There are lot of participation possibilities for other member countries, such as Hungary.

For academics it is an important tool and framework to provide a comprehensive view about strategic communications.

THANK YOU!

Dr. Jozsef Lajos NEMETH, PhD

National University of Public Service
Faculty of Military Sciences and Officer Training
Budapest, Hungary
E-mail: nemeth.jozsef@uni-nke.hu

FEKETE Károly

EVOLUTION OF MILITARY SCIENCE: REAL AND VIRTUAL WORLDS

KAROLY FEKETE:
11/11/2015

EVOLUTION OF MILITARY SCIENCE: REAL AND VIRTUAL WORLDS



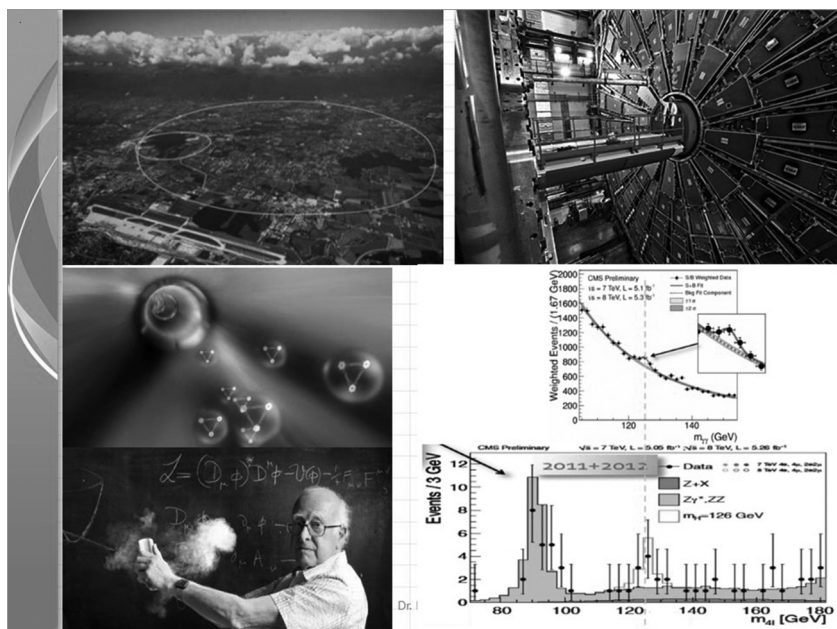
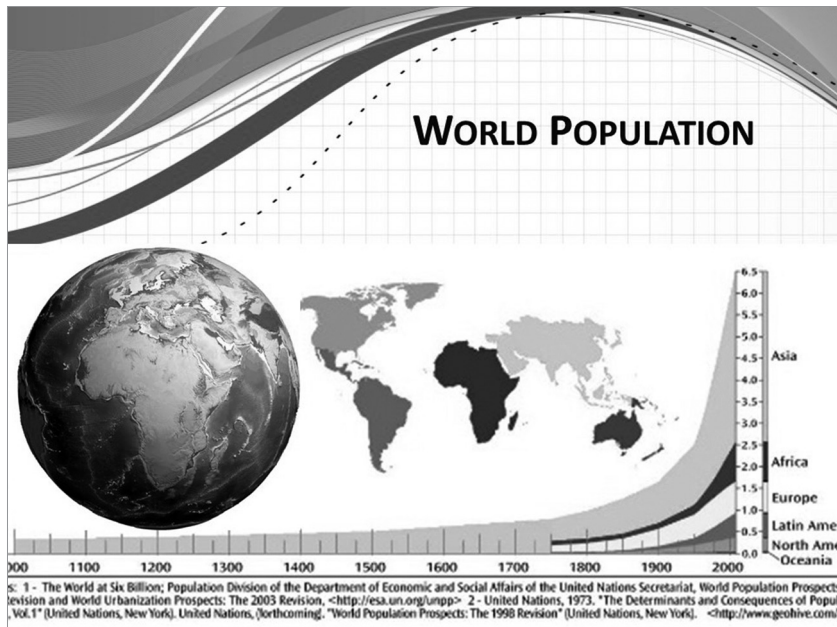
A TUDOMÁNY EVOLÚCIÓJA:
A VALÓS ÉS A VIRTUÁLIS VILÁGOK

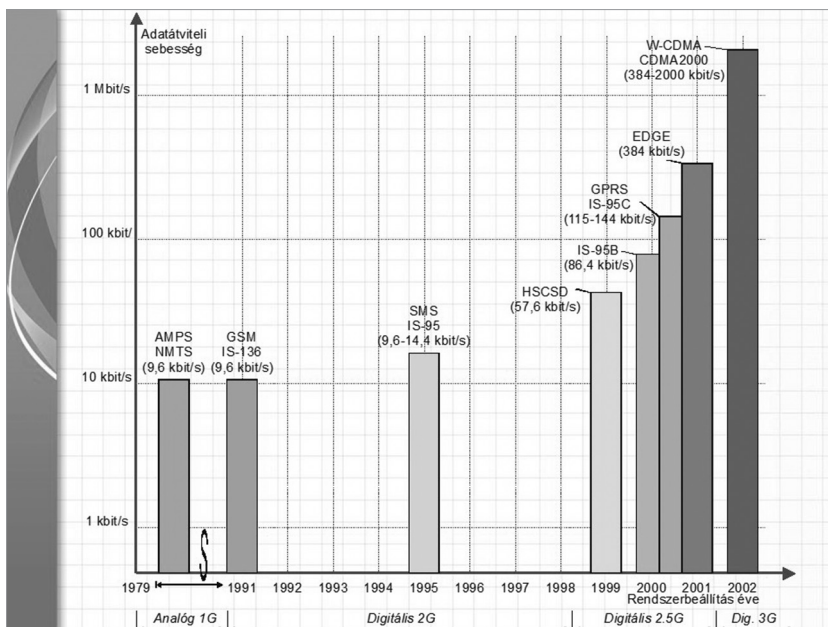
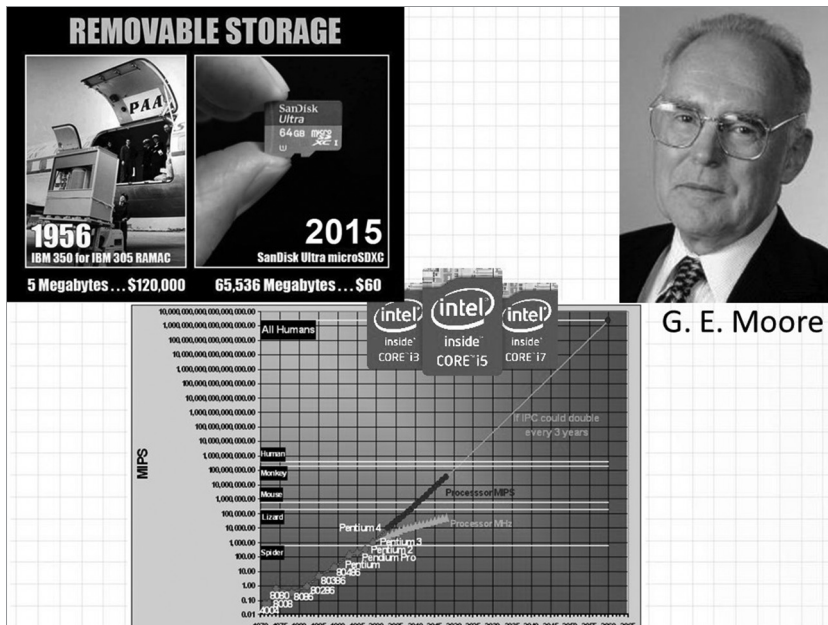
A MAGYAR

TUDOMÁNY ÜNNEPE



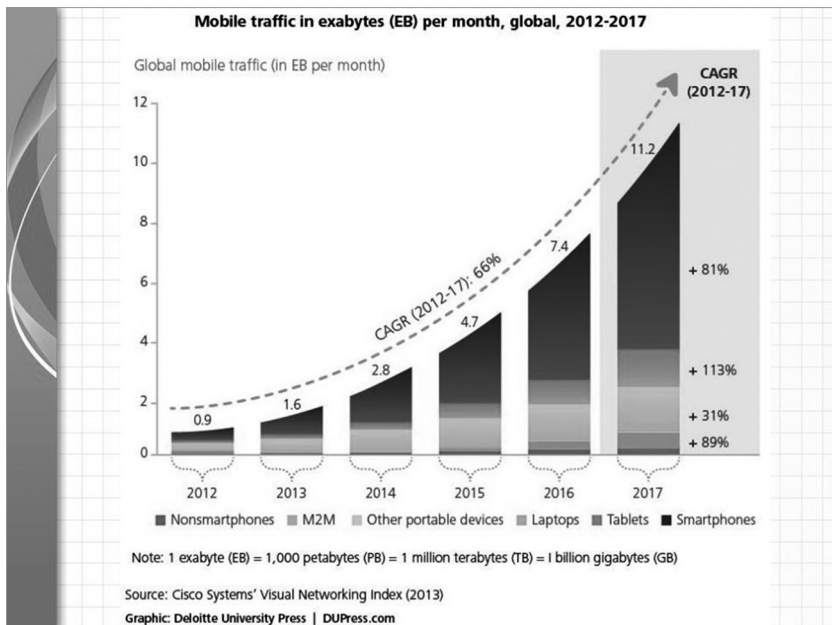
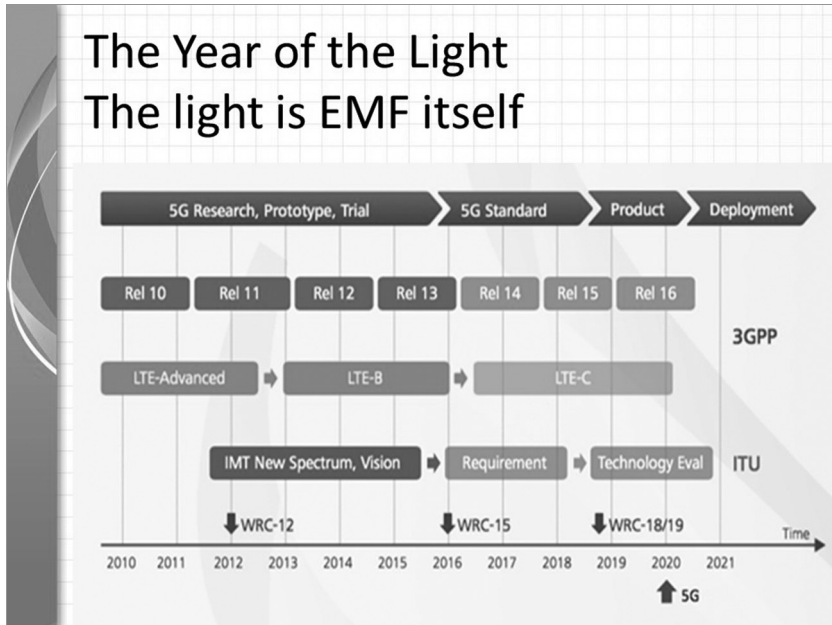
Dátum	Az esemény címe	Helyszín
2015. november 3.	<u>Értékkörzés az irodalomban</u>	NKE Hadtudományi és Honvédtisztképző Kar
2015. november 4.	<u>Önkormányzatiság napjainkban</u>	NKE Ludovika Campus
2015. november 5.	<u>Magyar Tudomány Ünnepe alkalmából rendezett ünnepi szenátusi ülés</u>	NKE Ludovika Campus
2015. november 5.	<u>Immunitási tünetek a közhatalom felelőssége körében</u>	NKE Ludovika Campus
2015. november 5.	<u>Európai válságok – Európai válságkezelés, 2005-2015</u>	Stefánia Palota - Honvéd Kulturális Központ
2015. november 6.	<u>A Haza szolgálatában</u>	NKE Ludovika Campus
2015. november 9.	<u>A magyar közjogi komparatiztika története a polgári korban II.</u>	NKE Közigazgatás-tudományi Kar
2015. november 11.	Kommunikáció 2015	Stefánia Palota - Honvéd Kulturális Központ
2015. november 11.	<u>Vallástudományi magasles – Hoppál Bulcsú könyvének megvitatása</u>	NKE Közigazgatás-tudományi Kar
2015. november 16-17.	<u>From the Holy Alliance to the European Union (1815-2015): 200 years of European nation-states</u>	NKE Ludovika Campus



