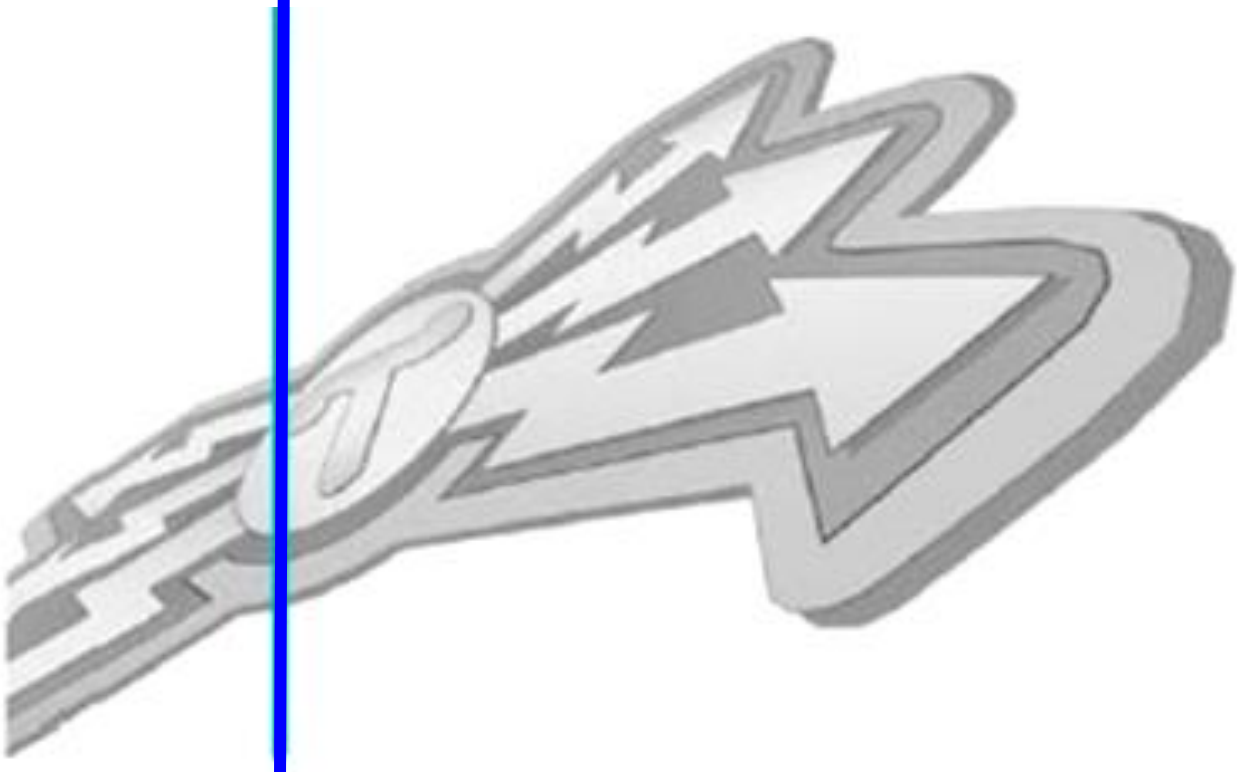
HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the National University of Public Service

6. évfolyam 2. szám
2015



2015. december 31.

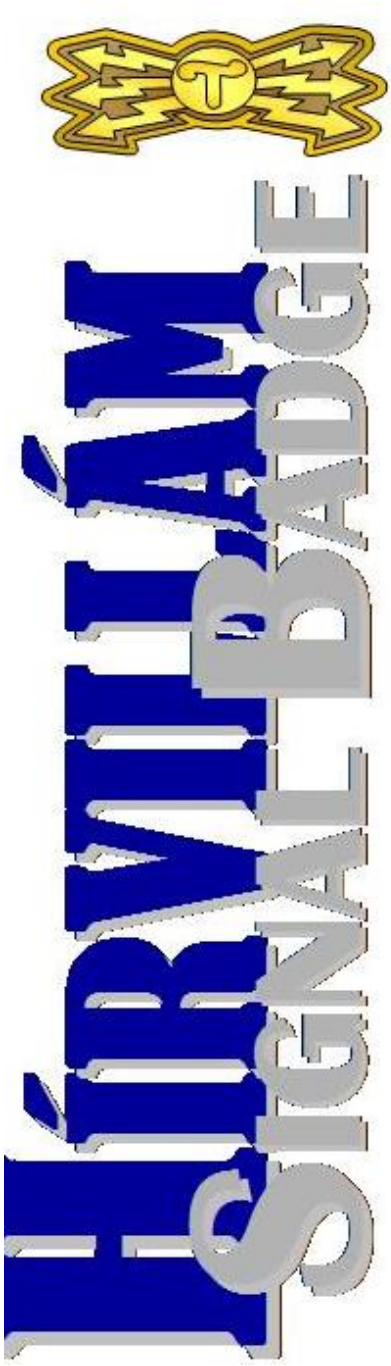
HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem Híradó Tanszék
tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement
at the National University of Public Service

Megjelenik évente két alkalommal
Published twice a year

6. évfolyam 2. szám

Budapest, 2015



HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-407 mellék)

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Ismét eltelt egy esztendő. Sikeredett szűkös erőforrásaink mellett, igen sok külső segítséggel és támogatással mindkettő szakmai-tudományos konferenciánkat eredményesen – *és megítélésem szerint sikeresen* – megrendezni.

Idén nyolc fiatal tiszt került a Híradók nagy családjába:

Bertók Ádám hdgy.	Szabó Gergő hdgy.
Domokos Máté hdgy.	Szabó Kristóf hdgy.
Gömör Réka hdgy.	Szabó Szilvia hdgy.
Kappeller Zsolt hdgy.	Szanyi Sándor hdgy.

Az ERASMUS mobilitási program keretében lehetőségünk volt egy fő – *most már negyedéves hallgató* – lengyelországi képzésére. Hasonlóan az elmúlt évhez, szintén az ERASMUS programnak köszönhetően a külföldi hallgatói részképzés mellett fiatal oktató kollégáink rendszeresen tartottak előadásokat társintézményeinkben a környező országokban, valamint különböző nemzetközi konferenciákon.

Sajnálatos módon tanszékünk állománya a tanév kezdete óta három kiváló oktatóval csökkent, ennek ellenére közösségünk továbbra is kész arra, hogy az újévben is folytassa oktatási, kutatási és tudományos munkáját szakmai kultúránk elmélyítése és hírnevünk bővítése érdekében.

Mindezen gondolatok jegyében kívánunk Boldog Újévet, illetőleg kellemes időtöltést az idei év második számának áttekintéséhez!

Budapest, 2015. december 31.

Kerti András
a Szerkesztőbizottság
elnöke

In Memoriam Dr. habil. Pándi Erik

Dr. habil. Pándi Erik, a Nemzeti Közszolgálati Egyetem egyetemi docense életének 45. évében tragikus hirtelenséggel elhunyt.
A Bolyai János Katonai Műszaki Főiskolát kitüntetéssel végezte el 1993-ban, majd 1996-ban az Eötvös Lóránd Tudományegyetemen szerzett egyetemi diplomát. 2005-ben „Summa Cum Laude" minősítéssel PhD fokozatot szerzett, majd 2010-ben a Zrínyi Miklós Nemzetvédelmi Egyetemen habilitált.
A rendőrségnél és a belügyi szerveknél mérnöki, alosztályvezetői, osztályvezetői, főosztályvezető helyettesi és főosztályvezetői beosztásokban tevékenykedett, egyúttal rendőrségi főtanácsos volt.
Az NKE-n és jogelődjén, a ZMNE-en főiskolai tanári és egyetemi docensi munkakörben egy évtizeden át oktatott és 2009-2012 között tanszékvezetői beosztásban látta el feladatát a Híradó Tanszéken.
Tudományos munkásságát több, mint százötven publikáció, jegyzet, tankönyv, tudományos periodikumok főszerkesztősége, pályázatok, tudományos konferenciák vezetése, hallgatók és doktoranduszok témavezetése fémjelzi.
Dr. habil. Pándi Erik egyetemi docens személye és kiemelkedő tudományos-szakmai tevékenysége nagy űrt hagyott hátra. Temetéséről később intézkednek.

Emlékét a Nemzeti Közszolgálati Egyetem és a Híradó Tanszék munkatársai kegyelettel őrzik.

MEGYERI Lajos: Nagy energiájú rádiófrekvenciás hullámok és lézerek katonai alkalmazási lehetőségei

Absztrakt
A modern nem halálos fegyverek kialakulása és fejlesztése elsősorban az elektronika fejlődésének és találmányainak köszönhető. A polgári életben használatos technológiák átalakításával olyan eszközök készíthetőek, melyek hatásosan alkalmazhatók élőerővel szemben, elkerülve az emberi élet kioltását és megtartva a célpontban lévő szinte valamennyi infrastruktúrát és haditechnikai eszközt. Jelen cikkben a szerző ismerteti a nem halálos fegyverek több fajtáját, valamint működési elvüket.

Abstract
The modern development of non-lethal weapons and the development and improvement is primarily due to the invention of the electronics.Transformation technologies for use in civil life of devices can be created, which can be used effectively against anybody, avoiding the loss of life and keeping almost all the infrastructure and equipment of military technology in the destination.In this paper the author describes the non-lethal weapons more basic types, and concept of operation.

Kulcsszavak: *nem halálos fegyver irányított energiájú fegyver, rádióhullámok, lézerek ~ non leithal weapon, directed energy weapon, radiowaves, lazer*

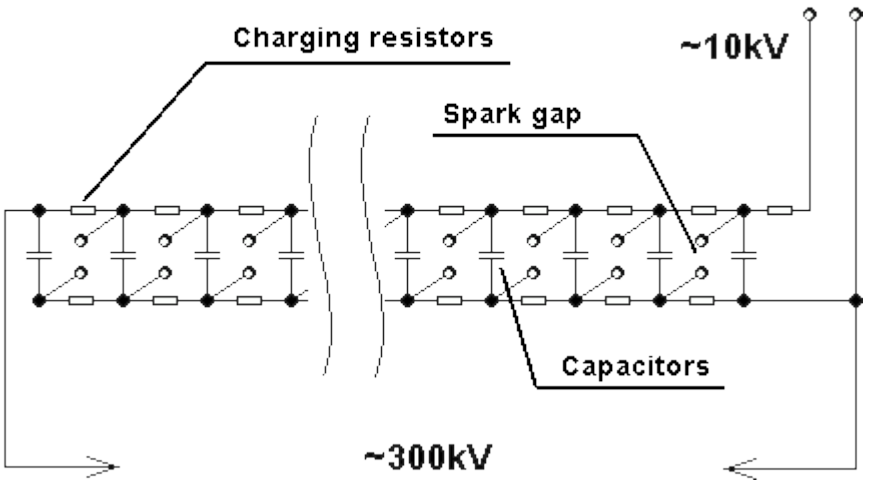
Nagy energiájú rádiófrekvenciás fegyverek

A nagy energiájú rádiófrekvenciás kisugárzások alkalmazásának célja elsősorban a félvezetők, integrált áramkörök túlterhelése, károsítása, a villamos alkatrészek szigeteléseinek átütése, végső soron az elektronikai eszközök tönkre tétele.

A nagy energiájú rádiófrekvenciás fegyverek általános felépítése:

Energiaforrás, mely a mikrohullámok generálásához szükséges nagy mennyiségű energiát előállítja, tárolja. Megvalósításának egyik változata:

- Marx generátor: Erwin Otto Marx találta fel 1924.-ben. Az Amerikai Szabadalmi Hivatalban 5,382,835 számon bejegyzett MARX generátor lényegében egy ellenállásokból, kondenzátorokból, és szikraközökből kialakított energiaforrás. Az áramkör nagyfeszültségre feltöltött kondenzátorok sorozata, amely nagyfeszültségű, (akár 2 MV) impulzusok előállítására alkalmas ns nagyságrendű ideig.



4. ábra Marx generátor működési elve [1]

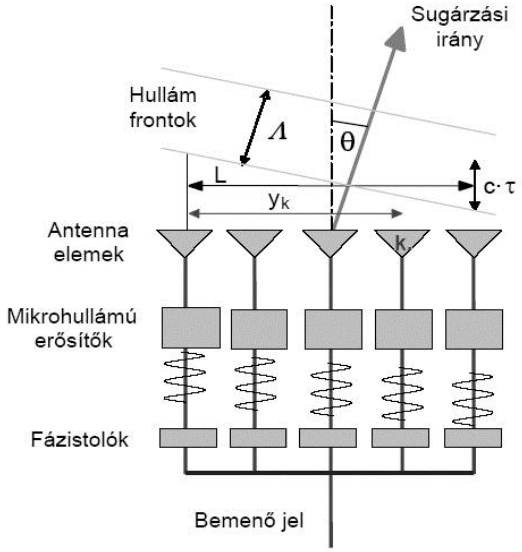
Alternatív energiaforrás lehet még a Magneto hidrodinamikus Generátor, amelyben az állandó mágneses térben áramló forró vezető anyag – gázplazma - nagy sebességgel való áramlása kelt nagy elektromos feszültséget.[2]

Mikrohullámú rezgéskeltő, amely a nagyfrekvenciás jeleket előállítja. Megvalósításának egyik változata a f**rekvencia-sokszorozó klisztron,** amely egy üregrezonátoros mikrohullámú elektroncső. Az üregrezonátor olyan rezgőkör, amelynek méretei összemérhetőek a hullámhosszal és a rezonancia-frekvenciájának megfelelő elektromos rezgések elektromágneses állóhullámokat keltenek bennük. A frekvencia-sokszorozó klisztronoknál a kimenőjel frekvenciája 10-15-szöröse a bemenőjel rezgésszámának, azonban a cső kimeneti teljesítménye és hatásfoka kicsi. Ezen klisztronfajtát nagy stabilitású, mikrohullámú jel előállításánál alkalmazzák oly módon, hogy egy kvarcoszcillátor jelét előbb hagyományos módon, majd a mikrohullámú tartományban frekvencia-sokszorozó klisztonnal sokszorozzák. Ez a sokszorozási elv 10 GHz-ig alkalmazható. A

frekvencia-sokszorozó klisztron könnyen felismerhető arról, hogy a katód felőli ürege nagyobb, mint a kollektor felöli kimenő ürege.[3]

Antenna, amely a generált mikrohullámokat a kívánt irányba sugározza ki. Lehetnek tölcsérsugárzók, helix antennák vagy egyéb speciális kialakítású antennák.

Fázisvezérelt antenna: A fázisvezérelt antennarendszerek sorban vagy 2 dimenzióban elhelyezett diszkrét sugárzó elemekből álló rácsok, melyekben a kibocsátott elektromágneses nyaláb irányítása és formálása, fókuszálása az egyes antennaelemekre adott jelek fázisának változtatásával történik, úgy, hogy az elemekről érkező hullámok a kívánt helyeken konstruktív interferenciával erősítik egymást, a nem kívánt helyeken pedig gyengítik, illetve kioltják egymást (destruktív interferencia).[4]



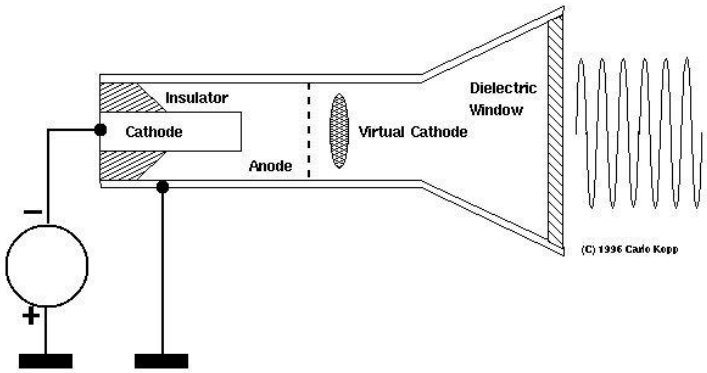
5. ábra Fázisvezérelt antennarács működésének vázlata [5]

L: az antenna hossza, y_k*:* a *k.*-ik elem koordinátája, *c:* a hullám terjedési sebessége, *Λ:* a hullámhossza, *ϑ:* a terjedési irány normálissal bezárt szöge, *τ:* az adott irányhoz tartozó maximális időkésleltetés

A kisugárzandó jelet az egyes antennaelemekhez tartozó fázistolókra kapcsolják, melyek fázistolása változtatható a kívánt nyalábalaknak és iránynak megfelelően. Szükség esetén a sugárzó elemek előtt erősítők is vannak.

Vircator (Virtual Cathode Oscillator)

Az axial vircator egyszerű felépítésű és a vircatorok közt a legnagyobb kimenő teljesítményt tudja biztosítani. A fedélzeti rádiófrekvenciás fegyverként képes impulzus jellegű energia kisugárzásra, többször felhasználható eszköz. Az impulzus idő általában µs nagyságrendű. Parabola vagy tölcsérsugárzó antennája segítségével irányított nyaláb formájában továbbítja az energiát.



6. ábra Axial Vircator elvi felépítése [6]

Működése: A katódból felgyorsult elektronáramlás indul az anód rácsa felé. Az elektronok nagy része átjut az anód rácson és buborékszerű vákuumot hoz létre az anód mögött. Megfelelő körülmények között ebben a felöltődött vákuumban mikrohullámú frekvencia képződik (oszcillálódik). Ha ez a vákuum egy rezonáns üregben jön létre, amelyik továbbvezeti, igen magas csúcsfeszültség érhető el. Hagyományos mikrohullámú mérnöki technológiával tovább növelhető a feszültség. A kimeneti teljesítmény 170 kW és 40 MW között lehet, a frekvencia a cm és dm hullámtartományba esik.[7]

Impulzus bombák

A nagy energiájú elektromágneses impulzus technológiája és a nagy energiájú mikrohullámú technológia eljutott arra a szintre, hogy a hagyományos E bomba technikailag is megvalósíthatóvá vált, új lehetőségeket nyitva az információs hadviselés területén.

„A Sivatagi Vihar” hadművelet légi műveletei során világossá vált, hogy a légi fölény elérésének egyik feltétele lehet az ellenség információs infrastruktúrájának a megzavarása, működésképtelenné tétele, megsemmisítése. Ezzel a művelettel elektronikusan „megvakíthatják” az ellenséget, ne legyen képes a légi célok azonosítására. A hadművelet első éjszakáján a hagyományos robbanófejjel ellátott bombázók túl elfoglaltak voltak ahhoz, hogy speciálisan az információs infrastruktúrát támadják, a célpontok kijelölése sem volt megvalósítható.
A modern ipari létesítmények elleni eredményes támadás feltétele speciális eszközök használata az információs rendszerek megsemmisítéséhez. Ebből a célból építették az elektromágneses bombát, mely nagyon hatásos az információs rendszerek megsemmisítésére.[8]

Elektromágneses impulzus hatás (Electro Magnetic Pulse - EMP):

Az elektromágneses impulzus hatását már a nagy magasságú nukleáris robbantások kezdeti szakaszában felfedezték. Ez a hatás egy gyors lefutású (200 – 400 ns), de intenzív elektromágneses impulzus, amely a nukleáris robbanás egyik hatásaként a robbantás helyétől növekvő gömbszerűen terjed. Az energiaimpulzus erős elektromágneses mezőt hoz létre, különösen a robbanás közelében. A mező olyan erős, hogy rövid életű tranziens feszültségeket hoz létre több kV feszültséggel az elérhető vezető anyagokon, vezetékeken, áramkörökön.

Katonai szempontból fontos, hogy véglegesen károsítja az áramellátó és elektronikai eszközök legtöbbjét, különösen a számítógépeket, rádiókat és radarokat.

Az átlagos számítógépek igen érzékenyek a nagyfeszültségű impulzusokra, mert alkatrészeik nagy része Metal Oxide Semiconductor (MOS) alkatrészekből áll. Ezeket az eszközöket nagyon kis energiájú, az eszköz belsejében néhány 10 V-ot elérő sugárzással tönkre tehetik. Az impulzusok elleni védekezés nem oldható meg teljes körűen, mert hiába árnyékolják le az eszközöket elektromos szempontból, a be és kivezető kábelek antennaként működnek és az eszközbe vezetik a kárt okozó feszültséget.

A számítógépes adatfeldolgozó rendszerek, híradó rendszerek, közúti és vasúti jelzőrendszerek, jelfeldolgozó egységek, repülésirányítási rendszerek, fedélzeti számítógép vezérlésű járművek potenciális áldozatai lehetnek az elektromágneses impulzus hatásának. Súlyosan sérülhetnek a telekommunikációs hálózatok, az azokat összekötő rézkábelek hosszától függően. A különböző vevőegységek különösen érzékenyek az EMP hatásaira, a kisméretű nagyfrekvenciás tranzisztorok és diódák könnyen sérülnek, rendszerint tönkre mennek a nagyfeszültségű impulzus hatására. Az elektronikai harc eszközeit,

műholdakat, valamennyi hullámsávban működő kommunikációs eszközt potenciálisan veszélyezteti az EMP impulzus.[9]

Az EMP sugárzás kétféleképpen, az „első ajtón" („Front-door"), és a „hátsó ajtón" („Back-door") hatolhat be egy rendszerbe. A „Front-door" behatolás antennán keresztül történik, így okozva károkat a hírközlő berendezésben, mely az antennához kapcsolódik. Ez akkor a leghatásosabb, ha az EMP frekvenciája egyezik a frekvenciával, melyen az adott berendezést, antennát üzemeltetik.

„Back-door" behatolás jön létre, amikor az EMP hatására a berendezés vezetékein, belső összeköttetésein tranziens áramok (alacsonyabb frekvenciákon), állóhullámok (magasabb frekvenciákon) alakulnak ki, és e vezetőkhöz kapcsolódó áramkörökben károk keletkezhetnek. A készülékek borításán kialakított hűtőréseken, ventillátor-réseken, a fémlemezek pontatlan illeszkedései mentén a mikrohullámú sugárzás könnyebben áthatol, mint az alacsonyabb frekvenciájú sugárzás.[10]

A nagy energiájú elektromágneses fegyverek közül az elektromágneses impulzusbomba (EMP) a leghatékonyabb. Az elektromágneses impulzusfegyverek hatékonyan vethetőek be elektronikus hadviselésben és légitámadás során. Az E-bombaként is ismert eszköznek vannak nukleáris és nem nukleáris alapú implementációi is. Az EMP fegyver nukleáris változata a nagy magasságban felrobbantott nukleáris töltet által keltett intenzív, de rövid ideig tartó elektromágneses mező hatásait használja ki. A robbanáskor keletkező több ezer voltos elektromágneses lökéshullám visszafordíthatatlan károsodást okoz a területen elhelyezkedő elektronikus eszközökben. A nem nukleáris elektromágneses impulzusfegyverek egyéb megoldásokat használnak a nagy energiájú elektromágneses lökéshullám előállítására.

Ezek a fegyverek kisebb hatóerővel rendelkeznek, de nincs radioaktív kiszóródásuk, így jobban alkalmazhatóak precíziós műveletekben. A tápenergiát előállító eszköz lehet a Marx generátor vagy a fluxus kompressziós generátor. A fluxus kompressziós generátor több MJ energiájú elektromos energiát képes előállítani rövid (10-100 μs) ideig. A viszonylag kisméretű eszköz több MW impulzusteljesítményű energiaforrásnak számít. Működési elve azon alapul, hogy egy induktív energiatárolóban tárolt elektromágneses energiát robbantással, a tekercs meneteinek rövidre zárásával áramimpulzussá alakítja.

Alkatrész típusa	Energia [J] (1 µs-os impulzussal)
GaAs MESFET	$10^{-7} – 10^{-6}$
MMIC	$7×10^{-7} – 5×10^{-6}$
Mikrohullámú diódák	$2×10^{-6} – 5×10^{-4}$
VLSI	$2×10^{-6} – 2×10^{-5}$
Bipoláris tranzisztorok	$10^{-5} – 10^{-4}$
CMOS RAM	$7×10^{-5} – 10^{-4}$
Műveleti erősítők	$2×10^{-3} – 6×10^{-3}$

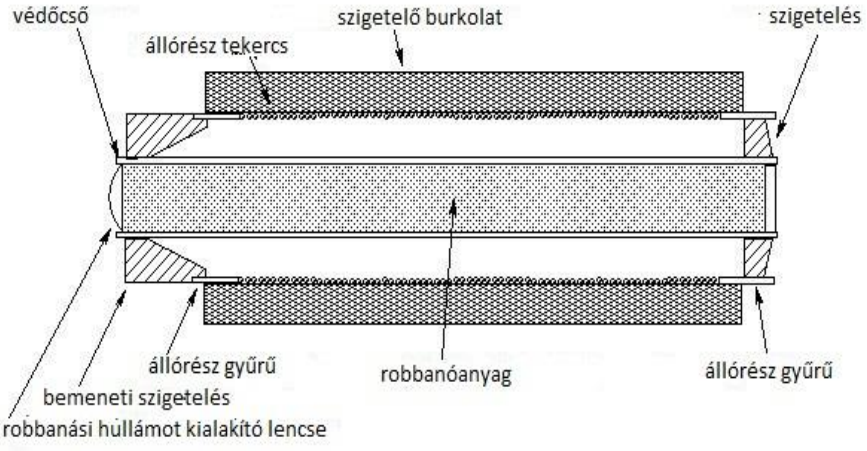
1. táblázat Elektronikus eszközök tönkretételéhez szükséges energiaszintek.[11]

Axiális FCG (Exposively Pumped Flux Compression Generator)

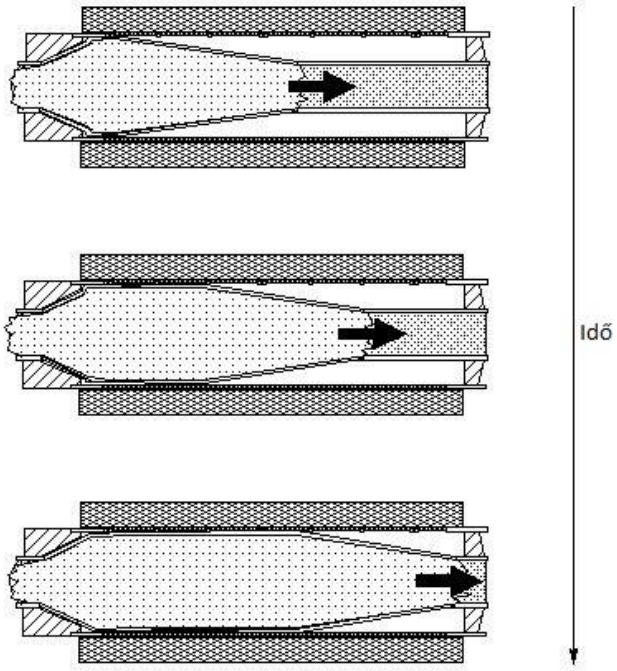
A legkiforrottabb technológiája a bomba formájú FCG–nek van. Elsőként Clarence Fowler mutatta be a Los Alamosi Nemzeti Laboratóriumban (LANL) az ötvenes évek végén. Azóta az FCG eszközök széles skáláját fejlesztették ki úgy az Egyesült Államokban, mint a Szovjetunióban.

Az FCG eszköz képes néhány 10 MJ energia előállítására 10-100 µs időtartamra viszonylag összetartó nyalábban. A csúcsteljesítmény szint néhány TW-tól néhányszor 10 TW terjed. Az FCG használható önállóan vagy egylövetű impulzus táp energia ellátást nyújthat egy mikrohullámú csőnek. Ez a teljesítmény kb. 10-100 - szorosa egy átlagos villám elektromos teljesítményének. Az axiális FCG eszköz felépítése látható a 7. ábrán.

A konstrukció alapötlete az, hogy nagy sebességű robbanó anyaggal, egy mágneses térrel rendelkező tekercs meneteit egymáshoz préselik a robbanás sebességével az eredeti mágneses mezőt ezzel hatalmas mértékben megnövelve. A kezdeti mágneses mezőt külső tápforrással biztosítják, például egy Marx generátorral.[12] Az FCG működése látható a 8. ábrán.



7. ábra Axiális FCG elvi vázlata [13]

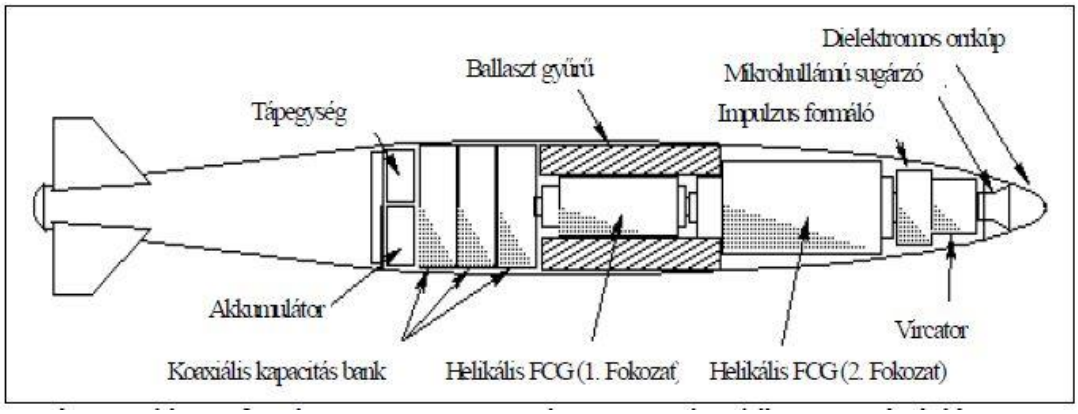


8. ábra Axiális FCG működése [14]

Az „E" bomba

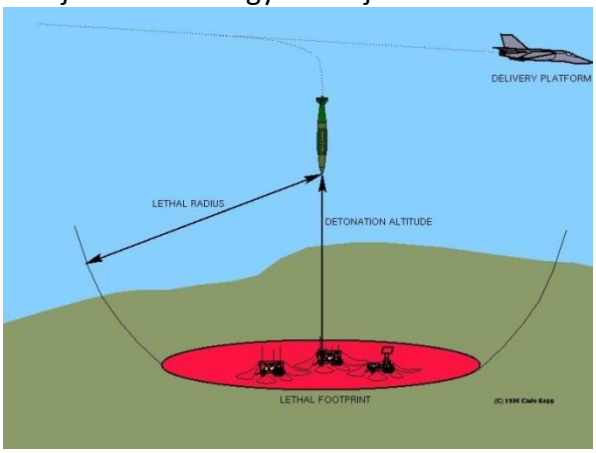
Az E- bomba tulajdonképpen az FCG vagy a Vircator alkalmazása hagyományos bombatestbe szerelve. Az E-bomba célba juttatására hordozó

repülőgépet, vagy cirkálórakétát használnak. A rendszer az alkalmazás szempontjából optimális magasságban végrehajtja a harci rész indítását, azaz az elektromágneses impulzus gerjesztését. Természetesen az elektronikai eszközökre gyakorolt hatás körzete jól meghatározható, mivel irányított sugarat állít elő, nem pedig magas légköri atomrobbantást. A nem kifejezetten célobjektumok védelme ez által biztosítható, a célok is szelektálhatóak, a felesleges rombolásokat a minimálisra lehet korlátozni.[15] A 8. ábra a Kétfokozatú fluxuskompressziós generátorral és Vircatorral rendelkező E-bomba felépítésének egy változatát mutatja be. A bomba tömege: 900kg, hossza: 3,84m, átmérője: 0,46 m.



9. ábra Kétfokozatú fluxuskompressziós generátorral és Vircatorral rendelkező MK 84 burkoltba épített E-bomba felépítése [16]

Az E – bomba célba juttatásának egyik módja látható a 10. ábrán:



10. ábra E- bomba célba juttatása és hatósugarának modellezése [17]

Az elektromágneses impulzus kézigránát

Az eszköz jelen pillanatban még csak terv, az Egyesült Államok pályázatot írt ki a kifejlesztésére. A HPM (High Power Microwave) gránátra azért lenne szükség, hogy elektronikát használó eszközöket semlegesítsenek vele szakszemélyzet nélkül, például egy házilag gyártott bomba detonátorát. Az elképzelés szerint akkorának kell lennie, amekkorát egy katona kézi erővel is mozgatni tud. A pályázati kiírásban megjegyezték: olyan eszközre lenne szükségük, ami 40 milliméteres gránátvetővel, RPG-vel, illetve Stinger, Hydra és Javelin típusú rakétavetőkkel is kilőhető. Az elképzelés bírálói szerint az előállítás aránytalanul drága lesz és a fegyver hatásfoka is kétséges, primitívebb technológiájú robbanó eszközökre nem lesz kellő hatással.

Az eszköz képzeletbeli változata már régóta létezik például a HALO vagy a Call os Duty számítógépes játékokban.[18]

A rádiófrekvenciás fegyverek elsősorban az elektronikus eszközöket támadják, semmisítik meg, Ebből a szempontból nevezhetjük ezeket akár humánus fegyvereknek is. Esetenként bizonyos teljesítménysűrűség mellett halált is okozhatnak. Mérettől és az alkalmazás módjától függően, harcászati, de akár hadműveleti jelentőségű műveletek sikeres végrehajtását is támogathatják.

Lézer fegyverek

A lézer: egy olyan fényforrás, amely indukált emissziót használ egybefüggő fénysugár létrehozására. Neve az angol Light Amplification by Stimulated Emission of Radiation kifejezés rövidítése, a laser magyarosításából származik. Az első lézert az amerikai Theodore H. Maiman fejlesztette ki 1960-ban.

A lézer előállításának fizikai alapjai:

A lézerek olyan fényforrások, amelyek igen vékony, nagyon kis széttartású fénynyalábot sugároznak ki, melyben a teljesítménysűrűség igen nagy lehet. A lézer egyszínű (meghatározott hullámhosszúságú) fényt bocsát ki. Ha egy atomban lévő elektront gerjesztünk, akkor az elektron általában rövid idő múlva alacsonyabb energiájú állapotba, gyakran alapállapotban ugrik, miközben az atom a két energiaszint különbségével megegyező energiájú fotont sugároz ki. Albert Einstein mutatta meg 1917-ben, hogy ez a kisugárzási folyamat egy ugyanilyen energiájú foton segítségével befolyásolható. Ezt a hatást indukált emissziónak nevezzük. A gerjesztett atomra ugyanolyan energiájú foton esik, mint amilyent magából kisugározna. A beesés pillanatában a beeső foton hatására azonnal megtörténik a

kisugárzás, ezért nevezzük a folyamatot indukált emissziónak (kibocsátásnak). Ilyenkor a beeső foton nem nyelődik el, hanem ugyanabban az irányban folytatja útját. A kisugárzott második foton is ugyanebben az irányban halad, az első fotonnal megegyező frekvenciával, sőt vele azonos fázisban. A beeső és a továbbhaladó fotonok szempontjából a jelenséget a foton megkétszereződésének tekinthetjük.

A lézerezés azt jelenti, hogy az indukált emisszió egymásután sokszor megtörténik. Így meghatározott frekvenciájú, azonos irányban haladó, egymással megegyező fázisú fotonokat, vagyis lézersugarat kapunk.

A lézerezés megvalósulásához néhány alapvető feltételnek teljesülnie kell. Először is egy aktív közegre, a lézeranyagra van szükségünk, amelynek atomjai vagy molekulái kisugározzák a fényt. Másodszor egy olyan módszerrel kell rendelkeznünk, amellyel a lézeranyag atomjainak jelentős számát gerjesztett állapotba hozhatjuk. A lézeranyag gerjesztési folyamatát pumpálásnak nevezzük. Végül meg kell találnunk a módját, hogyan érhetjük el, hogy a fény ne szökjön ki addig a lézeranyagból, amíg kellően sok indukált emissziós fotonkétszerezés nem történik. Ezt úgy valósíthatjuk meg, hogy a lézeranyagot úgynevezett optikai rezonátorba helyezzük, amelyben tükrökön verődik oda-vissza a fény. A tükrök közös tengelyének irányában kisugárzott fény sok további indukált emissziót okoz, míg a tengelytől eltérő irányú fény gyorsan elhagyja a rendszert.[19]

A lézer fény tulajdonságai:

- a létrejött fény időben és térben koherens, a lézer által kibocsátott hullámok fázisa a sugár minden keresztmetszeténél azonos;
- a lézernyaláb keskeny és nagyon kis széttartású nyaláb. A lézerfény nagyrészt párhuzamos fénysugarakból áll, nagyon kis szóródási szöggel. Ezzel nagy energiasűrűség érhető el szűk sugárban, nagy távolságokban is;
- a lézerek energiája kis térrészben koncentrálódik, a lézerfény teljesítménysűrűsége a megszokott fényforrásokénak sokszorosa lehet;
- a lézer által kibocsátott hullámok mágneses mezejének iránya állandó;
- a lézerek fénye egyszínű. A lézersugár egy olyan elektromágneses hullám, amely közel egyetlen hullámhosszú összetevőből áll.[20]

A lézerek polgári hasznosítása

Napjainkban nagyon sok lézert használunk, sokszor szinte észre sem vesszük. Ilyenek a CD-lejátszókban, DVD-kben, CD-írókban működő lézerek, vagy a lézernyomtatókban lévők. Ezek nem gázlézerek, hanem úgynevezett félvezető lézerek, amelyekben pontosan párhuzamos falúra csiszolt félvezető kristályok adják

a lézeres hatást. A párhuzamos falakat fémmel vonják be, ezek tükröznek. A pumpálás a félvezető átmeneti rétegekben történik, úgynevezett elektron-lyuk párok megsemmisülésekor keletkeznek a lézerezésre alkalmas fotonok.

Lézerek típusai és főbb felhasználási területük:

GÁZLÉZEREK: (GAS LASERS)

- Hélium-neon lézer (543.5 nm - 3.3913 µm) Holográfia, színképelemzés, vonalkód megvizsgálás, beigazítás, optikai demonstrációk.
- Argon lézer (488.0 nm - 528.7 nm) Retinális fotóterápia (cukorbetegségért), kőnyomás, más lézerek pumpálása, litográfia.
- Kripton lézer (416 nm - 799.3 nm) Tudományos kutatás, argonnal keverik, hogy fehér-világos lézereket hozzon létre, szórakoztató műsorok.
- Xenon-ion lézer (UV és IR tartományban széles spektrum) Tudományos kutatás.
- Nitrogénlézer (337.1 nm) Más lézerek pumpálása, légszennyezés mérés, tudományos kutatás, rezonátorüreg nélkül működhetnek.
- Széndioxid-lézer (10.6 µm, 9.4 µm) Anyagok vágása, olvasztása, sebészet, anyagmegmunkálás.
- Szénmonoxid-lézer (2.6 - 4 µm ; 4.8 - 8.3 µm) Fotó akusztikus színképelemzés, vágás, hegesztés.
- Excimer lézer (193 nm* (ArF), 248 nm* (KrF), 308 nm* (XeCl), 353 nm* (XeF)) LASIK, sebészet, félvezető gyártáshoz használják még.

VEGYI LÉZEREK: (CHEMICAL LASERS)

- Hidrogén-fluorid lézer (2.7-2.9 µm) Lézer fegyver kutatás, MW (megawatt) tartományban
- Nehézhidrogén-fluorid lézer (3.6 - 4.2 µm) MIRACL, pulzált energialövedék, taktikai nagy energiájú lézer.
- Kémiai oxigén-jód lézer (1.315 µm) Lézerfegyverzet, tudományos anyagkutatás, az U.S.-ben a hadsereg lézere, megawatt tartományban megy.

SZILÁRDTEST LÉZEREK (SOLID-STATE LASERS)

- Rubin-lézer (694.3 nm) Holográfia, tetoválás eltüntetés, minden idők első lézere.
- Nd:YAG (1.064 µm ; 1.32 µm) Anyagalakítás, vágás, lézeres célkijelölés, sebészet, kutatás, zöld lézer pumpálás, impulzusos, gyakori.
- Nd:YCOB Nd:YCa4O(BO3)3 (Neodymium ittrium kalcium oxoborát) (1.060 µm) Nagy fényerejű zöld lézerekhez használják.
- d:Glass (Üveg) (1.062 µm ; 1.054 µm) Extra nagy teljesítményen használják (terrawatt) fúziós segédlézer, 3. felharmónikusát használják.
- Ti:sapphire (Titánium zafír) (650m-1100nm) Színképelemzés, LIDAR, kutatás, ultraerős ultarövid impulzusok IR tartományban.
- Tm:YAG (Túlium YAG) (2.0 µm) LIDAR

- Yb:YAG (Itterbium YAG) (1.03 µm) Kilowattos folyamatosüzem, telekommunikáció, 25% elektromos hatásfok, hegesztés, vágás.
- Ho:YAG (Holmium YAG) (2.1 µm) Szöveteltávolítás, vesekő eltávolítás, fogászat.

FÉLVEZETŐ LÉZEREK (SEMICONDUCTOR LASERS)

- AlGaAs (0.63 µm-0.9 µm) (Alumínium-germánium-arzenid) Optikai lencsék, lézer pointerek, telekommunikáció, CD-olvasó lézer (780nm), pumpálás
- InGaAsP (1.0 µm-2.1 µm) (Indium-germánium-arzenidfoszfát) Telekommunikáció, más lézer pumpálása, gyógyászat, megmunkálás.
- Ólomsó (3 µm-20 µm) Függőleges üregfelszín emittáló lézer (VCSEL) (850 nm-1500 nm) Telekommunikáció.
- Kvantum-kaszkád lézer (közép IR -től mély IR -ig) Kutatás, ütközés-elkerülés-radart tartalmazhatnak, ipari-folyamatvezérlés, és orvosi diagnosztika, mint például a lélegzetelemzők.
- Hibrid szilikon lézer (közepes IR) [21]

Kis energiájú lézerek (Dazzler)

Szem káprázтatására, ideiglenes vakításra, használnak a látható fény tartományában működő lézereket, szakmai szóhasználattal dazzlereket (dazzling /káprázтató/ lézer). A kis energiájú lézer „reflektor” átmenetileg megzavarja az ellenséget arra kényszerítve, hogy forduljon el a fényforrástól vagy hunyja be a szemét. Megfelelően kiképzett állomány számára ez az idő elegendő, hogy a szükséges ellenintézkedéseket megtegye.

A SABER 203

Saber 203 laser illuminátor átmenetileg rontja az ellenség tűzkiváltó képességét. A lézer hatásos hatótávolsága kb. 200-300 m. A vezérlő egység félvezető alapú lézert használ, az átalakított 40 mm-es gránátvetőbe szerelve. A lézert egy gránát betöltési mozdulattal lehet a helyére rögzíteni, és a vezérlő egység oldalán lévő gombbal lehet működtetni a lézert, ami egy folyamatos sugárként világítja meg a célt. Vészhelyzetben azonnal kivehető és a gránátvető eredeti feladatának ellátására azonnal alkalmas

A SABER-203 alkalmazása során megfigyelték, hogy az eszköz még pótlólagos pszichés elrettentő hatással is rendelkezik. Ugyanis, amikor a célszemély rájön, hogy megvilágították, és fegyver irányul rá, általában elrejtőzik vagy elmenekül. Az eszközt a Directed Energy Directorate (DE) of the U.S. Air Force Research Laboratory (AFRL) fejlesztette ki 2005-ben [22]

A dazzling lézereket a személyeken kívül technikai eszközök optikai elemeinek vakítására is használhatják. Telepítésük bármilyen járműre lehetséges. A rendszer hatékonysága stroboszkópikus fényhatással kombinálva, növelhető. Optikai érzékelők ellen alkalmazva képes infravörös tartományban is működni. Lehetséges védekezési mód az ilyen fegyverek ellen keskenysávú optikai szűrők alkalmazása, melyek a lézer frekvenciáján szűrik a fényt.

A SaberShot „photonic disruptor" (Laser Dazzler), nagy felbontású föld lézert használ, hogy átmenetileg megvakítsa és összezavarja az ellenséget nagy mélységben. Az eszköz rendszeresítve van az Egyesült Államok haderőinél. A Dazzlerek a legkülönbözőbb formákban léteznek, a toll méretűtől, melynek hatótávolsága 200 m, a pulzáló típusoké 500 m, a puska méretűig, melynek hatótávolsága eléri a 2 km-t [23].

9. kép SABER 203 Lézer fényvető M-203 gránátvető csövében [24]

Elektrolézerek

Az elektrolézer az elektrosokk fegyverek egyik fajtája. Lézer segítségével egy elektromosan vezető plazma csatornát (laser-induced plasma channel LIPC) hoznak létre a levegőben. A lézer nagyon rövid időre felforrósítja a levegőt a céltárgyig, ionizálja a levegőt. Ha elég intenzív a lézersugár, az elektromágneses mezője elég erős ahhoz, hogy elektronokat szakítson ki a levegő molekuláiból ezáltal elektromosan vezető plazmacsatornát képez a céltárgy irányába.
Egy 10^{-12} s ideig tartó nagyfeszültségű impulzust küldenek át a vezetővé vált plazmacsatornán a célba. Az impulzus feszültségétől függően lehet halálos vagy nem halálos az energiaszint. Az ilyen nagyfeszültségű impulzusok kisülése látható a

10. képen. A lézer segítségével továbbított energia (Laser Guided Energy LGE™) technológiáját 2002-ben kezdték kifejleszteni az amerikai Applied Energetics cégnél a USA védelmi minisztériumával kötött szerződés alapján az USA tengerészete és légiereje számára. Napjainkban arra törekednek, hogy finomítsák az LGE rendszereinek használhatóságát és alkalmassá tegyék katonai alkalmazásra. Technológiákat dolgoznak ki az IED-k (Improvised Explosive Device - házi készítésű robbanó szerkezet) semlegesítésére. Az LGE lehet a következő lépés ebben a fontos misszióban, lehetővé téve az IED –k semlegesítését biztonságos távolságból. [25]

A témában jelenleg publikáltan az amerikai Picatinny Arsenal cég folytat kutatásokat, a fegyver elkészültéről nincs hivatalos információ [26]

10. kép Nagyfeszültségű kisülés a LIPC csatornán, a mesterséges villám kísérlet [27]

Vakító lézerek, lézerfegyverek repülő önvédelmi alkalmazásban

A repülő eszközök ellen alkalmazott infravörös keresőrendszerű rakéták keresőfejének zavarására kifejlesztett aktív eljárás.

