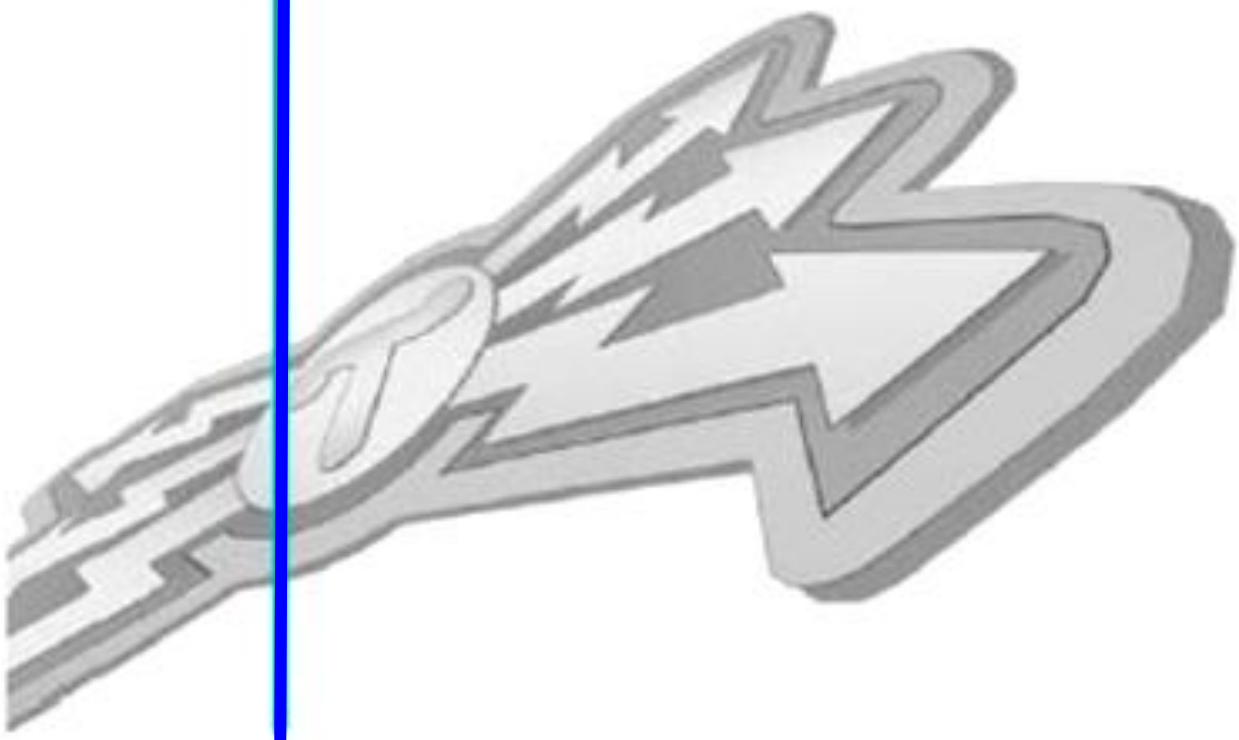
HÍRVILLÁM

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 1. szám
2015



2015. június 30.

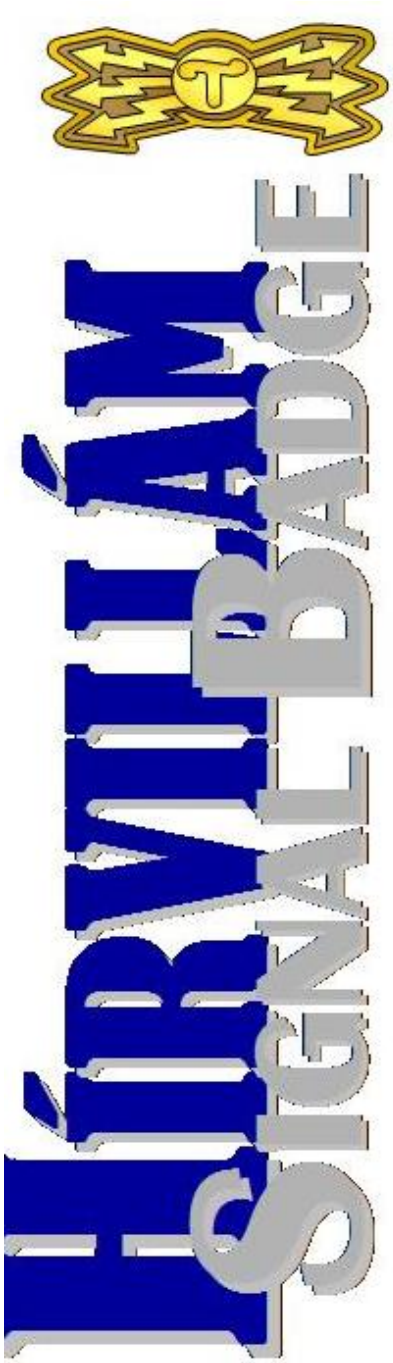
HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem Híradó Tanszék
tudományos időszaki kiadványa

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 1. szám

Budapest, 2015



Felelős kiadó/Editor in Chief
Dr. Fekete Károly alezredes

Szerkesztőbizottság/Editorial Board

Elnök/Chairman of the Board
Dr. Pándi Erik r. ezredes

Tagok/Members
Dr. Farkas Tibor százados
Dr. Horváth Zoltán alezredes
Jobbágy Szabolcs százados
Dr. Kassai Károly ezredes
Dr. Kerti András alezredes
Dr. Németh József
Prof. Dr. Rajnai Zoltán
Dr. Szöllősi Sándor ny. őrnagy
Tóth András százados

Szerkesztette/Co-ordinating Editor
Dr. Pándi Erik r. ezredes

HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-110 mellék)

hhk_hirado_szakcsoport@uni-nke.hu

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Tavaszi félévünk sikeres volt. Kimondottan. Hallgatóinkkal csak egy bajunk volt, nem volt velük baj. Terveink sikerültek mind oktatási, mind tudományos szempontból.

Tehát a 2014/15. tanév tavaszi szemesztere kedvezően alakult oktatási egységünk számára. Szokásainkhoz híven ismételten megszerveztük Balatonkenesén a Nemzetközi Katonai Információbiztonsági Konferenciát, amelyet eredményesnek értékelték mind a résztvevők, mind a szervezők.

Természetesen a társ tanszékek együttműködésével sikeres kiképzési gyakorlatokat folytattunk Püspökszilágyon, illetve Ócsán.

Hadnagyaink közül egy, a 2011-ben végzett volt növendékünk Szalai Máté hdgy. külszolgálatra indult, ugyanakkor idén hatan végeztek a 2011-13-as évfolyamokból az Óbudai Egyetemen okleveles villamosmérnökként, biztonságtechnikai mérnökként, illetve mérnök-tanárként. Örülünk ennek, hiszen a BSc felkészítésünk ezek szerint megfelelő alapot adott az MSc szak problémamentes, sikeres elvégzéséhez.

Végzős hallgatóink sikeres záróvizsgát tettek (Bertók Ádám htj., Domokos Máté htj., Gömör Réka htj., Kappeller Zsolt htj., Szabó Gergő htj., Szabó Kristóf htj., Szabó Szilvia htj. és Szanyi Sándor htj.), így szeptembertől elfoglalhatják új, felelősségteljes beosztásukat.

Remélem, hogy egy kellemes nyári kikapcsolódást követően, ősszel, közösségünk ismét folytatja oktatási, kutatási és tudományos munkáját szakmai kultúránk elmélyítése és hírnevünk bővítése érdekében.

Ezen gondolatok jegyében kívánunk kellemes időtöltést az idei év első számának áttekintéséhez!

Budapest, 2015. június 30.

Pándi Erik
a Szerkesztőbizottság
elnöke

Pausits Péter[1] - Szögi Gábor[2] - Fődi Gábor[3]: Biztonságtechnikai szempontok az osztott munkatérben működő robotok esetén

Absztrakt
A robotok folyamatos nagyléptékű fejlesztésének köszönhetően, a előremutató statisztikák alapján 2020-ra várhatóan minden háztartásra jutni fog átlagosan egy olyan robot, amelynek fizikai méretéből és erejéből adódóan komoly veszélyforrást jelent a vele egy térben elhelyezkedő személyre. Legyen az kezelő, kiszolgált személy, vagy akár sebészeti beavatkozás alatt álló beteg. A rohamosan fejlődő eszközöket nem minden esetben követi a megfelelő biztonságtechnikai szabályozás. Viszont ez a jövőben elengedhetetlen lesz, mert különben a fejlesztések koordinálatlanul fognak történni és a kivitelezés során nem a biztonság és a kockázatok csökkentése lesz az elsődleges szempont, hanem az anyagi érdek. Viszont egy ipari robottal ellentétben, baleset esetén a gazdasági és erkölcsi hátránynál nagyobb veszély fenyeget minket, az emberi élet kockáztatása. Ennek érdekében, számos kockázatcsökkentő szabályozást kell megalkotni, annak érdekében, hogy a fejlesztések a biztonságos határok között maradjanak. Ennek érdekében viszont előremutató nemzetközi szabványosításra és moderálásra van szükség, amelyet minden fejlesztőnek, gyártónak és felhasználónak a legszigorúbban alkalmaznia kell.

Abstract
This article shows development of robots.