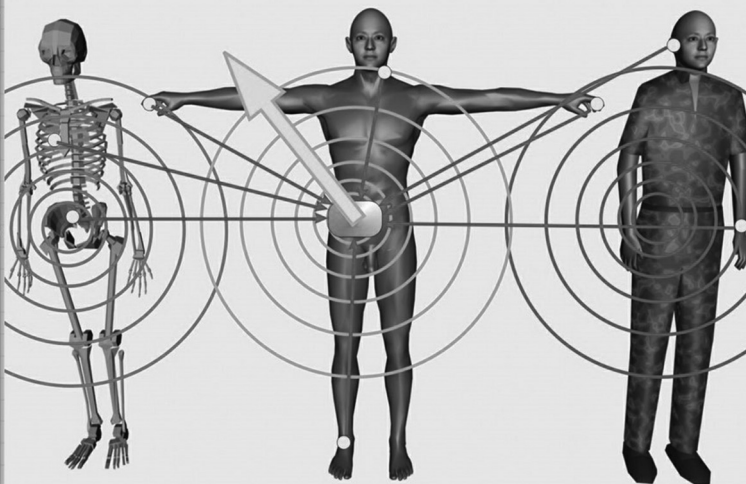


The Year of the Light

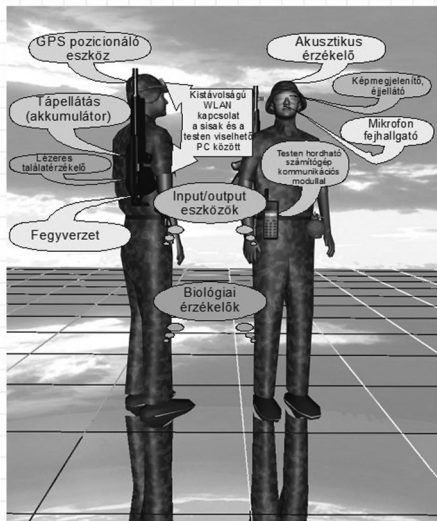
The light is EMF itself

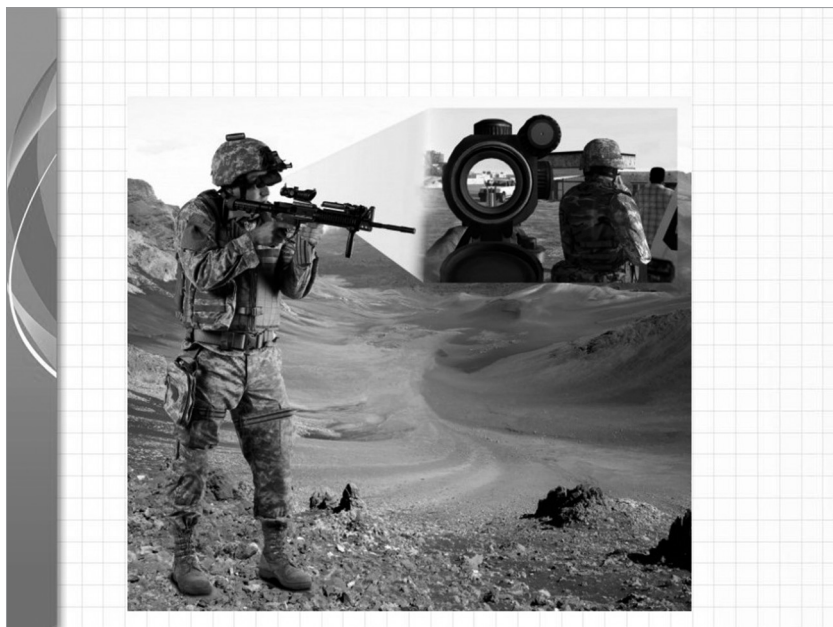
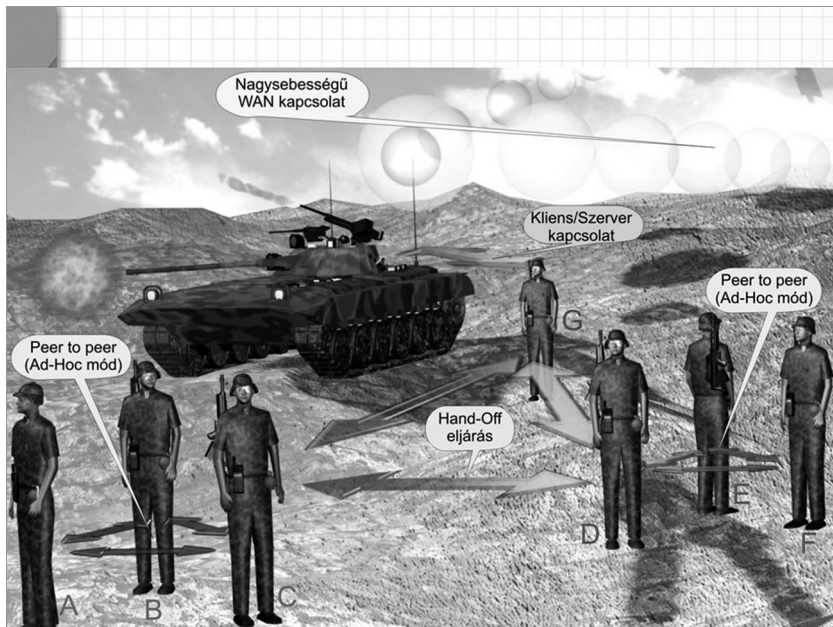


HEALTH SENSORS WITHIN THE BODY

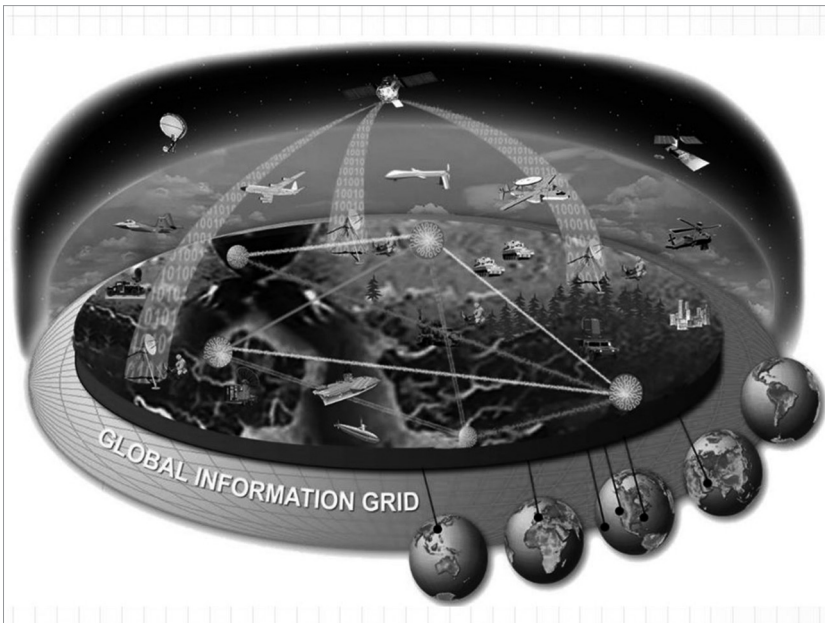


BODY LAN





Virtual theatre operation





REFERENCES:

- [HTTP://WWW.VRS.ORG.UK/VIRTUAL-REALITY-MILITARY/](http://www.vrs.org.uk/virtual-reality-military/)
- CLAY WILSON: AVATARS, VIRTUAL REALITY TECHNOLOGY, AND THE U.S. MILITARY: EMERGING POLICY ISSUES, CRS REPORT FOR CONGRESS, OC RS22857 APRIL 9, 2008, DON TAPSCOTT AND ANTHONY WILLIAMS, WIKINOMICS, PENGUIN GROUP, NEW YORK, 2006.
- MICHAEL PECK, SOLDIERS LEARN HAZARDS OF WAR IN VIRTUAL REALITY, NATIONAL DEFENSE, FEBRUARY, 2005, [HTTP://WWW.NATIONALDEFENSEMAGAZINE.ORG/ISSUES/2005/FEB/UF-SOLDIERS_LEARN.HTM].
- FEKETE KÁROLY: A KOMMUNIKÁCIÓ INFORMATIKA ÉRTÉKALKOTÓ HATÁSA, EVOLÚCIÓS FOLYAMATOK, ÚJ HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA (1991-2007) (ISSN: 1216-7436) 50: (9) PP. 12-17. (1996)
- ANDRAS TOTH: NETWORK CENTRIC COMMUNICATION SYTEMS TO SUPPORT SIGNAL MILITARY DECISION MAKING PROCESS, IN: ZOLTAN RAJNAI, BELA PUSKAS, GABOR VANDERER, MIKULÁŠ ŠOSTRONEK, ROMAN BEREŠIK, MARIÁN BABJAK, DANUŠA SPILÁ (SZERK.), PROCEEDINGS OF THE INTERNATIONAL CONFERENCE NEW TRENDS IN SIGNAL PROCESSING 2014. 176 P. ,TATRANSKÉ ZRUBY, SZLOVÁKIA, 2014.10.15-2014.10.17. LIPTOVSKY MIKULAS: ARMED FORCES ACADEMY OF GENERAL MILAN RASTISLAV ŠTEFÁNIK, 2014. PP. 112-115.

SZABÓ Levente – SZABÓ András

KIKÉPZÉS A KIBERTÉRBEN



NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR

Kiképzés a kibertérben

előadók:
Szabó Levente szds.
Szabó András fhgdy.

Kommunikáció 2015 Konferencia



NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR

Az előadás felépítése

1. Trendek a Kiberbiztonság területén
2. Kiberbiztonsági képzések csoportosításának lehetőségei
3. A NATO főbb kiberbiztonsági gyakorlatainak bemutatása
4. Összegzés



<http://ikonskalev.com/images/Social-Security-Disability-Attorney-in-Seattle.jpg>



Trendek a Kiberbiztonság területén

- Komplex rendszerek
- Web 3.0 fenyegetések – az egyén mint célpont
- Kiberbűnözés mint iparág
- “Sub rosa” warfare
- Támadások számbeli és minőségbeli fejlődése



A megakadályozás helyett a reagáláson a hangsúly!



Megoldások:

- Felkészülés és felkészítés
- a technológiák testre szabása
- Monitorozó képesség növelése

Cyberbiztonsági képzések csoportosításának lehetőségei

Jellege szerint:

- Elméleti
- Gyakorlati
- Vegyes

Végrehajtása szerint:

- Bsc, Msc képzésben,
- tanfolyam jellegű,
- online (elearning, webcast),
- gyakorlat.