Guardian

2003 novemberében egy utasszállító repülőgép elleni rakétatámadás miatt a DHL az összes repülőgépét kivonta a bagdadi repülőtérről. A rakétát nem egy másik repülőről vagy stabil telepítésű rakéta kilövő állványról, indították, hanem egy vállról indítható rakétát használtak, melyet egy, legfeljebb két fős személyzet is képes kezelni. Hasonló támadást hajtottak végre az al-Qaida terroristái egy izraeli gépet fenyegetve felszállás közben a kenyai repülőtéren 2002 év végén.

Annak ellenére, hogy az incidensekben senki nem halt meg, a szakértők szerint csak idő kérdése, hogy százak haljanak meg egy hasonló támadásban. A

katasztrófaveszély arra késztette a Nemzetvédelmi Minisztériumot, hogy egy három éves projekt keretében kifejlesszenek egy utasszállító gépeken használható rakétavédelmi rendszert.

A Guardiant úgy tervezték, hogy önállóan működjön, a repülő személyzet beavatkozása nélkül. Egy érzékelő szenzorsor felfedezi a közeledő rakétát,amely a repülő felé közeledik, és az információt továbbítja az infravörös pozíció azonosító kamrának. A rendszer számítógépe elemzi a bejövő jeleket, hogy azonosítsa a veszély valódiságát ezután közvetlen infravörös lézersugarat bocsát a közeledő objektumra. A lézer hamis célinformációt jelenít meg a rakéta irányító-rendszerében, így az elfordul a repülő irányától. Az észlelés, behatárolás, zavarás műveletek együttes ideje 2-3 s. A rendszer automatikusan jelzi a pilótának és a légiirányító központnak, hogy zavarást váltott ki egy fenyegetésre.

A rendszer egy külső, 460 mm (18 inch) hosszú konténer, súlya 250 kg (550 lb) és ezt a repülő törzse alá függesztik fel. Ez látható a 11. képen. A konténer levehető és másik repülőre átszerelhető egy óra alatt. A rendszer 1 millió US$ repülőgépenként. A Northrop Grumman cég, a rendszer fejlesztője úgy becsüli, a rendszer megvásárlása utasonként körülbelül plusz egy dollárral emeli meg a jegy árát utazásonként.

A Guardiant az AN/AAQ-24 Nemesis rendszerből fejlesztették, amely egy katonai, irányított infravörös ellentevékenységi rendszer. Elemei: rakéta előjelző rendszer, integráló egység, lézer torony. 1997-ben készült el és 2000. évben állították rendszerbe a kisméretű, merevszárnyas gépek és helikopterek védelmére. [28]

11. kép A Guardian rakéta elhárító rendszer konténere a repülő orra alatt [28]

Becslések szerint, mintegy 700 000 vállról indítható rakéta (MANPAD) készült a világon számos országban. Sajnos több ezer darab ellenőrizetlen helyen van, fekete piaci kereskedelembe került, ahol akár terroristák is megvásárolhatják viszonylag olcsón. A vállról indítható rakéták legfőbb célpontjai a repülőgépek, amelyek különösen sebezhetőek fel illetve leszálláskor. Eddig körülbelül 1000 civil áldozata van az ilyen típusú támadásoknak.

Átégető típusú lézerek, nagy energiájú lézerek

Polgári célú alkalmazás:

Nagy teljesítményű lézer fejes vágóeszközöket alkalmaznak a legkülönbözőbb, elsősorban fémvágó, aprító gépekben.

Tudományos kutatásokban használják például a jövő sugárkezelése, az úgynevezett hadronterápia kutatáshoz, amelynek során a rákos daganat nyeli el a rá irányított energia nagy részét, a környező sejtek pedig kevesebbet kapnak a sugárzásból.

Fehérjemolekulák belső szerkezetét is vizsgálhatják vele, amiből a gyógyszerkutatás profitálhat. Az anyagkutatásban a lézerfizika által lehetővé tett kísérletek olyan felfedezésekhez vezethetnek, amelyek a nukleáris reaktorok öregedési folyamatainak lassítását teszik lehetővé. Elemek átalakítását, a radioaktív hulladékok kezelésének problémáit is kutathatják

A nagy energiájú lézerek fejlesztése az 1960-as években kezdődött egy sor tudományos áttörés és mérnöki találmány eredményeképpen. Kezdetben a fő problémát az okozta, hogy a lézerek előállításba pumpált kW vagy MW energiáknak csak néhány 10 százaléka hasznosult, a többi hő veszteséggé vált.

Az USA légierejének légi szállítású lézer laboratóriumában (US Air Force Airborne Laser Laboratory) fejlesztették ki elsőként a használható kémiai lézer technológiát YAL-1A ABL néven, 1977-ben.[29]

A népszerű nézet szerint a nagy energiájú lézer (HEL High Energy Laser) a célra irányítva elpárologtatja azt. A valóságban ez nincs teljesen így. Különleges technológiai eljárásokkal bonyolult eljárásokkal tudnak csak valóban hatásos és bevethető HEL fegyvert készíteni.

A HEL–nek van a legnagyobb esélye a közeljövőben, hogy nagy jelentőségű eszközzé váljon. Jelenleg a sugárfegyverek bár emlékeztetnek a sci-fi birodalmára, terjedelmük és magas áruk miatt még nem tartoznak a hadseregek általánosan használt eszközei közé.

A nagy energiájú lézer, fegyver, mint rendszeresített eszköz a nagyhatalmak fegyvertárában, napjainkban bukkant fel. Ezek az eszközök különleges lehetőséget nyújtanak célpontok támadására fénysebességgel. Hatásosan támadhatók vele a legkülönbözőbb fegyver típusok, különösen a ballisztikus eszközök. Ezek a fegyverek nem működnek minden időjárási körülmények között egyformán, leghatásosabbak tiszta és száraz időben.

A nagyhatalmak folyamatosan nagy erőfeszítéseket tesznek a nagy energiájú szilárdtest lézerek előállítására, amelyek a lézer diódák alkalmazását jelentik majd. Ha megvalósul, nagyot lendít majd a lézer eszközök katonai alkalmazhatóságán kisebb súlya egyszerűbb kezelhetősége, szélsőséges viszonyokat jobban tűrő képessége miatt. Jelenleg a megoldandó probléma az, hogy a megépíthető 25 kW-os lézer esetében a betáplált teljesítmény 90 százaléka hő veszteséggé válik, és ezt a hőt el is kell vezetni az eszközről.

Az Egyesült Államok 1983-ban bejelentette a Stratégiai Védelmi Kezdeményezést (Strategic Defense Initiative - SDI), mely csillagháborús program néven vált ismertté.

Fő célkitűzése az volt, hogy kifejlesszen és telepítsen egy Föld és űrvédelmi rendszert abból a célból, hogy megvédje az Egyesült Államokat a nukleáris ballisztikus rakéták támadástól. Három lépcsős védelmi rendszert terveztek. Első lépcsőben a támadó rakéta megsemmisítése az indításkor, a repülés középső illetve végső fázisában, az okozott hatás minimalizálására. A tervekben földi telepítésű lézer fegyverekkel, az űrben telepített tükrök segítségével célozták volna meg az ellenséges rakétákat.

A technikai megvalósításra még legalább tíz év kutatómunkára lett volna szükség. Hazai és nemzetközi politikai nyomásra, tekintettel a várható kiadásokra a kezdeményezés már a kezdetkor kudarcra volt ítélve. A rendszer nem készült el és nem alkalmazták. Az alkalmazott újítások és tudományos eredmények azonban részét képezik a ma használatos rakétaelhárító rendszereknek.[30]

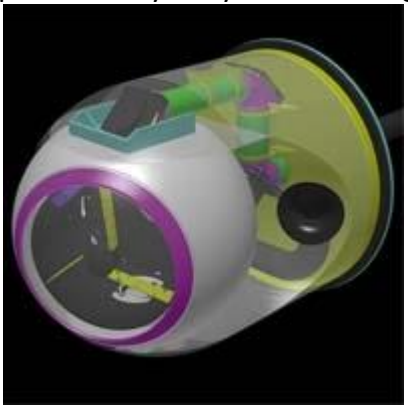
Légiszállítású lézer AL-1A Airborne Laser (ABL)

A hidegháború befejeződésével, a stratégiai védelmi kezdeményezés leállt, de néhány terv túlélte. 1996-ban az Egyesült Államok légiereje szerződést kötött a Boeing – TRW és Lockheed Martin cégekkel egy ABL rendszer prototípusának elkészítésére egy Boeing 747 repülőgépen. Az elkészült ABL repülőgép látható a 12. képen. Az ABL MW teljesítményű lézerrel és az atmoszférikus torzítást kiegyenlítő rendszerrel készült, ami lehetővé tette a ballisztikus rakéták indítási fázisban történő megsemmisítését.

12. kép Boeing/TRW/LM YAL-1A Airborne Laser Concept (USAF) [29]

Az ABL rendszer védelmi hatóköre több száz km átmérőjű kör, amelyben képes megsemmisíteni az elindított ballisztikus rakétákat az indítási fázisban, amikor a legkönnyebben észlelhetőek és legsérülékenyebbek.

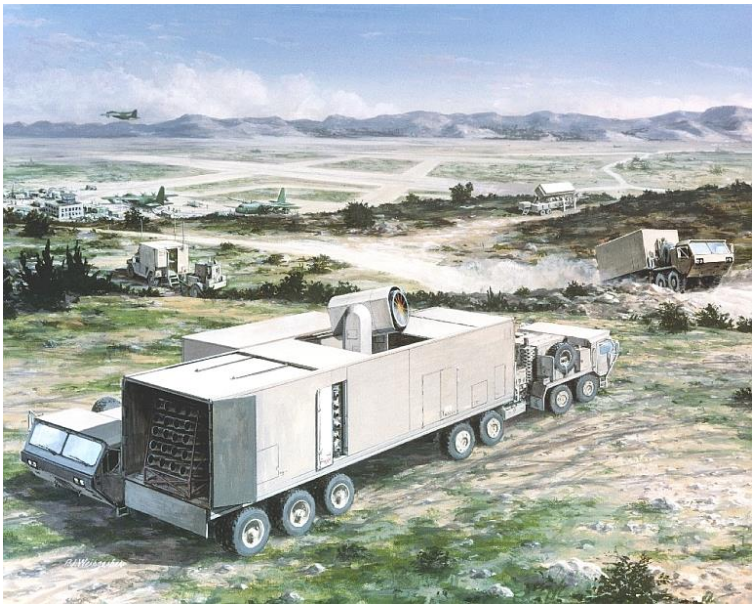
A terv szerint a repülőgépet a ballisztikus rakéta indításával fenyegető ország határára küldenék, hogy megsemmisítse a ballisztikus rakétákat még az indítás helyén. A fegyver 20-40 rakéta megsemmisítésére alkalmas a 12-18 órás bevetés alatt. Az ABL másik alkalmazása az alacsony pályán keringő felderítő és kém műholdak tönkretétele vagy megsemmisítése. Legfeltűnőbb jellegzetessége az ABL-nek a gép orrába épített optikai torony melybe az elsődleges lézer tükröt szerelték.



13. kép COIL torony a tükörrel [29]

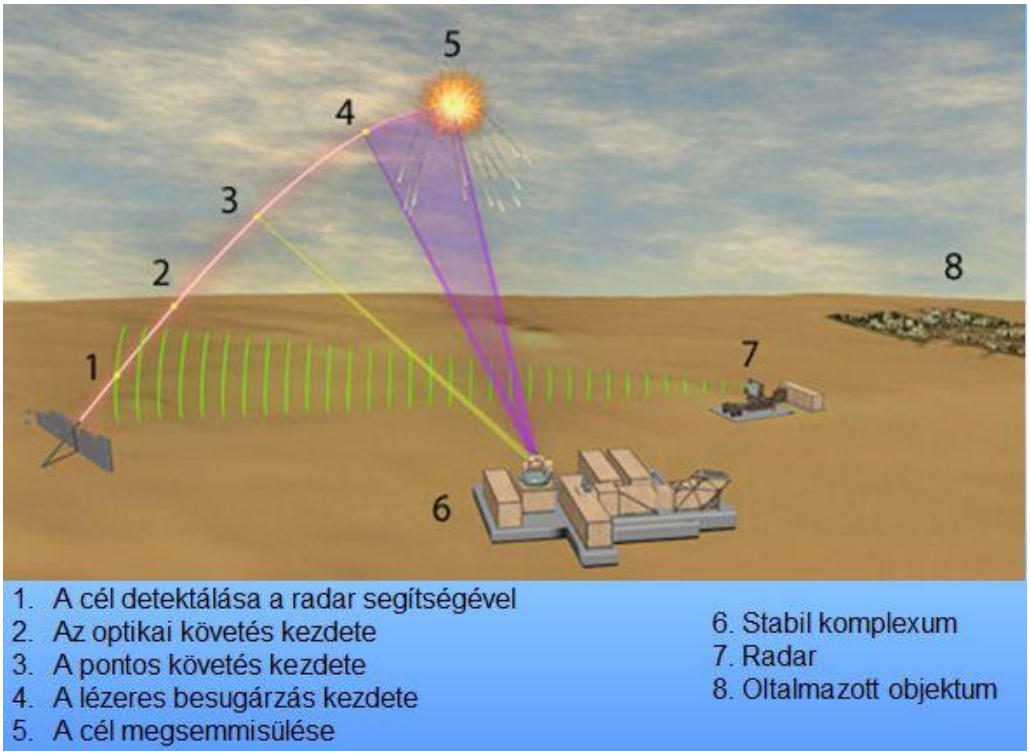
Taktikai, nagy energiájú lézer (Tactical High Energy Laser) (THEL)

A THEL lézer fegyvert az USA és Izrael közösen fejlesztette ki 1996-ban. Két változata van, a stabil telepítésű és a mobil változat. (MTHEL). A mobil változat a 14. képen látható.



14. kép Mobil telepítésű THEL [29]

A fejlesztés célja az volt, hogy megsemmisítsen tüzérségi rakétákat (Katyusa), tüzérségi gránátokat, aknavető gránátokat, alacsonyan szálló repülőgépeket. 2000 és 2004 között tesztelés alatt megsemmisítettek vele 122mm és 160 mm-es Katyusa rakétákat, különböző tüzérségi lövedékeket beleértve aknavető sorozatokat is.



11. ábra A THEL rendszer működésének vázlata [29]

A THEL rendszer deutérium fluorid kémiai lézert használ. Ezt a típusú lézert elsőként az USA tengerészeti erőinél alkalmazták MIRACL (Mid-Infrared Advanced Chemical Laser) néven. 1983-tól kezdve széles körű tudományos kutatást folytattak Új Mexikóban, a nagyenergiájú, MW nagyságrendű, lézer létrehozására.

A kutatások eredményeként született a THEL, amely fázisvezérelt radarokat használ a célok felderítésére és a lézer sugár irányítására. A THEL viszonylag kis hatótávolságú eszköz, a védendő terület határán kell telepíteni, szemben más nagyobb hatótávolságú védelmi rendszerekkel. mint például a SAM (Surface to Air Missile).

Fejlett taktikai lézer (The advanced tactical laser) (ATL)

Az Egyesült Államok katonai programja olyan nagy energiájú lézerfegyver kifejlesztésére, amely elfér egy V-22 kétrotoros konvertiplánon vagy egy C-130 repülőgépen. A lézer az Airbone Laser továbbfejlesztése, hatótávolságát 20 km-re tervezik. Hatásosan alkalmazható cirkáló rakéták és nagyobb tüzérségi lövedékekkel szemben. A lézer MW teljesítményű oxigén ionid (COIN) típusú.[36]

A rendszert többször tesztelték, harci alkalmazásra még nem áll készen. A berendezés nagy mérete, óriási energia szükséglete, és annak alacsony fokú hasznosítása, kis hatótávolsága mind kiküszöbölendő probléma, melyeket a nagy energiájú szilárdtest lézerek kifejlesztésével terveznek megoldani.[29]

A lézer fegyverek alkalmazása napjainkban már elérhető technológia, de a jövő tudományos felfedezései tovább növelhetik majd jelentőségét a katonai alkalmazások terén Jelenleg a kinetikus energiájú fegyvereket még nem váltotta le ez a modern technológia. Taktikai és harcászati szintű műveletek sikeres megvívását már ma elősegíti a lézer fegyverek alkalmazása, elsősorban az ellenséges rakéták elleni védekezés tekintetében.

Összefoglaló

Az irányított energiájú fegyverek a modern kor eszközei, a tudományos felfedezésekkel párhuzamosan folyamatosan tökéletesednek illetve új fegyverfajták jelenhetnek meg. Nagy előnyük, hogy többségükben skálázható a hatásuk, az irritáló kellemetlen hatástól a nagy energiájú átégető lézerekig. Ez a felhasználási területek széles skáláját teszi lehetővé. A nem halálos fegyverek lehetőséget biztosítanak a parancsnokok, katonák számára a háborús és nem háborús katonai műveletek végrehajtása során amikor a hagyományos fegyverek alkalmazása valamilyen oknál fogva nem lehetséges, katonailag nem indokolt, nem célszerű, vagy alkalmazásuk túlzott mértékű lenne.

A nagy energiájú rádiófrekvenciás fegyverekre jellemző, hogy hatását szinte kizárólag az elektromos berendezésekre fejti ki. Az elektronikai berendezésekre nézve visszafordíthatatlan károsodásokat okoz. Az ilyen fegyvert használó támadónak nincsen szüksége arra, hogy ismerje támadott rendszert, a hatás visszafordíthatatlan, akkor is kárt okoznak a célrendszerben, ha azok nem működnek (kikapcsolt állapotban vannak, vagy áramtalanítottak)

Ezeknek a fegyvereknek a széleskörű alkalmazását ma még a bonyolult felépítésük gátolja, még nem működnek minden körülmények között megbízhatóan, legalábbis a kinetikus energiát használó, hagyományos fegyverekkel szemben. Az Egyesült Államok rakéta védelmi stratégiája is még a hagyományos kinetikus töltetet hordozó rakéták használatát részeríti előnyben.

Az elkövetkező években az irányított energiájú fegyverek alkalmazásának jelentősége tovább növekszik majd. Az információs infrastruktúrák folyamatos térhódításával, a katonai vezetési pontok, illetve a harcmező informatizálódásával óriási mértékben megnőtt a katonai vezetési – irányítási rendszerek sérülékenysége

egy esetleges impulzus jellegű támadással szemben. Egy ilyen jellegű támadással szembeni védekezés költséges és teljes mértékben nem is zárhatja ki a rendszerelemek sérülését. Véleményem szerint a fentiek alapján kijelenthető, hogy a 21. század nagy technikai áttörését a katonai alkalmazásokban az irányított energiájú fegyverek jelentik majd.

Felhasznált irodalom

[1] http://www.physicsexperiment.co.uk/content/marx.html 2015-12-21
[2] http://www.vilaglex.hu/Fizika/Html/MHDGener.htm 2013-04-15
[3] http://www.elektroncso.hu/cikkek/mikrocso.php 2013-04-15
[4] Reményi Judit „Optoelektronikai eszközök és információ-technológiai alkalmazásaik” PhD értekezés, Budapest, 2005. BME;
[5] Reményi Judit „Optoelektronikai eszközök és információ-technológiai alkalmazásaik” PhD értekezés, Budapest, 2005. BME;
[6] http://www.globalsecurity.org/military/library/report/1996/apjemp.htm2013-04-15
[7] http://www.globalsecurity.org/military/library/report/1996/apjemp.htm 2013-04-15
[8] http://www.globalsecurity.org/military/library/report/1996/apjemp.htm 2013-04-17
[9] http://www.globalsecurity.org/military/library/report/1996/apjemp.htm
[10] D. Curtis Schleher, „Electronic Warfare in the Information Age”, Artech House Publishers, ISBN-13: 978-0890065266; pp.471-478.
[11] D. Curtis Schleher, „Electronic Warfare in the Information Age”, Artech House Publishers, ISBN-13: 978-0890065266; pp.471-478.
[12] Copp Carlo: Information Warfare - Cyberterroism: Protecting Your Personal Security in the Electronic Age" by Winn Schwartau, 1996 Thunder's Mouth Press, 632 Broadway 7th Fl, New York, New York, ISBN: 1-56025-132-8, http://www.infowar.com
[13] http://www.airpower.maxwell.af.mil/airchronicles/cc/apjemp.html alapján 2013-04-17
[14] http://www.airpower.maxwell.af.mil/airchronicles/cc/apjemp.html 2013-04-17
[15] Bartha Tibor mk ezredes A nem halálos fegyverek és alkalmazásuk lehetőségei az MH nem háborús műveleteiben PhD értekezés 60. oldal Budapest 2005.

[16] Bartha Tibor mk ezredes A nem halálos fegyverek és alkalmazásuk lehetőségei az MH nem háborús műveleteiben PhD értekezés 60. oldal Budapest 2005.
[17] http://www.airpower.maxwell.af.mil/airchronicles/cc/apjemp.html 2013-04-17
[18] http://www.wired.co.uk/news/archive/2012-11/21/hpm-grenades 2013-04-17
[19] http://tudasbazis.sulinet.hu/hu/termeszettudomanyok/fizika/fizika-11-evfolyam/a-rontgensugarzas-es-a-lezer/a-lezer 2013-04-18
[20] http://hu.wikipedia.org/wiki/L%C3%A9zer 2013-04-17
[21] http://www.omegalabs.eu/html/lezer_tipusok.html 2013-04-17
[22] http://www.defensereview.com/new-laser-technologies-for-infantry-warfare-counterinsurgency-ops-and-le-apps/ 2013-04-18
[23] http://www.defense-update.com/products/s/sabershot.htm 2013-04-18
[24] http://www.defensereview.com/new-laser-technologies-for-infantry-warfare-counterinsurgency-ops-and-le-apps/ 2013-04-18
[25] http://www.appliedenergetics.com/default.aspx/laser-guided-energy 2013-04-20
[26] http://www.army.mil/article/82262/ 2013-04-20
[27] http://defense-update.com/features/du-1-05/NLW-DEW.htm 2013-04-20
[28] http://science.howstuffworks.com/guardian.htm 2013-04-19
[29] http://www.ausairpower.net/APA-DEW-HEL-Analysis.html 2013-04-20
[30] http://www.coldwar.org/Articles/80s/SDI-StarWars.asp 2013-04-20

NYIKES Zoltán: A „Nagy Adat”, mint a létfontosságú rendszerek része

Absztrakt

Napjaink információ mennyisége és annak szükséglete óriási mértékben növekszik, az évek alatt megsokszorozódik. A kritikus infrastruktúra biztosítja az állam és polgárai jólétét. A mindennapi döntéshozatalok, egyre több és különböző információt igényelnek. A publikációban a Big Data és a kritikus infrastruktúra kapcsolata kerül bemutatásra. Az elmúlt időszakban a Big Data megjelenése és alkalmazása nagy hangsúlyt kapott. A publikáció bemutatja a Big Data jelenséget, fogalmi és gyakorlati szinten. Bemutatásra kerül a Big Data története. Megvizsgálásra kerül az alkalmazásának feltételei és lehetőségei, mely az elkövetkezendő időszak gazdasági növekedését fogja szolgálni. Bemutatásra kerül a Digitális Nemzeti Fejlesztései Program, ami Magyarország kormányzata és az Európai Unió finanszírozásában létrejövő fejlesztés, amely a magyar társadalom jólétét növelő beruházás, melynek alkalmazásával a Big Data mindenki számára könnyebben elérhető digitális szolgáltatás lehet. Megvizsgálásra kerül Big Data kockázati a biztonsági tényezői, melyek elengedhetetlenek a kritikus infrastruktúra védelemének, és a személyes adatok védelmének hatékony biztosításához.

Abstract

In the article the writer shows the connection between Big Data and Critical Infrastructure. He deals with the history of Big Data, the possible use of it, which supports the near real time economic growth.

Kulcsszavak: *Big Data, nagy adat, adatvagyon, adatfelhalmozás, 4V modell, adatgyűjtés, adatfeldolgozás, adatkezelés, adatvagyon-gazdálkodás, smart city, okos város, Digitális Nemzeti Fejlesztési Program, szupergyors internet, digitális közösség, digitális gazdaság, E-közigazgatás, digitális kompetencia, Nemzeti Digitális Közmű*

1. Mi az a Big Data?

Az ipari társadalmat a XX. század végén felváltotta az információs, tudásalapú társadalom. Ez a változás jelentősen átalakította a mindennapjainkat. A rengeteg digitális eszköz használat a *90-es* évektől kezdődően, egyre több és több digitális adat generálódását, felhalmozódását eredményezte. Mai világunkban már a

terabájt és a *petabájt* fogalmak lassan hétköznapivá váltak, válnak. Aki az információs technológiával foglalkozik, annak már nem idegenek az *exabájt* és a *zettabájt* fogalmak. Ezek már akkora adattömegek, amelyek feldolgozása, tárolása komoly infrastruktúrát és erőforrás-bevonást igényel. Ezen adattömegek, illetve a hozzá kapcsolódó tevékenységek összefoglaló elnevezésekén megjelent a *„Big Data"*fogalom, mely napjainkban egyre divatosabb kifejezéssé kezd válni.

1.1 Adataink és méretei

Ahhoz, hogy ezeknek az irdatlan adat tömegeknek jobban szemlélhetőbbek legyenek, az alábbiakban néhány példán keresztül bemutatásra kerül az adatok mennyisége.

- Egy gépelt oldal megközelítőleg 30 kilobájt adatot jelent.
- Egy MP3[1]-as zeneszám 5 megabájtot jelent.
- Egy mozifilm megközelíti az 5 gigabájtot.
- Egy terabájt adat becslések szerint 6 millió könyv tárolását teszi lehetővé.
- Hogyha 1 petabájt adatot DVD[2]-kre kellene kiírni, akkor úgy 55 emeletnyi DVD-t kellene beszerezni hozzá.
- A 2003-as esztendőben a világon körülbelül 5 exabájt adat keletkezett.
- Ez a szám 2011-ben már 1.8 zettabájtra emelkedett a világ adattermelése vonatkozásában.

A további példa elgondolkodtató és ijesztő a jövőre nézve. Az NSA[3] által a 2013-as év végén átadásra került új adatközpont Utahban[4] 1 yottabájnyi adat tárolására alkalmas.
Az Intel[5] cég 2013-as felmérése alapján, az interneten percenként 640 terabájt adat továbbítódik, amely 204 millió e-mail-t, több mint 3 millió keresést, 6 millió Facebook bejegyzést, 30 órányi videó feltöltést és 1,3 millió videó megnézését

1 MP3; egy veszteséges tömörítésen alapuló, zene tárolására használt fájlformátum,

2 DVD - „Digital Versatile Disc"; digitális sokoldalú lemez, amely körülbelül 4,7 GB adatot képesek tárolni egy rétegen,

3 National Security Agency (Nemzetbiztonsági Ügynökség); az Amerikai Egyesült Államok rádióelektronikai hírszerző szervezete,

4 Az Amerikai Egyesült Államok 45. állama

5 Intel Corporation egy eredetileg amerikai vállalat, mely mára nemzetközivé nőtte ki magát. Elsősorban mikroprocesszorairól ismert.

jelent a YouTube[6]-on, illetve 50 gigabájtnyi adat termelődik percenként a Large Hadron Collider[7] esetében. [3]
Belátható, hogy ez a rengeteg adat olyan tekintélyt parancsoló, hogy érdemben illik vele foglalkozni.

2. A Big Data jelenség

Az élet természetes velejárója, hogy mindig új és újabb dolgokat kell kitalálni, vagy éppen régieket átfazonírozva újnak beállítani. Az informatikai piac is előszeretettel dob be könnyen megjegyezhető kifejezéseket, melyek mögé trendet és természetesen terméket, szolgáltatást is társít. Korunk egyik ilyen hívószava a *Big Data* lett, amelyről nem kisebb dolgot állítanak a szakemberek, minthogy ez a terület lesz a *21. század olaja*. Azaz az adatok minél teljesebb körű összegyűjtése, strukturálása és elemzése fogja meghatározni és előre vinni a világ gazdaságát.
A *Big Data* definíciója ugyan nem kristályosodott ki, de az elfogadható, hogy a világban egyre nagyobb mennyiségben és egyre változatosabb formában fellelhető komplex adattömegek módszeres begyűjtését, analizálását kell érteni alatta. Az elemzési folyamat végén olyan következtetésekre juthatnak a kapott információkból a döntéshozók, amelyekkel nagyobb üzleti értéket képesek felmutatni, mint abban az esetben, amikor nem használnak big datához köthető módszereket. [6]
A *„big”* azt jelenti, hogy nagyon sok adatból álló adatbázis vagy adatkészlet. Olyan sokból, hogy azt már nehéz a megszokott, általánosan rendelkezésre álló adatbázis-kezelőalkalmazásokkal manipulálni. Óriási adattömeg, amelynek kezelése (létrehozása, tárolása, feldolgozása, továbbítása, lekérdezése stb.) a technikai lehetőségek határát feszegeti.
A *Big Data* jelenséget a következőképpen írhatjuk le: hatalmas, nagyfokú változatossággal és komplexitással jellemezhető, gyorsan keletkező és szaporodó adattömegek megjelenése, amelynek hasznosítására kevés idő áll rendelkezésre. [7]

6 YouTube; egy videómegosztó weblap, ahol a felhasználók videoklipeket tölthetnek fel és nézhetnek meg

7 Large Hadron Collider; Nagy hadronütköztető a CERN 2008-ban átadott részecskegyorsítója és ütköztetőgyűrűje

2.1 A 4V modell

Sokkal több adat létezik napjainkban, mint néhány évvel ezelőtt, és céllá vált e különféle forrásokból származó adathalmazok összesítése, szintetizálása, méghozzá a jobb, sikeresebb üzleti döntések meghozatala érdekében.
„Volume" - az információ mennyisége. Az adatok mennyisége napjainkra valóban sokkoló méreteket öltött.
„Variety" - az adatok sokfélesége, változatossága. A közösségi média csak egy része a *Big Data*-nak, bár kétségkívül jelentős része. Ide sorolhatóak még a viselkedéstani (fogyasztói magatartással kapcsolatos) adathalmazok, a tranzakciós adatok, a videók, a fényképek, a GPS adatok, a hangfelvételek stb.
„Velocity" - az adatok terjedési sebessége. Az adatokhoz való hozzáférés és az adatelemzés sebessége nagyon megugrott, lehetővé téve ezzel az ún. streaming adatok (adatfolyamok) elemzését.
„Veracity" - Az adatok érvényessége. A fentiek egyike sem ér semmit, ha az adatokat nem sikerül valós időben, a vállalatok számára az üzleti döntéseket segítő módon integrálni és szintetizálni. [8]

3. A Big Data kiaknázásához szükséges feltételek

Adatgyűjtés: Egy intézmény különböző adatforrásokból gyűjti össze az adatokat, amelyeket aztán masszívan párhuzamosított rendszerek segítségével - gyakran grid[8] technológia alkalmazásával - oszt szét; minden egyes csomópont az adatok egy részhalmazát dolgozza fel.
Feldolgozás: A rendszer ugyanezt a nagy teljesítményű párhuzamosságot használja fel annak érdekében, hogy gyors számításokat végezzen az adatokon minden egyes csomópontban, amelyek az eredményeket jobban felhasználható adathalmazokká csökkentik.
Adatkezelés: A feldolgozandó nagy mennyiségű adatok gyakran heterogének, mivel különböző rendszerekből származnak. Csaknem minden esetben szükség van az adatok értelmezésére, definiálására, tisztítására, gazdagítására és biztonsági célokból történő auditálására.
Mérés: Az alkalmazó szervezeteknek folyamatosan mérniük, monitorozniuk kell adataik minőségét, biztosítaniuk kell adataik összekapcsolhatóságát. A felhasználói

8 A grid egy infrastruktúra, mely közvetlen hozzáférést biztosít a gépi feldolgozóerőhöz és az adattároló kapacitáshoz is, mely megosztva helyezkedik el a Földön

követelmények határozzák meg, hogy pontosan mit szükséges mérni és milyen célt érdemes kitűzni az adatok minőségével kapcsolatban.
Felhasználás: Az adatok felhasználásának összhangban kell lennie a feldolgozás eredeti követelményeivel.
Tárolás: Az adatfelhő (data-as-a-service) trend kialakulásával az adatok egyre inkább egy adott helyen találhatók meg, míg az azokat elérő programok helye nem rögzített. Akár rövid távú kötegelt feldolgozás, akár hosszú távú megőrzés céljából tárolja a szervezet az adatokat, a tárolási megoldásokat tudatosan kell kezelnie.
Adatvagyon-gazdálkodás: Az adatokkal kapcsolatos felhasználói szempontú irányelveket és felügyeletet öleli fel, amely az előző 6 lépés mindegyikére vonatkozik. [9]

4. Big Data alkalmazása

4.1 Analitika a közszférában

A nagy mennyiségű adatok kiaknázásában rejlő lehetőségekkel és kihívásokkal a közszféra szereplői is szembesülnek – az ő munkájukat, beleértve a kormányzati döntéshozatalt is, szintén hatékonyan támogathatják az analitikai megoldások. A *Központi Statisztikai Hivatal* (KSH) pedig a 2011. évi népszámlálás adatainak központi feldolgozása során használja a SAS eszközét[9]. [10]
Az adatrobbanás mértékét jól érzékelteti, hogy az adóhatóságnál 1988 és 2000 között összesen gyűlt össze annyi adat, mint a 2013 első négy hónapjában. A feldolgozás már jórészt online folyamat, az évi *80 millió* ügyből csak másfél milliót intéznek papíralapon.
A beszerzett petabájtos tároló mellett pedig egyre bonyolultabb matematikai modellekre, elemzőképességekre van szükség. [11]

4.2 Big Data a népszámlálás segítségében

A magyar népszámlálás során *11,4 millió* kitöltött kérdőív került feldolgozásra a KSH-ban. A továbblépés lehetősége az adatbázisok összekötésében rejlik. Például a felsőoktatásban végzettek elhelyezkedését figyelő, a diplomás pályakövető rendszer még csak a NAV és az OEP[10] adatbázisaival van összekötve, de ha a

9 SAS egy üzleti analitikai szoftvereket szolgáltatásokat és üzleti intelligenciát fejlesztő multinacionális cég,

10 Országos Egészségbiztosítási Pénztár

foglalkoztatási hivatal adatbázisával is összekapcsolódna, akkor a rendszer nem csak regisztrálni tudná, de munkalehetőséget is ajánlana. [11]

4.3 Big Data a magyar mezőgazdaságban

Olyan környezetben, mint a mezőgazdasági termelés, különösen nagy eredményeket lehet elérni egy hatékony információs rendszerrel, mivel a rendelkezésre álló tudás kihasználása nehézkes. *Mezőgazdasági tudásközpont* létrehozását célzó kutatást indított a *Hewlett-Packard Informatikai Kft*., a *Széchenyi István Egyetem*, a *Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézete* (MTA SZTAKI), és az *eNET Internetkutató és Tanácsadó Kft.*, a projekthez a konzorcium több, mint *2 milliárd forint* támogatást nyert az *Új Széchenyi Terv* pályázatán - közölték a résztvevők az MTI-vel.
A projekt célja egy széleskörű tudásbázis létrehozása a "Big Data" elemző rendszer mezőgazdasági területre történő implementálásával. A kutatás során, az ország területén elszórtan ezer szenzoregységet helyeznek ki, s az adatokból, illetve az adatbázisokból és több egyéb nemzetközi nyílt tudásbázis segítségével kifejlesztenek egy komplex elemző, előrejelző és döntéstámogató megoldást. [12]

4.4 Big Data alkalmazása külföldön

A holland vízügyi alkalmazás

Hollandiában elindult a *Digital Delta* program, ami a Big Data hatékonyabb elemzéssel járul hozzá az árvízvédelem fejlesztéséhez és a holland vízgazdálkodási rendszer optimalizálásához. A kezdeményezés célja a katasztrófák és a környezetkárosodás megakadályozása, de a rendszer *15 százalékkal* csökkentheti a vízügyi feladatok költségeit is.
A program során felálló új felügyeleti rendszer a Big Data elemzése során olyan problémákra keres megoldást, mint az ivóvíz minőségromlása, a szélsőséges időjárás, vagy az árvíz- és aszályveszély. [13]

Big Data alkalmazása az USA bűnüldözésében

A BBC[11] *„The age of Big Data”* című dokumentumfilmjében [14] a Los Angeles egyik körzetében zajló rendőri munkát mutatják be elsőként. A rendőrségi

11 BBC – British Broadcasting Corporation, állami tulajdonú, brit közszolgálati műsorszolgáltató, egyben a világ legnagyobb műsorszolgáltatója.

adatbázis évtizedekre visszamenőleg tárolja a különböző bűneseteket. Az adatbázist egy kutatócsoport vizsgálta, egy algoritmus segítségével, amely a megtörtént bűntények mintázata alapján minden nap elkészít egy előrejelzést, amelyben kiemeli az előző napok eseményei és a múltbeli tapasztalatok alapján az adott napon kiemelt kockázatúnak minősülő helyeket. A járőrök kézhez kapták a kockázatos zónákat jelölő térképeket és az adott térségeket jóval gyakrabban érintették a menetrendszeri cirkálás közepette. Az eredmény megdöbbentő: a körzet egész *Los Angelesben* 26%-kal *csökkent* a rablások száma, *12%-kal* a vagyontárgy ellen elkövetett bűncselekmények mennyisége. A sikeren felbuzdulva az egész városra kiterjesztették a programot, és egyre több község veszi azt át.

Big Data az orvostudomány szolgálatában

Az orvostudomány és a „Nagy Adat" jelenség összefonódása teljesen természetes, elkerülhetetlen jelenség. A saját DNS[12]-ünk, mely közel *3 milliárd* karakter formájában kódolja önnön tervrajzunkat és használati utasításunkat. Kevés dolog fejlődik olyan ütemben, mint a genomszekvenálás[13]. A szekvenálás sebessége legalább annyira fontos paraméter, mint az ára. Míg egy évtizeddel ezelőtt a DNS analízis költségének *80%-át* maga a szekvenálás jelentette, addig most ez csak parányi töredéke a kiadásoknak. A költségek *60%-át* ma az adatok feldolgozása adja. A kihívást nem a nyers adatok előállítása jelenti, hanem azok feldolgozása. Most lehetőség van arra, hogy egy vérvételt követően elolvassák a páciens DNS-ét, és abból következtessenek arra, hogy mely proteinek termelése vagy működése tér el az elvárttól. Ez a váltás különösen gyümölcsöző lehet a rákos megbetegedések ellen folytatott küzdelemben. [15]

Big Data az "okos városokban"

Rio de Janeiróban[14] a pontos *időjárás előrejelzés* garantálja a megapolisz *közlekedésbiztonságát*, Birminghamben [15] mobilapplikáció segít a *parkolóhely*

12 DNS – dezoxiribonukleinsav; angol rövidítése: DNA - deoxyribonucleic acid, örökítő anyag

13 Genomszekvencia – bioinformatikai úton történő fehérjekódoló gének azonosítása.

14 Rio de Janeiró Brazília egyik legismertebb városa

15 Birmingham az Egyesült Királyság második legnagyobb saját önkormányzattal rendelkező városa.

keresésében, míg Szingapúrban[16] a forgalom valós idejű követésével dolgoznak a *dugók elhárításán* a városfejlesztők. [16]

A brit minta az adatbázisok egyesítésére

A brit kormány egyik legnagyobb jelenkori problémája az, hogy minden egyes részlege más és más adatbázisban dolgozik, az adatok megosztását pedig rosszul intézik egymás között. A kormány azon gondolkozik, hogy a létező összes adatbázist egyesíti. Mindez persze azt jelenti, hogy az emberekről minden adat egy helyen lenne. A hibák kiküszöbölésével mindenesetre 46 milliárd eurós megtakarítást remélnek. [17]

5. A Big Data és a jövő kihívása

5.1 A "nagy adat tudós"

A Big Data módszernek köszönhetően létrejött új kutatási eszközök folyamatosan változnak, lehetőséget teremtve az előrejelző elemzésre. Ez a folyamat jelentős és sürgető igényt generált az ún. data scientist[17]. [8]
A változásfolyamat a szervezetek minden területét érinteni fogja, elsőként természetesen az IT[18]-részleget. Minőségi váltás megy végbe az új munkakörök létrejöttével (tudományos adatelemző), és összességében az IT további munkahelyeket teremt. Ugyan az adatok kezelését informatikusok végzik majd, viszont a speciális szakmai tudást a többi részleg (pénzügy, marketing stb.) adja hozzá, de a partnerségi viszonyokat az IT fogja majd össze.
Az egész akkor hatékony, ha az adatfeldolgozás intelligens eszközökkel már ott lezajlik, ahol keletkezik az adat, különben hatalmas hálózati- és tárolókapacitási igény keletkezik.
Az adatközpontoknál most ugyanaz a változás megy végbe, mint ami egy évtizeddel ezelőtt például a PC-nél lezajlott. [18]

16 Szingapúr független ország, városállam Ázsia délkeleti részén.

17 data scientist – tudományos adatelemző

18 IT – Information Technology; információs technológia

5.2 Big Data-diploma

A következő két évben világszerte *4,4 millió* munkahelyet kell majd betölteni Big Data-elemzésben jártas szakemberekkel. Tudásuk abban a *2500 metropoliszban* is nélkülözhetetlen lesz. A vállalat ezernél több felsőoktatási intézménnyel indított már képzési együttműködést, Írországban már mesterszakon is lehet *Big Data-diplomát* szerezni. [19]

6. Infrastruktúrafejlesztés

6.1 A hardver és szoftver fejlesztése

Az adatoknak, illetve adatbázisoknak több szakaszból álló, a keletkezéstől az ismételt felhasználásig terjedő életciklusa van, amelyek mindegyikéhez megfelelő technikai hátteret és támogatást kell biztosítani. Erre az általános asztali gépek egyre kevésbé alkalmasak. Az adatok feldolgozása növekvő részben megosztott rendszereken, különleges, gigantikus méretű, rengeteg egymáshoz kapcsolt gépből (computer grid) álló adatközpontokban, az úgynevezett „számítástechnikai felhőkben" történik. A nyitott forráskódú szoftverek megjelenése és elterjedése, a webes szolgáltatások egyre alacsonyabbra kényszerítik a belépési korlátokat, ami olcsóbbá teszi a használatát. Az interneten nyújtott szolgáltatásokhoz és a gigantikus adatbázisok továbbításához megbízható szélessávú kapcsolatok kellenek. Önmagában a hardver nem elegendő: szoftverre is szükség van, ami alatt nem csak a programokat értjük. A „Big Data" jelenség lehetőséget nyújt ahhoz, hogy a tudományágak művelői a megfogalmazott kérdésekre matematikai statisztikai, adatbányászati eszközökkel keressenek választ, az adattömegben mintázatok, sokszor nagyon bonyolult, sokváltozós összefüggések után kutassanak tanulásra is képes alkalmazásokkal.
A számtalan féle forrásból kapott, sokfajta módon keletkeztetett adat feldolgozásához, kombinálásához és lekérdezéséhez szabványokra és szabványos meta adatokra[19] is szükség van. [7]
A „Big Data" szempontjából nyilvánvalóan fontosak a vállalati informatikai beruházások, amelyek éves nagysága manapság több trillió dollárra rúg és az elmúlt években jelentős emelkedést mutatott.

19 Meta adat jelentése: strukturált adatok az adatokról. Ilyenek a könyvtári katalógusok, a tárgyszó indexek, újabb formájukban a weben található dokumentumok leíró adatai.