Bevezetés

A világ fejlődése során mindig igény volt a termelő berendezések és termelési eljárások fejlesztésére. A céhek manufaktúrák kialakulását követően minden területen igény mutatkozott az emberi tényezők növelésére. A 18. századi ipari forradalom kirobbanásához vezető út kiemelt mérföldköve volt a James Watt által megalkotott gőzgép, mint az első olyan eszköz, amellyel nagyságrendekkel nagyobb mozgási energiát tudtak előállítani az emberi erőhöz képest. Ezzel együtt megszületett egy új, korábban nem ismert mértékegység az SI rendszerben a Watt, mint a teljesítmény mértékegysége. Innentől kezdve rohamosan fejlődött az előállított mozgási energia minél jobb nagyobb hatásfokú felhasználása. A

[1] OE Biztonságtudományi Doktori Iskola
[2] okl. biztonságtechnikai mérnök
[3] OE Biztonságtudományi Doktori Iskola

felhasználás elsősorban az ipari termelésben jelent meg, ami az Ipari Forradalom kirobbanásához vezetett. Innentől kezdve egy korábban nem látott rohamos fejlődés kezdődött meg az ipari szerszámgépek, megmunkáló egységek területén. A termelő berendezések fejlődése már a 19. században elérte azt a pontot, hogy nem volt elegendő a gőzgép által előállított energia, ennek hatására számos fejlesztés következett be más hajtóanyag felhasználása mellett, amíg Nikolaus August Otto 1876-ban szabadalmaztatta az első négyütemű belsőégésű motort, az Otto-motort. Ezzel az energiával újabb nagy ugrás következett be a fejlődésben, hiszen a gőzgéphez képest lényegesen nagyobb energiát tudtak előállítani. Ezzel párhuzamosan igény született a dinamó, mint villamos energia előállító berendezésre, amellyel a világ több pontján kísérleteztek. Már Jedlik Ányosnak 1861-ben sikerült a mozgási energiából villamos energiát előállítani, de végül Ernst Werner von Siemens szabadalmaztatta 1866-ban. Felismerték, hogy a villamos energiának kiemelt előnye minden más energiához képest, hogy kellő képen szabályozható, gazdaságosan szállítható az előállítótól a felhasználóig. Gyorsan felismerték a villamos energia előnyét az ipari alkalmazásban. Hosszú és széles körű alkatrész fejlesztések következtében 1952-ben Neumann János vezetésével megalkották az első, a villamos energiát információ tárolására hasznosító számítógépet, amelynek elvi működését a mai napig alkalmazzák a számítógépek fejlesztésében, melyet Neumann-elvként említünk. Az elmúlt több mint 60 év fejlesztései bizonyították, hogy a szabályozás, vezérlés, termelés, megmunkálás, kommunikáció, információ tárolás területén elengedhetetlen feltétel a villamos energia jelenléte.

A villamos energia, mint mozgási energia, mint pedig információtároláshoz szükséges energia hasznosítása óta, a fejlesztések során kiemelt figyelmet kaptak a robotok, mint a mesterséges intelligencia megvalósítása és az emberi tényezők hátrányainak kiküszöbölésére, illetve az energia megnövelésére alkalmazott elektromechanikai gépezet. A megnövekedett energia kezdetekben súlyos balesetekkel járt, mert nem volt kiforrott biztonságtechnikai szabvány, irányelv a robotok alkalmazására. Jelenleg a robotokat elsősorban az ipari környezetben alkalmazzák, amelyekhez már a legmodernebb biztonságtechnikai előírások vannak rendelve, melyek normális üzemben kizárják a legapróbb sérülés előfordulását is. Mivel a robotok jelenleg képesek önálló vagy kezelőszemélyzet felügyeletével ipari műveletek végrehajtására, anélkül, hogy fizikai kapcsolatba kerülnének élő szervezettel. Az osztott munkatér kizárásával a lehető legminimálisabbra csökkenthető a személyi sérülés lehetősége. Ezzel együtt megoldásra került a gazdaságilag nem kifejezhető kár lehetősége, az ember sérülése. De az önmagában okozott kár lehetősége még továbbra is fent áll, ami viszont csak gazdasági kárként

vezethető le. Viszont az automatizálás további fejlődése számos területen korlátokat okoz, amennyiben nem használható az ember-gép általi osztott tér lehetősége. Közel 30 éve folynak kutatások az orvosi és szerviz robotok fejlesztésében, amely önmagába foglalja az osztott munkatér alkalmazását. Hiszen egy sebészeti robot alkalmazása során kizárt, hogy ne érintkezzen fizikailag a robot egyes eleme akár a kezelő személyzettel, akár a beteggel. Ennek következtében egyre komolyabban folynak kutatások az osztott munkatér lehető legbiztonságosabbá tételére.
A cikk során bemutatást kap egy komplex robot cella biztonságtechnikai kérdései elektronikai, mechanikus és szoftveres oldalról. Megismerhetjük az iparban alkalmazott robotokra vonatkozó biztonságtechnikai előírásokat és ezek alkalmazásait, továbbá az osztott munkatér veszélyeit, az emberi tényezőben rejlő veszélyeket.

1. Biztonságelemzés

A fejlődés és a múltban bekövetkezett balesetek hatására egyre komolyabb figyelmet kap a biztonságelemzés és ezen belül elsősorban a kockázatelemzés. Felismerésre talált, hogy amennyiben a kockázatelemzést a kezdetektől fogva alkalmazzák, számos bekövetkezett baleset megelőzhető. Legyen az személyi sérülés vagy gazdasági- illetve erkölcsi hátrányt okozó baleset. Viszont ehhez a koncepció kidolgozásától kezdve, a tervezésen, gyártáson, beüzemelésen át a használat során mindig szem előtt kell tartani a kockázat elemzés feladatát. Ennek következtében számos kockázatelemzési eljárás került kidolgozásra, amely elsősorban matematikai valószínűség számítást és matematikai statisztikai számításokat alkalmaz. Kimondható, hogy a kockázatkezelés során a kockázat soha nem csökkenthető nullára, viszont mindent el kell követni, hogy a lehető legkisebb mértékűre csökkentsük a baleset bekövetkezésének valószínűségét.
A kockázatelemzés során egy modellt kell felállítani, ami a lehető legéletszerűbben modellezi le az adott gépet, helyzetet, környezetet és a személyzettel való kapcsolatot.

Az alkalmazott eljárások

<u>Előzetes veszélyelemzés</u>
Ezen eljárást akkor célszerű alkalmazni, amikor egy olyan gép, környezet fejlesztése történik, amiről nincs vagy csak nagyon kevés tapasztalati információ áll rendelkezésre. Ezek elsősorban a kísérleti, fejlesztési gépek tervezésénél fordul elő.

Ezen eljárás kiemelt szereppel bír a koncepció alkotási és tervezési fázisban. Ilyenkor egy faábrát kapunk a lehetséges veszélyhelyzetekről, veszélyforrásokról, a veszélyek egészségkárosító mértékéről. Majd rangsorolják a veszélyesség mértékének megfelelően a helyzeteket. Minden veszélyes helyzethez kidolgozásra kerül egy eljárás, ami feltételezhetően csökkenti a kockázatot.

Hibafa elemzés

Az elemzés célja, hogy alaposan megvizsgálják az összes lehetséges bekövetkező balesetet, és lépésről lépésre feltárják a bekövetkezés okát. Ezen kutatás során minden körülményt, környezeti-, emberi tényezőt számításba vesznek és teljesen a legapróbb kezdeti problémáig visszavezetik a folyamatot. Minden olyan szinten, ahol hiba következhet be, értékelik és a lehetőségekhez mérten minimálisra csökkentik a hiba mértékét. Köztudott, hogy egy baleset bekövetkezéséhez egy komplex, egymást követő hibák bekövetkezésére van szükség, nagyon ritka az az eset amikor egy tényező határozza meg a balesetet. Elsősorban azért, mert ezen események bekövetkezése látható, így könnyedén elkerülhető. A kockázatot általában egymásra épülő, nem tervezett események sorozatának bekövetkezése jelenti. Ezen elemzés a lehető legkorábban kívánja megoldani a problémát és így egyben a bekövetkezés kockázatát csökkenteni.

„Mi van, ha ...” elemzés

Az eljárás olyan kis komplexitású rendszer alkalmazása során kerül látótérbe, amikor az előzőekben ismertetett hibafolyamat mélysége 2 szintig terjed. Ezt az eljárást a komplexebb rendszerek esetében is célszerű alkalmazni, azon veszélyforrásokra, amelyek triviálisak. Ezzel a módszerrel érdemes vizsgálni, a már kiépített biztonsági rendszereket is, mégpedig a biztonsági rendszer meghibásodására való tekintettel. Pl. „Mi van, ha a biztonsági villamos hálózatban vezetékszakadás következik be?”. Így minden egyes részfeladat elemezhető, és amikor az elemzés nem jár eredménnyel, vagy túl komplex a bekövetkezés feltételrendszere, akkor érdemes más kockázatelemzési eljárást alkalmazni.

HAZOP (Hazard and Opreability Studies) elemzés

Egy kiemelten komplex elemzési eljárás, amely során minden részegységnek felelőse van, aki az adott terület szakértője. Ennek megfelelően megkeresik a kapcsolódási pontokat az egyes részterületek között, és a csomópontból kiindulva tárják fel a baleset bekövetkezésének lehetőségét, és azonosítják a lehetséges veszélyeket. Meghatározzák, hogy az egyes veszélyekhez milyen mértékben kapcsolódik az adott részterület és feltárják a lehetséges hibákat. Amennyiben nem

képesek az esemény bekövetkezésének lehetőtőségét a nullához közelíteni, közösen tesznek javaslatot biztonságot növelő intézkedésekre.

Eseményfa elemzés

Az eseményfa elemzés során a hibafa módszerhez hasonlóan egymásra hatással lévő események láncolatát tárják fel. Csupán itt a kezdeti eseményből indulnak ki, és minden bekövetkezett esemény által elindított újabb folyamatot rögzítenek, úgy hogy egyértelműen látható legyen az egymásra épülés. Ezzel átláthatóvá válik, hogy milyen következményekkel jár, amennyiben egy, a kezdetben elhanyagolható kis mértékű esemény bekövetkezik. Láthatóvá válik milyen láncfolyamatot képes elindítani és ezáltal egy nagymértékű baleset bekövetkezéséhez vezethet.

Meghibásodásmód és hatáselemzés

Ezen elemzés alkalmával összegyűjtésre kerül az egyes elemek meghibásodásának gyakorisága és az azokhoz rendelhető következmények. Ezeket az elemzéseket rendszeresen felül szokták vizsgálni a tapasztalatok figyelembevételével. Ezen eljárást FMEA (Failure mode and effects analysis) elemzésnek is szokták nevezni. Egy FMEA elemzésből egyértelműen kiderül, hogy a karbantartást, az egyes egységeket milyen rendszerességgel kell cserélni. Itt minden meghibásodást függetlenül kezelnek a többi meghibásodástól.