Témája szerint:

- technikai
tűzfal, AV, végponti védelem
- technológiai
pl.: Cisco, MS, stb.
- jogi (vagy „Policy-making”)

Gyakorlat orientált lehetőségek

- „capture-the-flag” hacker verseny
- Forensic challenge
- Red & Blue team game

Gyakorlat orientált IT biztonsági képzés célja



meglévő **elméleti ismeretekre épülő**,
intenzív **laborgyakorlatokkal** támogatott,
naprakész (*technológiák, eljárások terén*),
specifikus képzés (*szakterületekre /
technológiákra fókuszáló*)

Kiber „lőtéř”



http://media.nbcсандiego.com/images/621*349/shooting--range-military.jpg

Vs



http://www.bhclab.com/assets/images/shutterstock_300344546.jpg

A NATO főbb cyber gyakorlatainak bemutatása



Összegzés

- Gyakorlat orientált képzés kell a hatékony kibervédelmi képességhez!
- Komplex, különböző kompetenciákat fejlesztő gyakorlatok szükségesek!
- Szakemberek továbbképzése, karrierútja tervezést igényel!
- A gyakorlatok tervezése és levezetése (ütemezése, ellenőrzése) nagyban meghatározza azok eredményességét!
- A résztvevőknek előzetes felkészítést kell tartani (a szerepek, feladatok tisztázása érdekében)!
- A gyakorlatok idejére az állományt a napi munkavégzés alól mentesíteni kell!



Kérdések + Válaszok



SCHMUCK András

ÜZEMELTETÉS ÉS TELEPÍTÉS TÁVKÖZLÉSI HÁLÓZATOKON

Üzemeltetés és telepítés távközlési hálózatokon

„Kommunikáció 2015”
konferencia
Nemzeti Közszolgálati Egyetem

2015. november 11.

antenna
HUNGÁRIA

Az Antenna Hungáriáról

Tulajdonos: Nemzeti Fejlesztési Minisztérium

Fő tevékenység: ➔ Országos digitális földfelszíni televíziós és rádiós műsorszórás

➔ Optikai és vezeték nélküli távközlési szolgáltatások

➔ Hálózat szervíz- és karbantartási szolgáltatások

➔ Multimédia szolgáltatások

Nettó árbevétel: 20 mrd Ft (konszolidált, 2012-13-as üzleti év)



Az Antenna Hungária küldetése, hogy teljes körűen és a legmagasabb minőségben kiszolgálja ügyfelei igényeit az audiovizuális tartalmak eljuttatásában a hagyományos és új műsorterjesztési csatornákon keresztül, valamint kiaknázza az ehhez kapcsolódó egyedi távközlési infrastruktúra képességek szinergiáit távközlési hálózatok építésére, üzemeltetésére és üzleti hasznosítására.

ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petzvál József u. 31-33. www.ah.hu

antenna
HUNGÁRIA

Az AH infrastrukturális háttere

Infrastrukturális háttér

- 218 saját műsorszóró, átjátszó és távközlési telephely
- Országos lefedettséget biztosító nagysebességű digitális mikrohullámú gerinchálózat és az ehhez csatlakozó hozzáférési hálózat
- Vezetékes optikai hálózat Budapesten és 19 főút mentén
- VSAT hálózat - KKE régió piacvezető VSAT szolgáltatója az 55%-ban AH tulajdonban lévő Hungaro DigiTel Kft.
- DVB-T hálózat (lakossági lefedettség jelenleg: > 99 %)
- CDN hálózat
- 3,5 GHz, 26 GHz engedély – Pont-Multipont szolgáltatások

Országos Transzport Hálózat



Toronyinfrastruktúra



ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petöfi Sándor u. 31-33. www.ahnt.hu

antenna
HUNGÁRIA

Az AH távközlési szolgáltatásai



Üzleti távközlési szolgáltatások

Az Antenna Hungária üzleti távközlési szolgáltatásokat – menedzselt bérlet vonal, IP-VPN - nyújt ügyfeleinek, alapvetően a vezetékek nélküli képességek kihasználásával.

- **Menedzselt bérlet vonali szolgáltatás (MLLN)** - folyamatos és közvetlen kommunikációs összeköttetést biztosít, amely a gyors és biztonságos adat-, hang- és képátvitel mellett a telephelyek helyi hálózatainak összekapcsolására és az Internethez való csatlakozásra is lehetőséget ad.
- **Metro Ethernet szolgáltatás** (helyi hálózatok összekapcsolása) - folyamatosan menedzselt, rugalmasan méretezhető Ethernet alapú bérlet vonali összeköttetést biztosít
- **Internet szolgáltatás** – MLLN szolgáltatás, amely lehetővé teszi a belföldi és a nemzetközi Internet hálózatok gyors és biztonságos elérését, a folyamatos felügyeletet és készenlétet.
- **VoIP hangátviteli szolgáltatás** - korszerű internet protokoll technológiára épül, amely a magas minőség mellett alacsony költségű távbeszélő-kommunikációt biztosít ügyfeleinknek.
- **MPLS protokollon alapuló IP VPN** szolgáltatás segítségével virtuális magánhálózat alakítható ki, mely a telephelyek közötti adatforgalom lebonyolítását úgy teszi lehetővé, hogy az információáramlásból az illetékteleneket teljes mértékben kizárja.



Üzemeltetés (hibaelhárítás és karbantartás)

Az AH egyedi és megkerülhetetlen tornyokkal rendelkezik a magyarországi távközlési telephely piacon. Tapasztalatára és erőforrásaira építve az AH **külső partnereknek is nyújt telephely-karbantartási szolgáltatást:**

- 2G/3G/4G bázisállomás, ismétlő állomás, PDH/SDH átviteli és infrastruktúra hibaelhárítás és karbantartás több mint 4100 állomáson;
- Egyéb szerviz tevékenységek: bázisállomás és torony telepítés, üzemeltetés; szükség-áram fejlesztés (aggregátorozás); berendezési kártya cserék; eseti munkák (antenna csere, ügyfél-panasz kezelés, erőáramú hibajavítások); WLAN telepítések, üzemeltetés; időközi kötelező felülvizsgálati munkák elvégzése.



Infrastruktúra bérbeadás

Az AH bérbe adja

- a telephelyhálózataán levő tornyainak szabad kapacitását és műszaki létesítményeit, továbbá
- az országosan elhelyezkedő AH ingatlanok - földterület, iroda- és raktárhelyiségek, központi telephely - szabad területeit.

ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petöfi Sándor u. 31-33. www.ahnt.hu

antenna
HUNGÁRIA

2.1. Meglévő szolgáltatások

Műholdas távközlési szolgáltatások

Az Antenna Hungária leányvállalata, a Hungaro DigiTel Kft. révén a professzionális távközlés egy különleges technológiáját, a VSAT műholdas digitális távközlési technológiát is tudja alkalmazni az összeköttetések kiépítésénél.



Műholdas megoldások előnyei

- Szélessávú adatkapcsolat (és videókapcsolat) létesítése azonnal a helyszínről (jelenleg ez csak hosszú előkészítés után, költségesen, nem mindenhol és csak a jó előre megtervezett bevetések esetén lehetséges)
- Menetközben is kommunikáció kész (adat és videó átvitel menet közben)
- Műveleti területek azonnali váltása esetén is bevethető (nincs átszerelési idő)
- Földi hálózatoktól függetlenül mindenhol elérhető
- 3G/4G szolgáltatással ellentétben, nincs hatással rá a lakosság (pl. tömegrendezvény esetén, nem megfelelő az elérés)
- Magas rendelkezésre állás
- Nincs korlátozva magyarországi területre
- Biztonságos, nem Internet alapú, zárt hálózat

Professzionális műholdas megoldások
www.hdt.hu

ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petzvál József u. 31-33. www.ahh.hu

antenna
HUNGÁRIA

Telepítési és üzemeltetési szolgáltatások jellemzői

Távközlési hálózat életciklusa



A TELJES ÉLETCIKLUS JELLEMZŐI

- Komplex feladatok sorozata
- Egymástól függő lépések
- Az egyes folyamatok egymásra hangolása létfontosságú
- Felelősségi körök körülhatárolása kritikus
- Hálózatbiztonsági szempontok figyelembe veendőek

A hálózat létrehozása és működtetése során egységes szemléletre, a teljes folyamatot ismerő és abban kompetens partnerre van szükség

ELŐNYÖKA HÁLÓZAT SZEMPONTJÁBÓL

- ✓ Megbízhatóbb működés
- ✓ Költséghatékonyabb üzemeltetés
- ✓ Gyorsabb, gördülékenyebb folyamatok
- ✓ Tisztázott felelősségek

ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petzvál József u. 31-33. www.ahh.hu

antenna
HUNGÁRIA

Hálózatüzemeltetési képességeink

Az Antenna Hungária évtizedes szakmai tapasztalatánál fogva képes a vezeték nélküli hálózatok integrált kiépítésére és üzemeltetésére. Az AH a teljes életciklust végigkísérve mind a tervezést, az eszközök telepítését és üzembe helyezését, mind pedig a beszállítókkal való kapcsolattartást, a garanciák érvényesítését, a hibajavítást és a karbantartást teljes körűen el tudja végezni.



Az Antenna Hungária évtizedek óta végez bázisállomás-hálózat fenntartási tevékenységet, továbbá felhordó mikrohullámú hálózatok 24 órás rendszerű hibaelhárítását, karbantartását. A fenntartási tevékenységünket öt regionális szervizközpontból látjuk el, emellett további két szervizbázisról is folyik az üzemeltetés. Ez a területi eloszlás országos szinten teljes és egyidejű „lefedettséget” biztosít.

ÜZEMELTETÉSI SZOLGÁLTATÁSAINK

- Állomás akvizíciók
- Tervezési munkák
- Engedélyeztetések
- Telepítések
- Rádiós és infrastrukturális elemek hibajavítása és karbantartása
- 24/7/365-os diszpécser szolgálat
- Szükség áramfejlesztés
- Üzembe helyezések
- Eseti munkák
- Mérések
- Ügyfélpanaszok kivizsgálása
- Mobil torony felállítása szükséghelyzetek esetén
- Felülvizsgálati munkák (érintés és villámvédelem) ellátása
- Logisztikai feladatok

Referenciák

Cégünk mind saját részre, mind partnerei számára végez hálózat üzemeltetési tevékenységeket. Több évtizedes szakmai tapasztalattal és referenciákkal rendelkezünk ezen a területen:

- Telenor Magyarország – több mint 15 év tapasztalat, 4000 állomás



- Hungaro DigiTel – több mint 10 év tapasztalat, 3000 végpont



- Magyar Honvédség 2013 októberig – több mint 20 év tapasztalat, 110 állomás



- Vodafone Magyarország 2009 év végéig – 10 éves tapasztalat, 2500 állomás



ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petőfi közút u. 31-33. www.ah.hu

antenna
HUNGÁRIA

Összefoglalás

- A hálózatképzési és -üzemeltetési feladatok egy kézben tartása számos előnyt biztosít a távközlési hálózat tulajdonosának
- Az Antenna Hungária képes arra, hogy integrált szolgáltatóként valamennyi feladatot ellássa az értékláncban



Antenna Hungária erősségei üzemeltetés és telepítés területén

- Évtizedes tapasztalatok a távközlési létesítésben és üzemeltetésben
- Meglevő kompetenciák a teljes szolgáltatási értéklánc mentén
- Stratégiai szerepkör (állami vezetékek nélküli kompetencia központ)
- Saját hálózathoz, működéshez kapcsolódó üzemeltetési sinergiák
- Piaci szereplőkkel, alvállalkozókkal fennálló kapcsolatok
- Kormányzati és piaci referenciák

ANTENNA HUNGÁRIA ZRT. 1119 Budapest, Petzvál József u. 31-33. www.ahrt.hu

antenna
HUNGÁRIA

NYÁRI László

SMART DUST



NEMZETI
KÖZZSZOLGÁLATI
EGYETEM
HADTUDOMÁNYI ÉS
HONVEDTISZTKÉPZŐ KAR

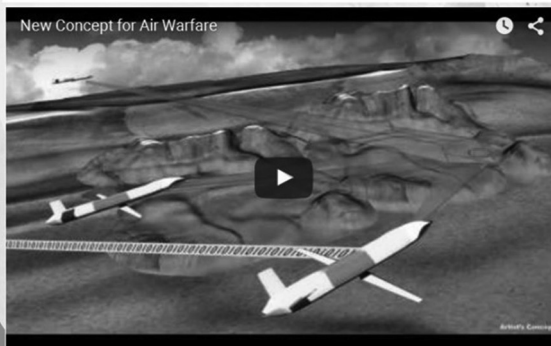
SMART DUST

A védelmi elektronika, informatika és kommunikáció legújabb területe



3. KUTATÁSI TERÜLET „Informatika és kommunikáció”

DARPA szerint az emberek és az okos technológiák együttműködésére épülő
"endszerek rendszerével" bármely ellenfél legyőzhető lehet.