Eközben az információk keletkeztetésének, menedzselésének és tárolásának fajlagos költsége az elmúlt öt évben a hatodára zsugorodott. [20]

6.2 Digitális Nemzeti Fejlesztési Program

Hazánkban is, mint az *Európai Unió* többi országában, beindult a Digitális Nemzeti Fejlesztési Program, amely a *szupergyors internetből*, a *digitális közösség és gazdaság fejlesztéséből*, az *E-közigazgatási* szolgáltatásokból, és a *digitális kompetenciák* fejlesztéséből tevődik össze. A kormányzat 2018-ra szupergyors internet lefedettséget szeretne kiépíteni az egész ország területén, ami azt jelenti, hogy minden háztartás és intézmény számára legalább *30 Mb/s* sávszélességű internet elérést kíván biztosítani. A program keretében ez a *Nemzeti Digitális Közmű (NDK)* nevet viseli. A program célja a sokkal szofisztikáltabb elérhetőség, az életminőség javítása, a teljes lefedettség biztosítása. A cél tehát nem csak az infrastruktúra végleges kiépítése, hanem a hozzáadott értékkel növelni az életminőség színvonalát a magyar lakosság számára. [21]

A közigazgatás céljai a fejlesztéssel

Jelen társadalmunkban az információ jelentősen befolyásolja a társadalmi kapcsolatokat. Központi elem az *információ* és ennek csatolmánya az *internet*. A lakosság körében az *E-vásárlás* egyre népszerűbb, mert kényelmes és gyors! A hivatali ügyintézés is egyre népszerűbb, bár a meglévő infrastruktúra és az elérhető hivatali szolgáltatások fejlesztése, bővítése elengedhetetlen és szükséges. A közigazgatási cél, hogy megjelenjenek az interneten, minél szélesebb szolgáltatási palettával, és minél nagyobb számú felhasználót elérve. A 2010-es években az *interaktív lehetőség* mellett az E-közigazgatásban a *fogyasztóbarát felhasználásra* kell törekedni.
Magyarország az infrastruktúra fejlesztésében jól áll, komoly előrelépések történtek mind a vezetékes, mind a mobil széles sávú lefedettségben. Ennek ellenére vannak olyan területek az országban, ahova nem ért el a fejlesztés. A *digitális otthon, a smart city, az E-közigazgatás* fejlesztése *kiemelt beruházásnak* számít. A *„Sikerkritériumok”* a célok, keretek, szereplők és felelősség négyeseként értendő. A *célok*: az infrastruktúra, a szolgáltatások, kompetencia fejlesztése. A *szereplők*: az állam, a piac, és az EU. A *keretek*: az adók, az EU-s források, és a szabályozás. A *felelősség*: az edukáció, az összhang, és az együttműködés. Magyarországon megkezdődött a megfelelő szabályozási környezet kialakítása. A program komplex, mert tartalmazza a hálózat, a kompetencia és a szolgáltatás

fejlesztéseit. Ezen program az *Európai Digitális Menetrend* és a *Nemzeti Infokommunikációs Stratégia*, a *Partnerség a Digitális Magyarországért* programok és tervek keretében valósulhat meg. A *Next Generation Access* (NGA) lefedettség Magyarországon 2013-ban már *75,7%* volt. A projekt megvalósulása során a hosszú távú előnyök messze magasabbak, mint azt gondolnánk. A projekt az előkészítési, a tervezési, a pályáztatási fázisok után, a hálózatok, azon belül is a helyi hálózatok, és azon túl a kimaradt területek építését tartalmazza. Ez az elmúlt idők legnagyobb hírközlési fejlesztési projektje. A *64/2014 EU irányelv*, melynek folyamatban van a honosítása, irányadó az országos elérhetőségű, az állam által biztosított hálózati lefedettség kiépítése szempontjából.
A projekt az Európai Digitális Menetrend *COM(2010)245*; az *Európai Parlament és Tanács 2014/61/EU irányelve* a nagy sebességű elektronikus hírközlő hálózatok kiépítési költségeinek csökkentésére irányuló intézkedésekről, a Nemzeti Infokommunikációs Stratégia, a *1162/2014. (III. 25.) Korm. határozata* a Digitális Nemzet Fejlesztési Programról, a *1631/2014. (XI. 6.) Korm. határozata* a „Digitális Nemzet Fejlesztési Program" megvalósításáról szóló intézkedések teremtik meg a jogszabályi hátteret annak, hogy az IKT, mint iparág 2020-ig milyen irányú fejlődésen kell, hogy keresztülessen, és ez által hozzá járuljon az Európai gazdaság működéséhez. A *Szupergyors Internet Projekt* (SZIP) megvalósulásához feltétlenül szükséges az adminisztrációs akadályok lebontása, a beruházások ösztönzése a stratégiai célok elérése érdekében. [21]

A magyar "smart city"

A következő kérdés a Digitális Menetrendben, hogy *mitől lesz egy város digitális*? Lehet sorolni, hogy az informatika, a hálózatok, a mobil penetráció. Valamint ide lehet sorolni a szolgáltatót, úgymint az állam, az önkormányzatok és a piac, továbbá a fogyasztót, mint állampolgárok, vállalatok. A „smart city" a *közbiztonság* javítása, a *városkártya* használatának növelése, az *eszközbiztosítás* és a *képzés* keretében kezdődött meg hazánkban több vidéki nagyvárosban, pl. Miskolcon, Nyíregyházán, Salgótarjánban.
A digitális város, mint „a már megvalósult jövő", a Wi-Fi szolgáltatást is tartalmazza a lakosság részére. De a „smart city" projekt *bevételt is termel* az azt alkalmazó közigazgatási egység számára. Az interneten foglalt szállások *60%-ban* bővültek. Ez a bővülés a foglalkoztatások számát is növeli.
A piaci szereplők számára árbevétel növekedést jelent, ha a felhasználók digitális írástudása növekszik. A társadalmi gátakt át kell törni a materiális dolgok és a digitális eszközök között. Ameddig ez a gát elszeparálja egymástól az embereket és

a digitális világ által nyújtotta szolgáltatásokat, addig a megálmodott jövő csak egy álom marad, amelyet csak nagyon kevesen tudnak a saját jólétük megteremtésére és fenntartására fordítani. A gátakat a költséghatékonysággal lehet felszámolni. [21]

A digitális írástudás fejlesztése

A digitális írástudatlanság társadalmi csökkentése érdekében több program is elindításra került az állam által, ilyen például a *TÁMOP 2.1.2-1/1*, amely az idegen nyelvi és informatikai kompetenciák fejlesztésére irányult, valamint a *digitális tankönyv* program, valamint a *kutatás-fejlesztési* támogatások, és nem utolsó sorban a *programozás* oktatásának erősítése. A digitális írástudatlanság csökkentését segíti elő a nagy számban terjedő mobil alkalmazási lehetőségek oktatási célú felhasználása. Úgy, mint a mobil platformokon futó tanagyagok és tanítást-, tanulást támogató alkalmazások fejlesztése.
Sajnos a mai *15 évnél* idősebb korosztály tagjai között *40,2%,* azaz megközelítőleg *3 millió ember* digitálisan nem kompetens ma Magyarországon. De ez a szám sajnos nem azt jelenti, hogy a maradék *7 millió ember* digitálisan kompetens lenne, mert ezek az emberek se használnak olyan tartalmakat, amelyek mindegyike kimeríti a digitális írástudás keretét. Ennek az oka lehet az, hogy az emberek félnek a felfedezni maguknak a digitális világot, nem érzik magukénak, amely azért okoz problémát, mert nem mélyednek el azokban az ismeretekben, nem alakulnak ki azok a digitális készségek, amelyek szükségesek lennének ahhoz, hogy megfelelő szinten tudják használni, kihasználni a digitális világ által nyújtott jólléti javakat. A digitális tartalmak alacsony számú alkalmazásának a társadalom körében még lehet oka az is, hogy a biztonsági kérdés folyamatosan napirenden van. Ezt megoldandóan a *biztonság kérdése* a kompetencia fejlesztésének fontos részét képezi, úgymint a *biztonságos adattárolás* és *biztonságos üzemeltetés* kérdése. [21]

7. A kockázatai és a biztonsági kérdések

A kritikus infrastruktúra védelmét szabályzói szinten az állam biztosítja a Kritikus Infrastruktúra Védelem Nemzeti Programról szóló 2080/2008. (VI.30.) Korm. határozattal. Valamint ezen kormányhatározat alapján kiadott, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. Törvénnyel és annak végrehajtásáról szóló 65/2013. (II.8.) Korm. rendelet. A magyarországi kritikus infrastruktúrákat, azon belül is a kritikus információs infrastruktúrát, mely magában foglalja az informatikai

közműveket, valamint azok védelmét Magyarország viszonylatában a szabályozása lefedi a védelem kialakításához szükséges területet. [22]

7.1 Kockázatok csökkentése

A Big Data jelenség a fentiek alapján azt a benyomást kelti, keltheti, hogy ez az *„adat-boom”* mindenki számára csak pozitív hatással jár. Sajnos, mint mindennek, ennek is megvannak a maga negatív tulajdonságai.
A *„digitális árnyék”*-nak (*digital shadow*) nevezett adatok tömege az, ami egy-egy emberrel kapcsolatban folyamatosan létrejön. Ezeknek a digitális (láb)nyomoknak egy része az *„árnyék”* gazdája által tudatosan keletkezeik, másik része azonban ismeretlen a tulajdonos számára. Ennek okán a személyes adatok védelme, napjainkban egyre nagyobb hangsúlyt kap. Magyarországon elfogadásra került a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Ez a törvény az információs önrendelkezési jog és az információszabadság biztosítása érdekében, a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokról, valamint az ezen szabályok ellenőrzésére hivatott hatóságról az Alaptörvény végrehajtására, az Alaptörvény VI.[20] cikke alapján készült.
A fenti törvény és az általa életre hívott Nemzeti Adatvédelmi és Információszabadság Hatóság által magyarországi viszonylatban biztosítja a személyes adatok védelmét. [7][23]

20 Magyarország Alaptörvénye IV. cikk: (1) Mindenkinek joga van a szabadsághoz és a személyi biztonsághoz.

(2) Senkit nem lehet szabadságától másként, mint törvényben meghatározott okokból és törvényben meghatározott eljárás alapján megfosztani. Tényleges életfogytig tartó szabadságvesztés csak szándékos, erőszakos bűncselekmény elkövetése miatt szabható ki.

(3) A bűncselekmény elkövetésével gyanúsított és őrizetbe vett személyt a lehető legrövidebb időn belül szabadon kell bocsátani, vagy bíróság elé kell állítani. A bíróság köteles az elé állított személyt meghallgatni és írásbeli indokolással ellátott határozatban szabadlábra helyezéséről vagy letartóztatásáról haladéktalanul dönteni.

(4) Akinek szabadságát alaptalanul vagy törvénysértően korlátozták, kárának megtérítésére jogosult.

7.2 Biztonsági feltételek kialakítása

A BalaBit [21] syslog-ng nevű megoldása az informatikai rendszerekben keletkező naplóüzenetek gyűjtését és feldolgozását valósítja meg. Jelenleg azonban a piacon található szoftverek az operációs rendszerek és alapvető rendszeralkalmazások naplóüzeneteire fókuszálnak, a felhasználók fő motivációja pedig az adatvédelmi szabályozásoknak való megfelelés, informatikai biztonsági kontroll és az üzemeltetés támogatása. Az alkalmazásokból való információgyűjtés viszont egy egészen más megközelítést igényel. Elég, ha egy ERP[22] rendszerben, online bankban vagy közösségi portálon végzett felhasználói aktivitásra gondolunk. [24]

Összefoglalás

A Big Data, mint a jövő *"olaja",* vagy *"aranybányája"* mit sem ér, hogyha azt nem tudjuk biztonságos módon elérni, tárolni. Látható, a létfontosságú információs közművek, mint a kritikus információs infrastruktúra részei, biztosítják a jólétünket, melynek a 21. század második évtizedében mára elengedhetetlen részét képezi a digitális jólétnek. A digitális jólét a szükséges és kellő mennyiségű publikus információ elektronikus úton történő feltétel nélküli elérését jelenti. Nap, mint nap döntések sorozatát kell meghozni. A minél pontosabb döntések meghozatala érdekében a gyors, pontos, naprakész, sok féle megjelenésű és nagy mennyiségű információra van szükség. Tehát ez esetben a Big Datá-t jellemző 4V modell érvényesül. A Big Data ezt követő életünk jelentős részét fogja képezni. Gondolva itt a gazdasági növekedésre, mely a sok formában megjelenhet, úgy, mint a foglalkoztatás növekedése, új szakmák kialakulása, ezáltal az oktatási struktúra átalakulása. Valamint az egészségügy modernizációja, a betegségek gyorsabb pontosabb diagnosztizálása, gyógyítása. Az adatok gyors és biztonságos átvitelét az állam a bemutatott Digitális Nemzeti Fejlesztési Program keretében kívánja megteremteni. Ez a projekt a kritikus infrastruktúra fejlesztését jelenti. Ahhoz, hogy a digitális jólét megvalósulhasson, ki kell alakítani az elérés lehetőségét, a elérhetővé kell tenni a különböző szolgáltatásokat, megfelelő tartalommal ellátva. Mindenképp szükséges a digitális írástudás növelése, amely a funkcionalitást sem nélkülözi. Mindez akkor hatékony, hogyha megfelelően vannak védve az adataink és az a közeg ahol az információink tárolódnak és továbbítódnak.

21 BalaBit – a világ egyik vezető IT-biztonsági szoftverfejlesztő vállalata

22 ERP – Enterprise Resource Planning System; integrált vállalatirányítási rendszer

Felhasznált irodalom

[1] Steven Rosenbush, Michael Totty: How Big Data Is Changing the Whole Equation for Business The Wall Street Journal, March 10, 2013, http://www.wsj.com/news/articles/SB10001424127887324178904578340071261396666?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424127887324178904578340071261396666.html, letöltve: 2014. március 18.

[2] IDC Nagy Adat és Üzleti Analitikai Fórum 2014, Budapest, 2014. 04. 24., http://idchungary.hu/hun/events/54405-idc-big-data-and-business-analytics-forum-2014/7-overview, letöltve: 2014. május 10.

[3] prof. Patrice Koehl: Big Data Why it matters, előadás, Department of Computer Science, UC Davis Genome Center, 2013. szept. 5., https://www.youtube.com/watch?v=_HI5pLCFbu0&list=PLKJRT9JmiGVcibyh1Fw7CjMdlpq2wC2uk, letöltve: 2014. június 8.

[4] SI-prefixumok, http://fizika.qwqw.hu/?modul=oldal&tartalom=1112407, letöltve: 2014. május 20.

[5] Bináris prefixumok, http://wiki.hup.hu/index.php/Bin%C3%A1ris_prefixumok, letöltve: 2014. május 20.

[6] Bitport: Nagy problémákat hozhat a Nagy Adat, 2013.05.14., http://bitport.hu/trendek/nagy-problemakat-hozhat-a-nagy-adat, letöltve: 2014. június 20.

[7] Adatrobbanás a vállalatvezetésben, Computerworld, 2011. november 10., http://computerworld.hu/cio/adatrobbanas-a-vallalatvezetesben-.html, letöltve: 2014. június 15.

[8] Piackutatás blog: Nagy Adat vagy nagy cirkusz?, 2014.02.10., http://piackutatas.blog.hu/2014/02/10/nagy_adat_vagy_nagy_cirkusz, letöltve: 2014. június 20.

[9] Prím Online: Hét lépés szükséges a big data kiaknázásához, 2013. április 15., http://hirek.prim.hu/cikk/2013/04/15/het_lepes_szukseges_a_big_data_kiaknazasahoz, letöltve: 2014. június 15.

[10] Piac és Profit: Nem alaptalan a „nagy adat” körüli felhajtás, 2012. október 26., http://www.piacesprofit.hu/infokom/nem-alaptalan-a-nagy-adat-koruli-felhajtas/, letötlve: 2014. június 20.

[11] hvg.hu: Adatrobbanás a NAV-nál, 2013. március 03.,

http://hvg.hu/tudomany/20130303_adatrobbanas_a_nav_nal, letöltve: 2014. június 20.

[12] Computerworld: Mezőgazdasági Big Data, 2014. április 21., http://computerworld.hu/computerworld/mezogazdasagi-big-data.html, letöltve: 2014. június 20.

[13] hvg.hu: Így védekeznek az árvíz ellen a hollandok, 2013. július 11., http://hvg.hu/tudomany/20130711_igy_vedekeznek_az_arviz_ellen_a_hollandok, letöltve: 2014. június 16.

[14] BBC Horizon 2013 The Age of Big Data, 2013. aug. 22. http://www.youtube.com/watch?v=CO2mGny6fFs&feature=share&list=PLKJRT9JmiGVcibyh1Fw7CjMdlpq2wC2uk, letöltve: 2014. június 20.

[15] Maverick: 83. Big Data és DNS: az orvostudomány forradalma, 2013. dec 16., http://voyager.blog.hu/2013/12/16/83_big_data_es_dns_az_orvostudomany_forradalma, letöltve: 2014. június 21.

[16] hvg.hu: Ez lesz a legmenőbb ágazat pillanatokon belül, 2013. október 02., http://hvg.hu/kkv/20131002_Okos_varosokat_terveznek_a_jovo_szakember, letöltve: 2014. június 20.

[17] Harangi László: Az ország minden adatbázisát egyesítenék a britek, 2014. augusztus 5., http://pcworld.hu/iskolakezdes/az-orszag-minden-adatbazisat-egyesitenek-a-britek.html, letöltve: 2014. június 15.

[18] SG.hu: Big Data: sok a kihasználatlan lehetőség, 2013. április 21. http://sg.hu/cikkek/96813/big_data_sok_a_kihasznalatlan_lehetoseg, letöltve: 2014. június 16.

[19] hvg.hu: Ez lesz a legmenőbb ágazat pillanatokon belül, 2013. október 02., http://hvg.hu/kkv/20131002_Okos_varosokat_terveznek_a_jovo_szakember, letöltve: 2014. június 20.

[20] Világtudomány.hu: A Nagy Adat, mint aranybánya..., http://vilagtudomany.hu/index.php?data%5Bmid%5D=7&data%5Bid%5D=1627&a-nagy-adat-mint-aranybanya, letöltve: 2014. június 16.

[21] Digitális Nemzet, digitális fogyasztók „Rajta vagyunk a bittérképen” c. konferencián elhangzottak alapján, Budapest, 2015.03.24.

[22] Andras Kerti, Zoltan Nyikes (2015): Overview of Hungary Information Security, The Issues of the National Electronic Classified Material of Transmission, SACI 2015 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics PROCEEDINGS, (pp. 327-334.), Timişoara, Romania May 21–23, 2015, ISBN: 978-1-4799-9910-1

[23] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[24] hvg.hu: 300 millió a felhasználói naplózás fejlesztésére, 2013. április 09., http://hvg.hu/tudomany/20130409_300_millio_a_felhasznaloi_naplozas_fejles, letöltve: 2014. június 16.

[25] Kerti András, Szabó Anna Barbara: Az információbiztonsági kockázatelemzés, mint a vállalati kockázatkezelés része In: Dr Fregan Beatrix (szerk.) Kockázatelemzés, kockázatértékelés: tanulmányok az Óbudai Egyetem Biztonságtudományi Doktori Iskola kutatásaiból. 207 p. Budapest: Óbudai Egyetem, 2013. pp. 120-177. (ISBN:978-615-5018-98-5)

DOMOKOS Máté: A különleges műveleti csoportok elvi feléptése és feladatrendszere

Absztrakt

A szerző a cikkben bemutatja egy különleges műveleti csoport elvi feléptését és feladatrendszerét, ennek megfelelően működésének rendjét, és az egyes szervezeti elemek alkalmazásának lehetőségét harci körülmények között.

Abstract

The author of the article presents the organisation and task system of a Special Operation Team, according of these its operation's schedule and the possibility use of individual organizational elements in combat conditions.

Kulcsszavak: *különleges műveletek, hadműveleti központ, híradó központ, US Mobile Training Team, gyorsreagálású erők*

A különleges műveleti erők

A különleges műveleti erők parancsnoksága hasonló feladatkörrel bír, mint egy hagyományos lövészzászlóalj vezetősége. A parancsnokság, a törzs aktív közreműködésével vezeti, és irányítja az alárendelt alegységeket, beleértve a harcoló századokat és a támogató elemeket egyaránt. Ők felelnek továbbá a folyamatos kiképzésért, a napirend és a feladatok kiosztásáért, és a kiszabott valamint elvégzett feladatok visszaellenőrzéséért is. Gyakorlatok, és éles harci műveletek során a tevékenységek irányítását a Taktikai Műveleti Központ (Tactical Operation Center – TOC) koordinálják, ahol a vezető szervek három részlegre tagozódnak:

– *Hadműveleti Központ (HK – Operation Center - OPCEN).* A Hadműveleti Központ felel a műveletek megtervezéséért, a felderítésért és az általuk szolgáltatott információk feldolgozásáért és osztályozásáért. Továbbá irányításuk alá tartozik a harcoló egységek közvetlen támogató erőinek az irányítása, ide tartoznak például a gyorsreagálású erők, vagy a légi támogató elemek.

– *Támogató Központ (LK – Support Center - SUPCEN).*A Támogató Központ felel a logisztikai támogatásért, mindennemű utánpótlás biztosításáért, és a szállítások megtervezéséért és lebonyolításáért.

– *Híradó Központ (HíK – Signal Center - SIGCEN).* A híradó központ feladata, az alegységek egymás és a parancsnokság közötti folyamatos és zavarmentes kommunikáció fenntartása, a híradás megszervezése, a híradó katonák feladatra való felkészítése és irányítása. Felelősségük alá tartozik továbbá a csapatok híradó eszközzel való ellátása is.

A harcbiztosító erők feladata, a támogató alegységek irányítása, akik az adminisztratív, logisztikai jellegű kiszolgálását végzik. A támogató erők gondoskodnak a felszerelések, a hadianyag, és az élelem kijuttatásának megtervezéséért a műveleti területre és magáért a szállításért is. Az ő felelősségük a későbbiekben, a feladatot végrehajtó csoportok támogatása és ellátása is. Az hogy egy adott támogató erők kapnak-e megerősítést, az a feladat jellegén múlik. Ők összedolgozva hozzák létre az Taktikai Műveleti Központ teljes infrastruktúráját, a híradó és informatikai biztosítását, és tevékenyen részt vesznek az objektum őrzés védelmében is.

A különleges erők sajátos feladatrendszerüknek köszönhetően, eltérő felépítéssel rendelkeznek, mint a Magyar Honvédség más alakulatai. [1]

A kezdeti időszakban a képzés és kiképzés területén rendkívül nagy segítséget nyújtott az Amerikai Egyesült Államok. Lehetőséget biztosítottak arra, hogy magyar katonák a tengeren túlra utazva hajtsanak végre bevált kiképzési programokat, amiket tapasztalt katonák felügyeltek. Ez a lehetőség igaz korlátozott számú magyarnak adatik meg, de az amerikai fél a mai napig fogadja hazánk katonáit, és nagy szakértelemmel képzi őket. Továbbá az általuk biztosított Mobile Training Team (Továbbiakban: US MTT) kiképzői, fáradságos munka árán képezték az első modern magyar különleges műveleti katonákat. Tudásukat fokozatosan átadva egyre szabadabb kezet adtak az általuk kiképzett magyar katonáknak. Ez azért volt fontos, mert korábban a Magyar Honvédség nem rendelkezett elegendő tapasztalattal ahhoz, hogy önállóan képezzen olyan katonákat, akik hatékonyan képesek különleges műveleteket végrehajtani. Az US MTT katonáinak köszönhetően, mára katonáink olyan szintre jutottak, hogy önállóan hajtják végre a frissen jelentkező állomány kiképzését. A katonák tapasztalatszerzésében komoly szerepet játszott az iraki és az afganisztáni missziós szerepvállalás is, ahol a magyar különleges erők komolyabb tapasztalatokkal rendelkező nemzettekkel hajtottak végre közös műveleteket. Ezekből a tapasztalatokból táplálkozva a katonák hitelesen át tudták adni tudásukat a fiatalabb generáció számára. A magyar különleges erők missziós szerepvállalása továbbá kivívta a szövetséges nemzetek tiszteletét, hiszen felkészültségük és feladat végrehajtásuk nem maradt el azon

nemzetekétől, akik már sokkal régebb óta alkalmazzák a speciálisan képzett erőket. [2]

A különleges műveleti csoportok elvi felépítése

A különleges erők, a hagyományostól eltérő feladatrendszerüknek köszönhetően, eltérő szervezeti struktúra alapján épülnek fel. Egy hagyományos zászlóalj általában a törzsből, 3-4 századból, a századok pedig 3-4 szakaszból állnak. Egy szakasz ideális esetben 30-35 főt számlál. A különleges műveleti kötelékekben a századok, a szokásostól eltérően nem szakaszokra, hanem 12 fős különleges műveleti csoportokra tagolódnak, ez jelentős szervezeti eltérés a hagyományos felosztáshoz képest. Hogyha a feladat jellege megköveteli, a csoportok képesek közösen is műveletet végrehajtani. A gyakorlat azt mutatja, hogy általában kettő csoport működik együtt, de természetesen ezt a feladat jellege határozza meg. Abban az esetben, hogyha két csoport szorosan dolgozik együtt, a két csoportparancsnok közül rangidős kerül kijelölésre. A rangidős lesz az, aki a művelet teljes ideje alatt parancsokat ad mindkét csoport személyi állományának. [2]

A harcoló csoportok fő feladata, a katonai felső vezetés által, számukra kiszabott különleges műveleti feladat megtervezése az arra történő felkészülés lebonyolítása és magának a feladatnak a minél magasabb színvonalú végrehajtása. Ez azt jelenti, hogy a csoport tagjai egymással szoros együttműködésben szervezik meg a műveleteiket, percről percre lebontva azok pontos menetét. Ezt követően a csoport parancsnokának a felelőssége, hogy a művelet végrehajtásához elengedhetetlen információkat közölje beosztottjaival, akik pedig különböző szakbeosztásuknak megfelelően megigénylik és átveszik az adott feladat végrehajtásához szükséges anyagokat, és felszereléseket. Az anyagok igénylésében és beszerzésében a logisztikusok nyújtanak segítséget.

Emellett helyet kap még két speciális csoport, akik vízi és víz alatti műveletek végrehajtására specializálódtak, valamint két csoport, akik ejtőernyős képességekkel rendelkeznek. Ezen felül minden harcoló csoport kiképzést kap arra, hogy hatékonyan és magas színvonalon képesek legyenek a helységharcok, a magashegyi műveletek, a vízfelszíni feladatok, és a nagy távolságú gépjárműves feladatok végrehajtására, aszerint, hogy azt az épp végrehajtani kívánt feladat megköveteli. Ennek megfelelően minden csoport képes megtervezni saját műveletét, földön, vízen és levegőben, végrehajtani az adott területre való eljutást, és az ottani effektív tevékenység végrehajtását. Ehhez természetesen szükségül van a logisztika folyamatos támogatására, és a parancsnokság és a felderítést végző

katonák információira. A csoportoknak hatékonyan kell feladatot végrehajtaniuk nemzetközi környezetben, együttműködve más országok erőivel abban az esetben is, hogyha elszigetelten ellenséges környezetben tevékenykednek, és csak minimális felsőbb utasításokat kapnak az elöljáróktól. Hogyha közös együttműködésre kerül a sor, akkor a kommunikáció nyelve kizárólagosan az angol függetlenül az együttműködő nemzetek nemzetiségét tekintve.

A különleges műveleti csoportokban minden katonának megvan a saját feladata, amire a kiképzés során specializálódik, ilyenek az egészségügyi, híradó, műszaki, és a fegyveres specialisták. Természetesen ezek megfelelői megtalálhatóak azon különleges műveleti csoportokban is, amik vízi illetve légi műveletekre lettek kiképezve. Minden feladatra két-két katonát képeznek ki, egyikük egy altiszt (senior) másikjuk tisztes (junior). A csoport tagjait úgy képzik ki, hogy alapszinten mindenki értsen a társai feladatához is, hiszen harcérintkezés során végzetes lehet egy-egy specializálódott katona elvesztése, abban az esetben ha társaik nem tudják legalább részben átvenni társaik szerepét.

A csoportokban helyet kap továbbá egy felderítésért felelős altiszt, és egy hadműveleti altiszt is, akik a műveletek előzetes megtervezésében jócskán kiveszik a részüket. Egy-egy specializációra fordított képzési idő 10 hónapot vesz igénybe. Ezt megelőzően kell részt venni egy komplex orvosi vizsgálaton, és sikeresen kell abszolválni a Különleges Erők kiválasztó kiképzését. [3]

Parancsnok (18A)

A különleges műveleti csoportok parancsnoka, általában századosi rendfokozattal bír, helyettese pedig két zászlós. Egyikük beosztását tekintve is a parancsnok helyettes, a másik a felderítő altiszt. A gyakorlati felépítés a rendfokozatokban eltérhet, de megközelítőleg az valóságban is így épülnek fel a csoportok. Műveletek végrehajtása előtt, a parancsnok a különleges műveleti csoportja aktív közreműködésével szervezi meg a feladatot, amit aztán ismertet a csoportja minden tagjával. A rendelkezésükre álló információkból dolgoznak, amiket a felderítés szolgáltat nekik. Minden specialista bedolgozza a tervbe az őrá vonatkozó részt, amit természetesen a parancsnoknak jóvá kell hagynia a véglegesítés előtt. A parancsnok tábori körülmények között, a katonái kiképzését is koordinálja és ellenőrzi, feladatot szab a számukra, fenntartja a katonák éberségét, és gondja van katonái felszerelésének állapotára is. Az ő felelőssége továbbá a beosztottjaival kapcsolatos mindennemű adminisztratív munka elvégzése vagy elvégeztetése és azok ellenőrzése missziós területen és hazai körülmények között egyaránt. Kiemelten fontos a feladatok megfelelő elosztása. Nem szabad abba a

hiába esni, hogy nem egyenletesen osztjuk el a munkát, hiszen ha mindig ugyanazok az emberek kapnak feladatot, megbízásokat, az nemcsak az egyén szempontjából káros, de a szervezet tekintetében sem jó. [4]

Fegyveres specialista (18B)

A különleges műveleti csoportok fegyveres specialistái foglalkoznak a fegyverekkel és a lőszerekkel kapcsolatos feladatok ellátásáért. Az ő feladatuk a műveletek előtti lőszerfelhasználás megbecslése, és a muníció kiosztása. A fegyveres specialisták a feladat függvényében igényelnek olyan gránátokat, speciális robbanóeszközöket, vagy esetleg lőfegyvereket, amik remélhetőleg előremozdítják a csoport által végrehajtani kívánt művelet sikerességét.

Műszaki specialista (18C)

A műszaki specialisták feladata igen összetett. A felelősségi körükbe számos fontos feladat végrehajtása tartozik. Az ő dolguk, a közlekedéssel, gépjárművekkel és az ezekkel összefüggő tüzelő- és üzemanyagokkal kapcsolatos műszaki és adminisztratív munka elvégzése. Ők a felelősek a csoport tagjainak elhelyezéséért, továbbá a ruházati anyagokkal kapcsolatos feladatok ellátásáért is. A ruházati anyagokkal kapcsolatos teendők magukba foglalják a személyes védőeszközök biztosítását a csoport tagjainak számára. Az utolsó felelősségi területe a műszaki specialistáknak, a vegyvédelmi szakanyagokkal történő feladatok elvégzése.

Híradó specialista (18E)

A híradó specialista felel a csoporton belüli, és a csoporton kívülre irányuló kommunikáció biztosításáért, a rendelkezésre álló legmegfelelőbb frekvencia megválasztásáért, és az összeköttetés minőségének figyeléséért. A híradó specialistának folyamatos kontaktban kell lennie a csoport parancsnokával, valamint folyamatos összeköttetést kell fenntartania az elöljáró szervekkel. A beérkező utasításokat azonnal továbbítania kell a csoport parancsnoka felé így biztosítva a vezetés irányítás megvalósulását. Minden csoport eltérő szisztémát követ, de általában a híradó specialistáknál van minden olyan eszköz, amivel az elöljárót el lehet érni. Ennek oka az, hogyha az összeköttetés minősége romlik, vagy a kommunikáció teljesen megszakad a híradó specialista az, aki a legjobban ért a rádiókhoz, és azokat ellenőrizve áthidalhatja az esetleges hibákat. Az ilyen problémákat legtöbbször a csatlakozók szétcsúszása, vagy a frekvencia rossz

megválasztása, vagy a változó időjárási körülmények okozzák. Az időjárás legjobban a rövid és a mikrohullámú terjedést befolyásolja.

A híradó specialisták feladata továbbá, hogy a feladat függvényében összeköttetést létesítsenek a támogató erőkkel, a QRF [1] katonáival, vagy más szövetséges csapatokkal. Ezen esetekben az összeköttetés felvételének feltételei és pontos paraméterei (melyik eszközön, milyen frekvencián, stb.) korábban megbeszélésre kerülnek. Hogyha váratlanul kell ilyesfajta összeköttetést létesíteni, a szükséges információkat az elöljáró titkosított formában eljuttathatja a csoport híradó specialistájának. A többnemzeti műveletek esetében a forgalmazás nyelve kizárólagosan az angol. Ez alól kivételt képeznek olyan esetek, amikor egy bizonyos nemzetiségű csoport úgy hajt végre műveletet, hogy soraiban csak az adott nemzet katonái harcolnak. Ilyenkor csoporton belül maguk között forgalmazhatnak saját anyanyelvükön is.

Egészségügyi specialista (18D)

Az egészségügyi specialista feladata az, hogy a harcérintkezések során megsebesült társait gyors elsősegélyben részesítse. Az egészségügyi specialisták szerepe tehát szintén kiemelt fontossággal bír, hiszen szaktudásuk életeket menthet a harctéren. Az egészségügyi specialisták, többek között CLS [2] végzettséggel is rendelkeznek, aminek köszönhetően feladatukat magas szintű szakértelemmel végzik. A sérült biztonságos helyre és jól felszerelt kórházba szállításáról a MEDEVAC[3] kérés során érkező helikopter gondoskodik. A MEDEVAC jelentést a híradó specialista adja le, egy olyan korábban elkülönített csatornán, amit csak és kizárólag erre a célra lehet igénybe venni. A sebesült kiemelését, egy kifejezetten erre a feladatra felszerelt helikopterrel végzik. Abban az esetben, hogyha nincs lehetőség arra, hogy külön csatornát különítsenek el a MEDEVAC igények számára az üzemi frekvencián adják le azokat. Ilyenkor a MEDEVAC kérések minden esetbe prioritást élveznek a többi közleménnyel szemben. A sebesültmentési igényt kódnevek alapján adják le, a kiérkező helikoptert pedig a csoportban az erre kiképzett katona irányítja egy alkalmas leszállóhely felé. A kiemelést követően, a helikopteren már orvosok kezelik a sérültet, akit lehetőség szerint azonnal korházba szállítanak. [5]

1 QRF – Quick Reaction Force – gyorsreagálású erők

2 CLS – Combat Life Saver – harctéri életmentő

3 MEDEVAC – Medical Evacuation – sebesült kimentés

A különleges műveleti csoport feladatrendszere

„Különleges műveletek olyan katonai tevékenységek, amelyeket struktúrájában erre a célra kialakított, szervezett, speciálisan kiképzett és felszerelt, kis létszámú katonai egységek hajtanak végre a hagyományos fegyveres erők által többnyire nem alkalmazott harceljárások és alkalmazási módok felhasználásával. Ezen tevékenységeket a katonai műveletek teljes spektrumában (békeműveletek, válsághelyzet, hadiállapot) a stratégiai vagy hadműveleti célkitűzések elérése érdekében önállóan, vagy a hagyományos fegyveres erők többi haderőnemével együttműködésben hajtják végre.” [6]

A különleges műveletek esetében, a katonai hadviselés alapelvei éppúgy érvényesek, mint bármely más katonai művelet esetében. Azonban előfordulnak olyan speciális helyzetek, amikor a feladat jellege megkívánja, hogy bizonyos alapelvekre nagyobb hangsúlyt fektessünk. Ezen helyzetekben az alapelvektől való részleges eltérést többek között az a tény követeli meg, hogy a különleges műveleteket végrehajtó alegységek a hagyományos erőkkel szemben maximum egy szakasszal megegyező létszámú katonával, és számottevő tartalék vagy utánpótlás nélkül hajtanak végre komolyabb felkészülést igénylő bonyolult feladatokat. [6] Az alacsony létszámú, de speciálisan képzett katonák csoportja a leghatékonyabb a különleges feladatok végrehajtásának vonatkozásában. Azoknak a parancsnokoknak tehát, akik a különleges műveleteket tervezik, pontosan ismerniük kell a hadviselés alapelveit és azt is, hogy azokat hogyan alkalmazzák a különleges műveleti feladatok tükrében. Figyelembe kell venniük a tervezés során azt, hogy a különleges műveleti erők nem helyettesítik a hagyományos erőket, viszont körültekintő alkalmazásuk esetén jelentősen növelhetik azok hatékonyságát. Fontos továbbá felmérni azt is, hogy a támogató, illetve a különleges műveleti feladatokba bevont erők alkalmasak-e arra, hogy kiszolgálják, adott esetben összedolgozzanak a speciális feladatokat végrehajtó alegységekkel, hiszen abban az esetben, ha a kooperáció nem működik, az a művelet sikertelenségéhez vezethet.

A különleges erők együttműködését a hagyományos erőkkel, két részre bontva szemléltethetjük a legmegfelelőbben. Ahogyan korábban említettem, a hagyományostól eltérő harceljárásokat és felszereléseket felsorakoztató különleges műveleti erők kifejezetten alkalmasak arra, hogy felvegyék a harcot az újfajta katonai fenyegetésekkel szemben. A speciálisan felkészített alegységeket képessé kell tenni arra, hogy szembe tudjanak szállni, és le tudják küzdeni a folyamatosan változó kihívásokat. Feladatrendszerüket hozzá kell igazítani az adott térség által

szabott követelményekhez, hiszen minden egyes missziós terület sajátos klímával, domborzattal, és helyi kultúrával rendelkezik. A közvetett (non-kinetic) képesség esetében a különleges erők tevékenységét szorosan együttműködve a hagyományos erők támogatják. Ezen feladatkört tekintve, a különleges erők folyamatos jelenlétükre, és komoly helyi ismereteikre támaszkodva billentik pozitív irányba a válsághelyzet alakulását. Ezen esetben a végrehajtandó műveletek kevésbé kockázatosak. A másik kategória a közvetlen (kinetic) képesség. Alkalmazása során a katonák feladata komolyabb tervezést és felkészülési igényel. A közvetlen műveletek olyan feladatokat foglalnak magukba, amik során a különleges erők azon képességeit használják ki, amik megkülönböztetik őket a hagyományos erőktől. A közvetlen műveletek alkalmával a katonák, speciális körülmények között adott felelősségi körzeten belül hajtják végre feladataikat. A műveleti területre érkezve megtalálnak, azonosítanak és semlegesítenek olyan kiemelten fontos stratégiai célpontokat, amik leküzdése pozitív irányba mozdítja az adott térségen belül zajló katonai tevékenységeket. Ezen esetekben általában a különleges műveleti erők támogatják a hagyományos erők feladat-végrehajtását.

A hagyományostól eltérő módszereket és harceljárásokat alkalmazó, különleges műveleti erők felszerelése is nagyban eltér a Magyar Honvédségben megszokottól. Feladataikat a katonai műveletek teljes spektrumában, békében, válságban, és konfliktusban is megbízhatóan képesek végrehajtani, stratégiai és hadműveleti célok elérésének érdekében. Műveleteiket képesek önállóan, vagy hagyományos erőkkel együttműködve végrehajtani, de számos esetben kooperálnak külföldi különleges, vagy hagyományos erőkkel is. A különleges feladatoknak dinamikusan kell követniük az aktuális műveleti terület politikai és katonapolitikai változásait, a biztonságpolitikai és katonai stratégiai változások ugyanis, a technikai fejlődéssel kiegészülve nagyban befolyásolhatják a különleges erők alkalmazásának lehetőségeit.

A különleges erők műveleti területen, az adott hadszíntér parancsnokának elgondolásai alapján hajtják végre feladataikat annak érdekében, hogy támogassák a hagyományos erők műveleteit, és megfelelő feltételeket teremtsenek számukra a harc megvívásához. A speciális képességekkel rendelkező különlegesen képzett erők, más csapatokkal szemben alkalmasak arra, hogy feladataikat rejtetten végezzék, fokozottan nehéz körülmények között, megelőzve így azon jelenségeket, amik a hagyományos erők alkalmazása során lépnének fel.

Alapvető feladatok:

1. Különleges felderítés és megfigyelés. (Special Reconnaissance – SR)
2. Közvetlen akciók. (Direct Action – DA)
3. Katonai segítségnyújtás. (Military Assistance – MA)

A három féle alapvető feladatrendszert, két jól elkülöníthető területen belül osztjuk szét. A katonai segítségnyújtás feladatkörét az indirekt, azaz közvetett műveletek közé soroljuk. Indirekt műveleti tevékenység végrehajtása során, a különleges erők olyan tevékenységet folytatnak, aminek következtében felelősségi területükön belül oly módon alakítják és befolyásolják környezetüket, hogy állandó jelenlétükkel pozitív irányba mozdítsák elő az adott térség katonai műveleteinek sikerességét. A másik kategória, amibe a közvetlen akciókat és a különleges felderítést és megfigyelést soroljuk a direkt, azaz közvetlen műveletek megnevezést kapta. Ezen műveletek során, a különleges erők kiemelkedő képességeiknél fogva nagy hatékonysággal alkalmazhatóak olyan feladatok végrehajtására ahol a hagyományostól eltérő a környezet, a feladat jellege, így a hagyományos erők képtelenek lennének sikert elérni. Ilyen feladatok esetében, az említett speciális körülmények között a különleges műveleti katonáknak közvetlen beavatkozó erőként kell fellépniük, fel kell kutatniuk, azonosítani és semlegesíteni az ellenséges fegyveres erőket. [8]

Összegzés

A cikkben bemutattam egy különleges műveleti csoport felépítését és feladatait. Kitértem arra, hogy melyek azok a szempontok amik meghatározzák egy ilyen alakulat szervezeti felépítését és technikai hátterét. Kifejtettem a csoportok alá- fölérendeltségi viszonyait, és a különleges alakulatok fontosságát a mai hadszíntereken. Ismertettem a sajátos struktúrát a felszerelés és feladatrendszer béli sajátosságokat, hiszen ezek azok a szempontok amik a különleges erőknél nagyban eltérnek a hagyományos alakulatoktól.

Felhasznált irodalom

[1] Bodoróczki János: A különleges erők történetének áttekintése, Hadtudományi Szemle, 2013. 6. évfolyam 4. szám, Budapest, 2013., pp.1-10.
[2] Dr. Forray László: A Különleges Műveleti Zászlóalj javasolt szervezeti felépítése, Hadtudományi Szemle, Budapest, 2012. 5. évfolyam 1-2. szám, Budapest, 2012.
[3] A különleges műveleti zászlóalj alkalmazási elvei, Nyt. szám: 237/138. 2010.
[4] Szelei Ildikó: A mindennapok pedagógiája a parancsnoki, vezetői munkában, Honvédségi Szemle, A Magyar Honvédség központi folyóirata, pp.: 56-59. (2012)
[5] FM 3-05.20 (FM 31-20), Special Forces Operations, Headquarters, Department of the Army, Washington DC, 1 April 2004.

[6] A különleges műveleti erők alkalmazási irányelvei, MH Összhaderőnemi Parancsokság kiadványa, nyt.szám: 94-658/2008, p. 4
[7] Tóth András, Farkas Tibor, Pándi Erik: A válságreagáló műveletek híradó és informatikai támogatásának elméleti alapjai; Hírvillám 1. évfolyam 1. szám, Budapest 2010, pp. 32-44.
[8] FM 3-05.130, Army Special Operations Forces Unconventional Warfare, Headquarters, Department of the Army, Washington DC, 30 September 2008

HRONYECZ Erika – KERTI András: An analyze on the attacks against critical infrastructure in Hungary, especially with internet media in scope

Absztrakt

A kritikus infrastruktúrák (KI) védelme az utóbbi évek eseményei hatására alapvető fontosságúvá vált. A szakirodalom feldolgozása során azonban feltűnt, hogy a cikkek, tanulmányok és egyéb művek vagy általánosságban foglalkoznak a témával, vagy a külföldön megtörtént eseteket dolgozzák fel, nem találtunk olyan tudományos publikációt, amely a hazai KI-t ért „támadásokat" dolgozná fel. Cikkünkben az interneten elérhető forrásokra használjuk mert az internet társadalmi tudatformáló tényezővé vált, a KI-t felhasználó lakosság zöme is innen szerzi be információinak nagy részét, és nem utolsó sorban nagyon egyszerű és gyors az információk visszakereshetősége.

Abstract

In this article, the authors describe the main definitions of the Critical Infrastructure that is the foundation for the future research. They demonstrate the fundamentals of the hungarian regulation, and specialize the disaster situations in recent years in Hungary, which were threatened the Critical Infrastructure. Above all the authors analyze the measures and conclusions of snow emergency in 2013.

Kulcsszavak: *kritikus infrastruktúra, hekker tevékenységek, információvédelem, internetes támadás*

Introduction

Protection of Critical Infrastructure (CI) became of substantial importance, because of the events of recent years – increasing tendencies of terrorism, natural disasters etc. [1] – as can be seen from the great amount of scientific publications referring to this field. Analyzing the literature it can be said, that the works are handling the field either in general, or based on foreign events, and we hardly manage to find such *scientific* publication, which elaborates the attacks against

domestic CI[1]. This is most certainly because treating this field, one can easily cross the moorland of politics. Our opinion is however, that objective handling of the events happened, based solely on professional and scientific work is inevitable. We regard this kind of work most important to get a picture of the actual state of critical infrastructure-protection on one hand, and to be able to increase the quality of the protection based on these researches on the other.

In this paper we refer to sources reachable on the internet – online news, regulations, and other kind of media – because during the process of protecting CI, great amount of sensitive and certified data can be created, and we are not meant to get into the act of violating any secrets. Other reason is that the internet became a force, shaping the mind of the society, since the main part of the population, using CI gets its information from the very same source Last but not least retrieving the information is very easy and quick by this mean.

Using the internet hides the trap anyhow, that too much and unsettled information can be reached, thus not all publications regarding the field, and not even all the events have been discussed, only those, which are regarded as to be important concerning the main goal of this paper.