MOSAR (Method Organised for Systematic Analysis for Risk) elemzés

Ezen elemzés során a már meglévő kockázatcsökkentő elemzéseket hatékonyságát is vizsgálják. Feltárják az alrendszerek közötti kölcsönhatásokat. A kockázatok elemzését követően kiértékelik a lehetséges kockázatok elfogadhatóságát, és ennek eredményeként javaslatokat tesznek a megelőzések további fokozása érdekében.

2. Rendszertervezési módszertan

Számos kutatás, fejlesztés létezik annak érdekében, hogy olyan módszertan kerüljön kidolgozásra, amely a koncepciótól a gyártáson át a karbantartásig iránymutatás legyen egy új robot fejlesztése során. A jelenleg legfejlettebb rendszer módszertan a hazard identification and safety insurance control (HISIS). A HISIS javaslata, hogy a robotok fejlesztése esetén egy széleskörű csapatnak kell együtt dolgoznia, akik közül mindenkinek figyelemmel kell lennie az alapelvekre. A HISIS 7 alapelvet fogalmaz meg, amelyek alkalmazásával minden aspektusból kellő figyelmet kap a robot fejlesztése, tervezése, alkalmazása és karbantartása.

A hét alapelv a következő:

- Elősírások és követelmények
- Veszély azonosítás (HI)
- Biztonsági biztosító irányítás (SIC)
- Kritikus biztonsági határok
- Felügyelet és irányítás
- Igazolás és validálás
- Rendszer folyamat rögzítés és dokumentálás

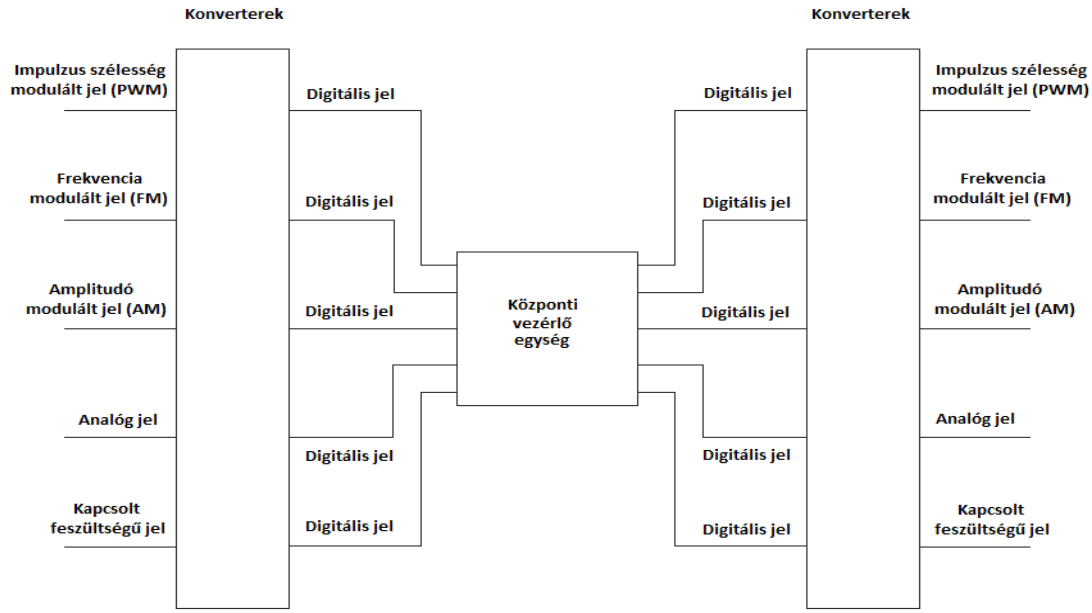
Az alapelvek megfelelő alkalmazása lehetővé teszi a robotok alkalmazása következtében felmerülő kockázatok csökkentését. A kockázat akkor csökkenthető a legminimálisabb szintre, ha a kezelő személy időben felismeri a veszélyt, és kellő időben reagál. A robotok szerepe nem csak a végrehajtandó műveletig terjed ki, hanem segítséget nyújt kezelőjének is a sztochasztikusan vagy determinisztikusan felmerülő veszély észlelésében, azonosításában, és amennyiben szükséges azonnali beavatkozásban a baleset elkerülése érdekében. A robotok segítségével töredékére csökkenthető a reakció idő, amennyiben a monitoring rendszer mintavételezési idejéből és reakció idejéből adódóan alkalmas a veszély megelőzésére vagy a baleset, sérülés által okozott kár legkisebb mértékűre történő csökkentésére. Ezen folyamat megfelelő minőségben és időben történő megvalósításához ad módszertant a HISIS.

3. A komplex robot cella

Egy komplex robot cella - legyen az ipari-, sebészeti- vagy szerviz robot – számos fő, biztonságtechnikai szempontból egymástól elkülöníthető részegységből áll. Ennek érdekében a fejlesztés során különböző szakemberekre van szükség, annak érdekében, hogy a lehető legmegbízhatóbb, kockázatmentes termék kerüljön kifejlesztésre. A három fő részterület az elektronika, a mechanika és a szoftver. A következőkben az kerül bemutatásra, hogy az egyes területek milyen szűk keresztmetszetekkel rendelkeznek biztonságtechnikai szempontból, illetve ezeket hogyan lehet feloldani, a baleset kockázatát csökkenteni.
Természetesen a különálló részterületek egymással szorosan együtt működnek, hiszen a kívánt művelet végrehajtásához egymással történő szoros együttműködés szükséges, mert ennek hiánya is jelenthet veszélyforrást.

4. Elektronika

Az elektromosság megjelenésétől kezdve elengedhetetlen a villamos jel jelenléte egy automatizált folyamatban. A szoftver a villamos jel tulajdonságait képes információként kezelni, illetve az aktuátorok a villamos jel által hordozott információ alapján képesek mozgási- és egyéb energiát szabályozottan létrehozni. Korábban léteztek teljesen mechanikus elven működő gyártó berendezések, amikor a lyukkártyák mechanikailag hordozták az információt. De jelenleg szoftveres és ezzel egybekötve elektromos vezérlés nélkül már gyakorlatilag elképzelhetetlen egy műveletet végrehajtó berendezés létezése.
Egy homogén rendszer működéséhez elengedhetetlen, hogy a környezeti és belső tulajdonságokról kapott különböző információk egy adott villamos jellé transzformáljuk. Természetesen a fejlődés következtében a villamos jel is további módosulásaira bontható, hiszen villamos jelnek tekintjük az analóg formában megjelenő amplitúdó- vagy frekvencia modulált jelet és a digitális formában megjelenő PWM (Pulse Width Modulation) jelet is. Ennek ellenére a Neumann-elven működő számítógép csupán a bináris jeleket (1. sz. ábra) képes kezelni, illetve bináris jel formájában képes az információkat továbbítani.



1. sz. ábra: Előállított villamos jelek kezelése és átalakítása

A központi processzor bonyolultságától és fejletségétől függően lehet 4-8-16-32-64 bites rendszerű, amely a be- és kimenetek szempontjából szintén kiemelt fontosságú a kimenetek és bemenetek szervezése során. Viszont az érzékelők nagyobbik többsége (1. táblázat) analóg jellé alakítja át az általuk mért jelet, illetve az aktuátorok pedig az analóg jelet alakítják át elsősorban mozgási vagy egyéb energiává.

Érzékelő típusa	**Mért tulajdonság**	**Működési elv, kimeneti jel**
PT 100, PT 1000 hőmérséklet mérő	Hőmérséklet nagysága	A hőmérséklet függvényében megváltozó ellenállás érték által kiváltott feszültségváltozás. A kimeneti pontok között mérhető feszültség analóg jel formájában jelenik meg.
Inkrementális jeladó	Pozíció mérés	Az elmozdult tárcsa a fotóelektronika segítségével az mérő egységben impulzus sorozatot generál, amelynek mennyiségéből elmozdulási nagyságot lehet számolni. Kimeneti jelként négyszögjel jelenik meg, ahol a felfutó élek száma a releváns a mérés során.
Inkrementális jeladó	Szögsebesség mérés	Az elmozdult tárcsa a fotóelektronika segítségével frekvenciamodulált jelet állít elő, amelynek frekvenciája minden időpillanatban egyenes arányosságban van a sebesség nagyságával.
Induktív-, kapacitív- és mechanikus kapcsoló	Jelenlét érzékelés	A mérési elvtől függően, az egyes kapcsolók kimenetén a megadott kimenettől függően megjelenik a kimeneti feszültség. A kimeneti jelet kapcsolt feszültségnek nevezzük.

1. sz. táblázat:- Érzékelő típusok elvi működés szerint

Ennek érdekében az elektronika felelős a kommunikáció homogén rendszerré alakításában, mégpedig valós időben hiteles információvá, mint a számítógép, mint pedig az aktuátorok számára.
Így az első szűk keresztmetszet a megfelelő szinten történő kommunikáció. Minden egyes jelátalakítás elkerülhetetlen minimális adat veszteséggel és időkésleltetéssel jár. Így törekedni kell arra, hogy a lehető legkevesebb konverzió történjen egy felmerülő környezeti tulajdonság és a szoftverhez történő információeljutás között. A tervezés során meg kell vizsgálni azon konverziókat amelyek kihagyhatók, vagy fejlettebb megoldással kiválthatók.
Mint az érzékelők tulajdonsága is az elektronika részfeladatai közé tartozik. Számos környezeti és belső tulajdonság létezik, amelyek befolyásolhatják egy robot biztonságos működését. Ilyen tulajdonságok lehetnek:

- hőmérséklet
- páratartalom
- fényviszonyok
- jelenlét
- pozíció
- elmozdulási irány
- sebesség
- nyomás

Az egyes tulajdonságok mérésére számos különböző mérési elven alapuló érzékelők léteznek. Jelenleg a legmodernebb érzékelők az optikai elven működő rendszerek szenzorok. Ezek rendszerint komplex méréseket hajtanak végre valós időben, azaz minimális időkésleltetéssel. Optikai elven már képesek vagyunk egy rendszerrel hőmérsékletet, fényviszonyokat, jelenlétet, pozíciót, elmozdulási irányt és sebességet mérni, amennyiben megfelelő mértékű a mintavételezési idő. Ennek ellenére a biztonságos információgyűjtéshez nélkülönözhetetlen az egyes tulajdonságok speciális érzékelővel történő mérése. Ugyanakkor egy érzékelő meghibásodását a különböző mérési elveken alapuló redundáns szenzorokkal tudjuk a leghatékonyabban kiküszöbölni. Az általuk létrehozott villamos jelek kiértékelésében kiemelt szerepet játszik a szoftver, mint döntéshozó részegység.
Összességében elmondhatjuk, hogy az elektromos oldalról elsősorban a homogén rendszer kialakítása, és az érzékelők jelentik a szűk keresztmetszetet. Ennek feloldására az egyszerűsítés és a redundancia jelenti a kockázatcsökkentő eljárást.