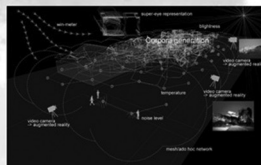
(Defense Advanced Research Projects Agency – Fejlett Védelmi Kutatási Projektek ügynöks.

3. KUTATÁSI TERÜLET

**Nem kerülhetjük meg,
a robotika már ma is jelen van szinte az életünk mindenterületén.
(autóipar, egészségügy, közlekedés, logisztika.). Az új és újabb alkalmazási
területeket még felsorolni is nehéz lenne,**



TALON teljes fegyverzetben

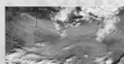


Lassan már nem telik el nap anélkül, hogy ne röppenne fel újabb hír arról, hogy drónokkal elképesztő légi felvételeket készítettek, csomagot kézbesítettek, focimeccset közvetítettek, építkezést felügyeltek, sőt életet mentettek – vagy éppen veszélyeztettek.

3. KUTATÁSI TERÜLET „TTI”

A TÉT Komoly!

4K kamerával támad a legújabb superdrón



A legkülönbözőbb „drónok” alkalmazási lehetőségei valóban új perspektívát, merőben új „forradalmi változások” sorát nyitja meg. Az ellenséget felderítő „okos por”, az emberi testbe hatoló sejt méretű szerkezetek sora rombolóbb belső sérüléseket okoz mint bármelyik fegyver.
Lesz-e tiszta robotháború?

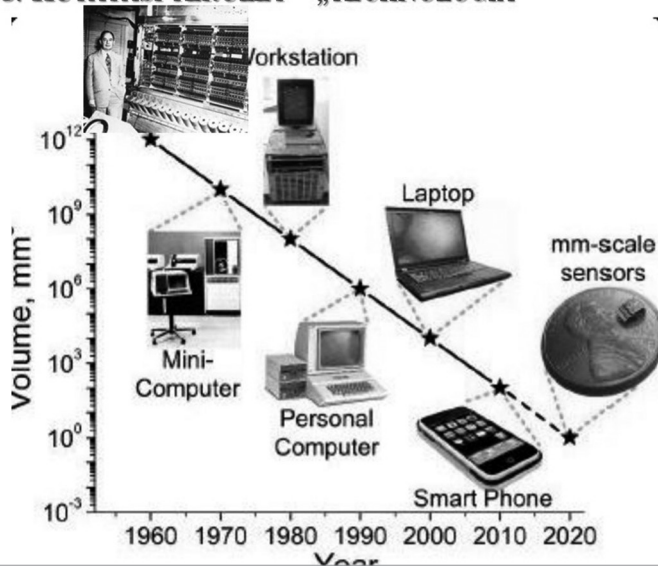
Nem kerülhetjük meg!!



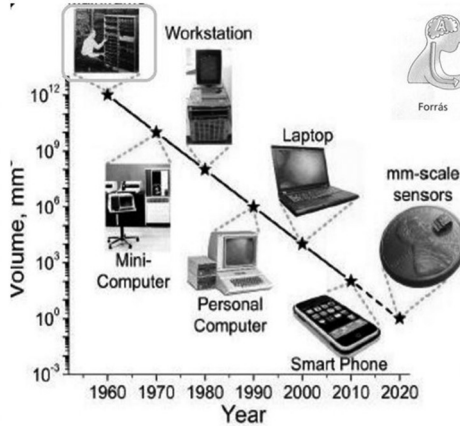
Abe Sinzó japán miniszterelnök: „a mesterséges intelligencia fejlesztése megoldást kínálhat a XXI szd. új kihívásaira.

Becslések szerint a dróniparág 2025-re csak az Egyesült Államokban 80 milliárd dolláros piaccá nőheti ki magát és legalább százezer új munkahelyet teremthet

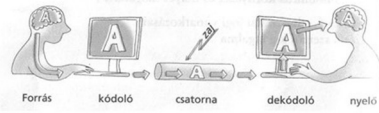
3. KUTATÁSI TERÜLET „TECHNOLÓGIA”



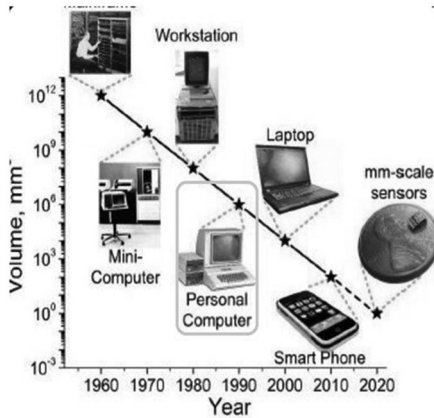
TECHNOLÓGIA



KOMMUNIKÁCIÓ



TECHNOLÓGIA



KOMMUNIKÁCIÓ

Az első technológiai ugrás!

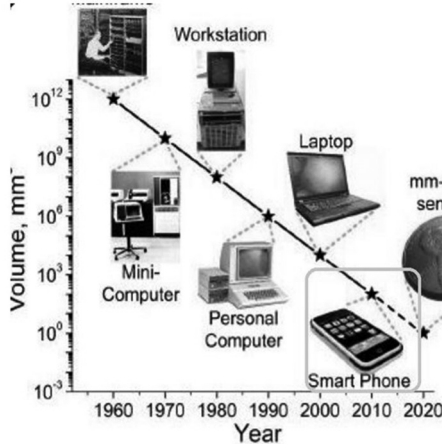
- Net személyes közelségbe került
- közösségi oldalak,
- skype,
- facebook stb.,
- felhő alapú megoldások.

A KOMMUNIKÁCIÓ

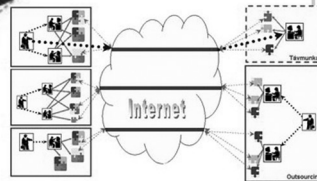


TECHNOLÓGIA

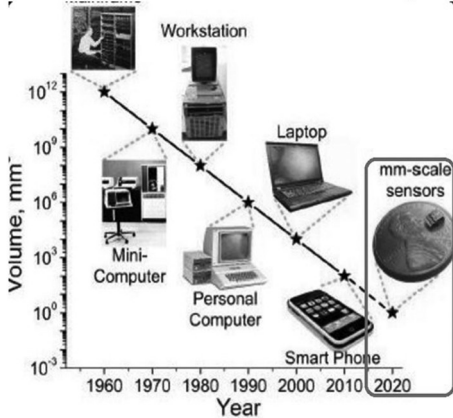
KOMMUNIKÁCIÓ



- A következő technológiai ugrás
- - mindenhol elérhető mobil alkalmazások,
- - multimédia, GPS, 4G,
- Globális kommunikáció.

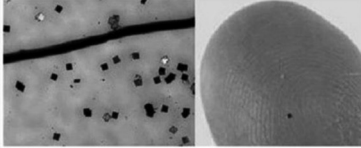


3. KUTATÁSI TERÜLET „TECHNOLÓGIA”



smart Dust

3. KUTATÁSI TERÜLET „TECHNOLÓGIA”



Smart-dust

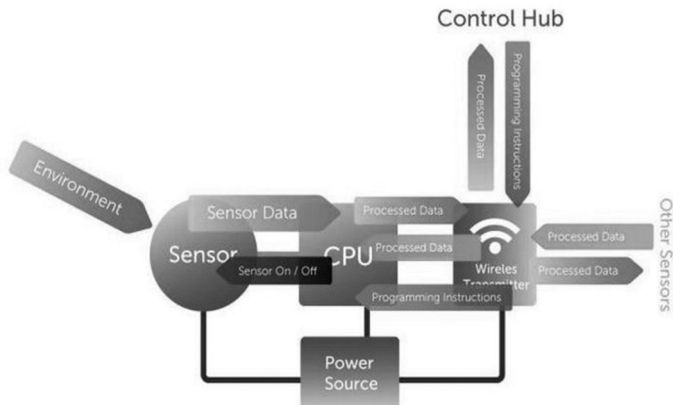
Hitachi Develops World's Smallest RFID Chip. Nicknamed "Powder" or "Dust", the surface area of the new chips is a quarter of the original 0.3 x 0.3 mm, 50µm-thick chip developed by Hitachi in 2003. And this RFID chip is only one-eighth the width of the previous model. – Hitachi expects this tiny size will open the way to new applications for wireless RFID chips. The RFID "powder" can be incorporated into thin paper, such as currency, creating so-called "bugged" money.

"These are made by Hitachi. They measure only 15X.15 mm each and have GPS capabilities! Sometimes called 'smartdust' as they can be sprayed on us and absorbed or taken in foods, drinks and even injected."

The RFID Loc8tor can identify special RFID tags from a distance of up to 183 meters (600 feet), and the RFID chips have GPS capabilities.

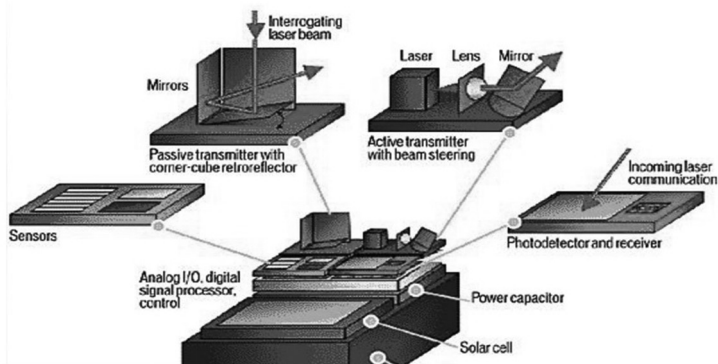
"By taking advantage of the merits of compactness, high authenticity and wireless communication, and combining it with Internet technology, the µ-Chip may be utilized in a broad range of applications such as security, transportation, amusement, traceability and logistics" – said Hitachi engineers who worked on the project.

3. KUTATÁSI TERÜLET „TECHNOLÓGIA”



3. Kutatási terület „technológia”

The goal of the smart-dust project at UC Berkeley is to build self-contained, millimeter-scale devices that include sensors, computational ability, bidirectional wireless communications technology and a power supply, while being inexpensive enough to be deployed by the hundreds.



SMART DUST (TECHNOLÓGIA)

basic smart dust chip

1-2 mm

smart dust chip
encased in electroactive polymer



smart dust chip +
electrode array



smooth
mode

shape change



rough
mode

3. KUTATÁSI TERÜLET TECHNOLÓGIA/TÉR

GONE WITH THE WIND...

Smart dust



TECHNOLÓGIA/TÉR

Mindenhol ott vagyunk!