Basic terms and the analyzed cases

Before going any further, we have to clarify two things; first the terms, being relevant to our research and their meaning, and second the cases being researched, and the reason, why exactly these have been analyzed. We would like to clarify three basic terms, these being: critical infrastructure, vital system-element, and attack. Regarding the first two ones, Hungarian regulation makes them clear:

Critical Infrastructure „[…] means such interconnected, interactive and mutually dependent network of infrastructural elements, objects, service, systems and procedures, which are of vital importance to the country (population, economy and government) and have a substantive part in maintaining a socially expected minimal law, order and national security, economic operability, healthcare and ecologic conditions.”[1.]

“Vital system-element: such part of a tool, object or system belonging to one of the branches defined by law, which is inevitable to secure the vital social tasks, [...] and that’s breakdown would cause the lack in securing such tasks, thus would cause serious consequences.”[2.]

1 We apologize to those authors, whose work we were not being aware of!

Thus the vital system-elements are the basically most important parts of the critical infrastructures. Which elements could possibly fit into the term "vital"? This has to be defined by the government, and more definitely by the departmental ministers. The law on defining vital systems and facilities[2] marks 42 sub-fields of 10 fields, where vital system-elements may be. Among others, the facilities of electric energy system, railroad traffic, and broadcasting are such. We made a distinction in favour of these, because in our opinion, these where the fields suffering some kind of attack in the last years.

In opposite to the other two terms, attack has to be clarified in this article. Speaking of an attack, we mostly think of some kind of human interact, like armed attack, or hacker activity. We don't have to go far however, to find examples of other kind of attacks, if we think about those of "General Winter" for example. Thus every factor, which can potentially cause damage, is regarded as peril until only possibility occurs, but in case of real damage, we speak of an attack. [3]

On the particular threats and possible attacks on CI-s, we get some information from the Hungarian "Green Book" [1]:

"In accordance with the PNCI[2], we distinguish especially the following threats [...]:

- threats in conjunction with intentional, and harming acts, and activities e. g.:

= criminal acts (e.g. arson, abuse, stealing, theft, sabotage, criminal acts against computer systems and data, jamming of communal facility),
= abuse of, and cyber attacks against critical informatic systems and networks, out of economic or political motive (cyber-terrorism, DDOS attacks, mass phising incidents),
= acts of terrorism, with its means and collateral actions (first of all abuse of explosives and arms, CBRN attacks),
= armed conflicts (e.g. war, attack of armed groups, civil war),

- threats of natural origin, which occur independently from human action, as natural disasters, as a result of climatic change, and the forces of nature, e.g.:

= flood,
= earthquake, devolution,
= wood fire

2 Protection of National Critical Infrastructure

= extreme weather conditions (windstorms, downpour, long-term drought, extreme cold, swelter, great snowfalls, snow-storms),
= sleety rain, constant fog, intense icing.

- Threats of civilization origins, technological threats, which are in conjunction with human action, and occur because of inappropriate human intervention, default, lack of caution, or technical constructional failures, e.g.:

= informatic programming failure,
= planning, and constructional failure,
= impact of a space object
= roadway, railroad, water and air traffic accidents,
= damage of environment, pollution of surface water, air pollution,
= accident in a dangerous industrial facility, exploitation of hydrocarbons, storing and transport of dangerous material,
= technological-technical accident, jamming of industrial facilities,
= nuclear accident,
= conflagration,
= epidemic."

With the terms having been clarified, let's see, which events of the last years can be measured as attacks against critical infrastructure in our opinion:

- extreme weather conditions between March 14-16 2013, because of which the roadway and railroad traffic of Trans-Danubian territory became faint for days, and several settlement of Borsod-Abaúj-Zemplén (BAZ) County remained without electricity.
- in January 2009, again because of extreme weather, electricity fell out for 2-3 days in some 120 villages.
- in May 2010, creaks Sajó, Bódva, Bodrog and Hernád flooded, defensive work became necessary, houses and roads got under water in some 208 settlements only in BAZ County, and in the villages involved electricity had been jammed.
- on October 4. 2010, the dam of the red sludge dump of Hungarian Aluminium Production and Trading Zrt. between Ajka and Devecser broke through. The slop fled the deeper lying parts of Kolontár, Devecser and

Somlóvásárhely. It destroyed the infrastructure in the territories concerned totally.

- in June 2013, a mass of water, braking all records ever since, arrived Hungary. Despite the defence being successful, it hindered railroad-traffic at Almásfüzitő, and it damaged electric-, communication- and road-system in the floodlands.
- in September 2006, protesters against the ruling government seizured the hall of the public media, and caused more than 200 million HUF damage in the facility.

Our list is not complete, but it can be outlined from these events, that no main attack against critical infrastructure, concerning the whole of the country did occur, only some of regional level. [4] The attacks and the critical infrastructure, being attacked in them, are summarized in the following table:

No.	date	event	attacker (threat)	infrastructure being attacked (threaten)
1.	September 2006	siege of the hall of public media	acts of intentional harm	broadcast
2.	January 2009	extreme winter weather	extreme weather conditions	electric system, roadway-, and railroad traffic
3.	May 2010	flood in Northern Hungary	flood	electric system, roadway-, and railroad traffic
4.	October 2010	red sludge catastrophe	technological-technical failure occurring in industrial facility	whole of infrastructure
5.	March 2013	extreme weather	extreme weather conditions	electric system, roadway-, and railroad traffic
6.	June 2013	flood on the Danube	flood	electric system, roadway-, and railroad traffic

Conclusions

The extreme snow situation of March 2013, like a veterinary horse, incorporated lots of problems, from which there is many to be learned in favour of protecting critical infrastructure. Anyhow it can be said, that the ones, participating in the rescue, have done anything and everything possible:

"So, a sum of 30 thousand people took part in the rescue works, civilians, and the members of municipalities as many as 6500 grabbed shovels. The 14 thousand people stuck on the roads (9 thousand cars, and 23 trains had to stay put on 15. March) had got shelter assigned in 227 settlements and 40 vehicles. Some 146 settlements could not have been reached by railroad, but till Saturday evening, every of them have been released."[7.]

If works of such great volume have been going on, why wrote the media about „snow chaos", and the incompetence of the governmental authorities? Not to speak of the everyday political fighting, the answer to our question lies in the supply with information, better said in its lack. It is truism, that we live in an information society, the Gulf War in 1991 being the first one that had been watched by the world from the armchair, through television. The population is craving news ever since, and the more involved in the events, the more this is true.

If we take a look on the report of the Ministry of Internal Affairs, it can be seen, that the discontent with the work of those involved in the rescue was increasing linear with the growing of physical distance from the events. From own experience by speaking with those concerned, it can be said, that they suffered greatly from the lack of information.

It can be laid down however, that the authorities involved in the rescue were not failing, if we have attention on the legislative background. Hungarian rule of law[1], but even the ruling of the EU doesn't prescribe the obligation of public information.[3][8.]. The regulations mentioned are only dealing with sensitive information on protecting critical infrastructure. Protection of critical information is but a nationwide task: "every actor (governmental, branch/business alliances, standardization authorities, owners, operators) take part in the running of critical infrastructure. Every actor has to cooperate in accordance with its given tasks and responsibility, and has to contribute to the defining and realization of the PNCI."[1] In this case, population is also amongst the actors. Protection, here repulse can only be maintained effectively, when *everyone gets the information required.*

3 It has to be outlined here, that public information isn't the same as public alarm!

Let's see an example, in which an online newspaper writes about the case, when some had to dig themselves out of snow in four hours, after waiting some 20 hours for nothing.[8] How does this connect here? Had these people have got the information of not being able to be rescued in let's say five hours, since rescue work cannot have been started everywhere at the same time, after waiting a rational amount of time – 1-2 hours – they could have began with the work earlier, they could have escaped earlier, and the road section could have been released earlier as well. The same can be confirmed from the case, where a father, together with his whole family was being held under snow all night long, and being worst, he said, was that next day, by daylight they had to learn, that some 200 meters away the road could have been passed easily.[10]

"Help yourself and God will help you". From these examples it can be seen, that people have willingness to help, and they like to help in emergency situations. This can also be said, when they are not concerned immediately by the events. Best example is the case of the flood in June 2013, when thousands of people have helped voluntarily to build sandbag-walls.[11][12] With the aid of volunteer engagement, work can be more effective, consequences can be mopped up quicker.

It is important to lay down anyhow, that volunteer work is not the same as defence duty, prescribed by the emergency law:

"16.§ During the defence, the mayor:

c) is assured to engage the citizen being under obligation of civil defence, to stand his/her duty by resolution."[13]

The latter can be ordered by the mayor, and is obligate, thus it can be more planned and calculated. Volunteer engagement in contrast, can be by far more effective, if we are able to utilize the zeal of the volunteers involved. Anyhow, given by the nature of this institute, the volunteers can most likely be used for auxiliary work only, since their number is hardly predictable, and the usefulness of their profession can change in accordance with the place of involvement and possibly even with the time of the day.

Question may be asked, how volunteer work can be utilized more effectively. We're supposed to find an answer in the field of controlling. A blog, named "444"[14] writes in a rather critical voice about the problems, irritating the volunteers involved in the rescue work against the flood. It can be said, that here too, the lack of information meant the biggest problem. It isn't a problem, to have to wait for a phase of work, rather if it seems to be unnecessary, and it's unknown, why, and how much has to be waited. Own experience says that the people have to feel, that what they are doing is important. To this reason, they also have to know, if at the given place no adequate task to the given number of volunteers may

actually be. For such cases, it isn't useless to prepare for transporting the surplus number of workers to places, where there is lack of them.

By the time of writing, we could manage to determine only magnitude of the people taking part in the defence against the flood voluntarily in 2013. It could be some sort of acknowledgement for the volunteers, if they could show their friend e.g. on the internet, when and where they did their part of engagement. This wouldn't mean much extra work, since even the critical blog, mentioned earlier has to recognize, that by their arrival at place, administration had been sufficient.[14] Acknowledgement could also increase efficiency.

Other form of utilizing volunteer work is the partaking in organizing the flow of information. A tendency to this, already evolving spontaneous, can be reached in the following online article:

"At the time, when the websites of the highway control and other authorities where impossible to reach, community media has shown an outstanding performance: people were able to refresh their information about road-blocks from blogs, the Facebook and other Web2 channels constantly. Many asked here for help or offered some for them being in trouble. Speaking of Web2, the blog Media 2.0 is worth mentioning, where a real comment-tsunami evolved, when a poster stated: in place of the state media and leading news portals, the country-side radio-stations and community media saved the car drivers from freezing death."[15]

Nowadays many possess devices securing mobile internet reaching, and they also get information online. At the snow emergency in March 2013 official web pages broke down, possibly due to a spontaneous DDoS attack caused by too many visitors. In our opinion, this leads to two possibilities and tasks for official organizations:

- Develop their own technical conditions, secure greater server capacity, and higher reaching speed.

- Utilize community pages, Web2 and the possibilities given by the ability and will of volunteers to communicate.

Utilizing Web2 isn't an idea of the authors; Hungarian Defence Force lived up the opportunity during the snow emergency:

"HDF covered the events on its Facebook page scrupulous for days; where the soldiers were at, in what kind of rescue work they were involved. Followers could get information first hand, in which hospital parturient women had been brought by tracked or other high performance military vehicles, or where seriously

ill people had been rescued, to whom the ambulance stuck in snow, could not reach."[15]

Everyone recalls the SMS sent by the BM on 15. March 2013, regarding the snow emergency. It got into focus of jokes and the crossfire of opposition, but in our opinion it has been an engagement leading forwards. In case, we learn from the failures during the mentioned procedure, we get a tool good to go in an emergency situation to reduce the effects of an attack against critical infrastructure.

Let's analyze which failures the ominous SMS had got:

1. It had been delivered to every person possessing a cell phone of Vodafone and T-mobile network, even being hundreds of kilometres away from the events.

2. It consisted of information being too universal. The text: "We will help! Don't abandon your vehicle! If you run out of petrol, sit into another vehicle! Ministry of Interior" held no information being useful to the ones stuck in the snow.

3. It reached the people too late. The road blocks caused by the weather coming from direction west, didn't occur everywhere at the same time, but cars stuck in the snow already in the afternoon of 14. March. The SMS had been sent only after 14 o'clock on 15. March, causing many to spend many hours already in custody of the weather.

Failure 1: isn't a failure, but a lack of legislation in reality. According to Attila Samu, senior adviser to the Ministry of Interior[5] the cell phone providers are not obligated to send messages of this kind. Thus, in emergency, like this, we are depending on the well-meaning of the providers.

Question is, if the circumstances, regarded by us as failure are somehow to be maintained. We have the opinion that the answer is yes. Let's see the possibilities in order:

First failure, according to the chief executive, was that the SMS could only have been delivered in this form, involving everyone in the same network. It is most likely, that this is also the case nowadays, but technically it is possible to maintain the identification of active cell phones at a certain territory. It is widely known that those cell phones are communicating constantly with the regional tower being next to them, even when we don't dial, or receive any calls. Naturally this communication involves also the number of the given cell phone. It is

practically only the question of HW and SW that if necessary, a list of the devices in reach of the given tower could be received. It is understand, that an SMS could be sent to more users simultaneously.

Even in this case it cannot be ruled out of course that also people would get the message, who are not concerned in any form by the events given. If we think about the events above: the highway is only a part of the territory covered by a certain tower, so if an SMS would have been sent in the manner consulted, some would have got it within the security of their room, outside the emergency on the road. However, this circle would even have been smaller this way, as it was in reality as the events occurred.

In our concern, a legal question is regarded as a greater problem. Namely the protection of personal data. Where and when one be, is regarded as personal data, and it can even possibly be a special kind of personal data. Collection and settling of such personal data is regulated by law[6], thus the list of data suggested by us to be collected in an emergency has to be clarified.

The second failure: Analyzing the information held in the message, question may occur, what the 160 characters of an SMS could be enough for. It seems to be quite small portion, if we consider that in favour to avoid misunderstandings, the regular shortenings of everyday messaging must not be used in this case. Our opinion is despite the above, that much of useful information can be sent this way, with the psychical effect being of even more importance, since the ones concerned by the events have not to feel themselves alone, and being abandoned in their situation. What kind of information may it be? For example:

- Certain information regarding the place of rescue: *"Based on our information you are being near an emergency situation, help is expected to arrive in one hour!"*

- Referring to a broader source of information. During the flood of June 2013, the radio station of Győr city already broadcasted data about the water level and the defensive works before the arrival of the flood. Similar to this, public media ran flood emergency radio, using the frequency of the station Neo FM. Utilizing this opportunity, attention of those in trouble can be called: *"Based on our information, you are being near an emergency situation. For further information, please listen to XXXXXX radio station on frequency 92.5 MHz!"*

The above are only some kind of ideas, content of the information has always to be aligned to the events, but from these two examples it can be seen that this kind of communication can also be useful.

Third failure was caused by the fact that the system isn't prepared for such kind of communication. According to Attila Samu[5]: "During the first phase of the rescue, biggest problem seemed to be, how to reach those trapped in snow. They have had to be calmed, and informed. Many possibilities had been analyzed, and it turned out that sending an SMS would be the easiest way."

We are sure, that in case, the technical and organizational measures had been introduced, and regulation obstacles would be tackled, in certain cases the staff coordinating rescue or defence, would be able even in the first hour to live up the opportunity given by sending SMS.

Dealing with the fourth failure is a task for the law-maker. We would like to reflect on some other issues that require legal regulation as well.

The first two questions of legal regulation have already been mentioned; namely the ability to collect data of personal kind during protection of critical infrastructure, and the responsibility of the operator by helping the flow of information in SMS.

The law on electronic media regulates in its 157.§ which data the operators are assured to handle during their work. Among others, point (2)f) mentions "the type of call or other service, the direction, starting and timeframe of communication, volume of data transmitted, the ID of the network, cell and the particular device using the service (IMEI), in case of IP networks, the identifiers"[16] used, as collectible. Point (10) of the same paragraph regulates the case of handing over data:

"The electronic communication provider – to assure the fulfilling of the regulated tasks of investigating authorities, prosecution, court, and national security agency authorized to acquire data by law – is obligated to hand the required data over, or secure access to them, in accordance with section (2)"[16]

Thus the law-maker has only to clarify in law, who and in which form has to deliver the data necessary to send the separated SMS in case of protection of Critical Infrastructure, or mop up of a catastrophe.

As a summarized conclusion of the attacks on CI analyzed above, we can say that in reduction of such attacks, information of the population, especially those concerned, is inevitable. With proper information it can be maintained, that volunteer engagement becomes more effective, and those suffering from the events can be of more confidence towards those participating in their rescue. Both are important factors in the judging of the rescue work. Every possible tool is to be

utilized during the information of the population, anyhow technical and legal problems have to be solved to maintain this.

Bibliography

[1.] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
[2.] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[3.] Tóth András, Töreki Ákos: A kritikus infrastruktúrák és azok védelmi lehetőségei, Hírvillám = Signal Badge (1) pp. 143-148.(2010)
[4.] Farkas Tibor: Questions and tasks of communication in disaster and crisis situations in Hungary; In: Fekete Károly (szerk.) Kommunikáció 2015: Communications 2015. 214 p. Budapest: NKE Szolgáltató Kft., 2015. pp. 117-126.
[5.] Minden vodás és T-mobilos kap sms-t http://index.hu/belfold/2013/03/15/minden_vodafone-os_es_telekomos_kap_sms-t/
[6.] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
[7.] http://mno.hu/belfold/hohelyzet-itt-van-pinter-sandor-jelentese-1148815
[8.] A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
[9.] http://www.origo.hu/itthon/20130315-akik-kimentettek-magukat-a-ho-fogsagabol.html
[10.] http://www.origo.hu/itthon/20130316-olvasoi-tortenet-a-marciusi-havazasrol.html
[11.] https://www.facebook.com/Arviz2013Osszefogas
[12.] http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_hirek&hirid=1895
[13.] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
[14.] http://444.hu/2013/06/05/arvizi-onkenteskedes-belulrol/
[15.] http://index.hu/belfold/2013/03/16/katasztrofa_minden_fronton/
[16.] 2003. évi C. törvény az elektronikus hírközlésről

[17.] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal, ISSN 1788-1919)

[18.] Négyesi Imre: Informatikai rendszerek oktatása a katasztrófavédelmi szakirányon (Hadmérnök on-line, V. évfolyam (2010) 2. szám, 25-40. oldal, ISSN 1788-1919)

LUTER Tibor: Szimpla MOSFET meghajtású plazmahangszóró kapcsolás és annak értékelése

Absztrakt:

A plazmahangszóró elektromos ívkisülés útján állít elő hangot. A levegőt melegítvén a két elektróda között, annak tágulását (hőtágulását) okozza, mely térfogatváltozást képesek vagyunk modulálni és az így keletkezett pici lökéshullámok sorozatát hangnak vagy zenének halljuk. Kevés ember van tisztában e lehetőség illetve eszköz meglétével kapcsolatban, ami részben köszönhető, hogy a piacon csak elvétve fordul elő egy-egy modell.
A mai állás szerint két kategóriát lehet szignifikánsan megkülönböztetni a plazmahangszóróval kapcsolatban – vannak hobbicélú építőkészletek és igen drága csúcsminőségű magashangsugárzók.
A hobbicélú eszközök általában DIY módon elkészíthetőek és nem képesek értékelhető hangminőség produkálására. A másik kategória késztermékei irrelevánsan drágák így egy átlagos háztartásban nincs helye, az otthoni felhasználás szinte lehetetlen.
Ebben a cikkben említést teszek különböző régebbről származó eszközökről és bemutatom az általam készített kapcsolást a tervezési fázistól kezdve a tesztelésig. A kísérleti eredmények azt mutatják, hogy még egy „low-cost" plazmahangsugárzó is, kombinálva egy sima elektromechanikus mélyhangszóróval képes minőségi frekvenciamenetet és élvezhető hangképet produkálni.

Abstract:

The writer shows int this paper his „low cost" plasma speaker and the switch of it which is made also by the writer. He got the result, that the plasma speaker combined with electromechanic speaker able to produce good quality of voice and frequency response.

Kulcsszavak: *plazmahangszóró, MOSFET, moduláció, Impulzusszélesség-moduláció, Szimpla tranzisztoros kapcsolás*

Bevezetés

A hagyományos hangszórók működésük során egy állandó mágneses térben szabadon mozgó tekercs által keltenek hangot. A tekercs a membránt oda-vissza, ki-be mozgatja és az így keletkező nyomás, nyomáskülönbséget keltik a hangot. Ezen hangforrások szinuszos jellel üzemelnek mivel a membrán a tömegénél fogva nem volna és nem is képes a négyszögjel hirtelen változásait (a ki és bemozdulást) azonnal reprodukálni.

1. ábra

Működési elv

Számos megoldás létezik nagyfeszültségű impulzusok generálására. A későbbiekben bemutatom az általam használtat.

A plazmahangszóró tehát nagyfeszültségű ívkisülések sorozatát állítja elő, mely a levegőt (főleg N2 és O2) felforrósítva a környezetében annak ionizációját eredményezi a két elektróda között. Erre a jelenségre az általános gáztörvény érvényes:

$$pV = nRT$$

p a nyomás, V a térfogat, n a gáz moláris mennyisége (konstansnak vett), R az egyetemes gázállandó, T a hőmérséklet.

Ha a hőmérséklet növekszik, akkor a nyomásnak és a térfogatnak is növekednie kell. A két elektróda között az ív hossza fix így az azt körülvevő gáz térfogata nem tud növekedni, így ez azt jelenti, hogy a nyomás növekedése szükségszerű. Ebből következik, hogy a nyomásváltozást érzékeljük hangként. Sajnos alacsony frekvenciák esetében a feltevés, hogy a gáz moláris mennyisége állandó, nem igaz ami nagyon rossz frekvenciaválaszt eredményez a mély tartományban. Ez a fő oka annak hogy a tárgyalt eszközt jóformán csak magas hangok kiadására tervezik (>2khz).

A sajnálatos hátulütője után vegyük előtérbe az érdemeit. Mivel nincs membrán se szignifikáns tömeg a hangkeltés mögött, ami potenciálisan alkalmassá teszi akár 150khz kiadására is. A frekvencia felső határát a forró, ionizált gáz mennyisége szabja meg, viszont lényegesen kisebb tömeget jelent egy membránhoz képest.

Háromféle elektromos üzemű plazmahangszóró típus van. Ezek a DC ív, AC ív, és koronakisülésen vagy ionszélen alapulók. Mind a DC és AC típusok óriási feszültséget használnak (7-30kV!) a gázkohézió megbontására és az ioncsatorna létrehozására és fenntartására. Amint sikerült a gázt (levegőt) vezető állapotba hozni, a modulált áram által keltett hullámok hangként jelentkeznek.

A korona kisülésen alapuló típusok is különböző elvek alapján működhetnek , ilyen például mikor a két töltött elektróda között erős elektromos mezőt hozunk létre amelybe beérkező vagy bent lévő részecske a katódhoz érve negatív töltésűvé válik és átáramlik az anód fele. Ennek az áramlásnak a szabályozásával szintén hang kelthető.

2. ábra [1]

3. ábra [2]

Részletesebben a megvalósításába nem mennék bele, a következőkben inkább az általam is megvalósított AC típust (Tesla mintájú, 2. ábra), azon belül is a fix ívhosszú (3. ábra) konstrukciót részletezem ki. A kutatás célja, hogy kiderítse, alkalmas-e egy efféle konstrukció jó minőségű, szépen csengő zene leadására.

Rövid történeti áttekintés

A tárgyalt téma nem egy új koncepció, már évtizedekkel ezelőtt, meglátta valaki benne a lehetőséget mint a hangszóró egy új és „lenyűgöző” formáját. Az elvi alapját pedig már az 1800-as években is ismerték már. 1957-ben került ki először a piacra szánt verzió. A plazmahangszórót általánosan csak magashangsugárzóként alkalmazták. Manapság a hasonló termékek két kategóriába sorolhatók: hobbicélú, nagyon drága jó minőségű, úgymond „high-end” termékek.

1. 1978-ban került az amerikai piacra a Hill Type-1 (4.ábra) elnevezésű sztereo hangfalpár, melyben fix hosszúságú ív muzsikált. Sajnos nem ért el átütő sikert, mivel a hangminőség javítására héliumgázt engedtek az ívhez, melynek a palackja a hangdobozban kapott helyet és természetesen időközönként újra-kellett tölteni.

4. ábra [3]

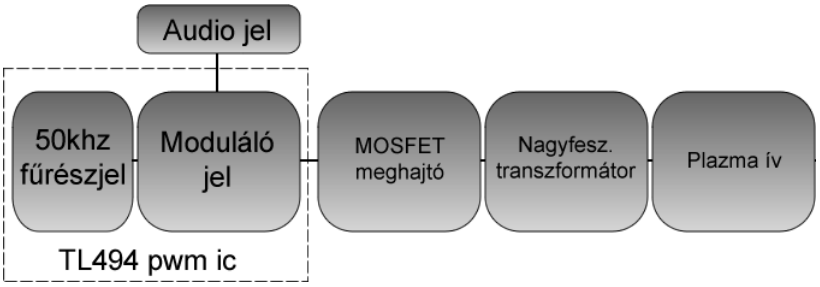
2. Ma két cég gyárt HiFi célú plazmahangszórót, ebből az egyik, a Lansche audio a termékét (5. ábra) 35 ezer dollár / pár áron kínálja.

5. ábra [4]

3. Számos hobbicélú elérhető akár az Ebay-en már 80-100 dolláros árkategóriában.

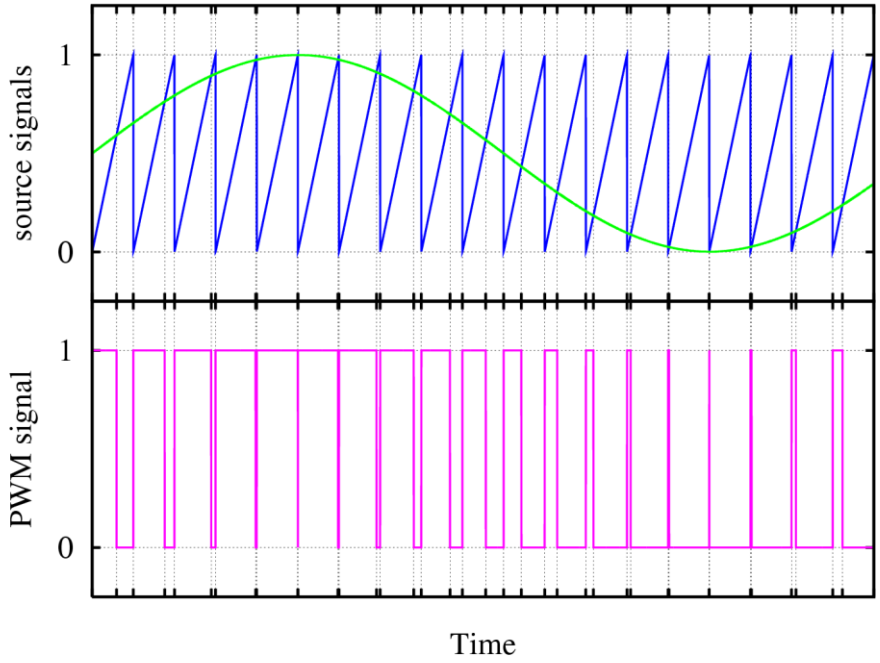
A kapcsolás áttekintése

A kapcsolás blokkdiagramja a 6. ábrán látható. A kapcsolás üzemeltethető 12V és 230V között. Ha rögtön hálózati feszültséggel tápláljuk, akkor megspórolunk egy nagyteljesítményű külön tápegységet (>300W). Érintésvédelmi és egyéb biztonsági okokból kifolyólag a kapcsolásomban 36V tápfeszültséget alkalmazok. A működése relatíve egyszerű.



6. ábra

A TL494 –es IC az 50khz-s vivőjelre rámodulálja az analóg hangfrekvenciás jelet, mely a kimeneten négyszögjelek formájában jelenik meg (7. ábra).



7. ábra: Impulzusszélesség-moduláció [5]

A moduláló jel változtatja mind a frekvenciát mind a kitöltési tényezőt. A kimeneti négyszögjel pedig kapcsolóüzemben hajtja a tranzisztort a megadott 36V-os tápfeszültségen. A meghajtó kimenetén lévő nagyfeszültségű trafó pedig a négyszögjel ütemében előállítja a plazma ívet. Az ilyen transzformátor nevezzük sorkimenőnek vagy „flyback" –nek, egész egyszerűen egy induktorként viselkedik, ha feszültséget kapcsolunk rá az áramerősség szép lassan növekedni kezd, melynek a mértéke a négyszögjel hosszától függ. Amint a tranzisztor vezetőből kikapcsolt állapotba vált hirtelen akkor a légmagban tárolt energia sokszorosan megjelenik ezen transzformátor szekunder tekercsén és megtörténik optimális esetben az ívkisülés.

A kapcsolás ismertetése

Ebben a részben bemutatom az elkészített kapcsolás főbb elemeit.

TL494 IC:

A kapcsolás legfontosabb eleme, mely segítségével végrehajtjuk az impulzusszélesség modulációt, ami egy olyan négyszögjel sorozatot eredményez, amit rákapcsolhatunk a flyback transzformátor primer körére. Ez a multi funkciós IC a feladatot úgy hajtja végre, hogy a beállított 50khz-es oszcillátor frekvenciára rámodulálja az audió jelet. A nagyfrekvencia szükséges a nagyfeszültségű trafó folyamatos vezérléséhez, melynek során az impulzus szélességét, hosszát az audió jel függvényében változtatva, a tekercsben és a légmagban tárolt energiát a szekunder tekercsre továbbíthatjuk minden egyes impulzus során.

Az oszcillátor frekvenciát az 5-ös és 6-os lábakra szerelt Ct és Rt, kondenzátor / ellenállás páros szabályozza a következő függvény szerint:

$$Fosc = 1 / (2piRtCt)$$

A frekvenciát lehetőleg a hallható tartományon kívülre szabályozzuk ami > 20khz. Az Rt természetesen lehet egy potenciométer is.

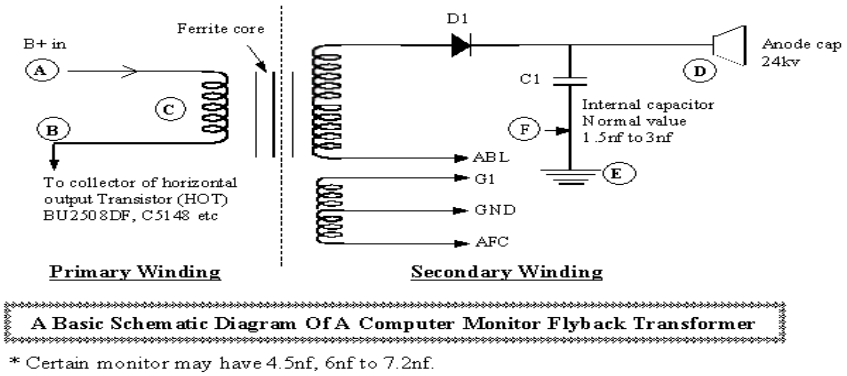
TC4420 FET meghajtó:

A meghajtó IC szerepe a MOSFET gate kapacitásának gyors feltöltése is kisütése. Ami simább tranzienseket eredményez így a végeredmény zajmentesebb lesz. Másrészt csökkenti a kapcsolási veszteségeket, ami kevésbé melegedő

tranzisztorokat eredményez, ezáltal a túlmelegedés könnyebben elkerülhető. A kis meghajtó ic közvetlenül a modulátor ic kimenetére kapcsolódik, és szintén tápellátást igényel.

„Flyback" transzformátor:

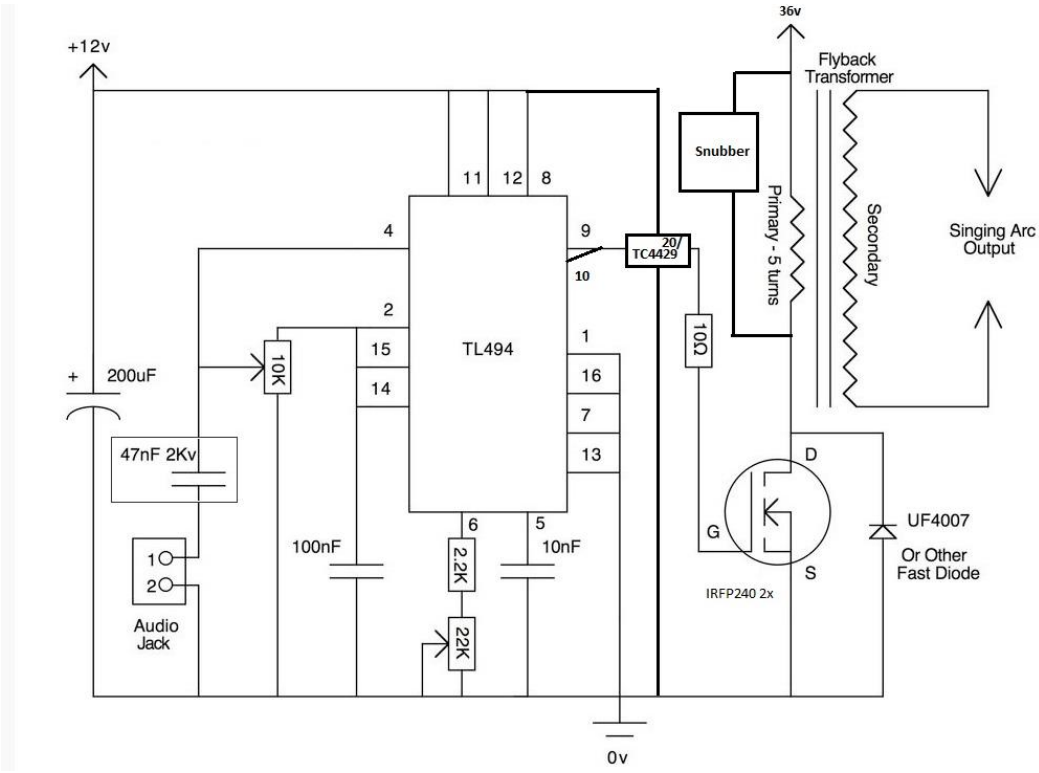
Vagy más néven sorkimenő transzformátor, egy kis menetszámú primer és egy sokmenetes akár >1000 menetes szekunder körből áll. A ferrit vasmag viszonylag kis légrésű 2 „U" alakból áll össze. A gyári sorkimenőknek több kivezetése is van, de mi csak az említett kettőt használjuk, sőt mi több a primer tekercsünket a vasmag szabad részére sajátmagunk is feltekerhetjük legalább 5-15 menet között, vékony szigetelésű 1-1,5mm2-es tömör réz drótból. Az elmondottak a 8. ábrán láthatók.



8. ábra [6]

A feszültség és a menetszám aránya:

$$Vs/Vp = Ns/Np$$



9. ábra: Szimpla tranzisztoros kapcsolás [7]

A működése tömören összefoglalva

A FET a transzformátor primer oldalát "kapcsolgatja", zárt állapotban a testre kapcsol, nyitott állapotban pedig az áram átfolyik a tekercsen. Az ívkisülés akkor történik mikor a FET zárt állapotból nyitottra vált.

Felhasznált irodalom

[1] http://www.easternvoltageresearch.com/audio_classe.html (2015. 02. 23)
[2] http://www.techeblog.com/index.php/tech-gadget/feature-geeks-use-plasma-tesla-coils-as-speakers (2015. 02. 23)
[3] http://www.stereophile.com/content/hill-plasmatronics-type-1-loudspeaker (2015. 02. 23)
[4] http://www.lansche-audio.de/eng/firma-4.html (2015. 02. 23)
[5] http://de.wikipedia.org/wiki/Pulsweitenmodulation (2015. 02. 23)
[6] http://protech2u.com/test-flybacktransformer-lopt.html (2015. 02. 23)

[7] http://scopeboy.com/tesla/flyback.html (2015. 02. 27)
[8] Alexeff, “A Plasma Loudspeaker Using a D. C, Carbon Arc,”IEEE Abstracts, 490. oldal, 2001.
[9] R. Sterba, “Distortion, Direction and Circuit modeling of a needle array plasma Loudspeakers,” The Faculty of the College ot Engineering and Technology, Ohio University, Ohio, 1991.
[10] http://www.easternvoltageresearch.com/audio_classe.html
[11] http://www.plasmatweeter.de/eng_corona.htm
[12] http://www.dos4ever.com/flyback/flyback.html
[13] http://www.plasmatweeter.de/plasmatronic.htm
[14] http://www.lansche-audio.de/eng/firma-4.html

DOMOKOS Máté: A különleges műveleti csoportok vezeték nélküli kommunikációs hálózata

Absztrakt

A szerző a cikkben bemutatja a különleges műveleti erők kommunikációs hálózatainak elemeit, működésüket, különös tekintettel a vezeték nélküli rendszerekre.

Abstract

In this publication the writer shows the communication networks of special operation forces, their elements and operations, in particular the wireless systems.

Kulcsszavak: *különleges műveleti csoport, vezeték nélküli hálózat, HARRIS, rövidhullám, ultrarövid hullám, mikrohullám*

Bevezetés

A hadviselés egyik meghatározó eleme a kommunikáció fenntartása. A hadisiker egyik kulcsa az, hogy a parancsnokok a csapatok mozgását összehangoltan tudják irányítani. Mivel a csata során sok váratlan esemény következhet be, amikre reagálni kell, elengedhetetlen hogy a parancsnokok folyamatosan kommunikálni tudjanak alárendelt vezetőikkel, akiknek az információkat még továbbítani kell a végrehajtó alegységek felé. Ez biztosítja azt, hogy az egymástól elszigetelten mozgó alegységek összhangban hajtsanak végre feladatokat, manővereket, és hatásosan vegyék fel a harcot az ellenséggel szemben. A parancsnokok és a beosztottak közötti kommunikáció fenntartása tehát már a korai időszakban is nagyon fontos volt. Annak érdekében, hogy az elöljárók folyamatos instrukciókkal láthassák el katonáikat, elengedhetetlen, hogy a csapatok számára rendelkezésre álljanak olyan eszközök, technikák, amelyek ezt lehetővé teszik. Ezek a távközlési eszközök korábban még igen kezdetlegesek voltak. Az emberek füstjelekkel, hegytetőkön rakott máglyákkal informálták egymást. A jó futókat kiválogatták, futárok lettek és csaták alkalmával ők szaladgáltak a parancsnok és a végrehajtó alegységek között, így továbbítva a parancsokat. Ezek a kezdetleges módszerek azonban sokszor megbízhatatlannak bizonyultak. A füstjeleket, és a tüzet jelentősen befolyásolták az időjárási körülmények, mindenki

számára láthatóak voltak, a futárok adott esetben elfelejtették vagy félreértelmezték a parancsot, és helytelenül továbbították azt. A tapasztalt katonák a csatában direkt a futárokat keresték, mert tisztában voltak vele, hogy az ő likvidálásukkal az ellenséges csapatok egy része, akár teljes egésze irányíthatatlanná válik, ami zűrzavart a másik fél számára pedig sikert eredményezhet. A hadászat fejlődésével a katonai távközlés is fejlődni kezdett. A későbbiekben már élesen elkülönültek egymástól a védelemben, támadásban, a szárazföldön, a tengeren és a levegőben alkalmazott távközlési eszközök és eljárások. Mindegyik típusnak megvan a maga előnye és hátránya is, főleg ezen tényezők amik meghatározzák azt, hogy az adott eszközt milyen területen alkalmazzák. Például a védelemben alkalmazott vezetékes híradás előnye, hogy megbízható an működik, nincs kisugárzása így megfelelő telepítés esetén a felderítése és lehallgatása nehéz, egyszerű kezelni, és stabilabb kommunikációt biztosít, ami független a környezeti és időjárási viszonyoktól. Hátránya hogy kiépítése időigényes, nem mobil, tehát csak a telepített helyén használható. Ezzel szemben a dinamikus műveletek során alkalmazott rádióhíradás kisugárzott jelek útján valósul meg, így könnyen lehallgatható, bemérhető és felderíthető, valamint instabilabb összeköttetést eredményez, amit az időjárás is befolyásolhat. Előnye viszont, hogy mobil, így mozgás közben is lehetővé teszi a kommunikációt. Mivel a különleges műveletek során a katonák állandó mozgásban vannak, kommunikációjuk a rádióhíradáson alapul. Vezetékes híradást csak a bázison belül valósítanak meg. Ez az oka annak, hogy a továbbiakban a telepített vezetékes híradást csak érintőlegesen ismertetem. [1] [2]

A katona, akinek kommunikációja megszakad az elöljárójával, és nincs vezetve irányíthatatlan lesz, és gyakorlatilag használhatatlanná válik a feladata végrehajtásának szempontjából, sőt adott esetben kifejezetten hátráltatja azt. A különleges erők számára, eltérő feladatrendszerükből adódóan kiemelt fontossággal bír a megbízható és folyamatos kommunikáció fenntartása épp úgy a csoport tagjai között, mint az elöljárók felé. Ennek érdekében, a műveleti területen feladatot végrehajtó alegységek több, egymástól független rádióhálót is készenlétben tartanak az elöljáró irányába, hogy egyik meghibásodása, vagy használhatatlanná válása se okozza a vezetés és irányítás megvalósíthatatlanságát. A nagyszámú tartalék rádióháló azonban önmagában nem biztosíték. Szükség van az egyes hálókban alkalmazott strapabíró, jól működő készülékekre, valamint a terep, év- és napszaknak megfelelő frekvencia megválasztására. A katonai műveletek során nagy az eszközök sérülésének veszélye, valamint folyamatosan ki vannak téve a szélsőséges időjárási körülményeknek is. Ezen okok miatt fontos szempont, hogy a készülékek a megfelelő anyagból, és minél magasabb

minőségben készüljenek. A folyamatos és megbízható kommunikáció feltétele továbbá, a híradó katonák megfelelő felkészítése. Ez magába foglalja azt, hogy a híradó specialista aktívan részt tudjon venni a tervezési és szervezési feladatokban, és képes legyen a honvédségben rendszeresített valamennyi rádiót szakszerűen és megbízhatóan kezelni. [3] A műveletek során folyamatosan ellenőriznie kell az összeköttetés minőségét, és a lehetőségektől függően javítani azt. Ahogy a különleges műveleti csoport elhagyja a viszonylagos biztonságot jelentő tábort, az összeköttetésnek attól a perctől kezdve élnie kell a csoport és a parancsnokság között. Ez azért nagyon fontos, mert az előre megtervezett menetrendben adódhatnak és adódnak is váratlan helyzetek, amiket sokszor az elöljárók segítségével kell megoldani. Az esetlegesen adódó váratlan helyzetekre minél gyorsabban reagálni kell, a művelet folyamatosságának fenntartása, és a sikeressége érdekében. A bázison belül, a rádióforgalmazásért és az okmányok szakszerű vezetéséért a híradó katona (Radio Telephone Operator - RTO) felel, míg a csoportoknál ezt a feladatot a híradó specialisták látják el. [4]

Az alábbi fejezetekben kifejtem a különleges erőknél alkalmazott 5 fő összeköttetési csatorna rendeltetését, azok működését, és a híradás megvalósítására használt eszközök típusát. Ezeket az összeköttetési módokat az épp végrehajtandó feladat jellege határozza meg. Ez azt jelenti, hogy a következőkben ismertetésre kerülő kommunikációs csatornákat nem kőbe vésett szabályok alapján hozzák meg így azok esetenként eltérőek lehetnek. Az általam alábbiakban leírt információk egy általános esetet tükröznek.

Ahhoz azonban hogy teljes egészében megértsük ezen rendszerek működését, véleményem szerint elengedhetetlen hogy képed adjak arról, hogy a rádiókészülékek által kibocsátott jelek milyen módon terjednek, és milyen tulajdonságokkal rendelkeznek. Azért fontos ezt a fejezet elején bemutatni, mert a későbbiekben láthatjuk, hogy akadnak olyan tartományok, amelyek alkalmazásával akár több ezer kilométeres távolságok is áthidalhatóak, azonban a változó környezeti hatásokkal összhangban kell változtatni az üzemi frekvenciát.

A katonai rádiók által kisugárzott rádióhullámok terjedési sajátosságai

A rádióhullámokat méreteik alapján kategorizáljuk, az összeköttetések tervezésénél ez határozza meg, hogy milyen feladatra melyik tartományból választunk frekvenciát. A haderőknél leggyakrabban használatos és harcászati szinten is jelenlévő tartományok a rövidhullám, az ultrarövid hullám és a mikrohullám. Minden egyes tartományt meghatározott típusú összeköttetés

létesítésére használják. Ezen három kategórián kívül természetesen egyéb tartományok is léteznek, amelyek megjelenhetnek a katonai távközlésben, de alkalmazási területeik korlátozottabbak így előfordulásuk ritka.