5. Mechanika

A robotok létjogosultsága elsősorban azért van jelen, mert képes kiküszöbölni az emberi tényező hátrányos tulajdonságait és képes megnövelni az ember által előállított energiát a folyamat elvégzéséhez szükséges szintre. Hiszen egy ipari robot szükség esetén több tonna tömeget is képes mozgatni, amire az emberi képesség nem elegendő. Továbbá egy sebészeti robot képes kézremegés nélkül a legpontosabb pozícionálással vágásokat végrehajtani, vagy olyan helyre eljutni, amire az emberi kéz méretéből adódóan nem képes. Továbbá képes munkát végezni veszélyes környezetben is, amely már egészségkárosító hatással lehet az emberi szervezetre. Viszont a tervezés során kiemelt figyelmet kell fordítani a megfelelő aktuátor kiválasztására és a mechanikai terhelés megfelelő méretezésére. Az aktuátorok elsősorban robotot mozgató precíziós egyenáramú villamos motorokat alkalmazunk, néhány esetben pedig hidraulikus motorokat, de ez nem jellemző a sebészeti- és szerviz robotok esetén, mert szabályozhatóságuk egy sebészeti beavatkozáshoz nem megfelelő. A sebészeti robotok esetén a kritikus tulajdonságot a pontosság jelenti. Így az aktuátor, mint motor kiválasztásánál speciális szervo motor alkalmazása szükséges. A szervo motorok többnyire PWM vezérelt motorok, amelyek egyben egy érzékelő is, így képes valós időben információt szolgáltatni saját pozíciójáról.
A mechanikai másik szűk keresztmetszete a stabilitás. Ennek érdekében a robotkarokat úgy kell megtervezni, hogy általuk végrehajtandó fizikai művelet legalább kétszeresét képesek legyenek végrehajtani. Továbbá egy osztott munkatérben előfordulhat, hogy külső sztochasztikus behatás éri a robot testet. Nem lehet megengedni, hogy egy ilyen hatásra kimozduljon a műveleti pozícióból. Ennek kiküszöbölésére, úgy kell megtervezni a robot testet, hogy az esetlegesen előfordulható külső fizikai behatásnak ellen tudjon állni, és továbbra is stabil tudjon maradni.
Így a mechanikai részegység által nyújtott kockázat csak úgy csökkenthető, ha az előírt karbantartás, az aktuátorok kiválasztása és a mechanikai tervezés túl van méretezve legalább kétszeres teherbírásra és üzemidőre az általa elvégzett műveletet tekintve. Sajnos nem megoldható a redundancia, a mechanikai kockázatcsökkentés esetén.

6. Szoftver

A jelenkor fejlett technológiájában már nélkülönözhetetlen egy számítógép használata minden olyan eszközben, amelyben elektronika van jelen. Ez jellemző az

érzékelőkre, aktuátorokra, kommunikációra. Valójában minden olyan elektronikai eszközt, amely tartalmaz programozható mikrokontrollert vagy mikroprocesszort, azokat számítógépnek nevezzük. Rendszerint ezek az eszközök célfeladatot látnak el, de rendelkeznek programmemóriával és gépi kód fut rajtuk. Ezen túl minden komplex robotrendszer rendelkezik egy központi irányító számítógéppel, amely feladata, hogy az érzékelőktől érkező villamos jel által hordozott információk alapján döntéseket hozzon és hatására vezérleje a robot működéséhez szükséges aktuátorokat. Feladata, hogy működésüket összehangolja, és a kapott információk alapján kockázatcsökkentő vezérlést hajtson végre. Így a szoftver egy olyan részterülete a robotnak, amely feltételezi, hogy a robotban található mechanika, elektronika és kommunikáció megfelelően, hibamentesen működik, illetve amennyiben hibát észlel, utasításba adja a kockázatcsökkentő döntéseket. Amennyiben nem képes megfelelő mértékben kiküszöbölni a problémát, úgy döntenie kell a robot leállításáról. Egy robotban működő összes programozható egység szoftverének maximálisan stabilnak kell lennie, nem megengedett a szoftverfutási probléma. Ezért a robotnak beüzemelés előtt számos tesztelésen kell átesnie, és a korábban említett kockázat elemző módszereket kell alkalmazni a kockázatok csökkentésére. A szoftver fejlesztése során figyelni kell arra, hogy a szoftver képes legyen a kezelőszemélyzet egyértelműen rendellenes utasításait felülbírálni és szükség esetén korrigálni. Viszont a kezelőszemélyzetnek is tudnia kell esetleges hibás működés esetén beavatkozni a szoftver futásába, amelynek legtriviálisabb módszere a vészleállító gomb alkalmazása.

A szoftver felelős a kommunikációs protokollok megfelelő kezelésért is. Rendszerint az ilyen komplex rendszerekben az egyes részegységek között busz rendszert alkalmaznak, de létezik közvetlen pont-pont közötti kapcsolat is. Az alkalmazni kívánt buszrendszer kiválasztása során kiemelt figyelmet kell fordítani a buszrendszer adat átviteli sebességére, megbízhatóságára, amely nagyban függ az alkalmazott távolságtól. A buszrendszerek kritériumai közé tartoznak, hogy mekkora számú eszköz mennyiség kommunikációjára alkalmas. A következő összehasonlítás a leggyakrabban alkalmazott buszrendszereket és tulajdonságait tartalmazza.

Megnevezés	Adatátviteli sebesség (kbit/s)	Kommunikációs eszközök maximális száma (db)	Maximális vezetékhossz (m)
CAN Bus	50-1000	64	40-1000
Profi Bus	9,6-12000	32	100-1200
LIN Bus	20	16	40
LonWorks	78-1250	32385 (127)	125-2200
Inter Bus	500	4096	200-13000
P-Net Bus	76,8	125	1200

2. sz. táblázat: Tulajdonságok csavart érpár alkalmazása esetén

Összegzés

A kutatás során megállapítható volt, hogy minden egyes rendszer fejlesztése során kiemelt figyelmet kell fordítani a kockázatelemzésre. Már a koncepcióalkotás folyamatánál számba kell venni a kockázati tényezőket, és már a kezdetekben megoldásokat kell keresni a kockázati tényezőkre. Minél komplexebb egy rendszer, annál nagyobb a veszélye, hogy egészségkárosító vagy gazdasági hátrányt okozó kockázatot hordoz magában. Megállapítható, hogy a jelenleg fejleszteni kívánt robot rendszerek elengedhetetlen részegységei a központi irányító berendezés, a megfelelő kommunikáció, az aktuátorok és érzékelők. Ezen részterületek számos kockázatot jelentenek és biztonságtechnikai szempontból számos szűk keresztmetszet ismerhető fel, amelyek feloldása nélkül nem garantálható a kockázatok csökkentése. Az egyes részterületek kockázatcsökkentését követően, szükségszerű, hogy a részfeladatok az egymással való kapcsolódási pontokon az elvárt szinten tudjanak együtt működni. A minimális kockázatok mellett, a komplex robot cellának tudnia kell működni az elvárt biztonsági szinten. Megállapítható, hogy az osztott munkatér az emberi tényező miatt sokkal nagyobb kockázatot jelent, mint a zárt térben működő robotok. Amíg zárt térben működik, úgy normális üzemmódban nem fordulhat elő személyi sérülés, hiszen a biztonsági előírásoknak köszönhetően, amennyiben a munkatérbe idegen anyag vagy személy kerül, úgy a folyamat azonnal leáll, így személyi sérülés nem következhet be. De az osztott munkatérben elkerülhetetlen az ember-gép közötti véletlen vagy szándékos fizikai kapcsolat. Így a kapcsolat kizárása nélkül a kockázatcsökkentést úgy kell elvégezni, hogy sztochasztikus és determinisztikus fizikai kapcsolat esetén se okozzon maradandó vagy egészségkárosító sérülést a robot a kezelő személyzetben vagy a kiszolgált személyben.

Felhasznált irodalom

[1] http://www.kvaser.com/about-can/can-standards/linbus/ (dátum: 2015. április 23.)
[2] http://www.freescale.com/files/microcontrollers/doc/reports_presentations/LINOVERVIEWPRESENT.ppt (dátum: 2015. április 23.)
[3] Novák Balázs - Terepi buszrendszerek összehasonlítása
[4] Dr. Csutorás Gábor - Biztonságtudomány
[5] L. Schreiter, D. Bresolin, M. Capiluppi, J. Raczkowsky, P. Fiorini és H. Woern, „Application of Contract-based verification techniques for Hybrid Automata to Surgical Robotic Systems”, 2014 European Control Conference (ECC), 2310-2315. oldal
[6] T. Kerezovic, G. Sziebig, B. Solvang és T. Latinovic, „Human Safety in Robot Applications – Review of Safety Trends”, 11th International conference on accomplishments in Electrical and Mechanical Engineering and Information Technnology (DEMI 2013), 1031-1039. oldal
[7] Jiajie Yu, Yingqiang Wang, Youping Li, Xianglian Li, Cuicui Li és Jiantong Shen, „The Safety and effectiveness of Da Vinci surgical system compared with open surgery and laparoscopic surgery: a rapid assessment”, Journal of Evidence-based Medicine 7. volume 2014. 121-134. oldal
[8] P. Kazanzides, Y. Kouskoulas, A. Deguet és Z. Shao, „Proving the Correctness of Concurrent Robot Software”, 2012 IEEE International Conference on Robotics and Automation, 4718-4723. oldal
[9] Min Yang Jung, Russell H. Taylor és P. Kazanzides, „Safety Design View: A Conceptual Framework for Systematic Understanding of Safety Features of Medical Robot Systems”, 2014 IEEE International Conference on Robotics and Automation 1883-1888. oldal

Horváth Zoltán: Szimmetrikus és aszimmetrikus rejtjelzést, valamint adatrejtést megvalósító programcsomag oktatásban történő alkalmazása-I.