TECHNOLÓGIA/TÉR



3. KUTATÁSI TERÜLET „TECHNOLÓGIA/TÉR”

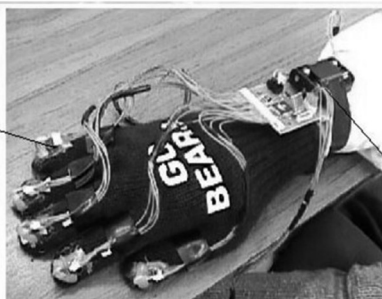


TECHNOLÓGIA

/IDŐ/JELEN



Finger accelerometer



Wrist controller,
RF transmitter and
battery pack

és persze a jövő "katonáiban"

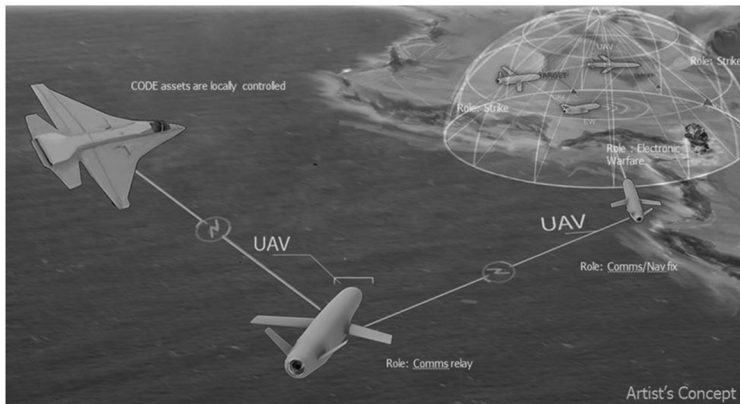
TECHNOLÓGIA

/IDŐ/JELEN



TECHNOLÓGIA /TÉR/GLOBALIZÁLT

- Információs tér (valós időben, mindenhol)



JÓ A MEGÉRZÉSEM?



Hm.. Hm.. Mit látnak szemeim?

Hm.. Hm.. Mit látnak szemeim?



GLOBALIS KOMMUNIKÁCIÓ/GLOBALIS HÁBORÚK?

Application to space exploration: smart dust sensors

Foglaljuk össze: lehetetlen?!

**Mert nem tudjuk mit hoz a jövő,
lessz-e piszkos háború?**



ion
drive

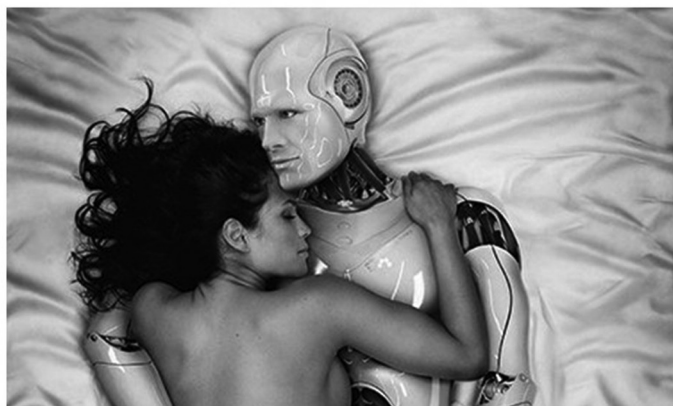
Low cost
Low payload
Massive redundancy

Globális háborúk? Globális kommunikáció

ez nem rémálom, ébredjünk fel!



KÖSZÖNÖM A FIGYELMET!



Nyári László NKE-KMDI
2015

CISCO CERTIFIED NETWORKING ACADEMY TRAINING, CCNA ROUTING & SWITCHING



CISCO

CISCO CERTIFIED
NETWORKING ACADEMY
TRAINING
CCNA Routing & Switching

captain Szabolcs Jobbagy
assistant lecturer

National University of Public Service
Faculty of Military Sciences and Officers Training
Institute of Maintenance
CIS Department



CISCO

Cisco Networking Academy System

- ☐ Global community
- ☐ More than 5.5 million people
- ☐ More than 165 countries
- ☐ More than 20.000 instructors
- ☐ More than 10.000 academies
- ☐ Foundation in 1997
- ☐ Operating since 1999
- ☐ IT skills and career building program
- ☐ For learning institutions and individuals worldwide

2

Cisco Networking Academy System

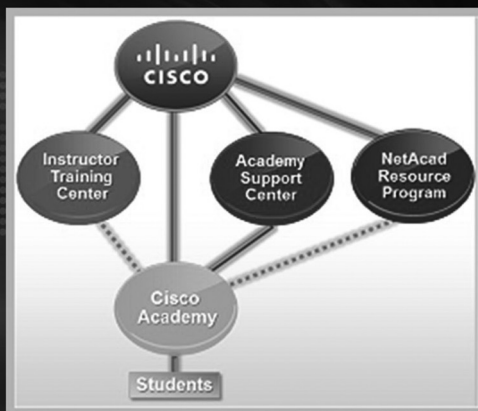


- ☐ General networking knowledge
- ☐ CISCO technological acquaintance
- ☐ Latest networking, security and cloud technologies
- ☐ Prepare for professional certifications
- ☐ Connect to a global community of employers and alumni to find a job and to start a career
- ☐ Theoretical and practical knowledge
- ☐ Hands-on labs, simulation and emulation tools

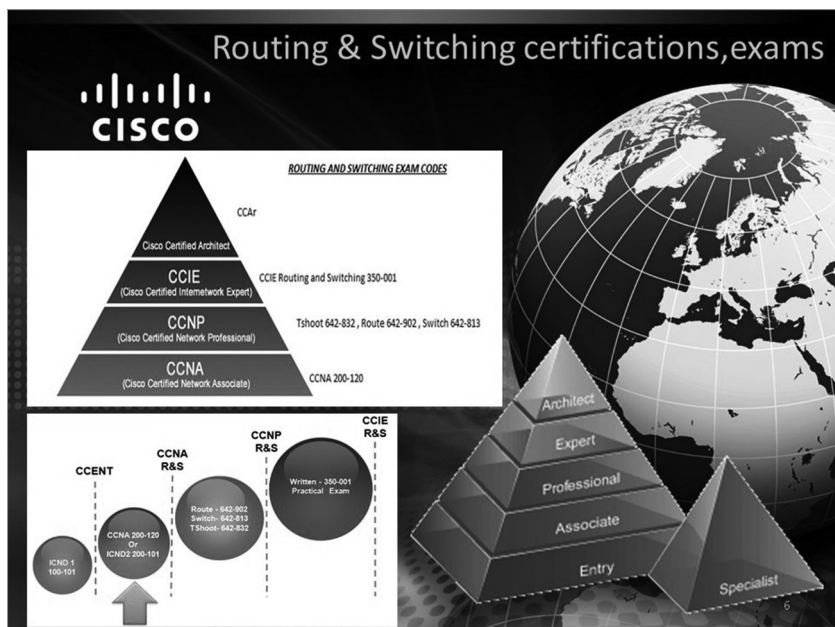


3

Cisco Networking Academy System



4



CCNA Routing & Switching



- ☐ Gateway to entry level networking jobs and IT careers
- ☐ Entry level network technician
- ☐ Preparation for the CCENT or CCNA certification exam or to study CCNA Security
- ☐ Develop a working knowledge of routing, switching, network applications, protocols and services
- ☐ Networking fundamentals
- ☐ Advanced concepts

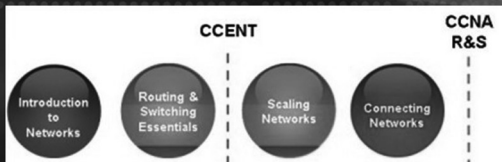


7

CCNA Routing & Switching Curriculums



- ☐ Introduction to networks
- ☐ Routing and Switching Essentials
- ☐ Scaling Networks
- ☐ Connecting Networks



8



CCNA Routing & Switching Curriculums

Introduction to Networks

- ☐ Exploring the network
- ☐ Configuring a Network Operation System
- ☐ Network Protocols and Communications
- ☐ Network access
- ☐ Ethernet
- ☐ Network Layer
- ☐ Transport Layer
- ☐ IP Addressing
- ☐ Subnetting IP networks
- ☐ Application Layer
- ☐ It's a network



9



CCNA Routing & Switching Curriculums

Routing & Switching Essentials

- ☐ Introduction to Switched Networks
- ☐ Basic Switching Concepts and Configuration
- ☐ VLANs
- ☐ Routing Concepts
- ☐ Inter-VLAN Routing
- ☐ Static Routing
- ☐ Routing Dynamically
- ☐ Single-Area OSPF
- ☐ Access Control Lists
- ☐ DHCP
- ☐ Network Address Translation for IPv4



10



CCNA Routing & Switching Curriculums Scaling Networks

- ☐ Introduction to Scaling Networks
- ☐ LAN Redundancy
- ☐ Link Aggregation
- ☐ Wireless LANs
- ☐ Adjust and Troubleshoot Single-Area OSPF
- ☐ Multiarea OSPF
- ☐ EIGRP
- ☐ EIGRP Advanced Configuration and Troubleshooting
- ☐ IOS Images and Licencing

11



CCNA Routing & Switching Curriculums Connecting Networks

- ☐ Hierarchical Network Design
- ☐ Connecting to the WAN
- ☐ Point-to-point Connections
- ☐ Frame Relay
- ☐ Network Address Translation for IPv4
- ☐ Broadband Solutions
- ☐ Securing Site-to-site Connectivity
- ☐ Monitoring the Network
- ☐ Troubleshooting the Network

12



- ☐ <http://www.cisco.com/web/learning/certifications/associate/ccna/index.html>
- ☐ <https://learningnetwork.cisco.com/community/certifications/ccna>
- ☐ <http://www.netacad.hu/hu/ccna-rs>
- ☐ <https://www.netacad.com/courses/ccna/>
- ☐ <http://www.training360.com/exams/Cisco-vizsga.aspx>



13



Thank you very much
for your attention!



Cisco Networking Academy
Mind Wide Open

Skills for today.
Skills for life.



PÉTER Attila

NATIONAL INSTRUMENTS – LABVIEW COMMUNICATIONS SYSTEM DESIGN SUITE



National Instruments
LabVIEW Communications System Design Suite

Péter Attila
Sales Manager

ni.com 1



“I need to quickly prototype ideas...but”

The Challenge	Why?
It takes too long to get from algorithm to a prototype The design process is too fragmented – the typical timeline with current industry tools is months to even years	Because of the architecture and tools The SDR architecture commonly requires computational elements on a general-purpose processor and FPGA, which require different skills and expertise



ni.com 2



Prototyping Is Critical for Algorithm Research



"Experience shows that the real world often breaks some of the assumptions made in theoretical research, so **testbeds are an important tool for evaluation under very realistic operating conditions**"

"...development of a **testbed** that is able to **test radical ideas** in a complete, working system is crucial"



NSF Workshop on Future Wireless Communication Research

ni.com

3



Software Defined Radio Architecture

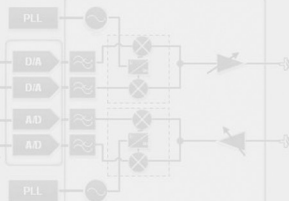
Multi-Processor Subsystem

- Real-time signal processor
 - Physical Layer (PHY)
 - ex FPGA, DSP
- Host processor
 - Medium Access Control (MAC)
 - Rx/Tx control
 - ex Host GPP, multi-core CPU