Általánosságok

A legfelső számon tartott tartomány a nagyon hosszú hullámok, amik mérete 100000-10000 méter, és 3-30 kilohertzes értékeket vesz fel. Nemzetközi jelölése VLF (Very Low Frequency). Ezt követik a 10000-1000 méter méretig terjedő rádióhullámok, frekvenciájuk 30-300 kilohertz között alakul. A hosszúhullámok felületi hullámként terjednek, tehát követik a föld görbületét. Ennek köszönhető, hogy elegendően magas kimenő teljesítmény mellett nagy távolságok hidalhatók át. A hosszú hullámokat többek között rádióműsor szórásra használták korábban, hiszen kevesebb adóval viszonylag nagy terület volt lefedhető. A hosszúhullámok jelzése LF (Low Frequency). A harmadik kategória a középhullámok tartománya, amik értékei 300-3000 kilohertz között mozognak. A hullámok mérete 1000-100 méteres nagyságig terjed. Jelölése MF (Medium Frequency). A középhullámokat szintén rádióműsor szórásra használják, ugyanis alacsony rezgésüknek köszönhetően a rádiójelek több ezer kilométer megtételére képesek. A korábban felsorolt három fajta rádióhullám esetében a leggyakoribb modulációs típus az amplitúdómoduláció.

Rövidhullámok

A következő tartomány, ami a középhullámokat követi, a rövidhullámok csoportja, amit szintén előszeretettel használnak civil rádióműsor szórásra, ugyanakkor már gyakran megjelenik a katonai alkalmazás terén is. A rövidhullám 3-30 megahertzig terjed, a hullámok mérete pedig 100 és 10 méteres nagyság között alakul. Jelzése HF (High Frequency) magyarban pedig RH (rövidhullám). Ez a tartomány kiválóan alkalmas nagy távolságú összeköttetés létesítésére, látóhatáron kívül is ugyanis ezen tartományba eső rádióhullámok visszaverődnek az ionoszféráról. A rövidhullámú terjedés szempontjából az ionoszféra legfelső rétegei fontosak, amik földfelszín feletti magassága körülbelül 50-500 kilométer és egyfolytában, változik. Ezt a változást jelentősebben befolyásolja a napszak, az évszak, a közeli égitestek mozgása illetve jelenléte, és a Nap sugárzása is. Az ionoszféra változásai az összeköttetés megszűnését eredményezhetik, a frekvencia megfelelő változtatásával azonban a változó légköri viszonyok mellett is

fenntartható a folyamatos kommunikáció. Székesfehérvárról az Összhaderőnemi Parancsnokságról például sikeresen létesítettek összeköttetést az Afganisztánban szolgálatot teljesítő katonákkal. Erre kezdetekben egy régi típusú analóg R-130-as rádiót használtak, amit később egy megbízhatóbb és korszerűbb Harris típusú rádióra cseréltek.

Ultrarövid hullámok

A 30-300 megahertzig terjedő tartomány, az ultrarövid hullámok (Very High Frequency) csoportja. Ezt a tartományt szintén gyakran, és régóta alkalmazzák katonai távközlésre, de a civil felhasználása is gyakori. Rádió, és tévéműsor szórására egyaránt alkalmas, valamint radarok is használják a tartományt. Katonai szempontból alkalmazása a szárazföldi csapatok vezetés-irányítási rendszerében a legszembetűnőbb. A hullámok mérete 10-1 méter között alakul. Ezt a tartományt kisebb távolságú összeköttetésekre használják, legtöbbször raj és szakasz szintű egységek között, valamint légi eszközökkel történő kommunikációra „AM[1]” modulációban. Ennek megfelelően elegendően nagy kimenő teljesítmény mellett egy URH (ultrarövid hullámú) rádió hatótávolsága 20 maximum 30 kilométer tereptől függően. Az URH tartomány esetében figyelembe kell venni a kétutas hullámterjedésre vonatkozó szabályszerűségeket. Kétutas hullámterjedés esetében a direkt hullámok mellett megjelennek a föld felszínéről visszaverődő indirekt hullámok is. A visszaverődés következtében az indirekt hullámok által bejárt út hosszabb, ez pedig fázis és amplitúdóbeli eltéréseket okozhat a vevő helyén. Ez az eltérés függ a visszaverő felülettől, a polarizációtól és a beesési szögtől egyaránt, és minőségi romlást okozhat a vételben.

Mikrohullámok

Az utolsó, katonák által is gyakran használt frekvenciatartomány az mikrohullámok csoportja. A 300 megahertz feletti tartománynak jelenleg nincs rögzített felső határa, hiszen a rádiótechnika rohamos fejlődése napról napra új eljárásokat eredményez a mikrohullámú tartomány esetében is. A mikrohullámokat a civil szférában is számos területen alkalmazzák hatékonyan. Távközlés területén például mobiltelefon rendszerek, műholdas műsorszórás, az orvostudomány is alkalmazza, de jó példa hétköznapi alkalmazására a mikrohullámú sütő vagy a wifi.

1 AM - Amplitúdómoduláció

Katonai alkalmazása nem sokban tér el ezektől, ebben a tartományban működnek a műholdas telefonok, a VSAT [2] antennák, és katonai reléállomások is. A mikrohullámú csoportot három részre szokás osztani.

1) Deciméteres hullámok: Az 1-0,1 méter közötti hullámokat a deciméteres tartományba sorolják. Frekvenciatartományuk a 300 megahertz és 3 gigahertz közötti értékeket veszi fel. Összeköttetés létesítésére csak látótávolságon belül alkalmas, épületek, vastag falak, masszívabb tereptárgyak takarásában nagy az elhajlás, és a térerősség szinte teljesen megszűnik. Az adó és a vevő közötti láthatóság tehát igen fontos, azonban egy irányított antennával nagy távolságok hidalhatók át. Az átvitel minőségét befolyásolják a légköri tényezők is, ilyen például a páratartalom változása ami látótávolságon belül is csillapítást okozhat.
2) Centiméteres hullámok: A 3-30 gigahertzes tartományba eső, és 0,1-0,01 méteres nagyságig terjedő hullámok csoportja a centméteres hullámok nevet kapta. Az összeköttetés létesítésének feltételei hasonlóak, mint a deciméteres hullámok esetében, csak látótávolságon belül működik, és tereptárgyak takarásában a térerősség rohamos csökkenése figyelhető meg. A légköri viszonyok komolyan befolyásolják az összeköttetés minőségét, azonban nagy sebességű átvitelt biztosít.
3) Milliméteres hullámok: A milliméteres hullámokat napjainkban még csak igen ritkán alkalmazzák, és ezt is kizárólag optikai rálátás mellett. Szabad téri alkalmazása nem biztosít megbízható összeköttetést mivel a 0,01 és 0,001 méter közötti hullámméreteket egy sűrűbb köd vagy zápor teljesen szétveri. Ilyenkor a csillapítás olyan nagy hogy az információ elveszik, és a kommunikáció teljesen megszűnik. A milliméteres hullámok frekvenciatartománya 30-300 gigahertzig terjed.

A Magyar Honvégségnél, napjainkban is rendszerben vannak olyan régi típusú rádióeszközök, amik nem képesek kielégíteni egy missziós feladatot ellátó kontingens távközlési igényeit. Ezek a készülékek, még a rendszerváltás előtti szovjet időkből valók, amiket azóta sem sikerült lecserélni. A missziós területeken nem használják őket, hiszen analóg eszközök, így nehézkes a digitális rádiókkal való

2 VSAT - Very-Small-Aperture Terminal

kommunikáció. A régi analóg rádiókat nem lehet olyan pontosan hangolni, mint a korszerű digitális társaikat, könnyen elhangolódnak például a változó hőmérséklet hatására, és nem támogatnak olyan szolgáltatásokat amelyek a rejtett kommunikációra adnak lehetőséget. Hátrányuk továbbá, hogy hatótávolságuk sok esetben kisebb, annak ellenére, hogy kimenő teljesítményük hasonló, mint a digitális rádióké. Ennek egyik oka a zajos vétel, a pontatlan hangolás és a készülékek igen tekintélyes kora. Tömegük sokszorosa a hasonló kimenő teljesítményt nyújtó korszerű eszközökéhez képest, és külön nagyméretű antennaillesztő egységgel rendelkeznek. A digitális rádiók már magukban hordozzák ezeket a plusz alkatrészeket.

A megszervezésre kerülő kommunikációs hálózatok

Az elöljáró és a műveleti csoportok közötti mikrohullámú és URH rádióháló

A magyar Különleges Erőknél, műveleti területen alkalmazott első számú rádióháló arra szolgál, hogy a katonák kapcsolatot tarthassanak az elöljáróval. Ezen a csatornán kapnak minden olyan információt, amire a művelet során szükségük lehet, és itt adnak le minden jelentést, amit a parancsnokok igényelnek. A rádió műszaki paramétereinek köszönhetően kiválóan alkalmazható arra is, hogy a támogató szerepet betöltő légierő repülőgépeivel vagy helikoptereivel tartsanak kapcsolatot. Segítségével irányítható a repülőgépek tűzcsapása, vagy a mentésre, kiemelésre érkező helikopter pontos leszállási helye. A készüléken több frekvencia előre beprogramozható, így azok a változó körülményeknek megfelelően tetszés szerint változtathatóak. A rádió, ha a feladat jellege megkívánja titkosított formában is képes a sugárzásra. Eszerint, hogyha a speciálisan erre a célra előre megírt kulcsok feltöltésre kerültek, akár minősített információk is közölhetők. Ezen esetekben a rádió felveszi a rá feltöltött kulcs minősítési szintjét, így a rejtjelkulcs minősítési szintjének megfelelően lehet információkat küldeni. [5]

Az összeköttetést az amerikai HARRIS cég által gyártott FALCON II (Army Navy / Portable Radio Communication – Továbbiakban: AN/PRC) AN/PRC-117F típusnévre hallgató háti rádióval valósítják meg. Ez a készülék számos olyan szolgáltatással rendelkezik, amik biztosítják a folyamatos és megbízható kommunikációt a csoportok és az elöljáró között. Az AN/PRC-117F frekvenciatartománya 30-512 MHz között van, tehát magába foglalja a teljes ultrarövid, és a mikrohullámú tartomány egy részér is. Mikrohullámú képességei lehetővé teszik, hogy műholdas kommunikációt is végrehajtson azon felül, hogy rádióhálóban képes a kommunikációra. Teljes frekvenciatartományán belül képes

valós idejű beszéd és adatátvitelre is. A készülék több fajta antennával is üzemeltethető, hogy adott esetben melyiket alkalmazzák azt a feladat jellege határozza meg. A rádió háton hordozható tehát a katonáknak megbízható összeköttetést biztosít akkor is, hogyha a feladatot gyalogosan kell végrehajtani. Akkumulátora, ebben az esetben 1 és 20 watt között állítható kimenő teljesítményt biztosít a készüléknek. Hatótávolsága jelentősen meghaladja a Magyar Honvégség által jelenleg is rendszerben lévő korábbi analóg rádiótípusokét, amik hasonló kimenő teljesítménnyel rendelkeznek, azonban üzemidejük kevesebb. Az AN/PRC-117F gépjárműbe illetve harcjárműbe is szerelhető ezen esetekben a fedélzeti teljesítményerősítőnek köszönhetően kimenő teljesítménye 150 wattig bővíthető. Járműbe szerelése esetén másik nagy előnye a megnövekedett teljesítmény mellett az, hogy nagyobb antenna is csatlakoztatható hozzá. Ezen két kiegészítés után a rádió hatótávolsága a gyalogos alkalmazáshoz képest jelentősen megnövekszik. Nem fedélzeti rádióként alkalmazva a rádió súlya 4,45 kilogramm akkumulátor nélkül, így tömege igen barátságosnak mondható.

1. ábra: AN/PRC 117F [6]

Az AN/PRC-117F egy szoftvervezérelt digitális készülék, modulációs típusai: FM[3], AM, PSK[4], CPM[5]. Azt, hogy melyik modulációs típust használják, azt feladat és a környezeti tényezők határozzák meg. -40 °C és 70 °C között megbízhatóan alkalmazható, nagy előnye az analóg rádiókkal szemben, hogy a hőmérséklet ingadozása esetén sem hangolódik el a korábban beprogramozott frekvenciáról. A

3 FM - Frekveciamoduláció

4 PSK - Phase Shift Keying - fázisbillentyűzés

5 CPM - Folyamatos Fázismoduláció

szoftverrádiók egyre szélesebb körben való elterjedésének oka az, hogy a készülékek szoftverei frissíthetőek, így részben korszerűsíthetők tehát elkerülhető az eszköz teljes cseréje modernizáció igénye esetén. Speciális, direkt erre a célra megírt kulcsokkal tölthetők fel, amik megbízhatóan titkosítják a kisugárzott adatokat. A frissítéseknek és a szabványoknak köszönhetően pedig biztosított az is, hogy a különböző típusok képesek legyenek az egymással való együttműködésre, akár beszéd, akár adatátvitelről van szó. Az eltérő generációjú rádiók közötti együttműködés a különleges erők esetében igen fontos, hiszen tevékenységük során gyakran működnek együtt más nemzeti erőkkel, akik felszerelése bizonyos esetekben elavultabb, gyakran pedig korszerűbb az általuk használtnál. Az AN/PRC-117F tehát megfelel a kor követelményeinek továbbá támogat frekvencia-hopping üzemmódot is, ami azt jelenti, hogy a frekvencia adás és vétel közben is 2 megadott érték között, véletlenszerűen változik. Ehhez az üzemmódhoz szükséges a hálóban használt rádiók időszinkronját egymáshoz igazítani, hogy a frekvenciatartományban összehangoltan tudják változtatni az értékeket.

Az elöljáró és a műveleti csoportok közötti RH rádióháló

A Különleges Erőknél, műveleti területen alkalmazott másodlagos rádióháló, egy rövidhullámú összeköttetésen alapul. Ezen a hálón szintén az elöljáróval történik a kommunikáció, aki folyamatos instrukciókkal látja el a katonákat. Együttműködő erőkkel történő kapcsolattartásra is alkalmazható, de az előző fejezetben említett rádióval ellentétben légi járművekkel való kommunikációra alkalmatlan. Ennek az összeköttetésnek a megbízható és folyamatos működése az egyik legfontosabb, hiszen az erők vezetése és irányítása teljes egészében ezen a hálón zajlik. Természetesen ennek megfelelően több, akár 4-5 tartalékfrekvencia is be van programozva az eszközbe, hogy minden fajta terep és időjárási körülmények között megfelelően működhessen a rendszer. A készülék, amivel ezt a fontos rádióhálót valósítják meg az amerikai HARRIS cég által gyártott FALCON II AN/PRC-150C típusú korszerű szoftverrádió. Ezen digitális rádiók nagy előnye, öregebb analóg társaikkal szemben, hogy hasonló kimenő teljesítmény mellett a súlyuk töredéke elődeiknek, egyszerűbb és sokkal pontosabb a hangolásuk, a hőmérséklet jelentős ingadozása esetén sem hangolódnak el, és rendkívül strapabírók. A digitális rádiók másik nagy előnye, hogy beépített titkosító berendezéssel rendelkeznek, amikre előre megírt kulcsok tölthetőek fel valamint adatküldésre is alkalmasak.

2. ábra: AN/PRC 150C [7]

Az AN/PRC-150C frekvenciatartománya 1,6 - 59,9999 MHz-ig terjed és belső memóriájára 200 darab előre felprogramozott csatornát lehet bevinni. A HARRIS készülékek támogatnak olyan szolgáltatást is, amivel egy felprogramozott rádióban tárolt frekvencia és üzemmód adatokat, át lehet küldeni más, szintén HARRIS típusú rádiókra, így nem szükséges minden készüléket egyesével felprogramozni. A készülék képes FM és AM (CW[6]; ALE[7]; 3G; 3G+) modulációra, így biztosítja az együttműködést az együttműködő erőkkel, valamint a korábban említett készülékhez hasonlóan támogat frekvenciaugratásos üzemmódot is. Az AN/PRC-150C alapvetően egy hordozható háti rádió, ennek megfelelően súlya 7,8 kilogramm így nem jelent komoly plusz terhet a híradó katonának. A gyakorlatban a készüléket gépjárműbe szerelve is alkalmazzák, ebben az esetben a rádióhoz csatlakoztatnak egy teljesítményerősítőt is, melynek köszönhetően a kimenő teljesítmény 20 wattról 150 wattra növekszik minek következtében a készülék hatótávolsága kedvező terepviszonyok mellett jelentősen megnövekszik. A készülék hatótávolságát továbbá az antenna típusa is befolyásolja, hiszen háton hordva kisebb antennát csatlakoztathatok a rádióhoz, mint járműbe szerelve.

6 CW – Continuous Waveform „MORZE”

7 ALE – Automatic Link Establishment

A különleges műveleti csoportok belső URH rádióhálója

3. ábra: AN/PRC-152C [8]

A különleges erők által alkalmazott harmadik számú rádióháló egy ultrarövid hullámú (URH) rádióforgalmi rendszer, aminek segítségével a különleges műveleti erők katonái, csoporton belül egymással folytatnak kommunikációt. Egy-egy művelet végrehajtása során a különleges műveleti katonák ideális esetben nem kerülnek messze egymástól, így a közöttük megvalósítandó összeköttetés biztosítására elegendő egy kicsi, könnyű, viszonylag alacsony teljesítményű készülék, amit könnyedén magukon tudnak viselni. A katonák, mivel a harc megvívása során mind a két kezüket használják, a rádióhoz fejhallgatót csatlakoztatnak, amin hallják társaikat, és egyben megvédi füleiket az éles harci zajoktól. A készülék, amivel mindezt biztosítják szintén a HARRIS cég gyártmánya és az AN/PRC-152C típusnévvel jelölik. Ez egy akkumulátorral együtt 1,18 kilogrammos kézi rádió, amihez egy ostorantennát csatlakoztatva körülbelül 1,5 kilométeren belül megbízható összeköttetés hozható létre. A készülék kimeneti teljesítménye maximálisan 5 watt, mely szükség esetén csökkenthető 0,25 vagy 1 wattra, de az újabb típusokat járműfedélzeti teljesítményerősítőre csatlakoztatva 50 watt is

elérhető. A készülék frekvenciatartománya, mint korábban említettem az ultrarövid hullámú tartományba esik, így a frekvenciák a 30 MHz és az 512 MHz közötti értékeket vehetik fel. A rádió pontos frekvenciaértékekre hangolható, -30 és +60 C fokos hőmérsékleti viszonyok között garantált a működése. Az AN/PRC-150C-es rádióban alkalmazott szoftver irányítja ezen rádiót is így szintén képes titkosított beszéd és adatátvitelre, valamint előre programozott csatornák tárolására, és a korábban bemutatott üzemmódok kezelésére.

Az AN/PRC-152C-es kézi rádiókat mint korábban említettem, elsődlegesen a csoporton belüli kommunikációra használják, azonban bizonyos esetekben ettől eltérhetnek. Hogyha a feladat jellege megkívánja, az ultrarövid hullámú tartományon folyathatnak kommunikációt az elöljáróval. Ebben az esetben a híradó specialista eltérő frekvenciát választ attól, mint ami a különleges műveleti csoport többi tagjának készülékére van programozva. Az URH rádióösszeköttetés továbbá kiválóan alkalmas a támogató erőkkel történő kapcsolattartásra. Ebben az esetben beszélhetünk a gyorsreagálású erőkről (QRF – Quick Reaction Force) akik feladatrendszerét a korábbiakban kifejtettem, kommunikálhatnak a csoportok a kiemelésükre, vagy egyéb célból érkező helikopterekkel, az együttműködő, esetleg más nemzetiségű erőkkel, és egyéb támogató elemekkel.

Az elöljáró és a támogatók irányába szervezett IRIDIUM kapcsolat

A különleges műveleti csoport negyedik különálló kommunikációs rendszerének célja az elöljáróval folytatott kapcsolattartás, valamint az esetlegesen rendelkezésre álló támogató erőkkel való kommunikáció biztosítása. Ez a csatorna általában tartalékként van jelen a különleges erők tagjainál, de megbízhatósága miatt előszeretettel alkalmazzák. Erre a feladatra egy műholdas telefon áll rendelkezésre. Az egyszerű mobiltelefonhoz hasonló készülék, olyan műholdakon keresztül létesít összeköttetést, amik direkt erre a célra lettek kifejlesztve és földkörüli pályára állítva. A műholdas rendszer első műholdját 1998-ban állították földkörüli alacsony LEO[8] pályára, ami földfelszín feletti magassága körülbelül 800 kilométer. A rendszer folyamatos fejlesztés alatt áll aminek köszönhetően még ma is megbízhatóan működik. A Motorola cég mérnökei által kifejlesztett rendszer, az Iridium nevet kapta. Az elnevezés onnan ered, hogy a föld teljes lefedésére a számítások szerint 77 műholdra lett volna szükség, és az iridium az a kémiai elem, aminek magja körül 77 elektron kering. A későbbiekben kiderült, hogy ennél

8 LEO - Low Earth Orbit – Alacsony Földkörüli Pálya

kevesebb eszközzel is lefedhető a föld teljes felülete, ami a projekt jelentős költségcsökkenését eredményezte. Az Iridium a mai napig az egyetlen olyan műholdas kommunikációt biztosító szolgáltató, ami 100%-os lefedettséget biztosít. A rendszert ma 66 aktív műhold alkotja. A nagyfokú rendelkezésre állás biztosítékaként továbbá a Motorola szakemberei a rendszer alapját képező 66 aktív műhold mellett 6 tartalék műholdat is fellőttek annak érdekében, hogy valamelyik meghibásodása esetén a kommunikáció biztosított legyen. A nagy mennyiségű űrszemétnek köszönhetően, nagy a kockázata egy esetleges idegen objektummal való ütközésnek. Erre az Iridium rendszer esetében is találunk példát, 2009-ben az Iridium 33 nevű műhold egy használaton kívüli katonai távközlési műholddal ütközött, és használhatatlanná vált.

A rendszerhez csatlakozó készülékeket strapabíró kivitelben készülnek mindegyikük ütés, por és mérsékelten vízálló. A 2011-ben megjelent IRIDIUM 9575 EXTREME már a katonai szabványoknak is tökéletesen megfelel.

4. ábra: IRIDIUM telefon [9]

Az Iridium telefonokat, nem csak katonai szervezetek, hanem a civil szféra is előszeretettel használja. A katasztrófavédelem, hajózási társaságok, különböző expedíciók résztvevői, túrázók, hegymászók, és olyan emberek is használják a műholdas telefonokat, akik olyan helyen dolgoznak ahol a GSM szolgáltatások nem elérhetőek. Az Iridium rendszer nagy előnye, hogy telefonos összeköttetést biztosít a Föld minden pontján, így a sarkkörökön, az óceánokon valamint az egész szárazföldön is. Alkalmas szöveges üzenet küldésére, valamint az új eszközök már internetelérést, GPS[9] szolgáltatásokat és online nyomkövetést is biztosítanak a felhasználók számára. Az Iridium egy cellás rendszerhez hasonlítható. A telefon a legközelebbi műholdra csatlakozik, amivel van rálátása, ami az adatot továbbküldi olyan műholdnak, ami a célállomással képes kommunikálni. Az adat tehát a két kommunikálni kívánó végállomás között több műholdon is keresztül mehet. Amennyiben a rálátás megszűnik az éppen adatot továbbító műholddal, a telefon azonnal másikat keres, így biztosított a mozgás közbeni zavartalan kommunikáció. Az Iridium rendszeren keresztül minősített adat azonban nem küldhető, mert adattitkosításra nem alkalmas. A Magyar Honvédség több mint 100 előfizetéssel rendelkezik, amit főleg a misszióban szolgálatot teljesítő erők használnak.

A GSM rendszerrel megszervezett „vész" összeköttetés

A csoportok ötödik kommunikációs lehetősége, a mindenki által ismert és használt, cellás GSM hálózat, aminek megbízhatósága az adott ország rendszerének kiépítettségétől függ. Egy adott terület lefedettsége, a bázisállomások és az átjátszó tornyok telepítésétől függ. Ezeket az elemeket oly módon kell egy adott területen elhelyezni, hogy a lehetőség szerint ne árnyékoljanak le egyetlen területet sem domborzati tényezők. Afganisztánban például az Egyesült Államok teremtette meg a jól működő GSM hálózatot, ami egy vész összeköttetési lehetőséget biztosít a katonák számára. Az ISAF[10] missziókban többször alkalmazták ezt a kommunikációs lehetőséget. Ha a katonai rádióhálókon és a műholdas telefonon sem megvalósítható az összeköttetés, és nincs semmilyen lehetőség sem a kommunikációra, akkor használják ki a GSM rendszer adta lehetőségeket. Egy hagyományos mobiltelefon készülék és egy SIM kártya szükségeltetik csupán és a kommunikáció máris biztosított a világ bármely bekapcsolt mobiltelefonjával. Ez a csatorna igen gyors összeköttetést, és könnyen megvalósítható kommunikációt

9 GPS - Global Positioning System - Globális Helymeghatározó Rendszer

10 ISAF - International Security Assistance Force - Nemzetközi Biztonsági Közreműködő Erő

eredményez abban az esetben, hogyha elegendően erős térerő áll rendelkezésre. Ezt a lehetőséget azonban csak vészhelyzetben alkalmazzák, hiszen az említett a csatorna nem titkosított. Előre megbeszélt kódnyelven a katonák tudnak kommunikálni, de ennek használatát megfelelően körültekintően kell végezni. Egy adott GSM rendszert az esetek túlnyomó részében annak az országnak a dolgozói üzemeltetik, amelyik ország területén a hálózat telepítve van. Tehát, egy olyan országban ahol a különleges műveleti katonák feladatot hajtanak végre nagy a lehallgatás veszélye. Továbbá a cellás rendszernek köszönhetően, a készülékek helyének meghatározása roppant egyszerű, hiszen a mobiltelefon készülék bizonyos időközönként jeleket küldd a legközelebbi toronynak. Ezekből a fogott jelekből könnyedén meghatározható, hogy az adott különleges műveleti csoport épp hol, melyik cellában tartózkodik. Értelem szerűen tehát csakis vészhelyzetben alkalmazható, és minősített adatot semmi képen sem tartalmazhat az ezúton leadott közlemény. Előnye azonban hogy amennyiben van lefedettség, megbízhatóan működik és adattovábbításra valamint helymeghatározásra is alkalmas. Az adatforgalomnak köszönhető a GPS funkció, aminek csak a telefonkészülék képességei szabnak határt. Az új generációs 3G és 4G képes mobiltelefonok megfelelő lefedettséggel ellátott helyen, nagyon gyors adatkommunikációra is képesek.

A különleges műveleti erők VSAT kommunikációs hálózata

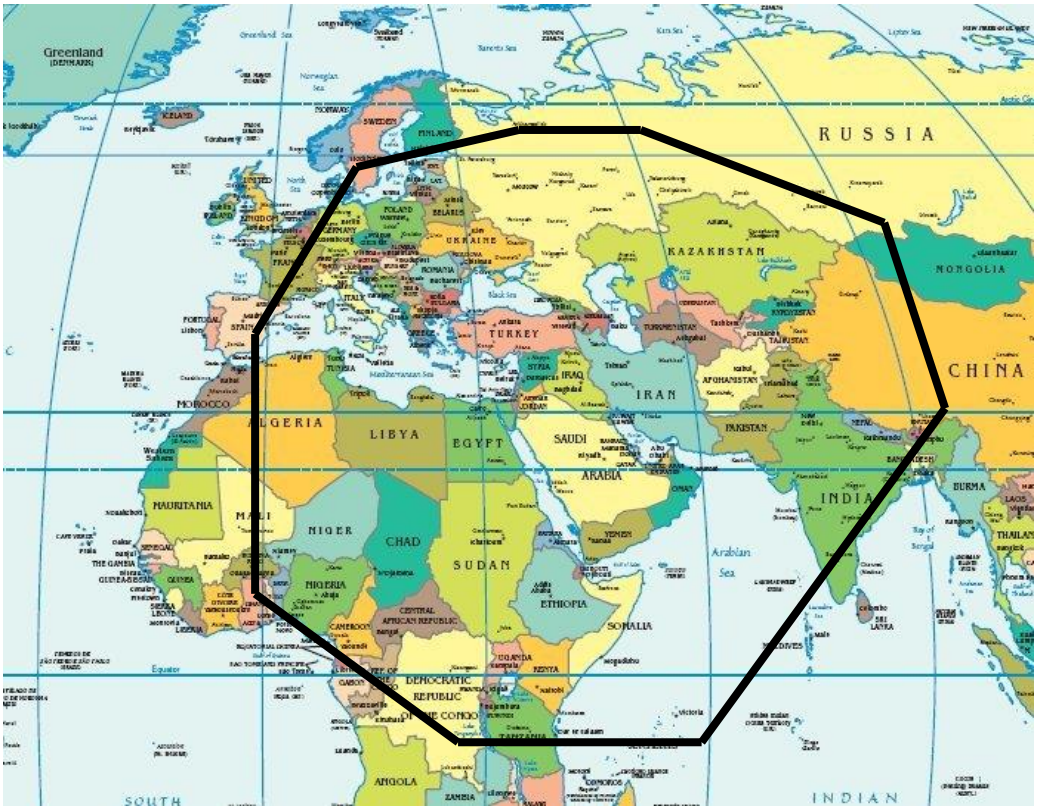
A Különleges Erők elsődleges összeköttetési vonala a hazai parancsnoksággal, VSAT rendszeren keresztül valósul meg. A rendszer megbízható, elektronikai felderítése és zavarása nem egyszerű az irányított antennának, a magas kisugárzott üzemi frekvenciának és a 200 watt körüli kimenő teljesítménynek köszönhetően. A VSAT rendszer egyaránt támogat valós idejű hang és adatkapcsolatot is. Azokon a missziós területeken, ahol a Magyar Honvédség katonái jelen vannak, biztosított számukra az internetelérés. Ezt többnyire műholdas távközlési rendszerek alkalmazásával biztosítják. A VSAT képesség segítségével, missziós területeken biztosítható Internet, Intranet és valós idejű hangátvitel. Ezeken a csatornákon folyik a katonák magánjellegű kommunikációja, valamint a parancsnokok ezen keresztül adják le jelentéseiket az elöljárók felé videokonferencia formájában. Hogyha a sávszélesség korlátozott, a jelentések leadásának idejére a magánjellegű kommunikációt korlátozzák, tehát letilthatják a katonák internet hozzáférését, a videokonferencia idejére. A VSAT eszközök magukba foglalnak minden olyan műholdas kommunikációra képes eszközt, amik három méter átérőnél kisebb parabola antennán keresztül folytatnak kétirányú kommunikációt.

A VSAT rendszer elemei:

- Antenna
- Kültéri egység
- Műholdas modem vagy beltéri egység
- Router
- Tápegység
- Távfelügyelethez szükséges eszközök

Fontos megemlíteni, hogy ezeket a rendszereket egy polgári cég, a Hungaro DigiTel Kft. biztosítja a Magyar Honvédség részére. A VSAT rendszerek geo stacionárius (továbbiakban: GEO) műholdakat használnak, amik keringési pályája körülbelül 36000 kilométer magasan van az átlagos tengerszint fölött. Meghatározó jellemzője a GEO műholdaknak továbbá az, hogy mindig az egyenlítő egy bizonyos pontja fölött keringenek, azaz a Föld forgási periódusával megegyező keringési idővel rendelkeznek. Ennek köszönhetően, a földfelszín egy bizonyos pontjáról mindig ugyanazon a helyen találhatóak meg az égbolton. A műholdak ezekben a rendszerekben mikrohullámú átjátszóállomásként üzemelnek, így az összeköttetés feltétele a fizikai rálátás, ami részben lekorlátozza a VSAT rendszerek alkalmazhatóságát. Ezen felül, a szatellitek alkalmazásából adódóan ez az összeköttetési forma igen költséges, hiszen egy műhold elkészítése, földkörüli pályára állítása és üzemeltetése rendkívül drága művelet, amit csak a fejlettebb országok engedhetnek meg maguknak. Azonban a VSAT rendszerek a könnyű és gyors telepíthetőség mellett, számos előnnyel is rendelkeznek. Ilyen például hogy egy-egy adott műhold ráláthatóságán belül mindenhol fogható a jel, biztosított az adatátvitel, és egy műholdra számos VSAT rendszer képes rácsatlakozni. Mérete kicsi így tárolása és szállítása nem állít jelentős problémát az alkalmazó katonai szervezet logisztikusai elé. A korszerűbb eszközökbe épített navigációs rendszer lehetővé teszi, hogy a kezelők egy gombnyomással pontosan be tudják lőni azt a műholdat ahonnan a jelet venni kívánják. Ehhez a készülékbe épített GPS járul hozzá. Ezen felül a készülékekbe olyan rendszereket is szerelnek, amik az időjárás változásaira reagálva egyfolytában javítják az összeköttetés minőségét ezzel növelve a rendelkezésre állást. A mikrohullámú, azaz a parabola antenna és a műhold közötti csatornák csillapítása elhanyagolható így az adat és hang kommunikáció valós idejűnek mondható.

Az eszköz telepítése gyors és egyszerű. Az automatizált antenna percek alatt pozícionálja magát. A beltéri egység elemei illesztőegységek és routerek, amik megfelelő felprogramozásával létrehozható a kapcsolat a felhasználók számára. A végpontok telepítése is egyszerű, nem igényel komolyabb felszereléseket.



5. ábra: A VSAT szolgáltatás elérhetőségi területe [10]

A VSAT rendszerek védelme igen fontos, hiszen a nagy sebességű műholdas kommunikációs képesség fenntartása elengedhetetlen missziós területeken. A beltéri egységek és a kábelek elrendezése a híradó szakemberek feladata, ami általában nem ütközik nagyobb nehézségekbe, azonban a kültéri egység elhelyezése már komolyabb problémákat vet fel. Az antenna elhelyezkedése ebből a szempontból kiemelten fontos, hiszen a készülék rendkívül sebezhető. Előfordult például, hogy a táborban elhelyezett VSAT antenna messziről látható volt, és ellenséges mesterlövészek tűzének köszönhetően az antenna fókuszpontjában elhelyezett fej megsemmisült, ami lehetetlenné tette a rendszer működését. A készülék természetesen javítható, de a tartalék alkatrészek rendelkezésre állásától függően a kommunikációnak ez a formája napokra akár hetekre kieshet. Az antenna ezen felül igen nagy teljesítményen, és vékony nyalábban sugároz, így azt olyan pontra kell elhelyezni, hogy a személyi forgalom, ami a tányér előtt halad el minél kisebb legyen.

Összegzés

Bemutattam a különböző frekvenciájú hullámok fajtáit, azok terjedési sajátosságait, és alkalmazási területeit. Kiemelésre kerültek a különböző frekvenciatartományok, amiket a katonai híradásban gyakran használnak. Kitértem a régóta használatos tartományokra, valamint azokra is, amiket nem régen használnak a katonai távközlésben. A második részben ismertettem a magyar különleges erőknél használatos rádiótípusokat, azok képességeit és harctéri alkalmazásuk lehetőségeit, és azt, hogy az adott készüléket milyen feladatra használják.

Felhasznált irodalom

[1] Farkas Tibor főhadnagy: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében – ZMNE, 2010. (PhD. értekezés)
[2] Tóth András, Farkas Tibor, Pándi Erik: A válságreagáló műveletek híradó- és informatikai rendszerének megszervezése; HÍRVILLÁM (SIGNAL BADGE) 2010/1. szám, pp. 13-31. (2010)
[3] Farkas Tibor: CIS officer training at the National University of Public Service: Capabilities and requirements; In: Miroslav Hruby (szerk.) Distance Learning, Simulation and Communication (DLSC) Conference, Brno 2015. pp. 84-90.
[4] Tóth András: A NATO kommunikációs rendszerének elméleti és gyakorlati vizsgálata, Kommunikáció 2014., Nemzeti Közszolgálati Egyetem, 2014., (ISBN:978-615-5491-94-8), pp. 65-77.
[5] Tóth András: A vezetés-irányítási rendszerek alkalmazásával szemben támasztott követelmények a csapatvezetésben, gyakorlati használata során felmerült észrevételek tapasztalatok, HADMÉRNÖK (1), 2009., pp. 276-283.
[6] http://www.escuadron111.com/wp/wp-content/uploads/2012/06/AN-PRC-117F_3_4_view_4-07_1_26-11346.jpg (2015.04.16.)
[7] http://www.satnews.com/images_upload/1698082725/Harris_ANPRC150C.jpg (2015.04.16.)
[8] http://rf.harris.com/media/AN-VRC-110_enlarged_26-11866.jpg (2015.04.16.)
[9] http://cdn3.volusion.com/32bt3.jhya9/v/vspfiles/photos/IRIDIUM-9555-SATELLITE-PHONE-2.jpg (2015.04.20.)
[10] Polgári műholdas szolgáltatások a Magyar Honvédség részére Műszaki leírás 2007.11.21.

[11] Dr. Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)
[12] Dr. Négyesi Imre: DIE UNTERSTÜTZUNG DER SOLDATEN MIT ECHTZEITDATEN (A KATONÁK TÁMOGATÁSA VALÓS IDEJŰ ADATOKKAL) (Hadmérnök on-line, VII. évfolyam (2012) 4. szám, 162-166. oldal, ISSN 1788-1919).
[13] Dr. Négyesi Imre: DIE ÜBERPRÜFUNG DER VORAUSSETZUNGEN VON COTS SYSTEMEN (COTS RENDSZEREK KÖVETELMÉNYEINEK VIZSGÁLATA) (Hadmérnök on-line, VII. évfolyam (2012) 2. szám, 371-376. oldal, ISSN 1788-1919).

PUSKÁS Béla: Információbiztonsági környezet kialakítása

Absztrakt

Manapság a Kritikus Infrastruktúrák közvetlen vagy közvetve az élet minden területén jelentős szerepet játszanak. Nélkülönözhetetlenek ahhoz, hogy az emberek biztonságosan élhessék a mindennapjaikat. Az esetleges hibás működés, a kívánt szolgáltatások elmaradása akár az ott élők életét is veszélyeztetheti. Így az esetleges műszaki meghibásodások, külső támadások elleni védelem különösen fontos feladat. A cikk megkísérli bemutatni a Kritikus Infrastruktúrák védelmének jelentőségét és azok védelmét.

Abstract

Nowadays the Critical Infrastructures (CI) play a vital role in the life of the modern world. They are essential tools to provide safe and convenient circumstances for the everyday life of human societies. In case of their malfunction, the effected services fail to fulfil their tasks, which can endanger the life of citizens living within their area of operation. Thus, their defence against technical breakdowns or hostile attacks is a matter of highest importance. The following article tries to introduce the significance of CIs and their proper protection.

Kulcsszavak: *Hálózat, Kritikus Infrastruktúra, Kritikus Információs Infrastruktúra, Szolgáltatásmenedzsment, kockázatkezelés ~ Networks, Critical Infrastructures, Critical Information Infrastructures, Service Management, risk management*

Bevezetés

Az informatikai rendszerek üzemeltetése során kiemelt figyelmet kell fordítani az informatikai (IT) biztonságra. Természetesen az információbiztonság nem egyenlő az IT biztonsággal, annál sokkal több, ugyanakkor nem tartalmaz olyan elemeket, amelyeket az IT biztonság igen. Mit is nevezünk tehát információbiztonságnak?

„Az elsődleges értelmezést tükrözi a NATO híradó és informatikai fogalomjegyzékének 2. változata is, amely szerint az információbiztonság ('information security') "az információk védelme a véletlen, vagy szándékos jogosulatlan megismerés, továbbítás, módosítás vagy megsemmisítés ellen. Megj.:

Az információ létezhet az emberi agyban, dokumentum formában és elektronikus formában.” [1]

A fenti megfogalmazásból is látszik, hogy egy igen szerteágazó és komplex dologról beszélünk. Először is az információt úgy szeretnénk megtartani, ahogyan az eredetileg keletkezett, illetve úgy módosuljon, ahogyan számunkra az kedvező. Mindezek mellett viszont a legfontosabb, hogy ezek az információk miden körülmények közt rendelkezésre álljanak a kívánt időben és helyen. Számolni kell azzal a ténnyel is, hogy az információk több helyen keletkezhetnek, illetve tárolódhatnak. Sokan a papír alapú és az elektronikus tárolásra gondolnak, de ott van a szinte kezelhetetlen emberi agy is, valamint a különböző típusú adathordozók is. Ráadásul ezek sokszor átfedéseket mutatnak. Komoly kihívást jelent az archiválás során az adathordozók időállósága. Szeretnénk, ha 10, 20 vagy akár 50 év múlva is meg tudnánk nyitni a dokumentumot, kutathatnánk benne úgy, hogy azon lévő információk az eredeti formában előhívhatóak legyenek. Ez igen elgondolkodtató egy olyan környezetben, ahol számolni kell az anyagfáradással, minőségromlással, a hardverelemek és szoftverelemek gyors változásával. A statikus tárolás mellett dinamikusan változik az információ helye, "szabadon" áramlik a különböző információs csatornákon, amelyek fizikai, biológiai vagy kémiai hatásokra visszavezethető okokból természetes úton változnak. Emellett mivel az információ hatalom és érték, így mindig lesznek olyan érdekek, amelyek miatt szándékosan és rosszindulatúan avatkoznak be egyesek az információ tárolásába, áramlásába, megismerésébe vagy esetleg annak megsemmisítésébe. Az üzleti életben különösen kimutatható az érték és ezt be is szokták árazni, tehát számszerűsítik egy-egy információ értékét. Szükséges tehát ezen információkat az egész életciklusukon keresztül megvédeni az élet minden területén. Ezzel egy új fogalom is megjelenik ezen a területen mégpedig az információvédelem. Az információ védelme egy tevékenység, amely a vagyonelemek meghatározásával indul, majd a kockázat elemzéssel folytatódik és végül ezekből meghatározzák a szabályokat és eszközrendszereket. A védelem során egy ideális állapotot kívánunk fenntartani, különösen a sértetlenség, bizalmasság és a rendelkezésre állás tekintetében. [2]

A továbbiakban az IT biztonságra fogok fókuszálni, de mint már írtam önmagában nem kezelhető csak ez a terület.

Emberek üzemeltetik az IT rendszereket, emberek a felhasználók, a rendszereknek ki és bemeneti pontjai vannak amelyekkel csatlakoznak más rendszerekhez, illetve átadnak információkat. Mindemellett az IT rendszerekre hat a környezete és ő is hat rá. Kialakul egy már-már kezelhetetlen komplex rendszer. A

nyílt rendszerek összekapcsolásakor már létezik az OSI[1] modell, de fontosnak tartanám ezek mellett a közösségi hálót (ide értem a személy családi, baráti, munkahelyi kapcsolatait is), szabályzók rendszerét, szervezeti struktúrákat (beleértve a beszállítókat, bedolgozó vállalkozókat és ügyfeleket), környezeti hatások hálózatát, infrastrukturális kapcsolatrendszereket (villamosenergia-, víz-, gáz-, üzemanyag-, távközlési-, úthálózatok; épületek, stb.), gazdasági folyamatokat és minden olyan hálózatokat is egy-egy rétegként kezelni. Amikor megvizsgáltuk a rétegek összetételét és viselkedését külön-külön, rátérhetünk a kapcsolódási pontok keresésére. Sokáig azt hihettük ezt nem lehet kezelni, de pont a bonyolultságot előidéző technikai fejlődéssel modellezhetjük a rendszereinket. Ebben nyújt segítséget az Internet, mint hálózat elemzése is. A rendszerek hierarchikus felépítésűek. A kialakuló különböző hatások nemcsak vertikálisan hatnak, hanem a különböző hálózatok egyes hierarchikus szinteken kapcsolódnak ilyen módon egymáshoz. Az így kialakult rendszer tehát attól lesz komplex, hogy az egyes rétegek közti kölcsönhatás eredményeképpen egy minőségileg új, az egyes részektől eltérő viselkedést mutat. Ebből következik az a téves kialakult gyakorlat, hogy a mai szabályzók és az esetek túlnyomó többségében az IT rendszerek biztonságát elemzők nem gondolkoznak komplex rendszerekben, noha gyakorlatilag ezt vizsgálnak. [3]

IT biztonságának kialakításának lépései

Egy szervezet IT biztonságának kialakítását a szervezeti hierarchia legmagasabb szintjén kell elkezdeni. Némileg megkönnyíti a helyzetet, amennyiben egy teljesen új rendszert kell kialakítani. Természetesen itt is, mint minden más esetben a legfelsőbb vezető dönt és egyben ő is a felelős. Éppen ezért a biztonságos IT rendszer kialakítása iránti elkötelezettsége a legfontososabb és a sikerességnek az egyik kulcskérdése is.

Biztonságpolitika

A felsőbb szinten el kell készíteni a szervezetre vonatkozó biztonságpolitikát. Ebben kell rögzíteni, a fent említett elkötelezettséget, amely támogatja a feladatok elvégzését. Tisztázni kell a célokat, az alapelveket és követelményeket. A

[1] OSI modell: Open Systems Interconnection Reference Model

dokumentációt ki kell hirdetni és elérhetővé kell tenni a dolgozók számára. Az érvekkel alátámasztott biztonságpolitikával mindenkinek tisztában kell lenni.

Stratégia

Ezt követően már elkészíthető a biztonsági stratégia, amely a célok elérésének módszerét, eszközrendszerét és időütemezését foglalja magában. Fontos, hogy folyamatosan érvényesüljön itt is, mint az élet sok más területén a PDCA2 elv. Eszerint miután az elkészült terv alapján végrehajtjuk a feladatokat folyamatosan ellenőrizzük a sikerességét, a környezeti hatásokat, majd beavatkozunk amennyiben ez szükséges. Ellentétben a biztonságpolitikával ezt már nem ismerheti meg bárki, mert tartalmazhat, illetve tartalmaz olyan elemeket is, amely károsíthatja, veszélyeztetheti a cég üzleti érdekét.

Operatív program

A stratégiai terveket operatív programokra kell bontani. Itt már a stratégiában előirányzott tervekkel kapcsolatos konkrét megvalósíthatósági tanulmányokat, ezek terveit kell elkészíteni, majd végre is kell hajtani.