Absztrakt
A szerző bemutatja, hogy a terület specialitásának megfelelően milyen programok alkalmazásával lehet a gyakorlati feladatok végrehajtása során elmélyíteni az elméleti ismereteket, különös tekintettel az alkalmazott algoritmusok leírására.

Abstract
The author explains that according to the area of specialty may deepen the theoretical knowledge, in particular the description of the algorithms used 27nt he implementation of practical exercises.

Bevezetés

Az oktatás során az elektronikus információbiztonság célkitűzése és területei jól levezethető, logikailag egységes képet alkotó ismeretanyagként közölhető.
Számos példa felhozható, mely alátámasztja a rejtjelezés és adatrejtés szerepét a bizalmasság, sértetlenség és rendelkezésre állás megvalósítása érdekében.
Az ismeretanyag közlését követő tanulási folyamat hatékonysága jelentősen növelhető gyakorlati feladatok megoldásán keresztül, bár megjegyzendő, hogy gyakorlati alkalmazásra a „számológépek aritmetikai képessége” enyhén fogalmazva kevés. A hallgató az elméletben tanultakat nem tudja gyakorlati tapasztalattal alátámasztani, ismereteit megerősíteni.
Ennek a problémának az áthidalhatóság érdekében született egy programcsomag, mely segítségével – valós időben – tanulmányozható a szimmetrikus és aszimmetrikus rejtjelezés, valamint a szteganográfia megvalósítása.
Ez a „játszva tanulás” lehetőségét rejti magában, mikor a hallgatók önfeledten, a programok alkalmazásán keresztül gyakorlati ismereteket is szerezve mélyítik el ismereteiket.
Ezen programcsomag az igény megfogalmazódásától az oktatásba történő alkalmazásáig mintegy egyéves kutató-fejlesztő munka eredménye.
Jelen cikk a programcsomag megvalósítás során figyelembe vett megfontolások, az abból kialakuló algoritmusok rövid megfogalmazását tartalmazza.

1. Kripto-számológép a természetes számok halmazán

A hagyományos, de még a tudományos kalkulátorok között sem találhatók olyan eszközök, melyek képesek bemutatni az egyes rejtjelező algoritmusok működését. Az egyes algoritmusok megvalósítása során előfordulhat, hogy több száz számjegyet tartalmazó természetes szám feldolgozása válik szükségessé.

1.1. Számábrázolás

Példaként említendően a feladat a következő, számítsa ki:

Y = 855 ^{2753}. <u>pontos</u> értékét!

Tudományos kalkulátort alkalmazna az eredmény a következő:

$$Y = 5.043288895841606873442289912739446663145387836003550931555496 \ast 10^{8071}$$

Ez az eredmény használhatatlan, mivel a számábrázolás nem támogatja a további aritmetikai műveletek végrehajtását, melyek eredményes végrehajtása az egyes rejtjelezést megvalósító algoritmusok szempontjából létkérdés (egész számok ábrázolása, hatványozás, egészosztás, maradékképzés, prímellenőrzés, kongruens számpár keresése). A pontos érték:

Y =
504328889584160687344228991273944666314538783600355093155549675645010556286120825599787442454281100543834986542893363849302464514415078517209179665478263530709963803538732650089668607477
…
…
237759965220309418558880039496755829711258361621890140359542349304247490536939927761142617964071001276432804287060835315945823059463268278612702033569803461432456970214843 75

A mintegy **8072** karakterhosszon keresztül (ez A/4-es méretben 2 lapot jelent) ábrázolt szám már alkalmas további aritmetikai műveletek végrehajtására.
Ha kivitelezhető, hogy a fenti példát említve 8072 hosszúságú karaktersorozatot tartalmazó pontos értékkel dolgozzunk, akkor megoldható a továbbiakban a már

említett egészosztás, maradékképzés és egyéb függvénykapcsolat megvalósítása. Ehhez a kulcs a számábrázolás megfelelő kialakítása.

1.2. Karaktersorozat (sztring) alapú aritmetika

A számítógépek (kalkulátorok) számábrázolása kötött. A bevitt adatok feldolgozása előre meghatározott adatstruktúrában történik (pl.: fixpontos egész, vagy lebegőpontos, hatvány alapú számábrázolás).
A rejtjelezés gyakorlati bemutathatósága érdekében alapvető fontosságú a számok pontos ábrázolása (pl.: egészosztás, maradékképzés során ez alapkövetelmény).
A számítógépek számábrázolási korlátait figyelembe véve célszerű az adatok karaktersorozatként történő feldolgozása. Ez lehetőséget biztosít az ábrázolható tartomány korlátainak áthidalására.
A hagyományos, „papír alapú” matematikai műveletek végrehajtása közismert. Ha az operandusok között végzett matematikai művelet hagyományos, „papír alapú” módszerrel történik, az ábrázolt eredmény helyi értékeinek kezelhetősége kitolható akár a memóriacímzés határáig. Nyilvánvaló, hogy ilyen extrém méretű számokkal történő műveletek végrehajtása megkövetel egy újfajta számábrázolást.

Hagyományos számábrázolás	**Szöveg alapú számábrázolás**
értékkészlet (integer típus): [-32768 … 32767]	értékkészletét a tárolt „szöveg” hossza határozza meg
feladat: a∗b	
input: a:=1234; b:=567;	input: a:=’1234’; b:=’567’;
eredmény: -21.218	eredmény: ’699678’
A helyes végeredmény: 699678	

1. sz. táblázat: Aritmetikai művelet végzése a természetes számok halmazán

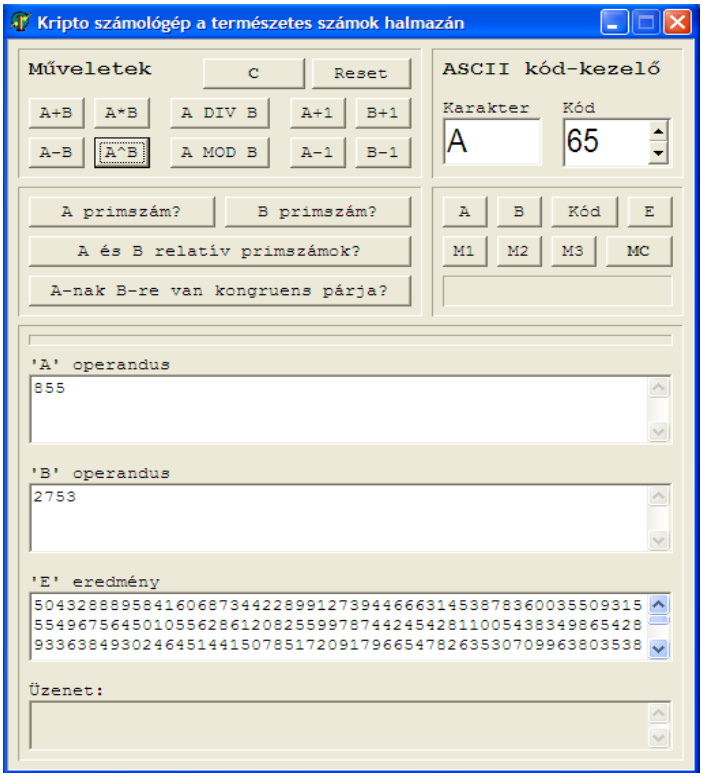
1.3. Aritmetikai feladatok, azok végrehajtása

A rejtjelezés gyakorlati ismereteinek elsajátítása során felmerülhet az aritmetikai háttér támogatásának hiányossága. Egy erre a célra kifejlesztett számológép képes támogatni az ismeretanyag feldolgozását, a gyakorlati feladatok kivitelezését.
A rejtjelezés algoritmusainak megértése és az ismeretek gyakorlati úton történő elmélyítése végett a következő funkciók megvalósulásának alkalmazhatósága indokolt (a természetes számok halmazán).

Funkciók:

- Alapműveletek végzése:
  - összeadás, kivonás, szorzás
  - egészosztás, maradékképzés
  - operandusok inkrementálása, dekrementálása
- Hatványozás;
- Prímellenőrzés:
  - az aktuális operandus prímszám?
  - az aktuális operandusok relatív prímek?
  - prímellenőrzés során (közös) szorzótényező megállapítása, ha van
- Kongruens számpár ellenőrzése;
- ASCII kódtáblázat kezelése (kód és karakter alapján);
- Operandusok (input, output adatok), ASCII táblázat és memória közti műveletek végrehajtása (drag and drop módszerrel).

Belátható, hogy a gyakorlati tevékenység során egy „kripto-számológép” felépítése és működése rendhagyó. Az előzőekben foglaltak alapján a képzés során célszerű egy speciális számológép alkalmazása. A számológép alkalmazásával a hallgatók képessé válnak egy folyamat végrehajtása (kulcsgenerálás, kódolás-dekódolás) során az elméleti ismeretek gyakorlati tapasztalatokon alapuló elmélyítésére.



1. sz. ábra: A kripto-számológép képernyőképe

2. Szimmetrikus és aszimmetrikus rejtjelzés, valamint szteganográfia megvalósítása

A programcsomag segítségével a hallgatók körbejárhatják a kulcselosztás, nyílt kulcsú rejtjelezés és az adatrejtés problémakörét.
A programok direkt adatbevitel mellett szövegfájlok, képfájlok (*.txt, *.bmp) kezelésére is alkalmasak.
A programok telepítése a futtatható ’*.exe’ fájl másolásával megvalósítható.

2.1. A programcsomag felépítése

- Szimmetrikus kódolást-dekódolást megvalósító program, mely a Polübiosz-tábla alkalmazásának algoritmusa alapján működik;
- Aszimmetrikus kódolást-dekódolást megvalósító program, mely az RSA algoritmus alapján működik;

- Adatrejtést megvalósító program, mely tömörítetlen 24 bites TrueColor (*.bmp) képfájlokat alkalmaz adatrejtésre.