Host Connection
Determines Streaming
Bandwidth Ex. Gigabit
Ethernet, PCIe

Baseband
Converters



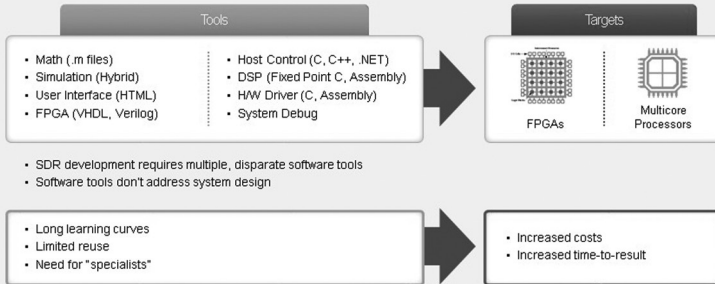
- RF Front-End
 - General Purpose RF
 - Dual LOs
 - Continuous Frequency Range

ni.com

4



Today's Development Challenge



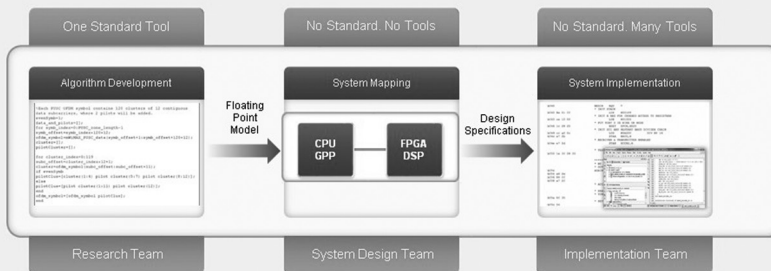
ni.com

5



The Challenge with Existing Tools

Disjointed path from concept to real-world signal



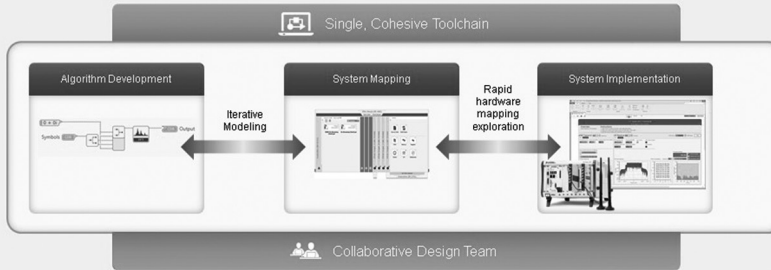
ni.com

6



The Ideal Solution

One continuous design flow that unifies the disparate design teams



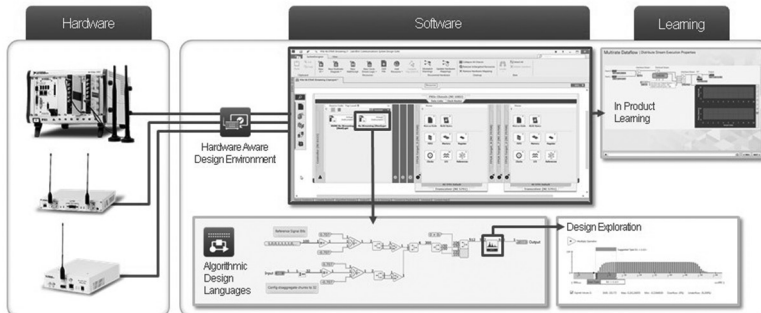
ni.com

7



LabVIEW Communications System Design Suite

The Revolution in Rapid Prototyping



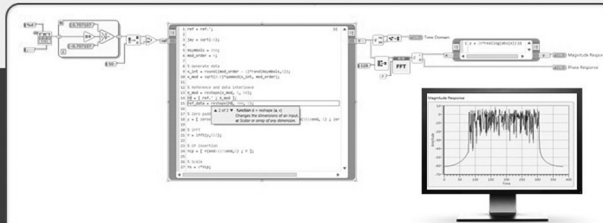
ni.com





Algorithm Design Languages

Processor



- Flexible design approach with dataflow (G), and text nodes for C and .m
- Text Nodes for C and .m support syntax highlighting and function completion
- Both G and the Text Nodes support full debugging with breakpoints and probes

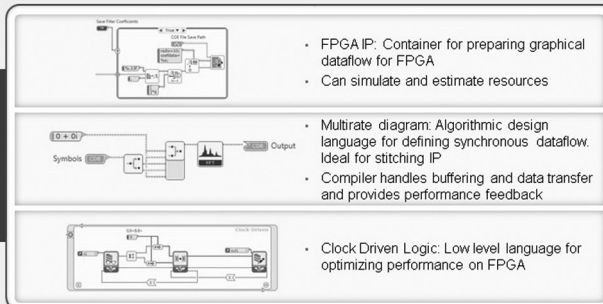
ni.com

9



Algorithm Design Languages

FPGA



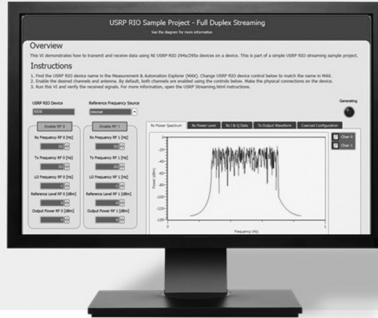
- FPGA IP: Container for preparing graphical dataflow for FPGA
- Can simulate and estimate resources
- Multirate diagram: Algorithmic design language for defining synchronous dataflow. Ideal for stitching IP
- Compiler handles buffering and data transfer and provides performance feedback
- Clock Driven Logic: Low level language for optimizing performance on FPGA

ni.com

10



System Implementation



Sample Projects: source code to start your design

- Synchronization and Timing Control across multiple RF Front-Ends & FPGAs
- Corrected RF, Arbitrary Rate Conversion, Frequency Shift



ni.com

11



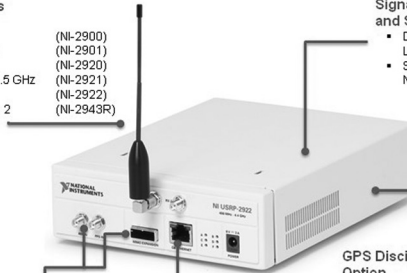
NI USRP Software Defined Radio

Tunable RF Front Ends

- Frequency Range
 - 70 MHz – 6 GHz (NI-2900)
 - 70 MHz – 6 GHz 2 x 2 (NI-2901)
 - 50 MHz – 2.2 GHz (NI-2920)
 - 2.4 – 2.5 GHz & 4.9 – 5.5 GHz (NI-2921)
 - 400 MHz – 4.4 GHz (NI-2922)
 - 1.2 GHz – 6 GHz 2 x 2 (NI-2943R)

Signal Processing and Synthesis

- Develop and explore algorithms with NI LabVIEW
- Simulate and process live signals with NI Modulation Toolkit



GPS Disciplined Clock Option

- Increased Frequency Accuracy

Multi Device Synchronization

- Easy 2x2 Synchronization
- Expandable to 8x8 or more

1 Gigabit Ethernet to PC

- Plug-and-play capability
- Up to 25 MS/s baseband IQ streaming

ni.com

12



SDR Components



Tx

- Digital to Analog
- RF Upconversion

· Modulation

Rx

- RF Downconversion
- Analog to Digital

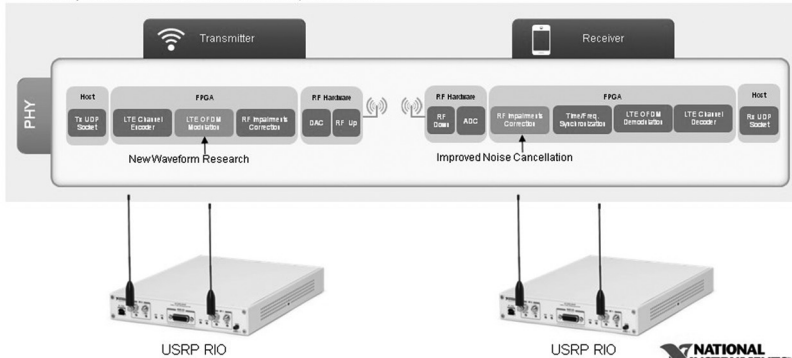
- Demodulation
- Signal Processing

ni.com



LTE & 802.11 Application Frameworks

Ready-to-Run Standards-Based Source Code Implementations



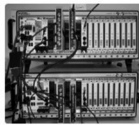
ni.com

14



NI Leading 5G Research and Prototyping

mmWave Cellular



Massive MIMO



LUND
UNIVERSITY

KU LEUVEN

New Waveforms



Alcatel-Lucent



TECHNISCHE
UNIVERSITÄT
DRESDEN



ni.com

15

NI USRP at Stanford University



STANFORD
UNIVERSITY



“

...with the NI USRP, we're able to provide exposure in introductory courses for the first time.

”

“

Students rated the class 4.94/5.0, likely making it one of the **highest ratings among all classes** in the School of Engineering at Stanford.

”

Dr. Sachin Katti

[Electrical and Computer Engineering]



ni.com

16

NÉMETH József Lajos

TURKEY AND STRATEGIC COMMUNICATION

Turkey and Strategic Communication

Dr. Jozsef Lajos NEMETH, PhD

National University of Public Service, Budapest, Hungary

CONTENT

Introduction

What is SC?

Remarkable features

Case Studies

Conclusion

HYPOTHESIS

In the last years Turkey's efforts to create and execute a comprehensive strategic communication system are visible in many forms: not just in actions taken by politicians, or using well-shaped messages for targeted audiences, but creating different think-tanks too.

WHAT IS STRATEGIC COMMUNICATION?

ORIGINS



**After 9/11
United States felt
misunderstood
politically and socially
by other nations and ethnic
and religious groups with
which it
had not maintained an
open flow of information.**

WHAT IS STRATEGIC COMMUNICATION?

GENERALLY

NATIONAL SECURITY

The diagram illustrates the components of the National Security Capabilities Compendium. A large box labeled "Capabilities Compendium" is shown on the left. To its right is a vertical stack of five smaller boxes, each containing a letter: "O", "I", "M", "E", and "I". Arrows point from each of these boxes to a list of capabilities on the right. The list includes "Diplomatic", "Informational", "Military", "Economic", "Law Enforcement", and "Intelligence".

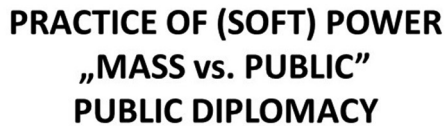
- Diplomatic
- Informational
- Military
- Economic
- Law Enforcement
- Intelligence

PRACTICE OF (SOFT) POWER

„MASS vs. PUBLIC”

PUBLIC DIPLOMACY

NATIONAL SECURITY

[illegible][illegible]

WHAT IS STRATEGIC COMMUNICATION?

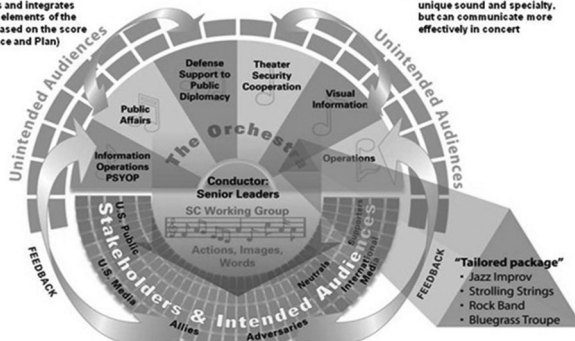
HOW DOES IT WORK?

Theory of SC -- like an orchestra
producing harmony



- Conductor (Senior Leader) coordinates and integrates the various elements of the orchestra based on the score (SC Guidance and Plan)

- All instruments retain their unique sound and specialty, but can communicate more effectively in concert



The selection, timing, and emphasis of SC instruments help orchestrate the message to stakeholders consistent with a desired effect or commander's intent. The Conductor must continuously adapt the score based on stakeholder feedback.

Source: <http://static1.squarespace.com/static/55324e15e440c396566e0a1f/55324e8de4b0323bd7301fa5a/55325262e4b0323bd731875b/1429381288890/orchestra/interpolate24Jun08.jpg?format=original>, date of download: 15 October 2015

STRATEGIC COMMUNICATION AND TURKEY GENERAL OVERVIEW

„The new dynamism and growth of Turkey as a regional power and a global actor must be communicated in an efficient and realistic manner to national and international audiences.“

„It reflects a new identity which the country wants to embrace to overcome its past mistakes and chart a new course for its social and political future.“

Source: Ibrahim Kalin: Soft Power and Public Diplomacy in Turkey, in: Perceptions, Autumn 2011, Volume XVI, Number 3., p. 17. and p. 12.

STRATEGIC COMMUNICATION AND TURKEY

GENERAL OVERVIEW

„The success in SC areas is indispensable for the sustainability of its national interests, regional effectiveness, and global responsibilities.”