Környezeti változók

Az eddigi és további kérdésekkel kapcsolatban figyelembe kell venni a környezeti változókat. Direkt használtam a változó kifejezést, mert a rendszerükre hatással lévő külsőkörülmények folyamatosan változnak. A felmérés során egy statikus képet kapunk az aktuális állapotról, de már a dokumentum elkészítésekor gondoskodni kell a változáskezelésről. Tehát mik is a környezeti hatások. Talán az egyik leginkább objektív a jogszabályi környezet. Össze kell gyűjteni és minden lépésnél vizsgálni kell a megfelelőséget. A törvények, rendeletek mellett ide sorolnám a különböző ajánlásokat is. Érdekes lehet, amikor egy szervezet több országban van jelen, van anyacége, vagy éppen leányvállalata. A másik nagyon fontos terület, amely befolyásolja a biztonsági folyamatokat az üzleti érdekek, mert eköré a mag köré kell építeni mindent. Figyelembe vegyük a szervezet munkafolyamatait, céljait, elvárásait, prioritásokat a rendszer működésével kapcsolatban. A vezetőségnek meg kell határozni mit várnak el az IT rendszertől. Az informatikai rendszerek valamilyen céllal lesznek kiépítve, amelyet vagy törvényi

[2] PDCA: plan(tervezés), do(végrehajtás), check(ellenőrzés), act(beavatkozás)

felhatalmazás alapján elvárt, vagy az üzleti elvárások szerinti folyamatokat követ le. Az informatikai vezetőnek pontosan kell tudni, hogy mit várnak el az általa felügyelt rendszertől. Egy sor dolgot kell dokumentumokban rögzíteni, mint például mennyi kiesés megengedett éves szinten, ez mekkora lehet folyamatosan, mennyi időn belül kell helyreállítani a rendszert, mennyi adatvesztés megengedett egy vészhelyzet során, mennyi pénz vagy/és humán erőforrásra számíthat az üzemeltetés és fejlesztés során, stb. Még mindig a második ponthoz sorolom be a szervezeti architektúrát, amely beosztásokat, munkaköröket tartalmaz. A beosztásokhoz alá-fölérendeltségi viszonyok és munkafolyamatok, irányítási jogkörök tartoznak.

Érdekeség a nukleáris létesítmények esetében az információbiztonsági kérdés, mert ott katasztrófák elkerülése érdekében kiemelt figyelmet kell szentelni az üzembiztonságra.

Pénzügyi erőforrás

A vezető elkötelezettsége, célok meghatározása "sajnos" pénzbe is kerül, így például a követelménytámasztás a rendelkezésre állást is meghatározza, melyet a szolgáltatási megállapodás SLA [3] is rögzít. Sajnos általában az informatikai költségekre a vezetők egy számukra megfoghatatlan, értelmezhetetlen kiadásként tekintenek, mert sok olyan elemet tartalmaz – szerverek, hálózati eszközök, levelező rendszerek, adattároló rendszer, mentő rendszerek, biztonsági rendszerek, és ezekhez tartozó szoftverek - melyek el vannak rejtve a felhasználók elől, közvetlenül nem, csak közvetve találkoznak velük. Mind a nemzetközi, mind a hazai tapasztalatok szerint az informatikai rendszerek megfelelő szinten történő működtetése érdekében az IT szektorra jutó költségeknek el kell érnie az összköltségvetés legalább 2 százalékát. Az ideális pedig a 4-5 százalék, amellyel ki lehet elégíteni az üzemeltetéssel járó mindennemű igényeket. A szervezet vezetőjének tudnia kell, hogy külön keret áll rendelkezésre a fejlesztésre, az üzemeltetésre. A fejlesztési projektek pedig befolyásolják az üzemeltetési költségeket is. Amennyiben emelni szeretném a rendszer minőségi, biztonsági szintjét költségekkel jár. Ez nem csak az eszközök, de a humán erőforrások finanszírozását is jelenti (képzés, tanulmányi utak, stb.). A biztonsági rendszer kialakítása szintén egy magas költség, amely a káresemény megelőzése céljából keletkezik, ugyanakkor a klasszikus értelemben nem hoz nyereséget. A veszteségek

[3] Service-level Agreement: szolgáltatási-szint szerződés

minimalizálása érdekében biztosítani kell a pénzügyi erőforrásokat e területnet részére is.

Felelős személyek kijelölése

A vezetésnek ki kell jelölni és dokumentumba foglalni az IT rendszer üzemeltetésében résztvevő felelős személyeket. A biztonság szempontjából fontos, hogy legyen biztonsági vezető, aki a rendszer tervezési szakaszától kezdve részt vesz a munkálatokban egészen a rendszer kivonásáig. Ezen kívül szükséges adatgazda és rendszerenként rendszerbiztonsági felügyelő, rendszeradminisztrátor (rendszermérnök, hálózatmérnök, alkalmazásmérnök, fejlesztő,stb.), "Help Desk".

Jogosultsági szintek

A felhasználók közt is érdemes különbségeket tenni a finomabb jogosultsági szintek beállítása érdekében. Már a tervezési szakaszba érdemes elkészíteni a jogosultsági mátrixot a feladatkörök alapján. Minden szinten be kell tartani a Need to Know elvet.

A humán erőforrás, az idő, a tudás és a pénz egyfajta szimbiózisban léteznek. Összegségükben mindig egy egységet kell kihozniuk, így amikor valamelyik összetevő veszít erejéből, a többinek kell erősíteni, mert képességvesztést szenved a szervezet. Optimális esetben minden jellemző optimális paraméterekkel rendelkezik.

Kockázatelemzés

Miután rendelkezésre állnak a fent felsoroltak el kell készíteni a kockázatkezelési tervet. Ehhez pedig a kockázatelemzésre lesz szükség.

"A kockázatelemzés meghatározása: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése."[4]

Az elkészített elemzést követően elképzelhető, hogy módosítani kell az eddig elkészült dokumentumokat. Ez a körforgás (PDCA elv) folyamatosan jelen kell, hogy legyen az IT rendszer működése során.

[4] 2013. évi L. törvény

Az üzleti szereplőknél a kockázati tényezők miatt bekövetkezett esetekben komoly pénzügyi hátrány érte őket. Így a képzeletbeli mérlegre feltett beruházási költségek és a várható katasztrófa miatti veszteségek láttán a döntéshozó vezetők "könnyen" meggyőzhetőek voltak. Az állami szektorban ugyanakkor a beruházási költségek mellett kár volt az adat jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele. Ez is káralapú meghatározás, de nem lehet konkrét pénzben kifejezni.

A kockázatelemzés egy igen komplex feladat, a mélységét tekintve pedig szinte meghatározhatatlan. A munkát segítő ajánlásokat tekintve az ISO[5]/IEC[6] 27000 szabványcsalád egy jó kiindulópont lehet. Ezen belül a 27005 foglalkozik konkrétan a kockázatkezelési eljárásokkal. Érdemes tanulmányozni az ITIL[7]-t, amely az informatikai rendszerek üzemeltetésével és fejlesztésével foglalkozik. Az ITB[8] ajánlásokat ide sorolva a Common Critériát is (ITB 16. ajánlása). Az informatikai vezetőnek szintén segítséget nyújthat a rendszer üzemeltetése során a COBIT [9]. Idesorolható még az adatközpont építéssel kapcsolatos ajánlások is, ilyen a DCA[10] Certification Guidelines for Data Centres. Ami Magyarországon igazából még nem számottevő, de kellene vele foglalkozni a természet és az adatközpontok harmóniájával foglalkozó LEED[11] minősítés. Természetesen ezen kívül akár több száz szabványt és ajánlást is fel lehetne sorolni, amelyet figyelembe kell venni az építés, üzemeltetés és rendszerből történő kivonás során. Közvetve vagy közvetlen mind kapcsolatban lennének a kockázatelemzéssel. Fontos, hogy ezek alapvetően jó kiindulási alapok, de az adott szervezetre alkalmazandó módszert ki kell dolgozni.

Ezen a ponton logikailag külön kell választani az új rendszer építését és a már meglévő elemzésével kapcsolatos teendők miatt.

Vagyonfelmérés

A meglévő rendszerek esetében egy nagyon pontos és hosszantartó vagyonfelmérést kell végezni. A kockázatok értékeléséhez alapinformációkra lesz

[5] Nemzetközi Szabványügyi Szervezet - International Organization for Standardization (ISO)

[6] Nemzetközi Elektronikai Bizottság - International Elektrotechnika Comission (IEC)

[7] Information Technology Infrastructure Library (ITIL)

[8] Informatikai Tárcaközi Bizottság

[9] Control Objectives for Information and Related Technology

[10] Data Centre Alliance

[11] Leadership in Energy and Environmental Design

szükség, mint minden döntés meghozatalánál ez követelmény. A rendszer működtetéséhez szükség van tőle "független" rendszerekre is, mint például az energiaellátó rendszer. A kockázat felmérésekor számolunk velük ugyan, de csak mint külső tényezővel. Azok rendszerelemeit nem tudjuk figyelembe venni, mint külső rendszer egészét, mivel nincs ráhatásunk a működtetésükre. Így határvonalat képezünk, meghatározzuk az átadási pontokat és feltételeket.

A vagyonfelmérésnél össze kell gyűjteni a fentebb említett információkat, mint például a jogi hátteret, működési környezetet, pénzügyi erőforrás rendelkezésreállására vonatkozó adatokat, üzleti folyamatokat. Minden esetben egy szervezet működésekor léteznek az üzlet sikeressége, vagy a közszférában a feladat végrehajtása érdekében (üzleti) folyamatok, és adatok. Természetesen ezek folyamatosan változnak igazodva a környezeti hatásokra adott válaszok szerint, de fontos, hogy ezeket pontosan definiálni lehessen a felmérés időszakában. A felmérés során modellezni kell a szervezet működéséhez és az üzleti folyamatokhoz szükséges folyamatokat. Itt lehetőség nyílik az egyes területeken egyszerűsítésekre, racionalizálásra is, bár szervesen ez nem kapcsolódik a kockázatelemzéshez. Az ISO/IEC 27005-ben a folyamatok és az adatvagyonok, mint elsődleges vagyonelemeknek jelennek meg.

Üzleti folyamatok

Az adatokat tekintve fel kell mérni az úgynevezett adatvagyont. Az üzleti folyamatok be- és kimeneti értékei lesznek ezek. Hasonlóan a számítógépes programhoz, ahol az adat és a folyamat alkotja az értékelhető programot. Ide kell érteni a szervezet által kezelt dokumentumokat is.

Épületek

Fontos vagyonelem az infrastruktúra elemei, amelybe bele tartoznak a kiszolgáló épületek is. Az épületeken belül megkülönböztetünk adatközpontot, számítógéptermet, (szerverterem, gépterem), szerverszobát, rejtjelező helyiségeket, kommunikációs helyiséget, raktárakat, műhelyeket, operátor helyiségeket, közlekedőket, egyéb kiszolgáló helyiségeket, stb. A hosszú felsorolás mellett ezek az objektumok, rendelkeznek paraméterekkel, amelyek fontosak a kockázatelemzésnél. Ilyenek lehetnek a falak anyaga, vastagsága; mennyezet és padlózat teherbíró képessége, vízáteresztő képessége; ajtók, ablakok méretei,

biztonsági jellemzői; EMC [12] jellemzők, az elektromágneses kisugárzás elleni védelem miatt; az épület alapozása, stb. Az épületek szempontjából fontos az elhelyezkedése is. Dokumentálni kell az alaprajzot, a talaj szerkezetét, az alatta lehetséges vízfolyásokat, az épület tájolását, más épületektől való távolságát, az oda vezető utak állapotát, az épületre ható lehetséges környezeti hatásokat; az épületen belüli funkcionális helyiségeket körülvevő helyiségek megnevezését; az épület állapotát, stb.

Hardverek

A következő nagyon fontos elem az informatikai rendszerekben az őt alkotó eszközök és fizikai, valamint technikai jellemzői. Ide tartoznak a kiszolgáló eszközök; a kliensállomások; adattárolók; mentési rendszerek; hálózati aktív eszközök a szerverszobán belül; Rack szegkények; a tápellátás biztosító szünetmentes berendezések; aggregátorok; légtechnikai berendezések, klímaberendezések, közműhálózatok, jellemzői; a berendezések zajszintjei és rezgés jellemzőik; villámvédelem; felügyeleti, biztonsági és tűzjelző berendezések, azok paraméterei; az eszközök javítására karbantartására szolgáló berendezések, szerszámok, alkatrészek; adattároló médiák; valamint dokumentációk (kezelési utasítás, biztonsági utasítás, garancia papírok, licenszek, szerződések, utasítások, stb.), amelyek lehetnek papíralapú vagy elektronikusan tárolva.

A rendszerelemek tulajdonságának vizsgálatánál azonban meg kell húzni egy határt, ahol megmondjuk, milyen mélységéig elemezzünk. Egészen atomi szintekig is vizsgálódhatnánk, ám ekkor biztosan elvesznénk a részletekben.

Szoftverek

A hardverek mellett természetesen fel kell mérni a szoftvereket is, amelyek a rendszer és az üzleti folyamatok működtetéséhez szükségesek.

Ezek az operációs rendszerek; a mentőszoftverek; kommunikációs szoftverek (levelező, üzenetküldő,stb.) a vírusvédő szoftverek; tűzfalrendszerek; végpontvédelmi szoftverek; felügyeleti szoftverek; Log gyűjtő és elemző szoftverek, titkosító és rejtjelező szoftverek; az irodai alkalmazás- vagy programcsomagok; az üzleti folyamatokat támogató szoftverek: web alkalmazás, adatbázisok, csoportmunkát és folyamatokat támogató szoftverek; adminisztrátori segédprogramok; stb. Itt is nagyon fontosak a jellemzők meghatározása, a

[12] EMC: Electromagnetic Compatibility - Elektromágneses kompatibilitás

verziószám, a frissítések dokumentálása. Az egyénileg fejlesztett szoftverek tekintetében gondoskodni kell a pontos dokumentálásról a fejlesztés megkezdésétől a selejtezésig, valamint célszerű auditáltatni is az elkészült programot.

Hálózat

A hardverelemeket összekötő hálózatnál kockázatelemzés szempontból is nagyon fontos a jó dokumentáltság a fizikai és technikai paraméterek meghatározása. Amennyiben a kiépítésnél nem tettük meg, fel kell mérni a hálózati kábelek nyomvonalát, típusát és csatlakozó felületeit. A kommunikációs Rackszekrény elhelyezkedése, fizikai technikai paraméterei és a benne elhelyezett aktív és passzív eszközök paramétereit figyelembe kell venni. Itt is figyelembe kell venni a környezetet, az elhelyezkedést, hogyan hathat rá más eszköz. Természetesen ide tartoznak a nem vezetékes átviteli utak és azokat létesítő eszközök is, valamint az infokommunikációs eszközök mellett a telekommunikációs eszközök is.

Környezet

Nem mindegy, hogy hol helyezkednek el a fenti rendszerelemek, ezért, bár már egyes helyeken említést tettem róla, de külön ki kell fejteni ebben a pontban is a környezeti jellemzőket. Ilyen az éghajlati viszonyok, talajszerkezet, a területi elhelyezkedés, amennyiben lehetséges objektívan meg kell határozni a gazdasági és politikai viszonyokat, biztonságpolitikai szempontokat is figyelembe véve. (Ez nagy valószínűséggel csak külső szemlélő által lesz igazán hiteles!) Az objektum elhelyezése a lakot településtől, népsűrűség, forgalom, életszínvonal, közlekedés szempontjából. A területre jellemző statisztikai adatok lekérése szempontjából fontos lehet a földrengés, árvíz, tűzvész, viharok (tornádó, hurrikán), hőmérsékleti adatok, napsütéses órák száma, hó adatok. A tengerszint feletti, illetve a földszinthez viszonyított elhelyezkedése lehet még meghatározó. Az fizikai és környezeti elhelyezkedés szempontjából a védelmi képességeinek a meghatározásához kell gyűjteni adatokat, hogy később ki lehessen alakítani a fizikai, elektronikai és az élőerős védelmet. Fel kell mérni milyen kommunikációs csatorna érhető el a kapcsolattartáshoz, azok milyen stabilak, megbízhatóak. Fontos, hogy milyen közműhálózattal kell számolni. Van-e lehetőség a valóban független betáplálásokra víz, gáz, villany vagy egyéb energiaellátás tekintetében. Ezek mennyire megbízhatóak. Meg kell vizsgálni a logisztikai utak állapotát, teherbíró

képességüket, időjárás és egyéb veszélyeknek való kitettségüket. Végül, de nem utolsó sorban fel kell mérni a környezetvédelmi szempontokat is, például hogy milyen előírásokat kell az adott helyszínen figyelembe venni.

Személyi összetételre vonatkozó adatok

A darabszám ebben az esetben is egy paraméter a sok közül, így itt is fontos a képzetség, a képesség, a tapasztalat, a megbízhatóság, életvezetés, kommunikációs készség, lojalitás stb. A korábban a felelős személyeknél leírtak pedig a személyek "típusát" adja meg.

Szervezetre vonatkozó információk

A fenti személyek jobb esetben valamilyen rendszer szerint vannak összerendelve. Az üzleti folyamatokat, az adatokat, az üzleti célt, az elhelyezkedést, hardvert/szoftvert és minden előző pontot figyelembe véve kialakul egy szervezeti struktúra a helyes működés érdekében. Ezekhez a pozíciókhoz (és nem a személyekhez) felelőségek és jogok lesznek delegálva. Vannak vezetők és beosztottak, munkaadók és munkavállalók. Minden szervezeti elemnek meg van a saját felelőségi köre, amit munkaköri utasításban rögzítenek. A pozícióknak és a szervezeti elemeknek is megvan az együttműködési területe és feltétele, valamint a határvonalak, amelyek behatárolják a mozgásterületet (ezek az átadási pontok is egyben). Vannak kommunikációs útvonalak, amelyeken áramlik az információ. Ez lehet utasítás, parancs, tájékoztatás, visszajelzés, stb. Ezekről is mind tudomást kell szerezni a felmérés során.

Következmények, hatások

Mit okozhat egy nem várt esemény bekövetkezése?

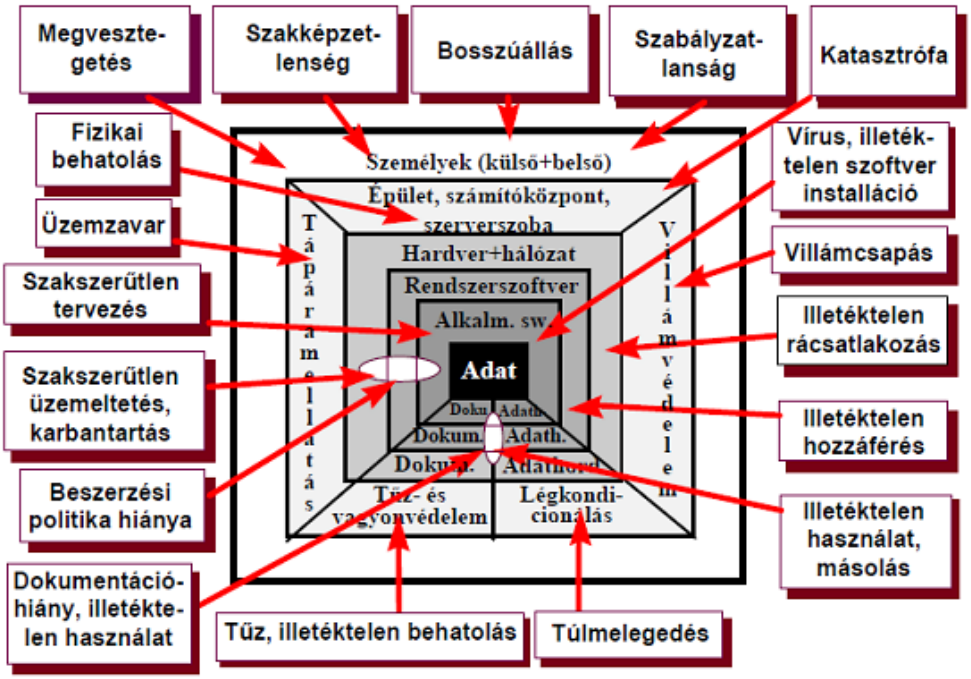
- Emberi élet közvetlen veszélyeztetése vagy egészségkárosítása;
- Gazdaságilag hátrány másokkal szemben;
- Pénzügyi veszteség;
- Hitelesség, megbízhatóság elvesztése pl. szövetségi viszonyokban történő bizalomvesztés, törvényi kötelezettségből adódó megnemfelelés;
- Magyarország szuverenitásának, területi integritásának, alkotmányos rendjének, belső stabilitásának veszélyeztetése;

- A nukleáris és vegyi létesítmények biztonsági rendszereinek a veszélyeztetése;
- stb.

Ezek voltak az alapadatok, amelyeket össze kell gyűjteni, rendszerezni, dokumentálni és folyamatosan naprakészen tartani.[4]

Egy új rendszernél a bemutatott felmérést részben lehetséges csak elvégezni, több dolgot előre meg kell tervezni, modellezni kell. Gondosan ki kell választani a helyszint, mindent figyelembe kell venni az infrastruktúrák tervezésekor, építésekor és ezek után jön az IT rendszer kiépítése. A rendszer, ami tartalmaz hálózati passzív és aktív eszközöket, kiszolgálókat és klienseket, valamint szoftvereket, amelyek optimális esetben kompatibilisek egymással. Amennyiben külső vállalkozóval építteti a szervezet az IT rendszerét biztosítékokat kell beépíteni a szerződésbe a sikeresség érdekében, valamint nagyon pontosan meghatározni a sikerkritériumokat, amely alapján a kész rendszer átvehető.

Amennyiben az alapadatok rendelkezésre állnak a rendszer működik a kockázat elemzéshez és az azt követő kockázatkezeléshez szükség van a szervezetet érő külső és belső hatások vizsgálatára. Az IT rendszert befolyásoló fenyegetettségekből és sérülékenységből egy listát kell készíteni és megvizsgálni annak bekövetkezésének valószínűségét, illetve milyen vagyonelemre hat negatívan és milyen mértékű lesz ez. Arra, hogy milyen szerteágazó hatások érhetik a rendszert egy ábrával szemléltetem:



10. ábra ITB 12. sz. ajánlása [5]

A személyekkel kapcsolatban a legnagyobb sérülékenység a képzetlenség vagy a túlzott elvárások okozhatják. Hasonló problémák lehetnek a szervezet tekintetében a rosszul megválasztott humánerőforrás elosztás, vagy a kommunikációáramlás rossz alkalmazása. Míg a veszélyforrásokat legtöbbször valami külső esemény személy okozza, a sérülékenység pedig a saját szervezet, szoftver, hardver illetve munkatársak hibájára vezethető vissza.

Fontos még, hogy tudjuk mi motiválhatja az elkövetőket a illegális tevékenység során, amit velünk szemben végeznek. Különböző motivációk létezhetnek, amelyek hajthatnak embereket, csoportokat. A hackereket például a hírnév, a kihívás, a pénz, csoportba való bekerülés; a terroristákat hasonlók kiegészítve politikai és vallási megfontolásokkal vagy média hírveréssel; szervezetbűnözői-, ipari kémkedés, számítógépes bűnözői körökre természetesen a legjellemzőbb a pénz és az erőviszonyok megszerzése; mindezek mellett manapság megjelentek az állami, vagy államilag finanszírozott ’kiber’ csapatok, amelyeknek a motivációja a katonákéhoz hasonló.

Kockázatkezelés

Amennyiben valamilyen fontossági sorrendet szeretnénk felállítani a kockázatkezeléssel kapcsolatban, akkor az előzőekből kiindulva a következőt kell megvizsgálni:

Mi az a fenyegetés, ami legtöbb vagyonelemet érint?

Mi az a fenyegetés, amely legtöbb folyamatot érint?

Mi az a fenyegetés, amely a legértékesebb folyamatot vagy vagyonelemet érinti?

Mi okozza a legnagyobb kárt?

Mivel kárértékű kockázatkezelést kell végrehajtani, ezeket a szempontokat kell figyelembe venni.

Az információból, amelyeket az elemzés során feltártunk, rendszereztünk egy jelentést kell készíteni, melyet a vezetés elé kell tárni. A dokumentumnak érthető kell, hogy legyen egy nem informatikus számára is, legyenek benne javaslatok, elvi ellenintézkedési tervek, érvelések. A vezető meghozza a döntését, hogy mi történjen a feltárt kockázatokkal.

Csökkentés

A legkézenfekvőbb döntés, hogy ha már ismerjük a problémát, annak hatását, akkor szüntessük meg vagy csökkentsük. A csökkentésre lehet példa, hogy a tűzjelző és tűzoltó rendszert korszerűsítsük, vagy a védendő terület környezetét tisztítsuk meg az éghető anyagoktól.

Elkerülés

A kockázatokat el is kerülhetjük. Erre példa, amikor a tervezési fázisban feltárunk olyan kockázatos lépéseket, amelyeket helyettesíthetünk kevésbé kockázatosokkal, akkor azt lecseréljük arra. Ezzel elkerültük a kockázatot. Az üzemelés során pedig kivezethetünk olyan szolgáltatásokat, amelyek kockázatosak.

Fenntartás

Születhet olyan döntés is, hogy nem reagálunk rá. Ez nem azt jelenti, hogy nem foglalkozunk vele, csak nem hozunk ellenintézkedést. Ebben az esetben is számolni kell a kockázattal, például intézkedési terveket kell kidolgozni az esetleges

bekövetkezéskor milyen reakció kell, hogy kövesse részünkről az eseményt. Itt állhat pénzügyi vagy egyéb más megfontolás is.

Áthárítás

A kockázat áthárításokat tipikusan szerződésekkel szokták megoldani, amikor egy külső cégre hárítják át a felelőséget. Szerződésben kell rögzíteni például, hogy mit várunk el az adott szolgáltatótól, mennyi legyen a rendelkezésre állás az elektromos betáplálásnál, valamint mennyi kártérítés jár nekünk, ha ez nem teljesül. [4]

IT biztonságának egyéb összetevői

A kockázatkezelést is elősegíti a hardverelemek és szoftverelemek nyilvántartása, illetve annak változáskezelése. Folyamatosan ismerni kell a rendszer alkotóelemeit. Ide sorolandó a szoftverek jogtisztasága, rendszeres karbantartása (pl. patch management) is. A licensz nyilvántartással összekötve rendelkezni kell egy másik nyilvántartással is, amely tartalmazza, hogy milyen szoftverek telepíthetőek, illetve milyen hardverek illeszthetőek a rendszerbe (BASELINE). A hardverelemek karbantartása elősegíti a biztonság növelését és az élettartam meghosszabbítását. Figyelemmel kell kísérni SLA-t, a már nem használt szolgáltatásokat és ahhoz tartozó szoftver és hardverelemek ki kell vonni a rendszerből, amellyel energiát lehet spórolni, valamint elkerülhető a felesleges kockázat.

Előfordulhat, hogy a rendszer tartalmaz saját fejlesztésű eszközöket és szoftvereket. Ezeket a termékeket mindig elkülönülten kell fejleszteni az éles rendszertől, amelyre csak mindenre kiterjedő vizsgálatot követően szabad feltelepíteni. A „Szoftvertermékek értékelése, minőségi jellemzők és használatuk irányelvei” című szabvány (MSZ ISO/IEC 9126) egy hierarchikus szempontrendszert ad a vizsgálathoz. Természetesen a piacon kapható szoftverek is csak egy hasonló vizsgálatot követően kerülhetnek be a BASELINE-ba. Az „Informatika. Szoftver életciklus folyamatok” című MSZ ISO/IEC 12207 szabvány is segítséget nyújthat a szoftverek teljes életciklusára az ötletek megfogalmazásától a szoftver visszavonásáig. [2] A vizsgálatot, majd a későbbi üzemeltetést is elősegíti a fejlesztés egész életciklusa alatt elvégzendő dokumentálás. Ezt minden esetben meg kell követelni, a szoftvert csak egy komplett dokumentációval szabad átvenni, amiben a különböző paraméterek mellett szerepel a fejlesztésben résztvevők neve,

elérhetősége. Gondoskodni kell, hogy a vásárolt, illetve fejlesztett eszközök, szoftverek üzemeltetési költsége legyen betervezve az éves költségvetésbe is.

A komplett rendszert érdemes egy külső, független szervezettel auditáltatni, amely elősegíti a fel nem tárt hiányosságok kiküszöbölését. Egyes rendszereknél pedig szükséges akkreditálni is a rendszert, amelyet valamilyen hatóság végez és mindkét esetben tanúsítvány készül, hogy az auditált, akkreditált rendszer megfelel az előírásoknak, vagy éppen valamelyik szabványnak, ajánlásnak. Az informatikai termékek és rendszerek biztonsági szintjének mérésére és értékelésére készült A Common Criteria, melyből 2003-ban magyar szabvány is készült (MSZ ISO/IEC 15408-1, -2, -3).

Természetesen az üzemeltetés során fontos a képzés. Többfajta oktatást kell szervezi az üzemeltető személyzet részére, illetve a felhasználók számára is. A szakmai oktatásokon túl, rendszeres biztonsági képzéseket kell tartani ezáltal növelni kell a biztonságtudatosságot. Fontos, hogy a felhasználók megértsék, az információbiztonság nemcsak a rendszeradminisztrátorok felelőssége. Itt meg kell értetni a biztonság fontosságát, illetve egyes folyamatokat be kell gyakoroltatni, hogy készség szinten tudják alkalmazni a résztvevők. Nagyon hasznos és hatékony módja a folyamatos biztonság tudatosításának az online képzés és vizsgáztatás. Ezt történhet véletlenszerűen kiválasztott személyekkel, illetve véletlenszerűen kiválasztott időpontban.

IT biztonsághoz köthető főbb szabványok

Az IT rendszer üzemeltetése során jogszabályokat és ajánlásokat kell, illetve érdemes betartani a biztonságos üzemeltetés érdekében. A törvények teljes felsorolását mellőzve kiemelek két fontos, a közelmúltban megjelent jogszabályt. Az egyik a 2009. XII. 29-n kihirdetésre került a minősített adat védelméről szóló 2009. évi CLV. törvény, valamint ennek rendeletei. A másik szintén meghatározó a 2013. évi L. törvény, mely az állami és önkormányzati szervek elektronikus információbiztonságáról szól. Mindkettő törvény nagyon fontos hiányosságot pótolt az IT biztonság szabályozásában.

Kvázi szabványok

Kvázi szabványoknak lehet nevezni az RFC-ket (Request For Comments: kéretik megkritizálni). Ezek olyan dokumentumok, melyeknek a célja, hogy a szabvánnyá válás előtt bárki kritikával élhet ellene. Így, hasonlóan egy nyílt

szoftverfejlesztéshez kialakulhat egy szakmailag megvitatott, mindenki által elfogadott szabvány, vagy elvetik és törlik a tervezetet.

Szabványok, ajánlások

Szabványok, amelyek alkalmazásával kidolgozhatóak az informatikai biztonsági követelmények elősegítik a rendszer biztonságossá tételét, valamint bizalmat közvetítenek más szervezetekkel szemben. Az ajánlások már egy kidolgozott, szakmai közösségek által elfogadott és jóváhagyott folyamatosan átdolgozott keretrendszert biztosítanak. A vázra ráültetve a saját szervezetünkre alkalmazható szabályrendszert hozhatunk létre. Tehát a szabvány nem egy kötelezően betartandó utasítás, hanem egy ajánlás, irányelv, amit kitöltve a helyi sajátosságokkal biztonságossá tehetjük rendszerünket.

Az alábbi szinteken különböztethetjük meg:
- nemzetközi szabványok;
- regionális szabványok;
- nemzeti szabványok;

Néhány az informatikai biztonsággal foglalkozó ajánlás, szabvány

- ISO/IEC 27000-s szabványcsalád. Az információbiztonság irányítási rendszereinek követelményei;
- NATO's C-M(2002) 49 (NATO's C-M(2002) 49 "Security within The North Atlantic Treaty Organization");
- ISO/IEC 17799 Az információbiztonság irányítási gyakorlatának kézikönyve;
- MSZ CWA 14167-1:2006 Elektronikus aláírások tanúsítványait kezelő megbízható rendszerek biztonsági követelményei. 1. rész: Rendszerbiztonsági követelmények;
- MSZ ETSI TS 101 456:2006 Elektronikus aláírások és infrastruktúrák (ESI). Minősített tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó szabályzatok követelményei;
- MSZ ETSI TS 102 023:2006 Elektronikus aláírások és infrastruktúrák (ESI). Időbélyegzés-szolgáltatókra vonatkozó szabályzatok követelményei;
- MSZ ETSI TS 102 042:2006 Elektronikus aláírások és infrastruktúrák (ESI). Nyilvános kulcs tanúsítványát kibocsátó hitelesítésszolgáltatókra vonatkozó szabályzatok követelményei;

- COBIT[13] az ISACA[14] által kidolgozott szabvány. Elsősorban egy oktatási anyag, amely felsővezetők, auditorok és IT szakértők számára készült;
- ISO/IEC 20000 (ITIL);
- Az Informatikai Tárcaközi Bizottság 12. sz. ajánlása;
- Közigazgatási Informatikai Bizottság 25. számú ajánlása;

ITIL

Ez a szabvány az informatikai szolgáltatással kapcsolatos módszertanokat tárgyalja, ami az üzemeltetéshez szükséges.

Az informatikai szolgáltatásokat két fő csoportba osztja, ami a szolgáltatásbiztosítás és a szolgáltatástámogatás. A csoportosítást talán legjobban úgy jellemezhetjük, hogy milyen az ügyféllel, felhasználókkal való viszonyuk. A részletesebb magyarázatnál látszik, hogy a szolgáltatásbiztosítás közvetlenül találkozik az ügyfelekkel, míg a másik csak közvetetten. A szolgáltatásbiztosítás a kiszolgáló eszközökkel foglalkozik, valamint a támogatók által meg nem oldott feladatokat végzi el. Semmiképpen nem szabad úgy felfogni, hogy a támogatás a gyengébb feladat. Éppen olyan fontos, mint a szolgáltatásbiztosítás. A gyorsaság a szolgáltatásbiztosításnál nagyon fontos. Fontos az empatikus tulajdonságok megléte, a tárgyalóképesség, és képesnek kell lenni a laikus megfogalmazásokat az informatika nyelvére lefordítani. Az informatikai üzemeltetést több lépcsőben kell felépíteni. Az első lesz a szolgáltatástámogatás, majd a szolgáltatásbiztosítás, a harmadik pedig a rendszertámogatás.

Szolgáltatástámogatás (Service Support)

- Ügyfélszolgálat, hibabejelentő (Sevice Desk, Help Desk)
  Az első vonalbeli munka elvégzése, mint hibaelhárítás, kérelmek kezelése (hozzáférés kérelem, jogosultsági kérelmek, stb...) felhasználói kapcsolattartás. Jellemzője a gyors reagálás, legtöbb esetben csak a munkalap felvétele történik meg.
- Incidenskezelés (Incident Management), problémakezelés (Problem Management)
  Az előforduló hibák lekezelése, a levont következtetések alapján a jövőbeli hibák megakadályozása a cél. Amennyiben nem oldható meg viszonylag

[13] Control Objectives for Information and Related Technology

[14] Information Systems Audit and Control Association

rövid időn belül a hibaelhárítás, akkor át kell adni egy magasabb szintű hibaelhárító csapatnak.

- Változáskezelés (Change Management)
  A rendszerben történő változás a normál működés - átmeneti állapot - normál működés folyamata. A "beállt" rendszerben történő változtatás mindig kockázati tényezőként jelenik meg. Azért, hogy ezt a kockázatot a minimálisra csökkentsük, elő kell rá készülni, ki kell dolgozni a lehetséges problémákra a választ, meg kell tervezni a folyamatokat. A változtatási kérelem érkezhet a felhasználóktól és az üzemeltető állománytól is.
- Konfigurációkezelés (Configuration Management)
  Annak érdekében, hogy kézben tarthatóak legyenek az IT szolgáltatások, rendszeres és folyamatos nyilvántartást kell végezni a szolgáltatásokról, a szoftver és hardver konfigurációkról. A nyilvántartásokat el kell érnie az IT személyzetnek, és mindig az aktuális állapotot kell mutassák.
  Célszerű létrehozni egy alapkonfigurációt (baseline), amely megmutatja, hogy milyen egy alap munkaállomás vagy milyen szoftverekből lehetséges összeállítani egy munkaállomást. Nem érdemes sok hasonló funkciót kielégítő szoftvert alkalmazni, mert egységes kialakítás megkönnyíti a támogatást, karbantartást.
- Kiadáskezelés (Relase Management)
  A változtatásokat, a fejlesztések eredményeképpen létrejött változtatásokat tesztelés után, annak kiértékelésével lehet az éles rendszerbe bevezetni. Ez egyaránt vonatkozik a hardver és szoftver elemekre. Ebből lesz kialakítva egy csomag, baseline, amelyekből engedélyezhető a rendszeresítés;

Szolgáltatásbiztosítás (Service Delivery)

- Szolgáltatásszint biztosítás
- Ezt a szolgáltatási megállapodásban (Service Level Management — SLM) kell megfogalmazni. A "megrendelő" rögzíti, hogy milyen elvárásai vannak a rendszerrel szemben. Ehhez a dokumentumhoz tud mindkét fél (megrendelő és szolgáltató) visszanyúlni az esetleges vitás kérdésekben. Így ez mindkét félnek hasznos alapdokumentum lehet. Erre lehet alapozni a pénzügyi és egyéb feltételek tervezésében is. Az üzemeltető állomány folyamatosan monitorozza a hálózatot annak érdekében, hogy az egyenletesen biztosítsa a kívánt minőségi szintet. Ide kapcsolódik még a Üzemeltetés megállapodás (Operation Level Agreement - OLA) fogalma,

amely a cégen belül két vagy több szervezetnek a megállapodását jelenti. Ennek segítségével az IT üzemeltető szervezet tisztában van a szervezetek között zajló folyamatokkal, ami szükséges az IT szolgáltatás biztosításához. A megállapodásokat mindenki számára érthető nyelven kell megfogalmazni, nem tartalmazhat szakzsargonokat.

- Rendelkezésre állás biztosítása (Availability Management — AM)
- Az előzőekben megfogalmazottak mellett a rendelkezésre állás megmondja, hogy milyen követelmény támasztható a rendszerrel szemben, figyelembe véve az informatikai infrastruktúra képességeit. A felhasználóknak tisztában kell lenni, hogy a rendszer esetleg nem lesz mindig elérhető, ugyanakkor biztosítva van a maximális leállási idő is, amely után a szolgáltatásoknak újra elérhetőnek kell lenniük. Megfelelő szintű kockázatkezeléssel megnövelhető a rendelkezésre állás. Eljárásokkal és komoly anyagi ráfordításokkal a rendelkezésre állást közelíteni lehet a 100%-hoz.
- A magas rendelkezésre álláshoz több lehetőség is kínálkozik. Ilyen a tartalék alkatrészképzés (ez hideg tartalékot jelent), ezzel gyorsan pótolhatjuk a kieső részeket a szervezet raktárából. Szoftveres virtuális alrendszerek létrehozásával szintén gyorsan reagálhatunk az incidensekre. Ilyenkor párhuzamosan futtathatunk egy tükrözött rendszert, amelyre átkapcsolhatunk. Ebben az esetben minimális lesz a kiesés (meleg tartalék). Kapcsolódva az előzőhöz, hibadetektáló szoftverekkel riasztást generálhatunk, esetleg automatikus hibaelhárítást végezhetünk, melyekkel elérhető a azonnali helyreállítás (forró tartalék). Ebben az esetben nincs kiesés. További lehetőség a hibatűrő diszkrendszer alkalmazása RAID (Redundant Array of Inexpensive Disks vagy Redundant Array of Independent Disks). Nem a legköltséghatékonyabb megoldás, de szintén elérhetünk vele magasabb rendelkezésre állást a csökkentett szinten történő futtatással. A telekommunikáció, összeköttetés területén bevált és szinte elvárt a duplikált összeköttetési útvonalak alkalmazása.
- Informatikaszolgáltatás-folytonosságbiztosítása (IT Service Continuity Management — ITSCM)
- A folyamatos és megbízható működés érdekében a kockázatok felmérésével el kell készíteni a katasztrófatervet, az incidenskezelési eljárásokat. Ezzel érhetjük el, hogy a normál működéstől eltérő események bekövetkezésekor is mindenki ismerje a feladatát és egy ív legyen a normál működés - leállás - normál működés közt.
- Kapacitásbiztosítása (Capacity Management — CM)

- A rendszer optimális működéséhez figyelembe kell venni, hogy az elvárt teljesítmény biztosítása rendelkezésre álljon a megfelelő időben, és ez mindig a szükséges költségráfordítással járjon. Ismerni kell a felhasználók munkafolyamatait, hogy tervezni lehessen a kapacitásbővítést. Ilyenek lehetnek a felhasználók számának változása, a munkavégzés helyének, módjának változása, a tárhely növekedésének üteme. Cél, hogy minimális legyen a túlterhelés, illetve az alacsony kihasználtság.
- Informatikaszolgáltatás pénzügyi irányítása (Financial Management — FM)
- Az IT sikeres működtetésének egyik legfontosabb feltétele a folyamatos és szükséges pénzügyi források biztosítása. Ennek érdekében el kell készíteni a rövid és hosszú távú pénzügyi terveket. A mindennapokban a felhasználók igényeinek elbírálása során elkerülhető a pazarlás, az erőforrások maximális felhasználását érhetjük el. [6]

Az ISO/IEC 27000-s szabványcsalád

Az információbiztonság szempontjából mindennapos gyakorlatnak tekinthető intézkedések közé tartoznak:

- Kockázatfelmérés és kockázatjavítás
  Az egyik legfontosabb dolog, hogy tisztában legyünk a rendszerünket veszélyeztető tényezőkkel. Lehet, hogy első hallásra meghökkentő, de mindig lesz a rendszerünkben olyan potenciális veszély, amelyet nem szüntetünk meg. Gondoljunk arra, hogy tökéletesen biztonságos rendszer nincs, de megközelíteni megtudjuk. El kell döntenünk mi az az incidens, amelynek elviselése még megengedett. Amennyiben ismerjük a kockázatokat, a rendelkezésre álló pénzügyi lehetőségekhez képest lehet majd meghatározni hol lesz a "határ", mi az, ami ellen már csak a bekövetkezése után reagálunk. Természetesen a meg nem szüntetett veszély bekövetkezésére meg kell legyen a válaszreakció.
- Az információbiztonsági politika dokumentuma
  A szervezetnek rendelkeznie kell a különböző szinteken jóváhagyott biztonsági és üzemeltetéssel kapcsolatos dokumentumokkal, amelyet oktatni, ismertetni kell a rendszerrel kapcsolatban álló személyekkel.
- Az információbiztonság szervezete
  Szükséges a belső és külső szervezetek viszonya, felelősségei, jogainak tisztázása. A vezetőségnek elkötelezettnek kell lennie az

információbiztonság iránt, és meg kell nevezni a szolgálati személyeket, azok a jogait és felelősségeit.

- Vagyontárgyak kezelése
  Ide kell érteni a fizikai vagyontárgyakat, a szoftvereket és az adatokat is, ezek információosztályozását el kell végezni, jól láthatóan megjelölni.
- Emberi erőforrások biztonsága
  A személyek vizsgálata, felügyelete a munkába állás előtt, közben és utána. Felelősségének, jogainak és kötelességeinek tisztázása.
- Fizikai és környezeti biztonság
  Biztonsági területek kijelölése, a berendezés biztonság megfogalmazása, azok elhelyezése, üzemeltetéséhez szükséges feltételek megteremtése, karbantartása. Továbbá ide sorolható még a berendezések kivonása a rendszerből.
- A kommunikáció és az üzemeltetés irányítása
  Ez a rész tárgyalja az üzemeltetési eljárások és felelősségek dokumentált meglétét, rendszertervezés rendszerbeállítás kritériumainak leírását, a megfelelő és folyamatos kapacitások biztosítását. Foglalkozik a rosszindulatú és mobil kódok elleni védelemmel, mentési mechanizmusok, stratégiák meghatározásával, hálózatbiztonság kezelésével. Fontos az adathordozók kezelése az egész életciklusuk során, az információcserének a szabályozása. Végül a naplózási eljárások rendjét írja le, ahol meg kell határozni mit, meddig, hová kell naplózni.
- Hozzáférés-ellenőrzés
  Igen érzékeny téma a felhasználók regisztrálása, jogok beállítása, jelszóhasználat, admin jogok tisztázása, felhasználó hitelesítés, hálózati hozzáférés-ellenőrzése, végpont- és útvonalvédelem. Két fontos elvet fogalmaznak meg ebben a pontban, az egyik a tisztaasztal- és tisztaképernyő-szabályzat, valamint a need-to-know elv.
- Információs rendszerek beszerzése, fejlesztése és karbantartása
  Fontos az életcikluson át tartó gondosság a beszerzéstől a kivezetésig. Minden ponton figyelembe kell venni a biztonsági előírásokat a rendszerbe történő beilleszthetőséget.
- Az információbiztonsági incidensek kezelése
  E címszó alatt van tárgyalva az eljárások megfogalmazása, adatok gyűjtésének módja, típusa. A későbbi hasonló incidensek elkerülése érdekében le kell vonni a tanulságokat.
- Információbiztonság tudatosság, képzések szervezése

A képzésekkel el kell érni a felhasználókban a tudatosságot, érezzék a biztonság fontosságát. A rendszer kezelése legyen készségszintű, ismerjék annak minden fontos elemét. A rendszerrel kapcsolatos folyamatokat, eljárási rendeket a felhasználóknak be kell tartani.