2.2. A programcsomag védelme

A programcsomag programjainak illetéktelen felhasználás elleni védelme érdekében kialakításra került egy program. Ez bejegyzi a jogosult számítógépre másolt programba a jogosult számítógép hálózati adapter MAC-címét.
A programcsomag programjai csak a számítógép hálózati kártya MAC-címének azonosítását követően futnak (Egy nem „érvényesített” másolat nem működik.).
Javasolt a védelmet megvalósító program közvetlen futtatása külső meghajtóról, illetve hogy erről a programról ne készülhessen illetéktelen másolat.

2.3. A programcsomag elemeinek működése

2.3.1. Szimmetrikus kódolást-dekódolást megvalósító program elvi alapjai

A Polübiosz-tábla

A kriptográfiában a Polübiosz-tábla az ókori görög történész, Polübiosz által feltalált eszköz, amely feltördeli az eredeti szöveg karaktereit, hogy azokat egy kevesebb szimbólumból álló karakterhalmazzal fel lehessen írni.

	1	**2**	**3**	**4**	**5**
1	*'A'*	*'B'*	*'C'*	*'D'*	*'E'*
2	*'F'*	*'G'*	*'H'*	*'I'*	*'K'*
3	*'L'*	*'M'*	*'N'*	*'O'*	*'P'*
4	*'Q'*	*'R'*	*'S'*	*'T'*	*'U'*
5	*'V'*	*'W'*	*'X'*	*'Y'*	*'Z'*

2. sz. táblázat: Polübiosz-tábla[4]

[4] [1] alapján

Minden egyes betű a rácsban elfoglalt helyének koordinátáival jellemezhető, például a "BAT" betűhalmaz "12 11 44" alakban írható fel. A görög ábécé 24 betűből áll, amely mindössze egy üres rubrikával elfér egy hasonló négyzetben.

A kódtábla kulcsolása

Mivel minden egyes betű a rácsban elfoglalt helyének koordinátáival jellemezhető, az elfoglalt hely koordinátáinak karakteres helyettesítésével a kulcsolás megvalósítható. Az alábbi táblázat bemutatja a kulcs létrehozásának folyamatát a Polübiosz-táblán.

	A	**C**	**D**	**8**	**Q**
B	*'A'*	*'B'*	*'C'*	*'D'*	*'E'*
F	*'F'*	*'G'*	*'H'*	*'I'*	*'K'*
9	*'L'*	*'M'*	*'N'*	*'O'*	*'P'*
1	*'Q'*	*'R'*	*'S'*	*'T'*	*'U'*
H	*'V'*	*'W'*	*'X'*	*'Y'*	*'Z'*

3. sz. táblázat: Kulcsolt Polübiosz-tábla

A Polübiosz-tábla sor- és oszlopszámai kóddal történő helyettesítését követően a "BAT" betűhalmaz (a 2. és a 3. táblázat alapján) "12 11 44" helyett "BC BA 18" alakban írható fel.

A Polübiosz-táblából kiindulva (2. táblázat), a kódolás/dekódolás végrehajtásához szükséges sor- és oszlopszámokat helyettesítő kóddal (3. táblázat) a kódoláshoz/dekódoláshoz alkalmazandó kulcs példaként:

BF91H-ACD8Q

A kódtábla kibővítése

A Polübiosz-tábla struktúráját követve kialakítható egy kibővített kódtábla, melynek elemszáma (oszlopainak és sorainak szorzata) lefedi a felhasználni kívánt karakterkészletet. A jelenlegi szövegfájlok (*.txt) karakterkészlete kb. 120 betű.

A karakterkészlet növelése magával hozza a kulcs méretének növekedését. Ez egy 10x12-es táblázat esetén természetesen 10+12 karaktert tartalmazó kulcs.

Kódolt távirat létrehozása

Távirat kódolása során a kódot 5-ös betűcsoportokban hozzák létre. Az utolsó betűcsoport ’X’ karakterekkel kerül kiegészítésre, hogy az is 5 karaktert tartalmazzon.

A 4. táblázat alapján, a kulcsolt kibővített kódtáblázat alkalmazása során (ahol a kulcs: 123456789W-ABCDEFGHIJKL) a "BAT" távirat kódja megfelel a "D6C7E 5XXXX", a "BATU" távirat kódja megfelel a "D6C7E 5E3XX", karaktersorozatnak.

A távirat jó olvashatósága érdekében a kulcs természetesen csak nagybetűket, illetve számjegyeket tartalmazhat. Az egyes kulcsszegmensben (oszlopszegmens, sorszegmens) természetesen nem lehetnek azonos karakterek. A kulcsban a félreérthetőség elkerülése érdekében a "0" (azaz nulla) karaktert ne alkalmazzuk, mert könnyen összetéveszthető az "O" (azaz nagy o-betű)-vel. Mivel töltelékkarakter, kizárjuk az "X" alkalmazását is.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**W**
A	’0’	’1’	’2’	’3’	’4’	’5’	’6’	’7’	’8’	’9’
B	’K’	’L’	’É’	’Á’	’?’	’Ó’	’Ü’	’Ö’	’,’	’Ű’
C	’J’	’H’	’G’	’F’	’D’	’S’	’A’	’!’	’Y’	’Í’
D	’P’	’Ő’	’Ú’	’M’	’N’	’B’	’V’	’C’	’X’	’:’
E	’O’	’I’	’U’	’Z’	’T’	’R’	’E’	’W’	’Q’	’.’
F	’/’	’y’	’g’	’ ’	’x’	’>’	’{’	’i’	’o’	’j’
G	’a’	’#’	’~’	’<’	’+’	’ | ’	’w’	’ " ’	’\’	’ő’
H	’t’	’_’	’d’	’ó’	’@’	’q’	’(’	’é’	’f’	’&’
I	’;’	’k’	’n’	’b’	’÷’	DEL	’[’	’s’	CR	’}’
J	’e’	’$’	’)’	LF	’§’	’l’	’í’	’c’	’-’	’p’
K	’...’	’ü’	’r’	’v’	’ú’	’z’	TAB	%	’ű’	’u’
L	’]’	’*’	’h’	’ ` ’	’ö’	’=’	’m’	’á’	’^’	’ ' ’

4. sz. táblázat: Kulcsolt kibővített kódtáblázat

2.3.2. Nyílt kulcsú (aszimmetrikus) kódolást-dekódolást megvalósító eljárás[5] elvi alapjai

RSA alapok, kulcsgyártás

Az RSA-titkosításhoz egy nyílt és egy titkos kulcs tartozik. A nyílt kulcs mindenki számára ismert, s ennek segítségével kódolhatják mások a nekünk szánt üzeneteiket. Valamely kulccsal kódolt üzenet csak a kódoló kulcs kulcspárjával dekódolható.

Az RSA-titkosításhoz a következő módon generáljuk a kulcsokat:

- Véletlenszerűen válasszunk két prímet, ***p***-t és ***q***-t;
- Számoljuk ki ***{ N = p · q }***-t, **N** lesz a modulusa mind a nyilvános, mind a titkos kulcsnak is (a kulcs második szegmense);
- Számoljuk ki ***{ F = (p-1)·(q-1) }***-t;
- Válasszunk egy olyan egész számot ***{ e }***-t, mely ***{ F }***-re relatív prím;
- Válasszunk egy olyan egész számot ***{ d }***-t, mely ***{ e }***-vel kongruens számpárt alkot ***{ F }***-re, azaz ***{ F }***-nek van olyan egészszámú többszöröse, mely érték ***{ e }***-re és ***{ d }***-re számított modulusa ***{ 1 }***;
- A kulcspár ezek alapján ***{ e és N }***, valamint ***{ d és N }***.

RSA kódolás, dekódolás

Az üzenetek kódolása és dekódolása ezt követően az alábbiak szerint valósul meg, ahol ***m*** az üzenet egy karaktere, ***c*** a kódolt karakter és ***mod N*** a maradékképzés ***N***-re:

- $c = m^e \bmod N$, és;
- $m = c^d \bmod N$.

Egy példa a kódolás és dekódolás bemutatására:

Legyen ***p=37*** és ***q=43*** prímszámok. Ezek alapján ***N=1591*** és ***F=1512*** adódik.

F-re relatív prím ***e=73***. ***F*** és ***e*** értéke alapján ***d=145*** számítható (***e*** és ***d*** kongruens számpár ***F***-re, azaz ***e·d = n·F + 1*** ahol ***n*** természetes szám). Ezek alapján a kulcspár $K_{1a}[73;1591]$ és $K_{1b}[145;1591]$.

Kódoljuk az ***m = 'A'*** üzenetet, majd hajtsuk végre a dekódolást (ASCII kódja: ***65***):

$c = m^e \bmod N$, azaz $c=65^{73} \bmod 1591 = \underline{1360}$, továbbá

$m = c^d \bmod N$, azaz $m=65^{145} \bmod 1591 = \underline{65}$, *azaz 'A'* ASCII kódja.

[5] [2] alapján

A program alkalmazása során célszerű (***e*** és ***d*** < ~500), valamint (***N*** < ~3000) értékeket választani. Túl nagy számok választása esetén a futási idő jelentősen megnő.

Dupla kódolás, dekódolás

Az üzenetek kétszeri, két kulcspárral végzett kódolása-dekódolása képes bemutatni a hitelesség és a letagadhatatlanság problémakörét. A kódolási és dekódolási sorrend ebben az esetben viszont nem tetszőleges.

Legyen $\mathbf{K_1\{(e_1;N_1)}$ **és** $\mathbf{(d_1;N_1)\}}$, valamint $\mathbf{K_2\{(e_2;N_2)}$ **és** $\mathbf{(d_2;N_2)\}}$ kulcspárok. Kódolás során a helyes kódolási sorrendet $\mathbf{N_1}$ és $\mathbf{N_2}$ éréke határozza meg. Ha ($\mathbf{N_1 < N_2}$), akkor a helyes kódolási sorrend először $\mathbf{K_1}$ kulccsal, majd azt követően $\mathbf{K_2}$ kulccsal történik. Ellenkező esetben a sorrend fordított. A dekódolási sorrend a kódolási sorrend fordítottja.