STRATEGIC PRIORITY FOR TURKEY

Source: Ibrahim Kalin: Soft Power and Public Diplomacy in Turkey, Perceptions, Autumn 2011, Volume XVI, Number 3., p.18.

STRATEGIC COMMUNICATION AND TURKEY

GENERAL OVERVIEW

**Public diplomacy is a
strategic communication tool.**

**The most important role played by the national
and international public opinion.**

**Very important goal is to spread the
„story of Turkey” (brand building).**

Source: Ibrahim Kalin: Soft Power and Public Diplomacy in Turkey, Perceptions, Autumn 2011, Volume XVI, Number 3.

STRATEGIC COMMUNICATION AND TURKEY

CASE STUDY I – NGOs: STRATIM

„The main objective of STRATIM (est. in 2008) is to organize targeted events in accordance with Turkey’s national communication strategy towards specific target groups.”

Team members are (former) senior level (AKP) politicians and professors with deep internal and international experience and with wide communication knowledge.

Source: <http://www.stratim.org.tr/en/about-us.html>, downloaded: 15 October 2015

STRATEGIC COMMUNICATION AND TURKEY

CASE STUDY I – NGOs: STRATIM

TOOLS:

- **events (fex the Istanbul Forum from 2009)**
 - **programs (regional, youth, security)**
 - **network building (including METU)**
 - **permanent reflections**

Source: <http://www.stratim.org.tr/en/about-us.html>, downloaded: 15 October 2015

STRATEGIC COMMUNICATION AND TURKEY

CASE STUDY II – NATO and EU

NATO

Center of Excellence Combating Terrorism

(ANK, 2004)

„SC for Combating Terrorism” – workshop book (2009)

Turkey’s European Union

Communication Strategy (2010, 2014)

**covers a wide range of principles, target audiences,
sets up deadlines**

STRATEGIC COMMUNICATION AND TURKEY

CASE STUDY III – ECONOMY

STRATEJICO.

CORPORATE COMMUNICATION | CORPORATE INTELLIGENCE | CORPORATE RELATIONS

Its predecessor dates back to 1987 as

„Strategic Research and Planning Company”.

**In 2005 it was described „an international strategic
communications company”.**

**In 2012 gets „a strategic partnership with Marmara
Group Foundation to manage the
Eurasia Economic Summit”.**

Source: <http://www.stratejico.com/AboutUs.aspx>, downloaded: 25 April 2013

CONCLUSION

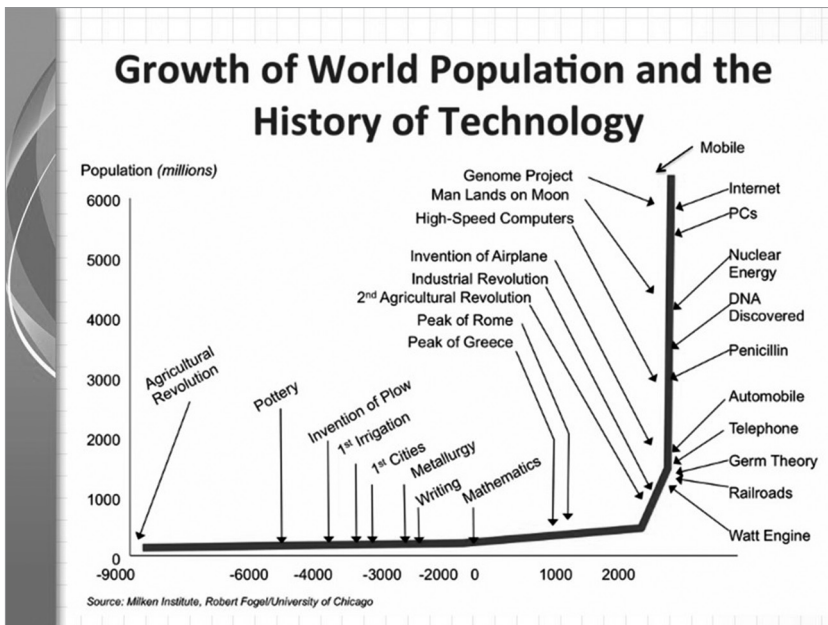
- SC exists in Turkey in different forms.
- Its national political content differs from its origins (GWOT), but these are playing very important role.
- Is this just a new layer to the existing ones?
- For the future SC will be important but maybe with a new feature, which sounds:
„synchronizing the messages through actions”.

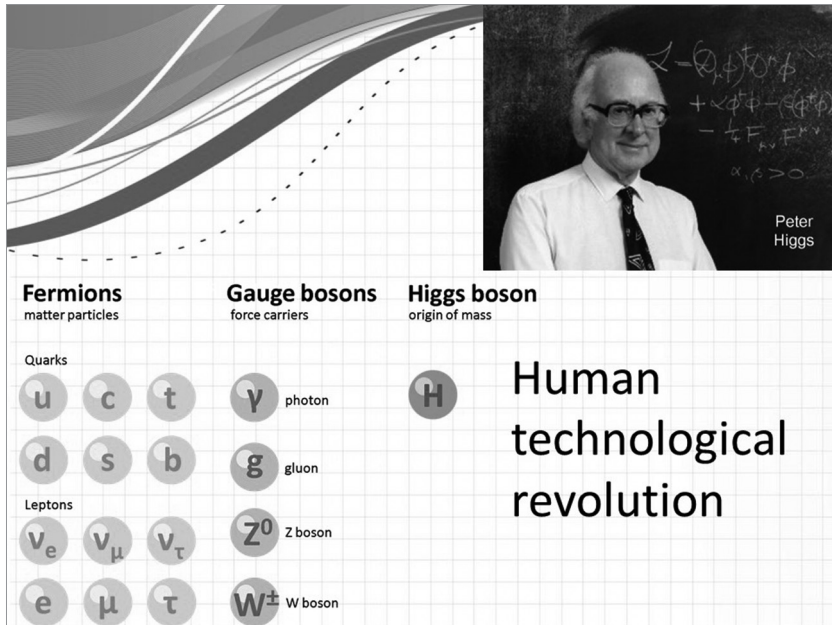
THANK YOU!

Dr. Jozsef Lajos NEMETH, PhD
National University of Public Service
Faculty of Military Sciences and Officer Training
Budapest, Hungary
E-mail: nemeth.jozsef@uni-nke.hu

FEKETE Károly

IS THERE ANY SINGULARITY WITHIN THE MILITARY COMMUNICATION?





Fermions
matter particles

Gauge bosons
force carriers

Higgs boson
origin of mass

Quarks

u c t

d s b

Leptons

ν_e ν_μ ν_τ

e μ τ

γ photon

g gluon

Z^0 Z boson

$W^\pm$ W boson

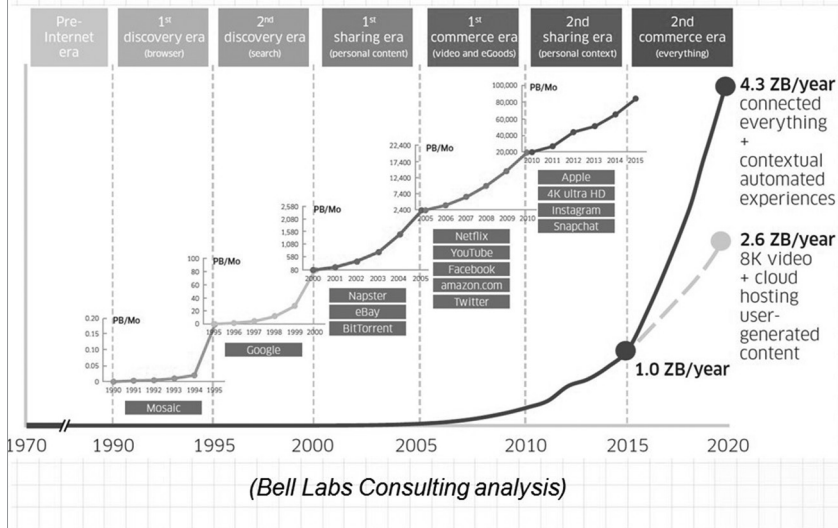
H

Human technological revolution

Technological revolutions

- Financial revolution 1600-1750);
- First Industrial revolution (1750-1850);
- Second Industrial revolution (1880-1920);
- Scientific-technical revolution (1940-1970);
- Information and telecommunications revolution (1980-2000);
- Cloud and Mobile revolution (2000- 2015).

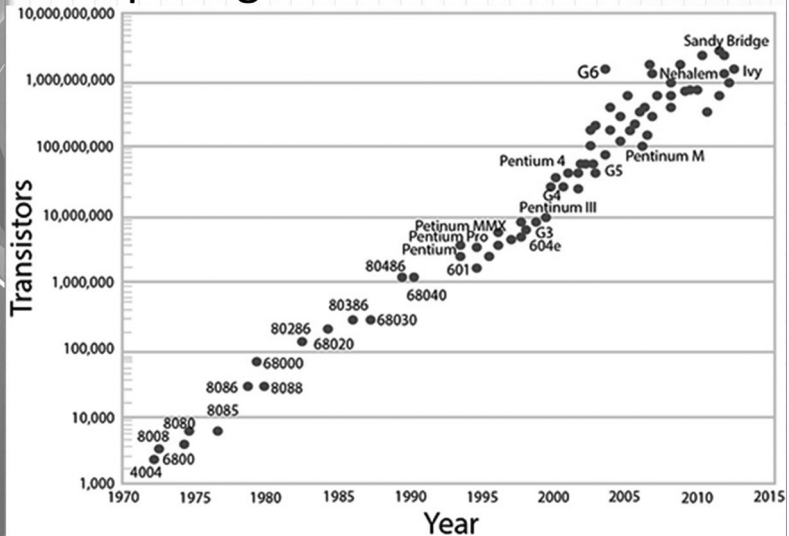
The growth in core network traffic



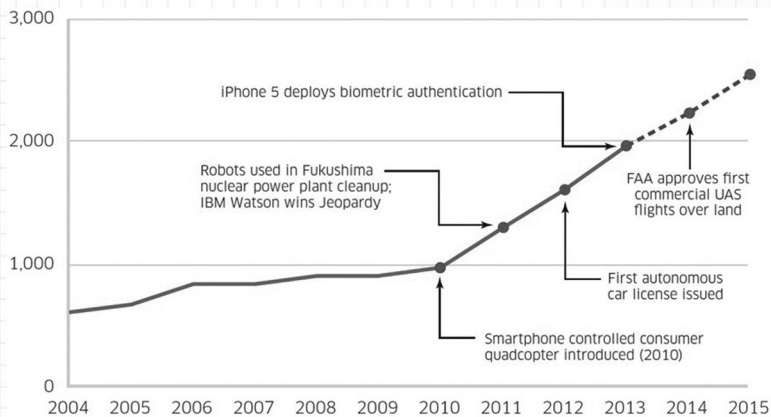
Nanotechnology

- Nano devices
- Nano pores
- Nano tubes
- Nano (molecular) circuits
- Nano materials & metallurgy
- Optical engineering
- Optical communications
- Energy storage
- Flexible electronics, wearable devices
- Micromechanical (Nano) sensors