- Működésfolytonosság irányítása
  A rendszer folytonos működése érdekében meg kell teremteni az ehhez szükséges feltételeket. Minimálisra kell csökkenteni a nem várt hatások bekövetkezését.
- Megfelelőség
  A szervezetet auditálni, a rendszert akkreditálni kell, annak érdekében, hogy egy független szervezet is kimondja, hogy a szabályok és belső folyamatok megfelelnek a szükséges biztonsági elvárásoknak. A rendszer üzemeltetése során törekedni kell arra, hogy megfeleljünk minden törvényi és szabályozási előírásnak, betartsunk minden szerződésben foglalt kötelezettségeket. Ide kell sorolni a szellemi tulajdonjogokat, a személyes adatok bizalmasságát és az adatvédelmet. [7]

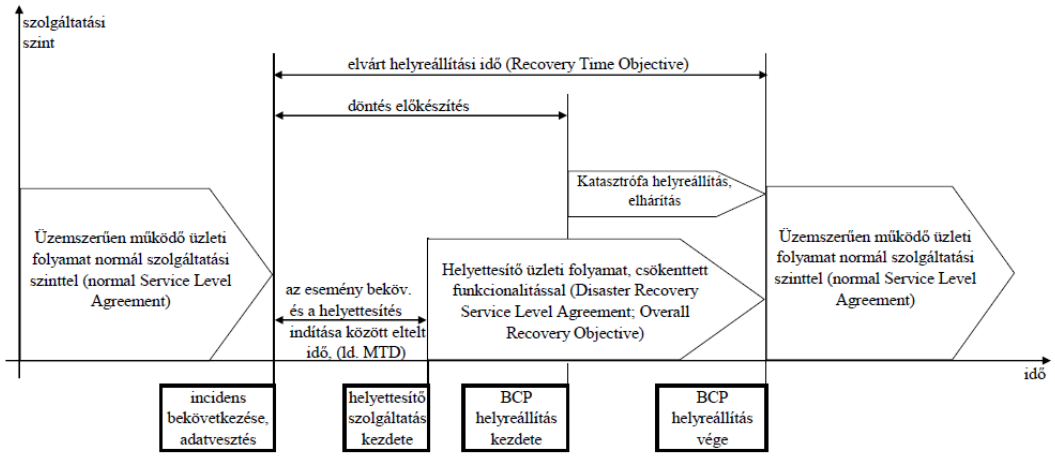
Két fontos szabványt segítségével biztonságosabban üzemeltethető az IT rendszer és elkészíthető a szervezet a Biztonsági Szabályzata, a Számítástechnikai Védelmi Szabályzata és a Számítástechnikai Biztonsági Üzemeltetési Szabályzata.

Ezek mellett mindenképpen szabályozni kell a logisztikai kérdéseket is. A legfontosabb talán a beszerzés, amelyben meg kell követelni a központosított hardver és szoftverbeszerzést, majd ennek nyilvántartását. Minden esetben tudni kell egy termék életútját. Ki kell jelölni és folyamatosan biztosítani hasonlóan a tűzvédelemnél a logisztikai, szállítási utakat.

Kiemelt terület még a biztonsági tárgyalásánál a személyi és fizikai biztonság. Ezeknek egy sor területe van, amellyel a kijelölt felelős személyeknek foglalkozni kell. Ilyenek az objektumvédelem, tartalék helyszínek biztosítása, a védendő információhoz, fizikai és logikai hozzáférés koordinálása, beléptető, riasztó és megfigyelőrendszer üzemeltetése, tűzvédelem, hőmérséklet és páratartalom megfelelő szintentartása, vízbetörés, vízszivárgás elleni védelem, stb.

A kialakított védelem egy információbiztonsági architektúrát alkot, amelyben minden személynek, eszköznek megvan a szerepe, felelőssége. Tisztázva vannak a kommunikációs csatornák, a vertikális és horizontális együttműködések. Együttműködést kell biztosítani a biztonsági területen belül dolgozókkal (a cégen belül a munkavédelemmel, egészségvédelemmel, tűzvédelemmel, stb.), az IT szakemberekkel, a külső cégekkel. A sikeresség csak egy központosított

információbiztonsági rendszerrel érhető el, amelynek része az egységes és homogén IT rendszer. Egy vállalaton belül indokolatlanul nem szabad elszigetelt IT rendszereket üzemeltetni, "egy kézben" kell összpontosuljon. A várható eseményekre cselekvési terveket kell készíteni. Minden esetben biztosítani kell az üzletmenet folytonosságát, még akkor is, ha krízis vagy katasztrófahelyzet áll elő. A "váratlan" eseményekre Üzletmenet Folytonossági Tervet (Business Continuity Plan) és Katasztrófa-elhárítási Tervet (Disaster Recovery Plan) kell készíteni. Az Üzletmenet Folytonossági Tervben szerepel az üzleti, szervezet működéséhez tartozó kritikus folyamatok, az azokat támogató informatikai rendszerek folyamatos és az elvárt szinten történő működés leírása, illetve ezek kiesése esetén helyettesítő eljárások, cselekvési tervek. A Katasztrófa-elhárítási Tervben kell szerepeltetni az IT rendszerek meghibásodása, leállása miatti súlyos szolgáltatás-kiesésekor elvégzendő feladatokat.



2. ábra Üzletmenet folytonosság modellje [2]

Összegzés

A leírtakból kitűnik, hogy a információbiztonsági irányítási rendszer kiépítése egy komplex és időigényes feladat. Gyakorlatilag a szervezet teljes állományának az összehangolt munkáját igényli, felügyelve és koordinálva a környezeti hatásokat, központosítottan felügyelve és üzemeltetve az IT rendszereket. Több jogszabály és szabvány is foglalkozik a témával, már-már elvész az ember köztük. Az ajánlások együttes alkalmazását segítette elő az IT Governance Institute és az Office of Government Commerce által készített tanulmány, amely a CObIT (információs rendszerek (technológiák) kontrollálása), az ITIL (az informatikai rendszerek

üzemeltetésével és fejlesztésével foglalkozik) és az ISO/IEC 27002 (Az információbiztonság irányítási rendszereinek követelményei) szabványokat együttesen elemezte. A gyakorlatban segítséget nyújthat egy integrált irányítási és kontrollrendszerek alkalmazása. Egy modulokból felépített szoftverrel koordinálni lehetne az üzemeltetett rendszerünket. Vannak ilyen jellegű szoftverek ma is, azonban a komplexitás miatt csak egy-egy területet képesek kezelni. Így marad az ember, aki fejében összefutnak az információk, majd képesség és képzettség függvényében dönt. Fontos azonban, hogy tervezéssel, szabályrendszerekkel, oktatásokkal és szenzorokkal minél magasabb szintvonalra emelje egy szervezet a biztonsági szintjét.

„A világegyetem káosz, mégis racionális törvények uralják” [15]

Felhasznált irodalom

[1] Munk Sándor: ROBOTHADVISELÉS 7. tudományos konferencia - INFORMÁCIÓBIZTONSÁG VS. INFORMATIKAI BIZTONSÁG, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, X. Hungária krt. 9-11., 2007.

[2] Dr. Michelberger Pál - Lábodi Csaba: Vállalkozásfejlesztés a XXI. században II., Óbudai Egyetem, 2012.

[3] Vicsek Tamás: A Magyar Tudományos Akadémia folyóirata, http://www.matud.iif.hu/03mar/vicsek.html. 2014.01.04

[4] ISO/IEC 27005: Information technology — Security techniques— Information security risk management, 2008.

[5] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda: Informatikai Tárcaközi Bizottság Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás, Budapest, 1996.

[6] KFKI Számítástechnikai Rt: Az ITIL módszertan áttekintése, 2002.

[7] MSZ ISO/IEC 27001: Informatika. Biztonságtechnika.Az információbiztonság irányítási rendszerei. Követelmények, 2006.

[15] Albert Einstein

[8] IT Governance Institute, Office of Government Commerce: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf. 2014.01.15

GÖMÖR Marianna: Minősített adatkezelés, komplex védelem megvalósítása

Absztrakt

A szerző a cikkben elemzi a minősített adatok védelmének különböző lehetőségeit, megvizsgálja az információk formáit. Feldolgozza a hatályos jogszabályokat, és mindezeknek megfelelően kialakít egy komplex védelmi környezetet.

Abstract

The author of the article analyzes various options for protecting classified information, assesses the forms of information. She processes the existing laws, and according to all these she forms a complex security environment.

Kulcsszavak: *információvédelem, minősített adatkezelés, fizikai biztonság, személyi biztonság, adminisztratív biztonság*

Bevezetés

A védeni kívánt információk számos formában fordulhatnak elő. Lehet ez adathordozón rögzített, továbbított, írásos formában megjelenő minősített adat; minősített információkat hordozó objektum vagy technikai eszköz; eljárás; nem tárgyiasított ismeretanyag; szóban közölt minősített információ. A védett információ valamennyi megjelenési formájára igaz, hogy minősített adatkezelés a jogszabályban foglalt fizikai, személyi, adminisztratív, elektronikus biztonsági feltételek együttes kialakítása nélkül nem jöhet létre.

Fizikai biztonság Infrastruktúra + élőerő	**Személyi biztonság**
Adminisztratív biztonság	**Elektronikus biztonság** - Rendszerbiztonság: • hardverbiztonság • szoftverbiztonság • hozzáférési jogosultságok • biztonsági mentés, helyreállítás • vírusvédelem • hálózatok biztonsága - Rejtjelbiztonság - Átvitelbiztonság

1. sz. ábra „Komplex védelem kialakítása”

Fizikai biztonság

Fizikai biztonság alatt azon rendszabályok összességét értjük, melyek az erőforrások elleni szándékos vagy gondatlanságból felmerülő fenyegetettségek megakadályozására hivatottak. Ide tartoznak a tényleges akadályok, mint a falak, sorompók, torlaszok, szögesdrótok, kerítések, behatolás jelző rendszerek, beléptető rendszerek, zárt láncú kamerarendszer, reagáló erő stb. „ *A rendszerre, valamint a rendszer minősített adathordozóira vonatkozó fizikai biztonsági követelményekre a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendelet előírásai az irányadóak.*” [1]

A fizikai védelmi rendszabályok kialakításánál figyelembe kell venni a kezelt adatok mennyiségét, megjelenési formáját, biztonsági besorolását, a helyi biztonsági környezetet, a helyszín és a szervezet veszélyeztetettségi szintjét,

nemzetbiztonsági kockázatokat, az információ tárolásának kívánt módját. A minősített adatok kezelő szervezet fizikai védelmét, a „mélységi védelem" elvének megfelelően, úgy kell felépíteni, hogy az több lépcsőben nyújtson biztonságot. A külső elemek biztosítják a védendő terület határait. A közbenső elemek észlelik az illetéktelen behatolást és riasztják a reagáló erőt. A belső elemek szerepe a késleltetés, megakadályozzák, hogy a behatoló minősített adatokhoz férjen hozzá még a reagáló erő megérkezése előtt. A nemzeti jogszabályokban olvasható környezetre, védelmi rendszerekre, infrastruktúrára vonatkozó előírások csak általános rendszabályokat fogalmaznak meg.

A rendszerek telepítését, és a későbbiek folyamán az üzemeltetését úgy kell végrehajtani, hogy illetéktelenek számára ne legyen elérhető a védendő információ. Az elvárásoknak megfelelően kell kialakítani az adatkezelő eszközök funkcióinak megfelelő csoportosítását és a zónázást. A különböző szintű fizikai védelemmel ellátott zónák létrehozása lehetővé teszi, hogy a felhasználók, üzemeltetők csak a munkavégzéshez szükséges rendszerekbe nyerjenek betekintést. A zónák közötti mozgásokra vonatkozó adatokat rögzíteni kell és meghatározott ideig tárolni. [2]

A nemzeti, NATO, EU minősített adatok tekintetében a jogszabályban meghatározottak alapján „Korlátozott terjesztésű!" minősítési szint vagy a feletti minősítéssel rendelkező adatokat biztonsági területen, adminisztratív zónában kell elhelyezni. Adminisztratív zónának minősül minden olyan helyszín, ahol a belépés ellenőrzött és regisztrált, illetve a személyek és gépjárművek a területen belül történő mozgása nyomon követhető. A „Bizalmas!" vagy ettől magasabb minősítési szintű minősített adatot kezelő elektronikus adatkezelő eszközök központi hálózati elemeit I. osztályú biztonsági területen kell elhelyezni. Míg a hálózathoz kapcsolódó felhasználói munkaállomásokat I. vagy II. osztályú biztonsági területen. I. osztályú biztonsági területnek minősül minden olyan helyszín, ahol a „Bizalmas!" vagy annál magasabb minősítési szintű minősített adat felhasználása és tárolása nyíltan történik, ezáltal a helyszínre való belépés egyben a minősített adat megismerését is jelenti. A terület fizikailag körbehatárolt és védett, ahova a ki- és belépés csak ellenőrző rendszeren keresztül lehetséges azon személyek számára, akik rendelkeznek az ehhez szükséges külön felhatalmazással és személyi biztonsági tanúsítvánnyal. II. osztályú biztonsági területnek minősül minden olyan helyszín, ahol „Bizalmas!" vagy annál magasabb minősítési szintű minősített adat felhasználása és tárolása oly módon történik, hogy az illetéktelen hozzáférést belső intézkedésekkel meg lehet akadályozni. Ebben az esetben a Nemzeti Biztonsági Felügyelet mátrixos pontszámítást alkalmaz, melynek lényege, hogy a kormányrendeletben felsorolt fizikai biztonsági intézkedésekhez tartozik egy pontszám, melynek alapján a minősített adatkezelésre engedélyt kérő szerv saját

magának ki tudja számolni a pontszámait és össze tudja vetni az elvárt szintekkel. A biztonsági területen alkalmazott rendszabályok betartását időszakosan ellenőrizni kell. A látogatók számára egyértelműen tudatni kell a tőlük elvárt magatartást, számukra jól látható helyen piktogramokkal, rövid magyarázatokkal. Fel kell hívni a figyelmüket, hogy a be- és kilépésnél adott esetben csomagellenőrzést is végrehajthatunk, továbbá, hogy a minősített adatkezelés helyszínére magántulajdonú kép-, hang-, video rögzítésére alkalmas elektronikus adatkezelő eszközök bevitele tilos, azokat az erre a célra kialakított tárolókban kötelesek elhelyezni. [1]

Igen ritka, hogy egy szervezet csak és kizárólag nemzeti minősített adatot kezeljen, így a fizikai védelmi rendszabályok kialakításakor már a NATO, EU által előírt követelményeket is célszerű szem előtt tartani. Így a későbbiek folyamán nem jelenthet problémát a szövetségi és külföldi minősített adatok cseréje, közös kezelése.

A biztonsági területen belül a nemzeti és a külföldi adatok egy helyiségben való együttes kezelése megvalósítható, amennyiben ezt az adatokra, eljárásokra vonatkozó követelmények lehetővé teszik. Ettől függetlenül tárolásuk forrásonként elkülönítve történik, amennyiben a tárolt adatok minősítési szintje nem egyezik meg, úgy a magasabb minősítési szinttel rendelkező adat biztonságára vonatkozó követelményeknek kell megvalósulnia.

A fizikai biztonság fogalmához tartozik a reagáló erő alkalmazása, feladatukat írásban kell rögzíteni. A kormányrendeletben meghatározottak alapján 4 különböző kategóriába sorolhatjuk őket, a személyi biztonsági tanúsítvány megléte, a járőrözés gyakorisága és útvonala alapján. Tagjai biztonsági felügyeletet látnak el, továbbá a Nyilvántartó riasztó központjának jelzései is a reagáló erők elhelyezési épületében vagy a rendőrségnél riasztanak.

A biztonsági vezető gondoskodik a biztonsági eszközök és rendszerek időszakos karbantartásáról. A helyiségek takarításakor, rendszerek karbantartásakor, javításakor is ügyelni kell arra, hogy a takarító-, karbantartó személyzet ne férjen hozzá illetéktelenül a minősített adatokhoz, így a feladatuk végrehajtása alatt folyamatos felügyeletet kell biztosítani.

Rejtjeltevékenységre vonatkozó fizikai biztonsági feltételek:

A rejtjeltevékenységhez szükséges helyiség kialakításánál is figyelembe kell venni azt a szempontot, hogy csak olyan személy férhessen hozzá a rejtjelanyagokhoz, akiknek a munkaköre ellátásához ez feltétlenül szükséges és megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkezik. Csak a Nemzeti

Biztonsági Felügyelet által kiadott rendszerengedélyben meghatározott módon telepíthető a rejtjelző eszköz, bármilyen nemű változtatást az Nemzeti Biztonsági Felügyeletnél kell engedélyeztetni. Ha a módosítás olyan mértékű és az eszköz biztonsága megköveteli, akkor új rendszerengedélyt kell kérni.

Személyi biztonság

A fizikai biztonsági feltételek megteremtése mellett kiemelt fontossággal kell kezelni a humán tényezőt is. Nem véletlen a mondás, hogy a legtöbb hiba a szék és a billentyűzet között található, vagyis az egyik legnagyobb hibaforrás maga az ember. Ennek megfelelően már a beosztásba helyezés előtt meg kell kezdődnie a teljes életciklust átfogó személyi alkalmassági ellenőrzéseknek. Hiszen a minősített adatot kezelő szervezetek számára nyilvánvaló követelmény, hogy a foglalkozatott személyek ne jelentsenek támadási felületet. A munkakör betöltése a jogszabályban meghatározott személyügyi eljárás után lehetséges, melynek során lefolytatott vizsgálatoknak egyértelmű képet kell kirajzolni a jelentkező alkalmasságáról vagy épp ennek ellenkezőjéről. Az eljárás végrehajtása alatt tiszteletben kell tartani a jelentkező személyiségi jogait. Csak olyan információk kérhetők be, amelyekhez a jelentkező írásban is hozzájárul. Fontos a beküldött adatok előírásoknak megfelelő tárolása, felhasználása, megsemmisítése.

A nemzetbiztonsági ellenőrzés megkezdésekor a minősített adatot kezelő szerv vezetője kitöltet egy kérdőívet, melyet írásbeli felkéréssel, indoklással együtt küld tovább a Nemzetbiztonsági Irodán keresztül a honvédelmi miniszternek, aki elrendeli a jogszabályokban meghatározott, kezelt adatok minősítési szintjének megfelelő ellenőrzési eljárás megkezdését. A Katonai Nemzetbiztonsági Szolgálat által kiadott szakvélemény eredménye alapján a jelentkezőnek kockázatmentesnek kell lennie, továbbá szükséges még a személyi biztonsági tanúsítvány, felhasználói engedély, titoktartási nyilatkozat megléte. A tanúsítványt nemzeti minősített adat esetén a szervezet biztonsági vezetője adja ki, míg NATO, EU minősített adatoknál a Nemzeti Biztonsági Felügyelet. A tanúsítvány mindkét esetben visszavonásra kerül, amennyiben a biztonsági feltételek megszűnnek.

Az alkalmasnak bizonyult személy számára a munkaköri leírásában, valamint a rendszer-specifikus dokumentumokban egyértelműen rögzíteni kell a feladat végrehajtásához szükséges követelményeket, felelősségeket, betartandó biztonsági rendszabályokat, jelentési kötelezettségeket, a követendő eljárásrendet, valamint a szabályok megsértésére kiróható szankciókat. A szervezet illetékes vezetője meghatározza a feladat ellátásához szükséges személyzet létszámát. Feladata, hogy az elektronikus adatkezelő rendszerekhez hozzáférési jogosultsággal rendelkező

felhasználók és üzemeltetők a minősített adatvédelem helyi működtetéséhez szükséges képzésen részt vegyenek, sikeres vizsgát tegyenek. A felelős az időszakos továbbképzések megismétléséért, hiszen sokszor előfordul, hogy egyes feladatok napi rutinná válnak, míg a többi ismeret idővel megkopik, pontatlan lesz, ami a bizalmas munkakört betöltő személyek számára nem megengedett. A rendszerhez tartozó speciális dokumentumok megismerése mindenki számára kötelező, a megismerés tényét aláírásukkal igazolniuk kell, továbbá írásban nyilatkoznak, hogy a leírtakat a későbbiek folyamán betartják. A nyilatkozatokat a szervezet biztonsági vezetője őrzi és nyilvántartja. A szervezet titkos ügykezelője naprakész nyilvántartást vezet a hozzáférési jogosultsággal rendelkező személyekről. A hozzáférések meghatározásánál ügyelni kell a „need-to-know" elv szigorú betartására. A személyi változások alkalmával ügyelni kell arra, hogy a hozzáférési jogosultságok, kapcsolódó adminisztráció mindig naprakészek legyenek.

Rejtjeltevékenységre vonatkozó személyi biztonsági feltételek:

Ha a szervezet rejtjeltevékenységet is folytat, akkor az ezen feladatot végrehajtó állománynak rendelkeznie kell rejtjel-hozzáférési engedéllyel. Az engedély kiadására jogosult vezető feltünteti azon tárgyköröket, rejtjelanyagokat, amelyekre az engedély vonatkozik, amely információ birtoklására a munkavégzőknek szükségük van.

A kezelői engedély kiadásának feltétele a konkrét rejtjelző eszközre vonatkozó kezelői tanfolyam gyakorlati anyagából tett sikeres vizsga. Ha az illetékes személy más-más típusú eszközöket kíván üzemeltetni, akkor minden típusra meg kell szereznie az engedélyt. Az eszközök kezelői szintű karbantartása ezzel az engedéllyel végrehajtható, de a komolyabb beavatkozást igénylő javításokat nem lehet elvégezni.

Adminisztratív biztonság

Az adminisztratív biztonság célja, hogy valamennyi dokumentum a minősítési szintjének, érzékenységének megfelelő védelmet kapjon. Ezzel garantálva a dokumentumok kezelése során az információ nyomon követhetőségének, bizalmasságának, sérthetetlenségének megőrzését. Továbbá biztosítja, hogy azok illetéktelen személyek számára ne legyenek megismerhetőek, viszont a megismerésre jogosultak részére rendelkezésre álljanak. Fontos, hogy a védelem az anyagok létrehozásától kezdve a teljes életciklus alatt a követelményeknek megfelelően legyen kialakítva. Dokumentum szó alatt nem csak a papír alapú

anyagokat értjük, ide tartozik valamennyi elektronikus adathordozó is, ezáltal ez a terület szorosan kapcsolódik az elektronikus információ biztonsághoz. Az adathordozók tekintetében az általános rendszabályok mellett figyelembe kell venni, az általuk megkövetelt speciális kezelési szabályokat, érdemes a felhasználókat az eszközhöz csatolt használati utasításokkal ellátni.

A nemzeti jogszabályok a minősített adatok tekintetében nyilvántartási kötelezettséget írnak elő. A megfelelően kialakított nyilvántartási rendszer lehetővé teszi az adatok ellenőrzését, nyomon követhetőségét. Az ezzel kapcsolatos feladatokat a szervezetnél kialakított Nyilvántartó, valamint az alárendeltségében létrehozható Kezelő pont látja el. A nyilvántartás az adathordozókon tárolt legnagyobb minősítéssel rendelkező adat minősítési szintjének megfelelően történik.

Az iratkezelés főbb okmányai a fő nyilvántartó könyv, az iktatókönyv, az iktatólap és az egyéb alapnyilvántartások. A főnyilvántartó könyvben kerülnek iktatásra az adott szervnél vezetett alapnyilvántartások és iratkezelési segédletek. Az alapnyilvántartások rendszerébe tartoznak azok az iratok, melyeket helyben készítettek vagy az adott katonai szervezethez érkeztek, ezen iratkezelési okmányok iktatása nyilvántartási számmal történik. Az iratkezelési segédleteknek nevezzük azokat a kezelési okmányokat, melyek biztosítják az iratkezelés rendjét, továbbá elősegítik az ügykezelést. Ezek nyilvántartási számként a fő nyilvántartó könyv sorszámát kapják. Az iktatókönyvben kell nyilvántartani a szervezethez érkezett, vagy ott keletkezett iratokat és gyűjtőíveket. Az iratok (gyűjtők) az iktatókönyv évente újra kezdett sorszámát kapják, az évszám egyidejű feltüntetésével. Az iktatólapokon (gyűjtőíveken) kerülnek nyilvántartásra az azonos ügyben folyamatosan keletkezett, rendszeresen készített és érkezett iratok. Gyűjtőívben kell kezelni a titokvédelmi vagy ügyintézési érdekből egy adott ügyre vonatkozó minősítési jelöléssel ellátott nyílt iratokat. Az egyéb, sajátos rendeltetésű vagy formájú iratok egyéb alapnyilvántartásban rögzítettek.

Amennyiben egy szervezet NATO minősített információkat is kezelni kíván, úgy köteles egy NATO nyilvántartót kialakítani. Ebben az esetben a szervezet biztonsági vezetője írásban fordul a Nemzeti Biztonsági Felügyelet felé, aki a helyszíni szemrevételezést követően meghatározza a szükséges követelményeket, melyek alapján megkezdődhet a Nyilvántartó kialakítása. A Nyilvántartó Feldolgozó és Tároló helyiségből áll, melyek egymással szomszédosak. A Feldolgozó helyiség egy vagy több helyiség, iroda, épület; a Tároló helyiség egy vagy több helyiségből áll. Ezek kialakítására a nemzeti jogszabályokkal szemben, a NATO, EU minősített adatok kezelésére vonatkozó jogszabályokból pontos paramétereket kapunk minden biztonsági elemre vonatkozóan.

A szervezet által kezelt nemzeti és NATO, EU minősített adatok tárolása elkülönített iratkezelési segédletben történik. Ha az adatfeldolgozás során külföldi- és nemzeti minősített adatot közösen kell felhasználnunk, úgy a külföldi minősített adatok számára fenntartott segédletet kell alkalmazni.

Rejtjeltevékenységre vonatkozó adminisztratív biztonsági feltételek:

Ha a szervezet rejtjeltevékenységet is folytat, a rejtjelanyagokat és az ehhez kapcsolódó rejtjelügyvitelt és rejtjelanyag-nyilvántartást elkülönítve kell vezetni. A tevékenységre vonatkozó pontos utasításokat a rejtjelszabályzatban vagy rejtjelbiztonsági dokumentációban kell rögzíteni. A dokumentációt a rejtjelző alaptanfolyam sikeres elvégzése után lehet kezelni.

Elektronikus biztonság

Elektronikus biztonság alatt a híradó-, informatikai, egyéb elektronikai rendszerek és azok támogató infrastruktúrájának védelmére alkalmazott biztonsági rendszabályok összességét értjük. Védelmet nyújtanak a véletlen és szándékos kompromittálódások ellen a rendszer teljes életciklusa alatt az adat készítésétől egészen a megsemmisítésig. A rendszerek telepítésekor figyelembe kell venni a lehetséges bővítéseket, mivel ez az a terület, ahol az alkalmazott technika a legtöbbet változik, fejlődik az évek során. A hadműveleti követelmények meghatározása után, még a kialakítás előtt

Célszerű pontosan meghatározni az informatikusok számára az elvárt hadműveleti követelményeket, milyen belső kommunikációt szeretnénk, lesz-e külső kapcsolat, információcsere, hogyan képzeljük a hálózat összekapcsolását, majd rájuk bízni a technikai megvalósítást. Kialakítás előtt végre kell hajtani a kockázatelemzést, majd ezt követően a kockázatmenedzsmentet.

A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló kormányrendelet az elektronikus biztonság tekintetében az alábbi területeket különbözteti meg:

- Rendszerbiztonság:
  - hardverbiztonság
  - szoftverbiztonság
  - hozzáférési jogosultságok
  - biztonsági mentés, helyreállítás

- vírusvédelem
- hálózatok biztonsága

➢ Rejtjelbiztonság
➢ Átvitelbiztonság

Rendszerbiztonság

Hardverbiztonság

A rendszer hardverelemeinek kialakításakor is garantálni kell, hogy a rendszerhez csak az arra jogosult személyek férjenek hozzá. Elsődlegesen fel kell címkézni a használt eszközöket, hogy mindenki számára világos legyen, hogy az eszközön milyen minősítési szintű adatokat kezelünk. A rendszerhez való jogosulatlan csatlakozás megakadályozása érdekében a gondoskodni kell a hardverelemek megbontás elleni védelméről, portok letiltásáról stb. Az eszközök esetleges meghibásodása vagy időszakos karbantartása céljából is csak a biztonsági dokumentációban megnevezett állomány bonthatja meg a védőcímkéket. Csak az hajthatja végre karbantartási feladatokat, aki rendelkezik a kezelt adatok minősítési szintjéhez előírt személyi biztonsági tanúsítvánnyal, valamint a rendszerbiztonsági felügyelet engedélyével. A címkék sérülése, véletlenszerű szakadása azonnali jelentésre kötelezett esemény. Az eset kivizsgálásáért és a biztonság helyreállításáért ugyancsak a rendszerbiztonsági felügyelet a felelős.

Szoftverbiztonság

A hardverelemeken túl az eszközökön alkalmazott szoftverek esetén is igazodni kell az előírásokhoz. A telepítésre szánt szoftverek biztonsági ellenőrzését a rendszerbiztonsági felügyelet végzi, vagy amennyiben ők engedélyt adnak rá, úgy az illetékes rendszeradminisztrátor. Az ellenőrzést, majd a telepítést követően a rendszeradminisztrátor beállítja az NBF által jóváhagyott biztonsági konfigurációt. A konfiguráció egyik legfontosabb eleme, a naplózás beállítása. Ha valamilyen biztonsági incidens történik, akkor a naplózás lehetővé teszi, hogy a kivizsgálás során kiderüljön, hogy ki követett el, milyen hibát. A naplófájlokat az illetékes hatóság bizonyos időközönként ellenőrzi, a végrehajtásról dokumentációt készít.

Hozzáférési jogosultságok

A már kialakított rendszerben a következő lépés a hozzáférési jogosultságok meghatározása. Az NBF által jóváhagyott jelszóházirendben meghatározottak alapján minden felhasználó rendelkezik egy egyéni azonosítóval és az ehhez tartozó jelszóval, melyekről a rendszeradminisztrátor naprakész nyilvántartást vezet. A rendszerhez tartozó jelszavakat egy lezárt borítékban gyűjti össze, melyet a kezelt adatok minősítési szintjének megfelelő biztonsági körülmények között tárol. A belépési kísérleteket a biztonsági rendszer rögzíti, a sikertelen és a jogosulatlan próbálkozásokat ellenőrizni kell. Amennyiben a jelszavak és azonosítók illetéktelen megismerésének csak a gyanúja is felmerül, a biztonság megőrzése érdekében azonnal le kell cserélni.

Biztonsági mentés, helyreállítás

Bármikor előfordulhatnak előre nem látható események, mint például, hogy a rendszer összeomlik vagy egy esetleges természeti katasztrófa következik be stb. Az ilyen esetekben felmerülő kár mértékének csökkentésére a biztonsági dokumentumokban meghatározott időszakonként másolatokat kell készíteni. A másolatokat az eredeti dokumentumoktól elkülönítve, a rendszeren kezelt legmagasabb minősítési szinttel rendelkező adat biztonsági követelményeinek megfelelően kell tárolni.

Vírusvédelem

A mai világban egyre többet lehet hallani különbféle elektronikus támadásokról, így egyre nagyobb jelentőséget kell fordítani a rosszindulatú kódok elleni védelem kialakítására. Ezért elengedhetetlen a megfelelő biztonságot biztosító vírusirtó szoftver alkalmazása, melyek automatikusan lefuttatják az ellenőrzéseket minden bekapcsoláskor, valamint külső adathordozó csatlakoztatása esetén.

Hálózatbiztonság

A hálózatbiztonságon különböző minősítési szintű rendszerek biztonságos összekapcsolását értjük, mellyel azt kívánjuk elkerülni, hogy a magasabb minősítési szinttel rendelkező hálózatban található információkhoz ne férjenek hozzá az

alacsonyabb minősítéssel rendelkező hálózatok felhasználói. A hálózatok összekapcsolásához az NBF engedélyének beszerzése szükséges.

Rejtjelbiztonság

„A rejtjelzés: minden olyan tevékenység, eljárás, amelynek során valamely minősített adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon és ennek következtében a minősített adat minősítés nélküliként kezelhető legyen, valamint a rejtjelzett adat eredeti állapotba történő visszaállítása.” [3]

A nemzeti, NATO, EU követelmények alapján rejtjelzést kell alkalmazni minden olyan esetben, ha a minősített adat elektronikus tárolása másképp nem megoldható, továbbá ha az adatok átvitele során az információ átlépi a védett terület határait.

Átvitelbiztonság

Az átvitelbiztonságnál alkalmazott rendszabályok megakadályozzák, hogy a továbbított adatok és vezérlőjelek módosítására, törlésére, az átviteli csatorna átirányítására irányuló támadások meghiúsuljanak, továbbá védelmet képeznek a teljes átvitel úton. A „Bizalmas” vagy annál magasabb minősítési szintű adatok bizalmasságának védelme érdekében a biztonsági intézkedések kialakításánál eleget kell tenni a TEMPEST követelményeknek. Ez azért lényeges, mert az általunk használt valamennyi elektronikai eszköz, berendezés másodlagos sugárzása következtében létrejövő nem szándékos, sugárzott, vezetett elektromágneses energia elemzése lehetővé teszi az információhoz való illetéktelen hozzáférést. A kompromittáló kisugárzás elleni védelem kialakításakor ezt szeretnénk megakadályozni különböző aktív és passzív rendszabályok bevezetésével. A védelem körébe nem csak a végberendezéseket kell bevenni, ide tartozik valamennyi rendszerben alkalmazott eszköz is. Az üzemeltetési környezet valamint a használt eszközök speciális kialakítása mellett második lehetőségként felmerül a biztonságos távolságok felmérése, ugyanis a kibocsátott energia egy bizonyos távolságon kívül már érdemlegesen nem bemérhető.

A NATO-ban használt csoportosítás ettől eltérő, de lényeget ugyanúgy lefedi: a számítógép és hálózat; TEMPEST; rejtjelzés; átviteli utak védelme; hálózatok biztonságos összekapcsolása. [4]

Összegzés

A leírtak alapján megfigyelhetjük, hogy a rendszerek, helyszínek biztosításakor nem mindig tudjuk élesen elkülöníteni a fizikai, személyi, elektronikus, valamint adminisztratív biztonsági kérdéseket. Minden egyes terület igen fontos részterülete az információbiztonság kialakításának. Ezek komplex, egymással pontosan összehangolt, koordinált alkalmazása révén érhetjük el a minimális kockázat szintjét, csökkenteni tudjuk a különböző támadások hatásait. Természetesen a környezet nagyban befolyásolja a védelem kialakítását. Például, tábori körülmények között, ahol nincs lehetőségünk az előírt fizikai infrastruktúra biztosítására, ilyen esetben át kell konfigurálni a kapcsolódó rendszabályokat úgy más módon, akár 24 órás felügyelettel, kell az adatok és adatkezelő rendszerek védelmét biztosítani.

Amennyiben valamennyi területen megvalósul a jogszabályban előírtak kialakítása, az ügyfél kéri a Nemzeti Biztonsági Felügyelettől a „Bizalmas!” vagy annál magasabb minősítési szintű minősített adat kezelésére vonatkozó engedély kiadását.

Felhasznált irodalom

[1] A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. korm. rendelet
[2] Tóth András, Jéri Tamás, Pándi Erik: A kommunikációs infrastruktúrákkal szembeni rosszakaratú tevékenységek, Hírvillám = Signal Badge 1:(1) pp. 276-288. (2010)
[3] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. korm. rendelet
[4] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (2015. 12.11)
[5] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi Szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal, HU ISSN 2060-0437)
[6] Dr. Négyesi Imre: COTS rendszerek alkalmazási lehetőségeinek vizsgálata (Hadtudományi szemle on-line, IV. évfolyam (2011) 4. szám, 111-116. oldal, HU ISSN 2060-0437)
[7] Dr. Négyesi Imre: DIE ÜBERPRÜFUNG DER VORAUSSETZUNGEN VON COTS SYSTEMEN (COTS RENDSZEREK KÖVETELMÉNYEINEK VIZSGÁLATA) (Hadmérnök on-line, VII. évfolyam (2012) 2. szám, 371-376. oldal, ISSN 1788-1919).

SZABÓ Anna Barbara: A minősített adatok védelemének elvi megközelítése

Absztrakt

A technika fejlődésével az államok működésük során egyre nagyobb információéhséggel bírnak, ugyanakkor rendkívüli teljesítménnyel létre is hozzák. Az információhoz történő gyors hozzáférés és az azzal való gazdálkodás lett a társadalmak mozgatója, az előny, vagy hatalomszerzés kulcsa és a biztonságuk záloga. Az állami és az állami érdekeltségű szervek kapcsolatai sokrétűbbek, intenzívebbek, lényegesen nagyobb adatvagyonnal rendelkeznek, ami a sérülékenységüket is fokozza. A korábbi társadalmi struktúrákhoz képest jobban függenek egymástól és rendelkezésre álló adatvagyontól. A változások eredményeként az adat és információ keletkezése, feldolgozása, továbbítása, tárolása, archiválása és megsemmisítése is részben, vagy teljes egészében a digitalizált környezetben történik, aminek eredményeként újfajta kihívásokra, igényekre és sebezhetőségekre kell felkészülni.
A tanulmány első felében ismertetni fogom a nemzeti adatvagyont, azon belül a minősített adatot és második felében egy a biztonságát célzó elvi követelményrendszert fogok felállítani. A kapott elvi követelményrendszer hiánypótló jelleggel képes passzív adathordozó esetében biztosítani a minősített adat megfelelő szintű védelmét.

Abstract

With the continuous development of the modern society, states need more data while they also tend to produce even more. Quick access to information is a key indicator of how well a society will react to modern challenges, will gain or lose power, opportunities. Relation between the state, its parts and departments is getting more complex, intense, and produces significantly more data asset. This deepens its vulnerability. Compared to the previous social systems, their modern counterparts are more dependent on each-other, and the data asset. Creation, manipulation, transfer, store, archive or creation of data and information, due to these developments, are mostly happen in the virtual environments. This creates new challenges, vulnerabilities and demands that have to be met.
The paper is organized as follows: the first half presents the national asset, more specifically the classified information, in the second half a set of theoretical

requirements will be given that aims to provide protection to it. This specification, as a suplement, is able to provide the needed security in case of confidential information stored on passive equipments.

Kulcsszavak: *adat, informatika, információ, követelményrendszer, nemzeti adatvagyon, védelem, data, informatics, information, national data asset, protection, requirement*

Bevezetés

A tanulmány célja ismertetni a nemzeti adatvagyont, mint csoportot és annak elemeit, valamint az információ védelmi követelményeket ISO szabvány, nemzeti jogszabály, valamint NATO követelményrendszer felhasználásával.

A fentiek ismeretében egy a nemzeti adatvagyon, azon belül a minősített adat biztonságát célzó elvi informatikai alapuló követelményrendszert fogok felállítani.

Nemzeti adatvagyon

Napjaink tudás alapú társadalmában az információ fokozott értéket képvisel, melynek hordozója az adat. Az MSZ ISO/IEC 27001:2014 szabvány szerint az információ annyi, mint értelemmel bíró adat. [1]

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint az adat:

"az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas". [2]

Bizonyos adatok nem megfelelő kezelése, vagy kontextusba helyezése, vagy annak jogosulatlan félhez való jutása, megismerésére súlyos gazdasági és társadalmi következményekkel járhat, ez különösen igaz a minősített adatokra.

A minősített adatok értelmezéséhez célszerű a nemzeti adatvagyont és annak az összes elemét meghatározni.

Az országok működésének meghatározó eleme a nemzeti adatvagyon. A nemzeti adatvagyon egy rendkívül heterogén csoport, mely fogalma alá tartoznak a

közfeladatot ellátó szervek által kezelt a személyes adatok, közérdekű adatok, és a közérdekből nyilvános adatok.

Személyes adat: az érintettel kapcsolatba hozható adat és az abból megállapítható, érintettre vonatkozó következtetés. Így különösen az érintett neve, azonosító jele, valamint a fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret. Dr. Péterfalvi Attila korábbi országgyűlési biztos hivatalból hozott állásfoglalása alapján interneten a felhasználói név is lehet személyes adat, amennyiben a felhasználónév mögött álló személy beazonosítható, és annak az interneten olvashatóak bizonyos adatok, melyek az érintettel kapcsolatba hozhatók, akkor ezek az egyén személyes adatainak minősülnek. [3], [4]

Különleges adat: olyan személyes adatok melyek faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre, egészségi állapotra, a kóros szenvedélyre vonatkoznak, valamint a bűnügyi személyes adat. [5]

Bűnügyi személyes adat: olyan személyes adat, mely a büntetőeljárás során, vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozik. [5]

Közérdekű adatok: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett információk, vagy ismeretek, a személyes adatok kivételével. Viszont független a rögzítés formájától, a kezelés módjától, önálló vagy gyűjteményes jellegétől. A fentiek alapján közérdekű adat a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre és annak az eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adatok. [5]

Külön kategóriának minősül a közérdekből nyilvános adat.

Közérdekből nyilvános adat: ami, minden olyan, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét közérdekből törvény rendeli el, ugyanakkor alapesetben nem tartozik közérdekű adatok körébe. Megismerésére minden polgár szóban, írásban vagy elektronikus úton igényt nyújthat be. Pl.: kötelezően igénybe veendő szolgáltatások, helyi önkormányzati képviselő tisztelet díja. [5]

Azokat a közérdekeket, melyek fokozott védelembe részesülnek minősített adatoknak tekintjük. A magyar jogrendszer kettőt különböztet meg: nemzeti minősített adatot és a külföldi minősített adatot.

Nemzeti minősített adat: *„a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.”* [6]

Külföldi minősített adat: *”az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.”* [7]

A két főcsoporton belül kármérték alapú minősítés szerint az adat "Szigorúan titkos", "Titkos", "Bizalmas" és "Korlátozott terjesztésű" lehet.

A minősítési kategóriák alkalmazása:

"Szigorúan titkos" minősítés által maximum 30 évig védhető a közérdek, amennyiben rendkívül súlyosan sérti jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé tétele, viszont az arra jogosult számára a hozzáférhetetlenné válása is.

"Titkos" minősítéssel maximum 30 évig azon közérdek védhető, mely jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé tétele, viszont az arra jogosult számára hozzáférhetetlenné válása azt súlyosan károsítja.

"Bizalmas" minősítéssel maximum 20 évig védhető közérdek, melynek jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé tétele, viszont az arra jogosult számára hozzáférhetetlenné válása azt károsítja.

"Korlátozott terjesztésű" minősítés a legenyhébb kategória, maximum 10 évre adható, amennyiben a védhető közérdek jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé tétele, viszont az arra jogosult számára hozzáférhetetlenné válása azt hátrányosan érinti.

A "Szigorúan titkos" és "Titkos" minősítésű adat rendkívül indokolt esetben minősítési idejük alatt új minősítési eljárással egy alkalommal ismét maximum 30 évre hosszabbíthatóak. Ugyanezen követelmények mellett a "Bizalmas" és a "Korlátozott terjesztésű" adat egy alkalommal 5 évre hosszabbítható. Kivéve, ha Magyarország – magánszemély jogos érdekével szorosan összefüggő – honvédelmi, nemzetbiztonsági, bűnüldözési vagy igazságszolgáltatási érdeke miatt két alkalommal, legfeljebb 20 évre meghosszabbítható. [8]

A Nemzeti Biztonsági Felügyelet feladata a minősített adat védelmének hatósági felügyelete, valamint a minősített adatok kezelésének hatósági engedélyezése és annak felügyelete. [9]

A nemzeti adatvagyon védelme érdekében rendkívül fontos a megfelelő információ védelem, ezért a következő fejezetben annak jogi és egyéb normák szerinti megoldásait fogom ismertetni.

Az információ védelme

Az országok társadalmi, gazdasági működésének szegmensei elképzelhetetlenek informatikai rendszerek nélkül. Ezen belül kiemelkedő fontosságú a köz-és az államigazgatás működését támogató szektor, így a minősített adatok keletkezése és kezelése se nélkülözheti az informatikai eszközök igénybevételét.

Az információkkal kapcsolatos általános követelmény:

- Bizalmasság elve: az információt csak az arra felhatalmazottak ismerhetik meg, valamint a jogosultsági kör és a jogosultság szintek meghatározása.
- Sérthetetlenség elve: az információ teljességének és pontosságának megtartása, állapotának biztosítása, az adat tartalmának és tulajdonságainak az elvárttal egyezése. Idetartozik az információ hitelessége, a letagadhatatlansága, valamint az elektronikus információs rendszerelemek rendeltetésüknek megfelelő használhatósága.