2.3.3. Adatrejtés

A szteganográfia nem az üzenet titkosításával, hanem elrejtésével foglalkozik. Fontos, hogy az üzenet létezéséről csak a címzett tudjon. A szteganográfia párja a kriptográfia, ahol a titkosított tartalom létét nem álcázzák, de az eredeti adattartalom csak a rejtjelezési eljárás és a hozzá tartozó rejtjelkulcs birtokában ismerhető meg.

A szteganográfia tipikus példája talán a láthatatlan tinta, amellyel egy másik szöveg sorai közé írják az üzenetet. A megfelelő eljárás alkalmazásával (pl. melegítés, vegyszerek) az írás újra láthatóvá válik.

A szteganográfia előnye a kriptográfiával szemben, hogy az üzenet nem hívja fel magára a figyelmet, de a kettő együttes alkalmazása biztosítja általában, hogy az üzenet titkos maradjon.

A digitális adatok sok lehetőséget kínálnak arra, hogy elrejtsünk valamit valamiben. Ilyenek például a képfájlok is. Mivel nagy mennyiségű adatot hordoznak, ezért a legkisebb helyiértékű bit (least significant bit, LSB) megváltoztatása minimális torzulást eredményez a képen.

Legalkalmasabb formátum talán a BMP, amely tömörítés nélkül tárolja a képet. Például egy TrueColor (24 bites), BMP kép minden képpont leírására 3 bájtot használ. Ezek a vörös, zöld és a kék összetevő intenzitását írják le (RGB). Ha kép mérete (elhagyva a fejlécet): 1024×768×3×8 = 18 Mbit = 2304 kByte, és ha minden képpont RGB komponenseiben alkalmazzuk a legalsó (LSB) biteket, a kép nem változik érzékelhetően. A rejthető adat mennyisége így 1024×768×3×1 = 2,25 Mbit,

azaz = 288 kByte. Ez az eredeti kép 12,5%-a. Ez tekintélyes adatmennyiséget jelent, és a fájlhossz sem változik.

TrueColor (24 bites nem tömörített BMP képfájl felépítése

A fájl három elkülöníthető részből tevődik össze:

- Fájlfejléc (14 bájt). A fájlra vonatkozó alapvető adatokat tárolja;
- Információs fejléc (40 bájt). Az eltárolt kép jellemzőit írja le (felbontás, színmélység, stb.);
- Bittérkép. A kép tényleges tárolási helye, ahol képpontról képpontra jegyzik fel azok színeit.

Adatrejtés TrueColor (24 bites nem tömörített BMP képfájlban

A fejlécek a megfelelő képfájl formátumának azonosíthatóságát szolgálják. Hossza állandó (14+40 byte). A fejlécek meghatározott helyein található bájtok értékei alapján meghatározható a fájlformátum (pl.: BMP), színmélység (pl.: 24 bites TrueColor), tömörítés (pl. nem tömörített). Ezek a legalapvetőbb információk. Hasznos információként egyéb paraméterek mellett meghatározható még példaként a képméret (kép szélessége, magassága pixelben). Ez alapján becsülhető a rejthető bitek mennyisége.

A bittérkép felépítése soronként, a kép aljától felfelé történik. Fontos sajátosság, hogy egy sort leíró bájtok száma osztható kell legyen néggyel. A bittérkép felépítése során ha ez nem teljesül, automatikusan #0 bájtokkal kerül kiegészítésre.

Például, legyen egy 55 pixel széles kép. Ebben az esetben egy sorhoz 3x55, azaz 165 bájt tartozik. Mivel ez nem osztható néggyel, ezért e sorinformáció kiegészítésre kerül további három #0 bájttal (165+3=168, és így (168 mod 4)=0).

Tekintettel arra, hogy ezen #0 bájtok jól meghatározható helyen találhatók a bittérképben, ha ezek legalacsonyabb helyiértékű bitjeit (LSB) is módosítjuk, ez rögtön elárulhatja az adatrejtés tényét. Legegyszerűbb szabály ennek elkerülése érdekében, hogy a bittérkép #0 bájtjait változatlanul hagyjuk. Ennek következménye lehet, hogy a töltelék #0 bájtok mellett a bittérképben található pixel színkomponens intenzitást leíró egyéb #0 bájtok miatt csökken a képfájl kapacitása, de természetes fényképeken ezek előfordulási gyakorisága csekély.

A rejtés színtorzítása a legalacsonyabb helyiértékű bitek (LSB) módosításának hatására csekély, szemmel észrevehetetlen. Az RGB komponensek intenzitásváltozása 1/255-öd része az értékkészletnek [0..255].

Tovább csökkenti a rejtés kimutathatóságát, ha a rejtéshez nem használt RGB komponensek legalacsonyabb helyiértékű bitjeit változatlanul hagyjuk, vagy véletlenszerűen beírt "0" vagy "1" bitekkel „zajosítjuk”.

Összegzés

A szimmetrikus és a nyilvános kulcsú rejtjelezés, valamint az adatrejtés az alapja számos biztonságos kommunikációs protokoll kialakításának. A teljesség igénye nélkül említem meg a digitális aláírás, hibrid titkosítás, stb. kialakítását. Nem mellékes a kulcselosztás problémakörének körbejárása.
Bár ez a programcsomag összességében csak három (a programok illetéktelen felhasználás elleni védelme miatt négy) programot tartalmaz, a következő, alább felsorolt gyakorlati lehetőségeket tartalmazza:

- a gyakorlati tapasztalatokon keresztül akár a „játszva tanulás”, akár irányított, előre kiadott feladatatok végrehajtásán keresztül az elméleti ismeretek gyakorlati elmélyítése;
- a kulcselosztás problémakörének gyakorlati megtapasztalása, a kulcs értékének felismerése;
- az elmélyített ismeretek alapján biztonságos kommunikációs protokollok kialakítása akár problémafelvető kérdés, akár irányított gyakorlati feladat végrehajtása során.

Összességében egy olyan programcsomag készült, mely a megszerzett elméleti ismeretek gyakorlati alkalmazásán keresztül képes az ismeretek elmélyítésére, és a programcsomag alkalmazásán keresztül biztosítja biztonságos kommunikációs protokollok kialakításának megismerését. A programok részletes leírása, bemutatása, a jelen cikk következő folytatásában kerül ismertetésre.

Felhasznált irodalom

[1] http://hu.wikipedia.org/wiki/Polübiosz-négyzet (2014. 05. 24.)
[2] http://hu.wikipedia.org/wiki/RSA-eljárás (2014. 05. 24.)
[3] http://hu.wikipedia.org/wiki/Szteganográfia (2014. 05. 24.)
[4] http://hu.wikipedia.org/wiki/BMP (2014. 05. 24.)
[5] Pándi Erik – Pándi Balázs: Az elektronikus közszolgáltatások nemzeti szabályozó hatóság részéről történő támogatottságának kérdései, Hadtudományi Szemle I: (1) pp. 106-144., Budapest, 2008. HU ISSN 2060-0437

Kerti András – Farkasné Hronyecz Erika: A közfeladatot ellátó szervezetek információs rendszereinek személyi biztonsága

Absztrakt
A szerzők bemutatják a személyi biztonsági kockázatokat.

Abstract
The authors show risk of personal safety.

Bevezetés

Az információbiztonság leggyengébb láncszeme az ember, ezt az állítást ma már senki sem tagadja, szinte közhelyként használjuk, viszont ha ez így van, akkor ez az a szakterület, amely legjobban körülhatárolt és kidolgozott. Sajnos ez nem így van. A jelen közleményemben a közfeladatot ellátó szervezetek információs rendszereinek személyi biztonságának állapotát vizsgálom meg, a vizsgálat végrehajtásához – mint a legjobb nemzetközi gyakorlat eszközét- az ISO/IEC 27002 szabvány személyi biztonságot meghatározó részeit veszem alapul. A cikk során nem vizsgálom az információbiztonsági hatósági feladatokat.
Mielőtt azonban a konkrét vizsgálatot elkezdeném, tisztázni kell két fontos kérdést: Miben különbözik a Közfeladatot ellátó szervezetek és a „civil" cégek információbiztonsága? Valamint mi az információs rendszer?

1. Különbségek

Megállapíthatjuk, hogy a közfeladatot ellátó szervezetek és a más cégek információbiztonságának technikai részletei, a kivitelezés semmiben sem különböznek: mindkét rendszerben szükség van a rosszindulatú kódok elleni védelemre, naplózásra a rendszerelemek fizikai védelmére és a többi jól bevált információbiztonsági tevékenységre. A különbséget a menedzsment megközelítésében látom. Addig, amíg a „civil" cég saját maga határozhatja meg az információvédelem megvalósításának módszerét például a COBBIT, ISO 27001 vagy teljesen saját módszer szerint, a közfeladatot ellátó szervezeteknek jogszabályok és az ezeket alátámasztó államirányítás egyéb jogi eszközei kötelező jelleggel határozzák meg a feladataikat.
Másik kérdés: Mi az az információs rendszer? Az információs rendszer a szervezet feladat eredményes végrehajtása érdekében létrehozott szervezet- és kapcsolatrendszer, amelynek legfontosabb feladata, hogy megfelelő információkkal

lássa el döntéshozásra kijelölt személyeket a döntési mechanizmusának segítése érdekében. Vagyis az információs rendszer nem más, mint a közfeladatot ellátó szervezetek döntési mechanizmusában dolgozó személyek összessége. Azonban ahhoz, ezek az egyének egyének munkájukat az elvárt szinten tudják végrehajtani, szükségük van információ-feldolgozó és tároló-, valamint információt továbbító rendszerekre, eszközökre és kapacitásokra, amelynek üzemeltetéséhez, biztonságának megvalósításához, szintén szükség van különböző szakemberek együttműködésére. Nagyon fontosnak tartom kiemelni, hogy egy információs rendszer nem csak a számítógépes rendszer lehet, információs rendszer lehet a kizárólag papír alapú adathordozót tartalmazó rendszer is!