Computing Power

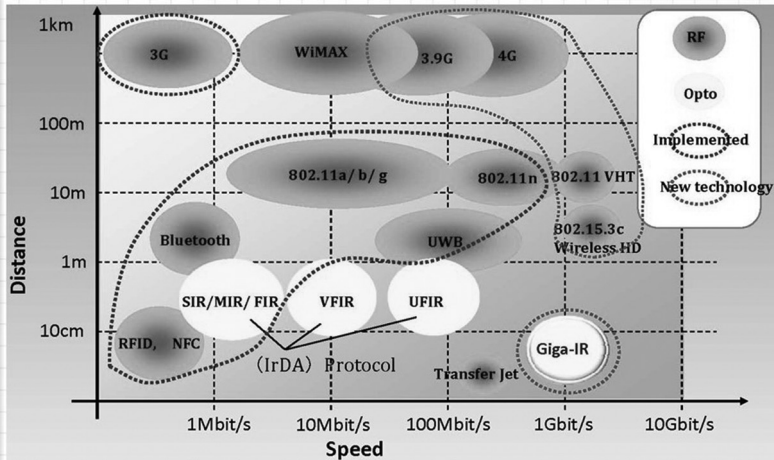


AI elements and investments



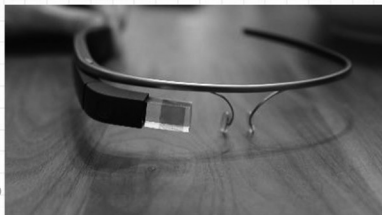
Source: Clark, J., 2015

Sped and distance comparison of different wireless protocols



Source: Kavehrad, M., 2014

COTS

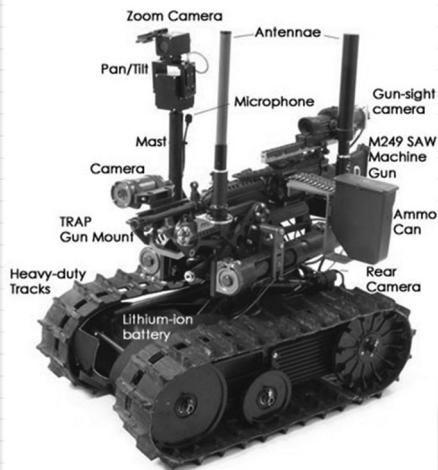


COTS

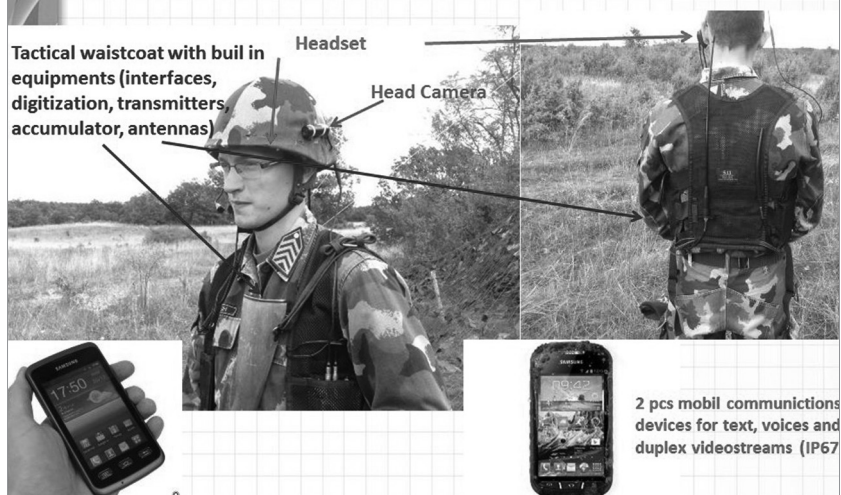


11

Military Tactical Robots, Throbots



Integrated wearable mobile data communications system



REFERENCES:

- CLARK, J., 2015. "I'LL BE BACK: THE RETURN OF ARTIFICIAL INTELLIGENCE," BLOOMBERG, BUSINESS, FEBRUARY 3 ([HTTP://WWW.BLOOMBERG.COM/NEWS/ARTICLES/2015-02-03/I-LL-BE-BACK-THE-RETURN-OF-ARTIFICIAL-INTELLIGENCE](http://www.bloomberg.com/news/articles/2015-02-03/i-ll-be-back-the-return-of-artificial-intelligence));
- MARCUS WELDON: THE FUTURE X NETWORK A BELL LABS PERSPECTIVE, CRC PRESS, TAYLOR AND FRANCAIS GROUP, BELL LABS & ALCATEL LUCENT, OCTOBER 22, 2015, ISBN 978-1-4987-5926-7
- RAY KURZWEIL: THE SINGULARITY IS NEAR, PENGUIN GROUP, 2006, ISBN 978-615-5229-26-8;
- MITCH BARNES, H.R. EVERETT, PAVLO RUDAKEVYCH: THROWBOT: DESIGN CONSIDERATIONS FOR A MAN-PORTABLE THROWABLE ROBOT, SPAWAR SYSTEMS CENTER, CODE 2371, 53560 HULL STREET, SAN DIEGO, CA 92152-5001, ROBOT WEST, 3485 SACRAMENTO DR. STE. C, SAN LUIS OBISPO, CA 93401, ([HTTP://CITESSEERX.IST.PSU.EDU/VIEWDOC/DOWNLOAD?DOI=10.1.1.62.2144&REP=REP1&TYPE=PDF](http://citesseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.2144&rep=rep1&type=pdf));
- VÁNYA LÁSZLÓ: HOGYAN VÉDEKEZZÜNK A DRÓNOK ELLEN?, REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK 25:(2) PP. 255-261. (2013), REPÜLÉSTUDOMÁNYI KONFERENCIA 2013. SZOLNOK, MAGYARORSZÁG: 2013.04.11 (NEMZETI KÖZSZOLGÁLATI EGYETEM)
- M. KAVEHRAD: BROADBAND WIRELESS LOCAL AREA NETWORKS, REMOTE SENSING, INDOORS NAVIGATION AND POSITIONING, THE CENTER FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY RESEARCH (CICTR), ([HTTP://CICTR.EE.PSU.EDU/RESEARCH/WC/](http://cictr.ee.psu.edu/research/wc/))



RÉPÁS Sándor

NYÍLT FORRÁSKÓDÚ KIBERBIZTONSÁGI SZOFTVEREK ALKALMAZÁSA KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME SORÁN

Nyílt forráskódú kiber-biztonsági szoftverek alkalmazása kritikus információs infrastruktúrák védelme során

Répás Sándor

Hálózati és hálózatbiztonsági tanácsadó

villamosmérnök MSc, közgazdász BA

CISA, CISM, CRISC, CCSI, MCT, CCNA, MCSE+I

Tartalom

- Bevezetés
- Licencek
- Zárt vs. Nyílt
- Jogszabályi háttér
- Példák
- Következtetések

Bevezetés

- Előtérbe került a kritikus információs infrastruktúrák védelme
- Új jogszabályi háttér, rengeteg feladat
- Szűkös anyagi erőforrások
- Kérdés: Alkalmasak-e a nyílt forráskódú kiberbiztonsági szoftverek a megkívánt szintű védelemre?

Nyílt forráskódú szoftverek

- Nyílt forráskódú (open source)
- Szabad szoftverek (free software)
- Szabad:
 - Futtatni bármilyen céllal
 - Tanulmányozni és módosítani
 - Másolatokat közzétenni
 - Tökéletesíteni és azt közzétenni



Két alapvető licencfajta

- Módosítás után:
 - Copyleft: azonos licencfeltételekkel terjeszthető
 - Permissive: eltérő licenc is alkalmazható

Néhány elterjedt licenc

- Apache License 2.0
- BSD 3-Clause "New" or "Revised" license
- BSD 2-Clause "Simplified" or "FreeBSD" license
- GNU General Public License (GPL)
- GNU Library or "Lesser" General Public License (LGPL)
- MIT license
- Mozilla Public License 2.0
- Common Development and Distribution License
- Eclipse Public License



Zárt vs nyílt

Zárt

- Magasabb egyszeri beruházási ktg.
- Magas szoftverkövetési díj
- Alacsonyabb üzemeltetési költség
- Gyártó függés kialakulása
- Fejlesztés megszűnése általában csak bejelentés után
- Gyártói támogatás beszerezhető
- Alacsonyabb közösségi támogatás
- Biztonsági célú kódelemzés általában kizárt
- Nem testre szabható, módosítható
- Forráskódhoz támadó általában nem fér hozzá
- Esetlegesen korlátozott jótállás kapható

Nyílt

- Alacsony beruházási ktg.
- Nehézkesebb frissítés telepítés?
- Magasabb üzemeltetési költség?
- Részbeni függés a fejlesztőktől
- Fejlesztés esetleges váratlan megszűnése
- Csak néhány gyártói támogatás, esetleg független szervezetektől
- Magas közösségi támogatás
- Biztonsági célú kódelemzés végezhető
- Tetszőlegesen módosítható
- Forráskódot támadó megismerheti
- Jótállás nincs

Néhány nyílt forráskódon alapuló termék

Gyártó és terméke	Alap	Típus
Sophos Email Appliance	FreeBSD	Biztonsági
McAfee SecurOS	FreeBSD	Biztonsági
Juniper JunOS	FreeBSD	Hálózati eszköz
Check Point IPSO	FreeBSD	Biztonsági
Cisco IronPort	FreeBSD	Biztonsági
Cisco Secure ACS	Linux	Biztonsági
Check Point SecurePlatform	Linux	Biztonsági
VMware ESX Server	Linux	Virtualizációs
genua genugate	OpenBSD	Biztonsági
Fox-IT DataDiode	OpenBSD	Biztonsági

Jogszabályi háttér

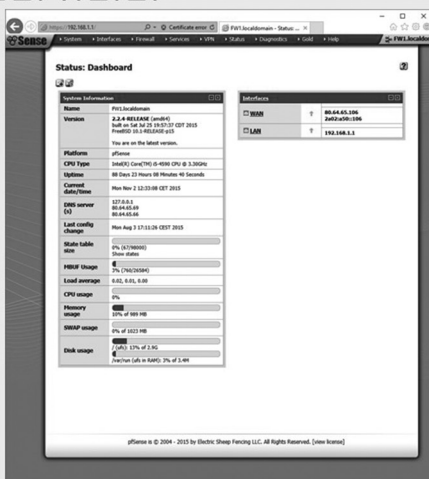
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (lrtv)
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (lbtv)
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (vhr)

Létfontosságú ágazatok

- Energia
- Közlekedés
- Agrárgazdaság
- Egészségügy
- Pénzügy
- Ipar
- Infokommunikációs technológiák
- Víz
- Jogrend – Kormányzat
- Közbiztonság – Védelem

Intézkedés 3.3.11.4.1.1.

- Az érintett szervezet az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat.
- Magyarázat: A hálózat kapcsolódási pontjait vírusvédelemmel kell ellátni.
- Lehetséges megoldás: pfSense+HAVP(+SslBump)



Intézkedés 3.3.11.5.1.1. és 3.3.11.5.1.2.

- Az érintett szervezet felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat; azonosítja az elektronikus információs rendszer jogosulatlan használatát.
- Magyarázat: A hálózatot behatolás detektáló, esetleg behatolás megelőző eszközzel kell védeni.
- Lehetséges megoldás: SNORT, vagy Suricata



Ferrás: snort.org



Ferrás: suricata-ids.org

Intézkedés 3.3.11.8.1.

- Az érintett szervezet sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.
- Magyarázat: Állományintegritás ellenőrző eszközt kell használni a számítógépeken.
- Lehetséges megoldás: OSSEC



Következtetések

- A szabad forráskódú biztonsági szoftverek hatékonyak a kritikus információs infrastruktúrák védelmére.
- Alkalmazásuk során ugyanazok a szabályok, mint más szoftverek esetén.
- Csak megbízható forrásból szabad letölteni.
- Letöltés után állomány integritásának ellenőrzés.
- Ajánlott a forráskódból a futtatható bináris előállítását saját hatáskörben elvégezni.
- Szinte minden kiber-védelmi feladatra van megbízható, szabad szoftver:
 - sokszor költséghatékonyabb, jobban az infrastruktúrához igazítható védelem

Köszönöm a figyelmet!

Répás Sándor

repa@ahol.com

<https://hu.linkedin.com/in/sandorrepas>