- Rendelkezésre állás elve: a jogosultak akkor férjenek hozzá az információhoz, mikor az szükséges. [10]

A minősített adatok védelméről szóló törvény a fentieken túl kiegészül az alábbi elvekkel:

- Szükségesség és arányosság elve: a közérdekű adat nyilvánosságát minősítéssel korlátozni csak minősített adatok védelméről szóló törvényben meghatározott feltételek mellett lehet, a védelemhez szükséges minősítési szintet alkalmazva, a feltétlenül szükséges ideig.
- Szükséges ismeret elve: csak az ismerheti meg a minősített adatot, akinek feltétlenül nélkülözhetetlen az állami- vagy közfeladata ellátásához. [11]

A fent ismertetett jogi előírásokon túl új elemként jelent meg, mint NATO norma az elszámoltatás elve:

- Elszámoltatás elve: az adat birtokosa felelős a nyilvántartásba vételért és az utasítások betartásáért. [12]

Az információ védelem magába foglalja a teljes életciklusában az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, komplex, folytonos és kockázatokkal arányos védelmét. Minősített adatok nyomon követhetőségéről, bizalmasságáról, sérthetetlenségéről, rendelkezésre állásáról a törvény szerint adminisztratív biztonsági intézkedésekkel kell gondoskodni.

Az információbiztonság egy rendkívül összetett terület, legalapvetőbben az információ-vagyon védelmét az információhordozó kezelésének védelmével lehet szabályozni. Az informatikai rendszereknél szakirodalom megkülönbözteti a fizikai és az operatív védelmet.

Fizikai védelemhez tartozik a környezet megfelelősége, amit minősített adatok esetében a Nemzeti Biztonsági Felügyelet hagy jóvá és ellenőriz.

Operatív védelem az információtechnológia használatának a szabályozása, mint az naplózások, vírus irtás és vírus definíciós adatbázis naprakészen tartása. A munkavégzésnek és a felhasználóknak szabályozása. [10] Minősített adatot főszabály szerint csak olyan személy használhat fel, akinek az állami, vagy közfeladat ellátása érdekében indokolt, rendelkezik megfelelő szintű személyi

biztonsági tanúsítvánnyal, titoktartási nyilatkozattal és felhasználói engedéllyel. A felhasználói engedélyben kerül meghatározásra, hogy a rendelkezési jogosultságok közül, melyekre jogosult a felhasználó. Amennyiben más minősítő által minősített adathoz szeretne hozzáférni Az alábbi rendelkezési jogosultságok lehetnek:

„a) állami vagy közfeladat végrehajtása érdekében történő ügyintézés, feldolgozás,
b) minősített adat nyilvántartásával kapcsolatos valamennyi tevékenység,
c) minősített adat birtokban tartása,
d) minősítési jelölés megismétlése, illetve a megismétlés megtiltása,
e) minősített adat másolása, sokszorosítása,
f) minősített adat fordítása,
g) kivonat készítése,
h) szerven belüli átadás,
i) szerven kívülre továbbítás, szállítás,
j) selejtezés, illetve megsemmisítés,
k) felhasználói engedély kiadása,” [13]

A minősítőnek az általa minősített adathoz a rendelkezési jogosultsága komplex, így a fentiek kiegészülnek az alábbiakkal:

„nemzeti minősített adat felülvizsgálatával, minősített adat külföldi személy vagy külföldi szerv részére hozzáférhetővé tételének engedélyezésével, minősített adat külföldre vitelének vagy külföldről való behozatalának engedélyezésével, titoktartási kötelezettség alóli felmentéssel.” [13]

A fent ismertettek alapján a következő fejezetben egy specifikációt fogok megfogalmazni az elektronikus adathordozón tárolt minősített adatok védelmére.

Elvi követelményrendszer a minősített adat védelmére: a passzív adathordozó aktívvá tételével

Manapság a megnövekedett adatmennyiség miatt elkerülhetetlen az adatok elektronikus adathordozón való tárolása, mely legelterjedtebb módja a pendrive. A fejezetben javasolt módszer minden többszöri írást támogató eszközre alkalmazható minimális változtatásokkal.

A törvény előírja, hogy elektronikus biztonsági intézkedések meghozatalát az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében.

Tekintve, hogy az adathordozók passzív eszközök, így a minősített adathoz való hozzáférés ténye naplózás külön az adattól elválasztható módon kerül dokumentálásra. Célom egy szoftver-hardver rendszere vonatkozó követelményrendszer elkészítése, mely megoldaná, hogy az elektronikusan kezelt minősített adat adattárolóján elválaszthatatlanul jelenjen meg minden felhasználói cselekvés.

Kiindulás:

A pendrive, mint hordozó egy passzív eszköz nem rendelkezik olyan számítási képességgel, mely a bejövő adatotokat, adatmozgásokat értelmezné, kiírná, naplózná. Ezt a felhasználói eszközből kerül kikényszerítésre, nem elég részletes, szabotálható.

Informatikailag már külön-külön megoldott a rendszer naplózása, a cserélhető meghajtó operációs rendszerbe való beépülése és a titkosítás is.

Cél:

A cél ezt egy zárt komplex, a minősített adattól elidegeníthetetlen környezetbe való helyezése. Célszerű a problémát a szubszidiaritás elve szerint megoldani. Ki kell dolgozni, hogy a cserélhető meghajtó és a dokumentum olvasó kölcsönös megbízhatósági rendszerben legyen.

Az elvi specifikáció levezetése

Dokumentum védelem “szintjei”:

- Megjelenítő alkalmazás kér jelszót, maga a dokumentum nem titkosított
- Dokumentum védett és megjelenítéséhez jelszó kell, de a jelszó nem tartalmaz kulcsot (pl.: irodai környezetben felhasznált Microsoft Office termékek)
- Dokumentum jelszóval védett, ami egy úttal a kulcsa is (nyilvános kulcsú titkosítás)
- A dokumentum elérése már maga is védett, jogosultsághoz kötött

Dokumentum elérés védelem módozatai:

1. Dokumentum fizikailag védett, hozzáférés személyhez kötött jogosultság ellenőrzésével történik, pl.: kulcsfelvétel, belépőkártya stb.
2. Dokumentum megszerzése és kezelése is limitált, eszközhöz vagy helyhez kötött, de ott bármi engedélyezett, pl.: belépés token használatával stb.
3. Dokumentum megszerzése, módosítása limitált és naplózott, a jogosultság helyhez kötött

Cél a 3. megvalósítása, a rendelkezésre álló eszközök mind jobb kihasználásával és a visszafelé kompatibilitás biztosításával.

Feltevések

- A dokumentumot elégséges az ismert gépekről megnyithatóvá és módosíthatóvá tenni, de minden módosítást naplózásra kell, hogy kerüljön.
- Külső gépek esetén szükséges lehet az olvasás biztosítása, de az írásé és a módosításé nem.
- A dokumentumok a gépek között szilárd hordozókon kerülnek át vagy zárt hálózaton.
- Rendellenesség észlelése esetén a további hozzáférés azonnal letilt.

Feltevések magyarázata

- Naplózás szükséges, hogy a korábbi állapotok visszaállíthatók legyen, a nyomon követhetőség és elszámoltathatóság elve megvalósuljon, azaz a büntetőjogi felelősség követhető legyen.
- Más szállítási módok esetén fellépő jogtalan hozzáférés esélyének kiszűrése
- Informatikai vészhelyzet esetén szükséges az olvasás biztosítása
- Külső eszköznél a felhasználó autentikáció jól megoldható, ellenben a

környezet és a használt eszköz nem kontrollálható.

A megvalósításához szükséges eszközök, lépések

- Felhasználó azonosítás és jogosultság ellenőrzése (pl.: LDAP). [14]
- Megnyitásra használt eszköz azonosítása (pl.: LDAP).
- Hordozó eszközök védelme erős titkosítással, ideértve a szoftver és hardver eszközöket is.
- Fájlok, mappák titkosítása titkosítással: modern fájlrendszerek támogatják az egyes fájlok titkosítását (pl.: NTSF)
- Hozzáféréshez szükséges program, programok telepítésének biztosítása külső eszközöknél.
- Az hordozó eszköz 'láthatóságának' módosítása a felhasználó és a környezet függvényében (pl.: LDAP, vagy annak lokális helyettesítése)

A hordozón tárolandó adatot, ide értve a teljes adat struktúrát is nyilvános kulcs alapú, erős titkosítással kell ellátni. A titkos kulcs megszerzése nélkül az adat nem hozzáférhető. Ha az eszközt saját hálózaton lévő géphez csatlakoztatják, úgy ott lehetőség van a központi kulcskezelővel, kulcsmenedzserrel való kommunikációra. Ezen kommunikáció során a kulcskezelő a gépet aktuálisan használó felhasználó jogosultságai alapján tudja az illesztő programot tájékoztatni arról, hogy mit láthat a felhasználó az adott állomány halmazról, illetve adja meg a szükséges kulcsokat. Külső gépes elérés esetén lehetőség van a titkos kulcs közvetlen bevitelére és így az állományok megszerzésére, írás azonban tiltott.

Az eszköz csatlakoztatásának lépései, folyamata

- Az eszköz csatlakoztatásakor saját illesztő program meglétének ellenőrzése és esetleges telepítése (ennek engedélyezésének hiányában az állomány nem lesz elérhető egyáltalán annak titkosítása miatt).
- Kommunikációs kísérlet a központi kulcs menedzserrel, illetve a gép konfiguráció ellenőrzése.
- Kulcs kérése a felhasználótól vagy a központi zármenedzsertől.

Állomány hozzáférés lépései

- Kapcsolat ellenőrzése a központi kulcs menedzserrel.
- Nincs kapcsolat, akkor visszalépés védett módba, de a hozzáférési kísérlet naplózása.
- Kapcsolat megléte esetén a pontos jogosultságok lekérése.
- Védett mód esetén az állomány megnyitásának engedélyezése, de a formátumon keresztül annak biztosítása, hogy csak korlátozott eszközökkel lehessen megnyitni.
- Ismert jogosultságok esetén annak megvizsgálása, hogy a felhasználónak van e joga az adott dokumentumhoz és ennek függvényében a szükséges adatok kiadása.

Eredmények összegzése

A fenti lépések külön-külön már megoldottak, felhasználók számára általánosan elérhető eszközökkel. Pl.: az ELDOS CallbackFilter terméke. Az ELDOS magában csak a fájlmódosítás naplózását biztosítja, hozzáférést szabályozza, de a hordozó eszköztől függetlenül telepítendő és csak a dokumentum olvashatósága esetén, annak másolását nem akadályozza meg. Ugyanakkor a fent ismertettek részleges kombinációja már felbukkan a használatban, de a teljes kombinált probléma megoldására specifikáció, vagy kész termék ellenben publikáció megíráskor nem volt ismert a felelhető szakirodalomban.

Konklúzió

Az államok működésében a nemzeti adatvagyon, azon belül a védendő közérdekek kiemelten nagy értékkel bír. Az adat megfelelő környezetben válik információvá. Az napjainkban a információ keletkezése, feldolgozása, továbbítása, tárolása, archiválása és megsemmisítése is részben, vagy teljes egészében informatikai technológiák bevonásával teljesül, ezért szükséges lenne a tanulmányban ismertetett bizalmasság, sérthetetlenség, rendelkezésre állás, szükségesség és arányosság, szükséges ismeret és elszámoltatás elvét informatikailag is garantálni. A tanulmány második felét képező elvi

követelményrendszer a fenti elvek betartására ügyelve képes passzív adathordozó esetében is biztosítani minősített adat megfelelő szintű védelmét.

Felhasznált irodalom

1. Magyar Szabványügyi Testület: Az információbiztonság irányítási rendszerének (ISMS) MSZ ISO/IEC 27001:2014 szerinti tanúsítása
2. Forrás: http://www.mszt.hu/web/guest/msz-iso-iec-27001 (2015.11.17.)
3. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. § (1) 1.
4. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.296212 (2015.11.17.)
5. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § 2.
6. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.296244 (2015.11.17.)
7. Az Adatvédelmi Biztos Állásfoglalásai Ügyszám: 1175/A/2006-3.
8. Forrás: http://abi.atlatszo.hu/index.php?menu=aktualis/allasfoglalasok/2006&dok=1175_A_2006-3, (2014.12.02.)
9. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § 3.
10. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.296244 (2015.11.17.)
11. A 2009. évi CLV. törvény a minősített adat védelméről 3.§ 1. a)
12. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.296205 (2015.11.17.)
13. A 2009. évi CLV. törvény a minősített adat védelméről 3.§ 1. b)
14. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.296205 (2015.11.17.)
15. A 2009. évi CLV. törvény a minősített adat védelméről 5.§
16. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.296205 (2015.11.17.)
17. A 2009. évi CLV. törvény a minősített adat védelméről 10.§
18. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.296205 (2015.11.17.)
19. Dr. Michelberger Pál- Lábodi Csaba: Vállalti információ biztonság szervezése = Vállalkozásfejlesztés a XXI. században II., szerk.: Nagy Imre Zoltán. Óbudai Egyetem, Budapest, 2012.
20. A 2009. évi CLV. törvény a minősített adat védelméről 2.§

21. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.296205 , 2015.11.17.
22. DOCUMENT C-M (2002) 49 SECURITY WITHIN THE NORTH ATLANTIC TREAN ORGANISATION (NATO); 2002. 06.17.
23. Forrás: http://www.freedominfo.org/documents/C-M(2002)49.pdf, 2014.02.10.
24. A 2009. évi CLV. törvény a minősített adat védelméről 18.§
25. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.296205 (2015.11.17.)
26. Papp Zoltán: LDAP-ról pár szóban Forrás: http://padre.web.elte.hu/ldap.html (2015.11.11.)

NAGY Balázs: Technikai hírszerzés helye, szerepe az információs fölény megszerzésében

Absztrakt

A generációk fejlődésével változnak a súlypontok az elérendő célokhoz vezető utak terén is. A régi formák új testet öltenek egy kézzel megfoghatatlan információs térben. Ahogy változik a környezet, úgy kell igazodnia az eljárásoknak is, hogy minél hatékonyabban sikerüljön kézhez keríteni a fölény kivívásához szükséges információkat. A jelen kor döntéshozóinak nincs egyszerű dolga, mivel a pozitívumot jelentő információmennyiség bővülését jelentő előnyök mellett szembe kell nézniük azok hátrányaival is úgy, mint a dezinformáció, információelárasztás, vagy annak a ténye, hogy a szemben álló fél is igen rövid idő alatt hozzá tud jutni értékes adatokhoz. Ennek következtében jelentős mértékben lerövidül a döntéshozás és akció ideje és igen felértékelődik a döntéshozók kezébe juttatott információ gyorsasága értéke és pontossága. Jelen publikáció az egyik hírszerzési ágat hivatott bemutatni és elhelyezni az információs műveletek rendszerében, felvillantva a többi területet is, hiszen ezek együttes alkalmazása adja a fölény sikeresebb kivívását. Ezen belül: bemutatja és értelmezi a generációs, új hullámú háborúkat; a vezetési fölényhez vezető utat, az adat- és információszerzés területeit; az információ felhasználásának és terjesztésének kulcselemeit; valamint a technikai hírszerzés jelentőségét és folyamatát.

Abstract

Due to the change of the old generations, the paths to the goals are changing too. The old shapes take on a new body in a virtual environment. As the environmant changes, so must we adopt the procedures to get the necessary infromation to gain spueriority. The decision makers of the present days do not have a plain thing, beside the benefits of the expansion of the information quantity, they have to face its disadvantages as well, for example the disinformation, information flooding, and the fact that the other party can achieve those information as fast as they can. Due to that the time of making a decision and taking an action strongly shortens and the importancy of the value, velocity and accuracy of the infromation allotted to the decisionmakers hands rises. The aim of the present publication is to represent an information gathering technique and to place it into the information operation system, showing the rest of the information gathering areas, since the common use of those areas led us to a more afficent superiority. As part of this: represents the

generation of the old and the new wave wars; the road leading to the leadership superiority; the areas of the data and information gathering areas; the key elements of the use of the information and its dissemination; and significance of the technical intelligence and its process.

Kulcsszavak: *technikai hírszerzés, információs fölény, információs műveletek, elemzés-értékelés, információ ~ technical intelligence, information superiority, infromation operations, analysis and valuation, information*

Bevezetés

A technikai hírszerzés területe mára nem csak a klasszikus értelemben vett hadviselésre használható fel, hanem a civil életben is egyre nagyobb teret nyer az alkalmazása, hiszen egyes vállalatok, melyek kontinenseket hidalhatnak át vagy egyes régiókat „uralnak", jelentősebb befolyással lehetnek adott ország stabilitására, valamint az országok közötti együttműködésre, mint a katonai erő maga. A hírszerzés fontosságára, vagy annak hiányosságaira könyörtelenül mutatattak rá a 2001 szeptemberében az Amerikai Egyesült Államokban történt terrortámadások. [1]

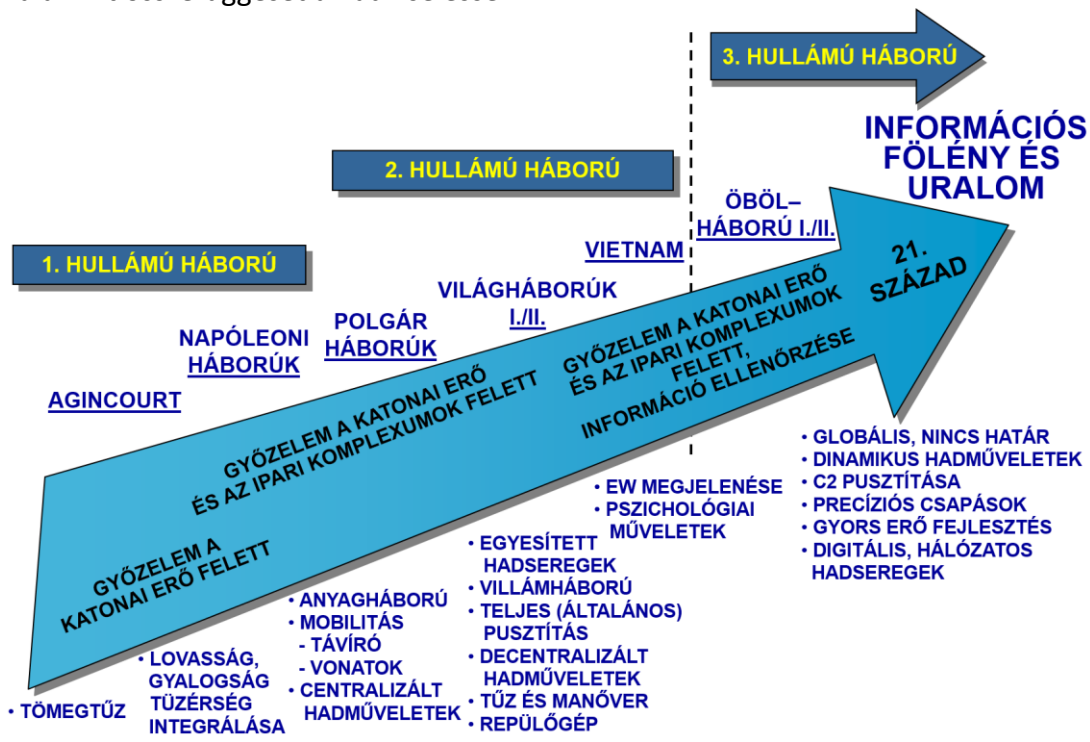
Ezért is esett egyrészről a választás az információszerzés ezen ágára, másrészről a technológiai fejlődés miatt, melynek köszönhetően információrobbanás következtében felszabadul adatmennyiség elemzése és értékelése nagyban megkönnyebbült és egy hatalmas terhet vett le az emberi feldolgozásról. A publikációban először a szélesebb kört értelmezve haladok a technológiai hírszerzés felé, elhelyezve azt az információs műveletek rendszerében. Kezdő lépésként az információs fölény fogalmi rendszerét vettem górcső alá.

Az információs fölény a rendelkezésre álló információs rendszerek és azok képességinek kihasználásával lehetővé váló, a társadalmi élet különböző területein történő előnyszerzés, valamint a kialakult helyzet olyan módon történő irányítása, mely során a szemben álló felet megfossza e képességtől. Ennek kivívását gyakran vezetési fölénynek is szokták tekinteni, ugyanis a hatékonyan felhasznált elemzett, értékelt információ, mint döntés előkészítő anyag elengedhetetlen eleme a kockázatok és veszteségek minimalizálásához, továbbá a sikeres műveleti végkimenetelhez.[1]

Az információs fölény volumene az egyes sikeresen megvívott hadműveletek következtében bővül, míg el nem éri azon a kiterjedését, ahol már információs uralomról beszélünk, melynek keretén belül a szemben álló felet teljes mértékben

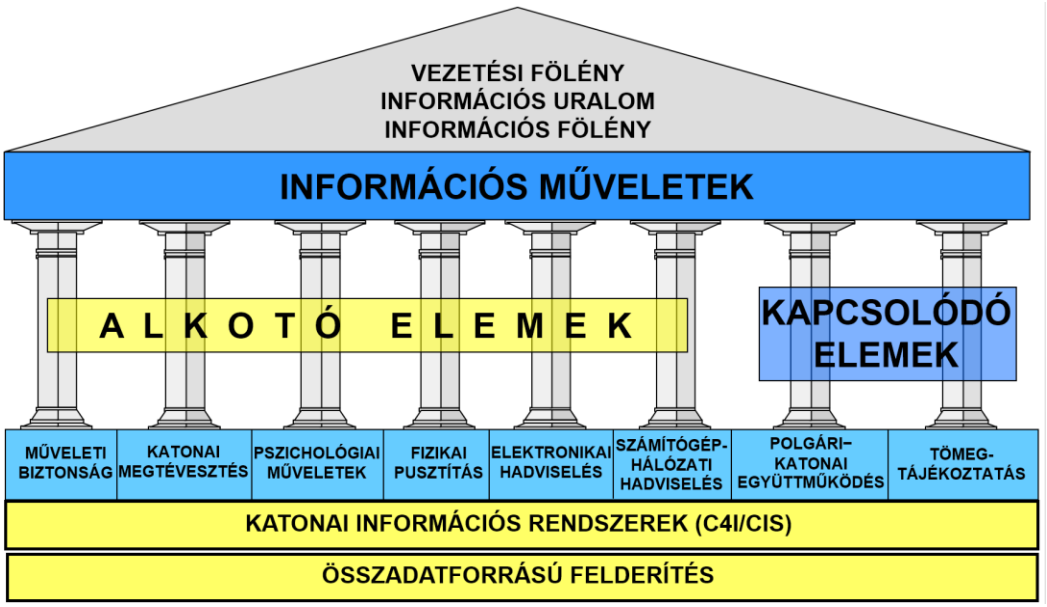
megfosztjuk az információ megszerzésének, továbbításának és feldolgozásának lehetőségétől.

Az elérni kívánt célok és szándékok állandósága mellett, a hadviselési módok változása az idő előrehaladtával gyökeres változásokon mentek keresztül. E változásokhoz nagyban hozzájárultak a technológiai fejlődések, melyek a hadviselésben megkövetelték a gyorsabb pontosabb információk rendelkezésre állását. Az alábbi ábra (1) ábra jól szemlélteti az alkalmazott technika fejlődését, valamint összefüggését a hadviseléssel:



1. ábra: hadviselési módok változása [2]

Az információs fölény kivívásában fontos szerepet játszik az információs műveletek alkotó- és kapcsolódó elemei, a vezetési információs rendszerek és az összadatforrású felderítések, melyek az információs műveletek támogató elemeit jelentik. Ezt az (2) ábra jól szemlélteti:



2. ábra: Az információs műveletek alapelemei [3]

Az információs műveletek alkotó- és kapcsolódó elemei tehát:

- Műveleti biztonság
- Katonai megtévesztés
- Pszichológiai műveletek
- Fizikai pusztítás
- Elektronikai hadviselés
- Számítógép-hálózati hadviselés
- Polgári-katonai együttműködés
- Tömegtájékoztatás

Az információs műveletekben szerepeltetett egyes elemek önállóan is működő tevékenységi körök, ám ezek együttes, összehangolt működése nagyságrendekkel növeli a műveleti hatékonyságot. Békeidőben jelentős megelőző hatással bír, mely hozzájárul az incidensek bekövetkezésének megelőzéséhez, azok felmerülésének előrejelzéséhez. Minősített időszakban pedig a műveleti területen tevékenykedő egységek biztonságát, a szemben álló fél zavarását, pusztítását, a helyi a lakosság megnyerését és végső soron a helyzet uralását szolgáltatott kivívni. Jelen publikációban a technikai hírszerzést, mint eszközt választottam az információs fölény megvívásában, melyet az információs műveletek alkotó elemei

közé sorolok. Véleményem szerint több elemet is érint úgy, mint műveleti biztonság, elektronikai hadviselés, számítógép-hálózati hadviselés. Műveleti biztonságot érinti mivel a megszerzett technológia és az abból fejtett információ nagyban hozzájárul katonáink, ügynökeink terepen végzett fedettségéhez és hatékony működéséhez. Érinti az elektronikai és a számítógép-hálózati hadviselést is, mivel a jelen kor hadviselése ebbe az irányba tolódik el és az információk megszerzése mára már fizikai jelenlét nélkül is bizonyos esetekben lehetséges.

Adat- és információszerzés módjai

Az adat- és információszerző képességek, lehetőségek függnek az adatszerzés jellegétől, módjától és eszközétől. Ezek alapján az adat- és információszerzés területei az alábbiak szerint csoportosítható:[4]

- *emberi erőforrásokkal folytatott információ és hírszerzés (HUMINT[1]);*

A legrégebbi adat- és információszerzési terület. Két részre tagozódik. Az első része a nyíltan és legálisan végzet adat- és információszerzés, melyet diplomáciai keretek között alapvetően diplomaták végeznek, amelyre legalizálást alapvetően az 1961-ben elfogadott diplomáciai kapcsolatokról szóló Bécsi Egyezmény adott. A másik részét a katonai missziók hír- és információszerző támogatását ellátó hírszerző elemekkel (a katonai hírszerzéshez tartozó NIC[2]; NIST[3]) folytatott hírszerzés alkotja. A katonai műveletek nyíltan végzett adat- és információszerzése mellett, gyakori az ügynöki, fedett hírszerzés. A nyílt diplomata és katonai adat- és információszerzése közös jellemzőjét, a tényleges hovatartozást, beosztást és részben a tevékenységet is nyíltan felvállaló, saját néven végzett információ- és hírszerzés adja.

E terület meghatározó jellemzője, hogy a hírszerzést a célterületen hajtják végre és az információforrások mindig személyek, illetve az információkhoz, dokumentumokhoz mindig személyeken keresztül jutnak hozzá. Előnye a többi adat- és információszerző móddal szemben, hogy olyan információkat is képes megszerezni, amelyeket a többi nem. További előnye, hogy lehetőség van a

[1] Human Intelligence

[2] National Intelligence Cell

[3] National Intelligence Support Team

visszacsatolásra, az információ forrás általi megerősítésére, pontosítására, vagy kiegészítésére. Hátránya lehet, a szándékos dezinformáció, pontatlan megjelölés, valamint az időtényező bővülése az információ feldolgozása és célba juttatása során.

- *rádióelektronikai felderítés (SIGINT[4]);*

Alapvetően hazai területen üzemeltetett passzív eszközök révén, szerzi meg az információt cél országban kibocsátott távközlési és más, elektromágneses hullámokat kibocsátó rendszerek felfedésével és lehallgatásával. A rádióelektronikai felderítés alapvetően két részre osztható:

- *a kommunikációs felderítésre (COMINT[5])*

A cél ország egy másik országnak szánt kommunikációjának (írásos üzenetek és/vagy hanganyagok) az elfogása

- *az elektronikai felderítésre (ELINT[6]) mely további két részre oszlik:*

  - FISINT[7]

    Radarok felderítése, de ide tartozik a cél ország haditechnikai eszközei, jellemzően műholdak, repülőgépek, hajók, tengeralattjárók tesztelése vagy működtetése során kibocsátott elektromágneses jelekből kinyerhető információk megszerzése

  - TELINT[8]

    Felderítő műholdak és pilóta nélküli repülőgépek adatcsatornáinak lehallgatása, vagy a távirányított eszközök (műholdak, rakéták, pilóta nélküli repülőgépek, stb.) által automatikusan közvetített, repülési jellemzőikre vonatkozó információk megszerzése

[4] Signals Intelligence

[5] Communications Intelligence

[6] Electronic Intelligence

[7] Foreign Instrumentation Signal Intelligence

[8] Telemetry Intelligence

- *nyílt forrású információszerzés (OSINT[9]);*

Az információs forradalom nyújtotta adatáradat egyik legnagyobb előnye a nyílt forrásokból elérhető adatmennyiség és a belőle előállítható hasznos információtartalom. Számos jegyzett anyag megtalálható és nyíltnak tekinthető, mely bárki számára megismerhető egyrészről a klasszikus formában elérhető anyagok könyvek, folyóiratok, cikkek, médiahírek, tanulmánykötetek, valamint az internetes felületen megtalálható anyagok. Utóbbi biztosítja a legnagyobb területet a nyílt adatok elérésre. Előnye mellett ugyanakkor hátránya a nagymennyiségű hiteltelen adatok, melyek elemzés és értékelés nélkül téves információkat nyerhetünk ki.[5]

- *képfelderítés (IMINT[10]);*

A műholdas, valamint a légi felderítés terjedésével és a technológia fejlődésével egyre több és pontosabb információt nyerhetünk ki a kiválasztott célország területeiről, objektumairól és eszközeiről. A képi felderítést napjainkban már összevonják a térinformatikai felderítéssel (GEOINT[11])

- *mérés- és jelmeghatározó hírszerzés (MASINT[12]);*

A technológia fejlődése és a precíziós eszközök megjelenése hívta életre és fejleszti azóta is a területet, mely a megcélzott eszközöket, tárgyakat és tevékenységeket az általuk kibocsátott, kisugárzott jelek alapján, szenzorok segítségével azonosítja. A mérés és jelmeghatározó hírszerzés szenzorai lehetnek:

- vegyianyag-elemzők, sugárzásmérők (NUCINT[13]),
- elektro-optikai felvevők,
- kisugárzott energiamérők, hangrögzítők (ACOUSTINT[14]),
- rezgésmérők, rádiófrekvenciamérők és anyagelemzők.

[9] Open Source Intelligence

[10] Imagery Intelligence

[11] Geospatial Intelligence

[12] Measurement and Signature Intelligence

[13] Nuclear Intelligence

[14] Acoustic Intelligence

- *technikai hírszerzés (TECHINT[15]);*

A terület főként a célországból szerzett haditechnikai eszközeinek közvetlen vizsgálata alapján nyert információk feldolgozását jelenti. Célja leggyakrabban a cél ország technológiai fölényének megtörése, illetve saját technológiai fölény biztosítása. Nem keverendő össze a technikai eszközökkel végzett hírszerzési ágakkal, módszerekkel, mint például a SIGINT, az IMINT vagy a MASINT.

- *kiberhírszerzés (CYBINT[16]).*

Egyre nagyobb térhódítást nyer a terület a számítógépek elterjedésével és a technológia fejlődésével. A nagysebességű adatcsomagok „vándorlását" biztosító száloptikák és nagy teljesítményű gépek segítségével az elektronikus célinformációk bizonyos esetekben operatív ügynökök bevetése nélkül megszerezhetők. A minősített információkat azonban titkosítási eljárások, tűzfalak és zárt hálózatok védik. Alapvetően három fajtája van: nyílt számítógépes hálózatokban védett információk megszerzése, a zárt számítógépes hálózatokban védett információk megszerzése és a számítógépes hálózatok által kisugárzott jelekből folytatott adatszerzés, mely utóbbit a kompromittáló kisugárzás elleni védelem (TEMPEST), illetve a Faraday-kalitka biztosít.

Az adat- és információszerzés módjai közül a technikai hírszerzést választottam, melynek segítségével technológiai fölényhez juttathatjuk saját csapatainkat segítve ezzel az információs uralomhoz való jutást. A későbbiekben olvashatjuk majd, hogy a választott ág több pusztán a technológia megszerzésénél. A terület felöleli a technológiát magát, annak teljes műszaki paramétereit és következtetéseket von le a kinyert adatokból. Mindemellett magának a technológiának a megszerzése is felölelhet több módszert és területet is, melyekhez képzett mérnökökön és ügynökök révén juthatunk hozzá, néha operatív területen keresztül.

Információ felhasználás és terjesztés kulcselemei

Fontos megemlíteni, hogy az információ felhasználásának és terjesztésének vannak kulcsfontosságú elemei, melyek nélkül, illetve azok időbeni hatályának módosulásával veszthetnek értékükből. Ezek a következők:[6]

[15] Technical Intelligence

[16] Intelligence gathered from Cyber Space

- *Időszerűség*

Az időszerűség két szempontból vizsgálható. Az első, hogy bármely információ, ami a rendeltetési helyét a szükségesnél később éri el, értéktelenné válik.

Az időszerűség másik összetevője, hogy az információk többsége, elsősorban harcászati, hadműveleti szinten, időérzékeny, ami azt jelenti, hogy az adat értéke az idő múlásával egyre csökken, illetve teljesen el is veszik.

Ennek alapján:

- Korai: az információnak nincs létjogosultsága, nincs rá még igény, előrejelzésnél alkalmazható
- Időben: az információnak nagy a létjogosultsága, az igény a legnagyobb, azonnali tájékoztatás
- Késői: az információnak már nincs létjogosultsága, nincs már rá igény, értékeléshez alkalmazható

A rendszernek készen kell állni, hogy minden elemével képes legyen a helyzetben bekövetkezett változásokat észlelni és jelentéseit a meghatározott rend szerint, haladéktalanul megtenni. Fokozatosan el kell érni a valós idejű terjesztés képességét.

- *Megfelelőség*

Nincs értelme olyan információ terjesztésének, mely nem ad választ a felhasználó által megfogalmazott kérdésekre, nem érthető, vagy a terjesztés olyan rendszeren keresztül történik, melyhez a felhasználó nem fér hozzá. Az információt a felhasználónak megfelelő formátumban kell továbbítani.

- *Felhasználhatóság*

A terjesztő és a felhasználó férjen hozzá minden fontos információhoz, adathoz. A feldolgozó köteles feldolgozni minden beérkező jelentést, információt, tájékoztatót. A feldolgozás során összevetik azokat a már korábban értékelt és elemzett adatokkal, vagy az azok alapját képező információkkal. Az információ értéktelen, ha a tájékoztatás nem megfelelő, vagy a felhasználó nem jut időben hozzá.

- *Reagáló képesség (operativitás)*

Folyamatosan figyelemmel kell kísérnie a felhasználó információval szemben támasztott követelményeit, az alárendeltek és más felhasználók igényeit. A terjesztő rendszernek (hálózatnak), a képesség függvényében, folyamatosan készen kell állni az információs igények kielégítésére, a fontossági sorrendnek megfelelően.

- *Biztonság*

Az információs rendszer és az adatforrások védelméről kiemelten kell gondoskodni. A terjesztő rendszer megbízható védelme biztosítja annak felhasználhatóságát. A rendszer védelme szempontjából folyamatosan értékelni kell, milyen információk hozhatók nyilvánosságra, melyek azok, amelyek fokozott védelmet igényelnek, mert illetéktelen kijutásuk súlyos veszteséget, vagy zavart okozhat. A terjesztő erőket időben el kell látni azokkal az információkkal, melyek a rendszer működése szempontjából hatáskörükbe tartoznak. [7]

Ahhoz tehát hogy eredményesen tudjuk támogatni a döntéshozókat a döntés előkészítésnél a fent említett szempontoknak kell megfelelni.

TECHINT jelentősége és folyamata

A technológiai hírszerzés területe az információs fölény majdan uralom megszerzésénél a technológia majd az abból kinyert adat feldolgozott információival járul hozzá. Elsősorban teszi a fegyveres erőket a technológiai meglepetések elkerülésére. Az ellenséges fegyverek karakterisztikáinak és képességinek ismerete lehetővé teszi a honi erők számára, hogy hatékony ellenintézkedéseket dolgozhassanak ki. Alkalmanként előfordul, hogy bizonyos technológiákat egyes nemzetek átvesznek a másiktól. E terület, mint az korábban is említésre került nem összekeverendő az egyéb hírszerzési ágakkal, módszerekkel, mint például a SIGINT, az IMINT vagy a MASINT.

A TECHINT maga a technológiára irányul, mely szerzett termék gyűjtéséből, feldolgozásából, elemzéséből, tehát elemzés-értékelési cikluson átesett információ kiaknázásából származik, így teret biztosítva a lehetőségek kiaknázására, mellyel megakadályozhatjuk a technológiai meglepetéseket, incidenseket. Ezzel a módszerrel növelhetjük az információs fölényünket, megakadályozhatjuk az incidensek bekövetkezését és meggátolhatjuk a szemben álló fél információs fölényéhez vezető törekvéseit.

A TECHINT többet tár fel pusztán a szemben álló fél eszközénél. Feltárja azon információkat, mely a technológia begyűjtésből, értékelésből, elemzés és külföldi tudományos és technikai információk értelmezésből jött létre, ez magában foglalja:

- a külföldi fejlesztésű alap és alkalmazott kutatásokat, valamint alkalmazott mérnöki technológiákat;
- a külföldi katonai rendszereket, fegyvereket, fegyver technológiákat, és anyagok tudományos és technikai karakterisztikáit, képességeit és korlátait, a kutatás-fejlesztéssel kapcsolatos jegyzőkönyveket, és az előállításukhoz szükséges termelési módszereket.

Tehát a begyűjtés nem csak magára az eszközre vonatkozik, hanem a folyamatra is melynek keretén belül adott termék/technológia fejlesztésre került és létrejött, azon ország vagy szervezet termelési rátájára mely a terméket előállítja, valamint feltehetően a termékkel kapcsolatos gazdasági és egyéb mutatókra.[8]

Tekintettel arra, hogy a tudományos és technikai információ fontos részét képezi egy ország versenyképességének a világpiacon, a technikai hírszerzés egybemosódik a gazdasági hírszerzéssel. Ennek fogalomkörét Egyesült Államok a következőképpen definiálta: „a kormány által támogatott vagy koordinált hírszerzési tevékenység, melynek célja, hogy jogtalanul vagy fedetten megszerezzen minősített adatokat és/vagy érzékeny politikai vagy védett információkat egy amerikai kormányzati hivataltól vagy cégtől, mellyel potenciálisan hatást tud gyakorolni egy idegen ország gazdasági versenyképességére és károsítja az Egyesült Államok gazdasági biztonságát.”[9]

A TECHINT produktuma egyfajta speciális juttatás, mely a fegyveres erők igényeit elégíti ki. E hírszerzési ág tevékenységi körét egy többcélú kézikönyv írja le az Egyesült Államok katonai doktrínáinak [10] A technikai hírszerzés folyamata jellemzően az alábbiak szerint osztható fel:

- *Anyagok és kapcsolódó dokumentumok begyűjtése*

A lehetőségek és esélyek jelentős szerepet játszanak külföldi eredetű fegyverek és felszerelések begyűjtésében. A begyűjtési fázis jellemzően akkor kezdődik, amikor egy katona valami érdekes dolgot talál a harctéren vagy egy disszidens pilóta egy géppel repül be egy baráti országba.

Bürokratikus eljárásrendeket hoztak létre a fejlesztési követelmények, mint például a kívánság lista, hogy irányítsa a szisztematikus begyűjtési törekvéseket. Az

anyagokat számos csatornákon keresztül be tudtak szerezni. Például anyagok szerezhetők be kereskedelmi utakon.

Egy attasé például egy külföldi hivatásostól információkat kérhet egy külföldi felszerelés egyes elemeiről. Titkos / fedett műveletek vetettek be annak érdekében, hogy kritikus ellenséges hadianyagokhoz juthassanak hozzá.

- *Hasznosítás (vizsgálat, elemzés)*

A hasznosítási szakasz különböző technikai és operatív vizsgálatokat tartalmaz. A szolgálatoknak jól kifejlesztett eljárásaik vannak az egyes anyagok tesztelésére. A tesztelés gyakran tartalmazza az elem működtetését és roncsolás mentes teszteléseket.

- *Az elkészült hírszerzési anyag bemutatása*

Az elkészült hírszerzési anyag a különböző jelentéseket és dokumentumokat foglalja magába. A technikai hírszerzési dokumentumok egy széleskörű anyagot tartalmaz rövid üzenetekből és jelentésekből, melyek ezen a területen készültek, kiszélesítve a kutatók által készített korábbi tanulmányokat.

Következtetés

Jelen anyagban kísérletet tettem, a technikai hírszerzési ág, információs műveletben történő elhelyezésére, és rövid bemutatására, hogy hogyan járul hozzá a honi erők számára az információs fölény, végül uralom kivívásához.

A történelem során mindig is, és várhatóan a jövőben is, egy igen hosszú ideig jelentős értékkel fog bírni az információ, melyről saját oldalról gondoskodnunk kell a megfelelő szintű védelméről, a szemben álló fél oldaláról pedig annak megszerzéséről. Az utóbbira az értekezés során több példát is felvázoltam, melyek közül a TECHINT ágára fektettem nagyobb hangsúlyt. Megjegyzendő azonban, hogy a megszerzett nyers adat a döntés hozók számára még nem elegendő, azok csak az elemzés értékelés folyamata után a megfelelő időben eljuttatva válnak csak igazán hasznára a döntéshozásnak.

Úgy vélem, hogy bár mint egyedülálló hírszerzési ág is igen nagy előnyt nyújthat a TECHINT, azonban az egyes hírszerzési ágak és elemek együttes kooperatív működése fejti ki a leghatékonyabb tevékenységet információgyűjtés területén, mely információk révén tehetünk szert a szükséges előnyökre és kontrollált környezet alatt tudjuk tartani a szemben álló feleket.

Felhasznált irodalom:

[1] Németh József: Egy vizsgálat anatómiája - 2001. szeptember 11., in: HADTUDOMÁNY, 2006/3 szám, 103-111. oldal
[2] Dr. Haig Zsolt– Dr. Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest 2005. 286 p. ISBN: 963-327-391-9
[3] Dr. Haig Zsolt: Védelmi elektronika, informatika és kommunikáció tudományszak. ZMNE KMDI, Budapest, 2008. november 27. p. 19. Letöltve: http://www.zmne.hu/kmdi/Haig_Zsolt_Vedelmi_elektronika.pdf (2015. 12. 18.)
[4] Dr. Haig Zsolt – Várhegyi István: A vezetési hadviselés alapjai. Egyetemi jegyzet, ZMNE, Budapest, 2000.
[5] Dr. Dobák Imre: A nemzetbiztonság általános elmélete. Egyetemi jegyzet, NKE NBI, Budapest, 2014.
[6] CLARK, Robert M.: Intelligence Analysis: A Target-Centric Approach. CQ Press, Washington D.C., 2010. p. 288. ISBN-13: 978-1452206127
[7] Mrs. Jacqueline Eaton - Mr. John Redmayne - Mr. Marvin Thordsen: Joint Analysis Handbook 3rd Edition. NATO Joint Analysis and Lessons Learned Centre, Lisbon, 2007. p. 122.
[8] Tibor Farkas , András Tóth: Electronic warfare in full spectrum operation, Proceedings of the International Scientific Conference: New Trends in Signal Processing, 2012.pp. 181-188. (ISBN:978-80-8040-447-5)
[9] Gus W. Weiss: The Farewell Dossier: Duping the Soviets. Studies in Intelligence (Central Intelligence Agency), 2008
Letöltve: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm (2015. 12. 18.)
[10] Porteous, Samuel: Commentary No. 59: Economic / Commercial Interests and Intelligence Services. Canadian Security Intelligence Service,Commentary series, 1995. Július, ISSN: 1192-277X
Letöltve: http://www.datapacrat.com/True/INTEL/CSIS/COM59E.HTM (2015. 12. 19.)
[11] Air Land Sea Applications Center: *TECHINT:* Multi-Service Tactics, Techniques, and Procedures for Technical Intelligence Operations, 2006 Június, p. 84. Letöltve: https://fas.org/irp/doddir/army/fm2-22-401.pdf (2015. 12. 19.)
[12] Dr. Négyesi Imre: DIE UNTERSTÜTZUNG DER SOLDATEN MIT ECHTZEITDATEN (A KATONÁK TÁMOGATÁSA VALÓS IDEJŰ ADATOKKAL) (Hadmérnök on-line, VII. évfolyam (2012) 4. szám, 162-166. oldal, ISSN 1788-1919).

[13] Dr. Négyesi Imre: Valós idejű adatfeldolgozás lehetőségei a hadseregekben I. (Hadtudományi szemle on-line, V. évfolyam (2012) 3-4. szám, 137-143. oldal, HU ISSN 2060-0437)
[14] Dr. Négyesi Imre: Valós idejű adatfeldolgozás lehetőségei a hadseregekben II. (Hadtudományi szemle on-line, V. évfolyam (2012) 3-4. szám, 144-148. oldal, HU ISSN 2060-0437)

Jelen számunk szerzői

Domokos Máté hdgy.	MH 34. BL KMZ
Gömör Marianna hdgy.	MH BHD
Hronyecz Erika	NKE HHK PhD hallgató
Dr. habil. Kerti András alez.	NKE HHK adjunktus
Luter Tibor	Puskás Tivadar Műszaki Szakkollégium
Megyeri Lajos alez.	NKE HHK tanársegéd
Nagy Balázs hdgy.	NKE HHK PhD hallgató
Nyikes Zoltán szds.	ÓE PhD hallgató
Puskás Béla	ÓE PhD hallgató
Szabó Anna Barbara	ÓE PhD hallgató

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás nélkül* - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Felelős kiadó: Dr. Fekete Károly mk. alezredes
Megjelent az NKE HHK Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-407 mellék)
hhk_hirado_szakcsoport@uni-nke.hu