2. A személyi biztonság kialakításakor érintett állomány

A fenti bekezdésekből láthatjuk, hogy információbiztonsági szempontból az információs rendszerrel kapcsolatba kerülő személyeket alapvetően két csoportra oszthatjuk: a felhasználókra – vagy ahogy a 335/2005 kormányrendelet fogalmaz és a továbbiakban én is ezt a kifejezést alkalmazom: **ügyintézők** -, akiknek a feladata a döntéshozók döntéseinek előkészítése, ezen munkájuk során az információs rendszert csak használják. A másik csoport, akik ehhez a munkához az információs rendszert biztonságos módon üzemeltetik. A felhasználók a szervezet rendeltetése, feladata alapján sokfélék lehetnek, azt azonban, hogy milyen biztonsági szakembereket kell alkalmazni egy közfeladatot ellátó szervezetnél jogszabályok írják elő, amelyet a következő táblázatban foglaltam össze:

Munkakör	A munkakört előíró jogszabály	Megjegyzés
Ügykezelő	335/2005. Kormányrendelet	
Elektronikus információs rendszer biztonságáért felelős személy	2013. évi L. törvény	Azonos lehet a biztonsági vezetővel.
Biztonsági vezető	2009. évi CLV. törvény	Csak akkor, ha szervezet minősített adatot is kezel.
Titkos ügykezelő	90/2010. Kormányrendelet	Csak akkor, ha szervezet minősített adatot is kezel.

Rendszerbiztonsági felügyelő	161/2010. Kormányrendelet	Csak akkor, ha szervezet minősített adatot elektronikus formában is kezel.
Rendszeradminisztrátor	161/2010. Kormányrendelet	Csak akkor, ha szervezet minősített adatot elektronikus formában is kezel.
Rejtjelfelügyelő	161/2010. Kormányrendelet	Csak akkor, ha szervezet minősített adatot is kezel, és rejtjelző eszközt is alkalmaz
Rejtjelző	161/2010. Kormányrendelet	Csak akkor, ha szervezet minősített adatot is kezel, és rejtjelző eszközt is alkalmaz

1. számú táblázat: kötelező foglalkoztatott

3. Az információbiztonság megvalósításának időszakai

A személyi biztonság feladatait, mint a biztonság többi szegmensének feladatait is permanensen az információs rendszer életciklusának teljes idején kell végrehajtani, azonban ezeket a feladatokat három jól elkülöníthető időszakra bonthatjuk: az alkalmazás előtti, az alkalmazás közbeni és az alkalmazás megszűnése kori feladatok.

Az alkalmazás előtti személyi biztonsági feladatok

A személyi biztonsági feladatokat a 27002-s szabvány foglalja össze a legjobban, amely alapján az alkalmazás előtti feladatok célja: „annak biztosítása, hogy az alkalmazottak, a szerződő felek és a használó harmadik fél megértsék felelősségüket és legyenek alkalmasak azokra a feladatokra, amelyekre szánták őket és csökkentsék a lopás, csalás vagy berendezések helytelen használatának kockázatát.”

Feladatok: „A biztonsági felelősségekkel az alkalmazás előtt kell foglalkozni megfelelő munkaköri leírásokban és az alkalmazási feltételekkel megadva. Minden

alkalmazásra jelöltet, a szerződő feleket és a használó harmadik felet megfelelően világítsanak át, különösen érzékeny munkakörökben."
Lássuk csak, mit is jelent ez:
„..megértsék felelősségüket… csökkentsék a lopás, csalás vagy berendezések helytelen használatának kockázatát" biztonság tudatos képzést kell számukra tartani.
„..alkalmasak azokra a feladatokra, amelyekre szánták őket" számomra ez kettő dolgot jelent: Egyrészt legyenek képesek a munkájukhoz tartozó feladatok ellátására, amely nem elsősorban információbiztonsági kérdés, hanem az ügyintéző szakmai felkészültségét jelenti. Miért fontos ez, és miért itt tárgyaljuk? Mert szakmai tapasztalatom az, hogy a legtöbb információbiztonsági probléma a saját feladathoz tartozó rendszerek hiányos ismeretéből adódik. Természetesen ezekkel a feladatokkal az informatikus nem tud mit kezdeni ezeknek az ismereteknek az elsajátítása az ügykezelő feladata, az elsajátítás ellenőrzése pedig a szakmai vezetőjéé. Másrészről pedig –ami már kifejezetten információbiztonsági feladat- legyen szükséges ismerete az általa használt információs rendszerről, annak működéséről.
„Minden alkalmazásra jelöltet… megfelelően világítsanak át, különösen érzékeny munkakörökben." Biztosítani kell, hogy csak megbízható emberek férhessenek hozzá a rendszer elemekhez és az információkhoz.
Összefoglalva az alkalmazás előtti feladatokat: átvilágítás, felkészítés információs rendszer alkalmazására, biztonsági oktatás. Nézzük meg, hogyan intézkedik ezekre a feladatokra a jogalkotó, alapul véve az előző táblázatot és kiegészítve a felhasználókkal:

Munkakör	Intézkedés a(z):		
	átvilágításra	Információs rendszer oktatására	információbiztonsági tudatosság oktatására
Ügykezelő	A szerv vezetője felelős:		
Elektronikus információs rendszer biztonságáért felelős személy	Büntetlen előélet	A törvény a Nemzeti Közszolgálati Egyetem hatáskörébe utalja	
Biztonsági vezető	megfelelő szintű személyi biztonsági tanúsítvány	felsőfokú iskolai végzettség	minősített adatok kezelésének vagy védelmének területén szerzett legalább egy év szakmai gyakorlat

Titkos ügykezelő	megfelelő szintű személyi biztonsági tanúsítvány	legalább középfokú iskolai végzettség	minősített adat védelmére vonatkozó rendelkezések, ismeretéből, gyakorlati alkalmazásából sikeres vizsgát tett
Rendszerbiztonsági felügyelő	megfelelő szintű személyi biztonsági tanúsítvány	bemeneti követelmény nincs	bemeneti követelmény nincs
Rendszeradminisztrátor	megfelelő szintű személyi biztonsági tanúsítvány	bemeneti követelmény nincs	bemeneti követelmény nincs
Rejtjelfelügyelő	megfelelő szintű személyi biztonsági tanúsítvány rejtjel-hozzáférési engedéllyel rendelkezik	nincs?	nincs?
Rejtjelző	megfelelő szintű személyi biztonsági tanúsítvány rejtjel-hozzáférési engedéllyel rendelkezik	az általa üzemeltetendő rejtjelző eszköz biztonságos üzemeltetéséhez szükséges elméleti és gyakorlati ismereteket nyújtó tanfolyamot elvégezte	
Ügyintéző felhasználó	nincs	nincs	nincs

Titkos ügyintéző	megfelelő szintű személyi biztonsági tanúsítvány	nincs	nincs

2. számú táblázat: kiegészített táblázat

A táblázatból látható, hogy a követelményrendszer nem egységes. A jogszabályok feltételezik, hogy az iskolai végzettség megfelelő informatikai ismeretekkel is párosul, minit például a biztonsági vezető és az elektronikus információs rendszer biztonságáért felelős személy esetében a felsőfokú végzettség, illetve a titkos ügykezelő esetében a középfokú végzettség. Tudjuk tapasztalatból, hogy az oktatási rendszerünkben a különböző iskolák különböző mértékben és szinten oktatják az informatikai ismereteket, ezért célszerű lenne ezeket a követelményeket egységesíteni, konkrét, szintenkénti informatikai ismereteket előírni.
Felmerül továbbá az a kérdés, hogy az a kár, amit egy olyan informatikai szakember tud okozni, aki semmilyen aminősített adattal nem rendelkezik összemérhető-e egy minősített adattal való visszaéléssel? Ennek a kérdésnek az eldöntésekor nézzük meg a Jogalkotó véleményét, ami BTK megfelelő paragrafusaiban csúcsosodik ki: Addig amíg **minősített adattal visszaélés** maximális büntethetősége nyolc év, addig az **információs rendszer felhasználásával elkövetett csalás** tíz évig terjedő szabadságvesztéssel büntethető vagyis a jogalkotó szerint is összemérhető a két cselekvés. Kétséges tehát, hogy addig amíg „bizalmas" minősítési szintű adatok ügyintéző által történő feldolgozásához személyi biztonsági tanúsítvány – és ehhez nemzetbiztonsági ellenőrzés- szükséges, addig egy nagy bonyolultságú elektronikus adatfeldolgozó rendszer biztonságáért felelős személynek elég a büntetlen előélet.

Az alkalmazás időszakában elvárt személyi biztonsági feladatok

Szintén a 27002 szabvány alapján nézzük meg, hogy mi a célja az alkalmazás időszakában a személyi biztonsági feladatoknak: „**b**iztosítsák, hogy az alkalmazottak, szerződő felek és a használó harmadik fél tudatában legyenek az információbiztonsági fenyegetéseknek és gondoknak, felelősségüknek, kötelezettségüknek és legyenek felszerelve, hogy támogassák a szervezeti biztonsági politikát rendes munkájuk alatt, és csökkentsék az emberi tévedés kockázatát.
Megfelelő szintű tudatosságot, a biztonsági eljárásokban való képzést és oktatást, és az információ feldolgozó eszközök helyes használatát biztosítsák minden

alkalmazottnak, szerződő félnek és használó harmadik félnek, a lehetséges biztonsági kockázatok legkisebbre szorítása céljából. Létre kell hozni egy hivatalos fegyelmi folyamatot a biztonság megsértésének kezelésére."

A szabvány alapján két dolgot tehetünk: megszervezzük a továbbképzéseket és fegyelmezünk. Azonban a bemeneti feltételek nem csak a tudás szintjén kopnak el, de maga az ember is változhat. Aki a munkakör betöltésekor megbízhatónak számított, lehet, hogy mára már nem az. Ezt a kritériumot a minősített adatokat kezelő rendszerek estében a jogalkotó úgy oldotta meg, hogy a személyi biztonsági tanúsítványt ötévente meg kell hosszabbítani és ennek az alapja az új nemzetbiztonsági ellenőrzés, a büntetlen előélet időszakos vizsgálatára azonban nincs intézkedés.

A továbbképzések rendszere sem egységes. Az elektronikus információs rendszer biztonságáért felelős személy továbbképzésnek tartalma, módszer jogszabályban van rögzítve, biztonsági vezetők éves továbbképzése a Nemzeti Biztonsági Felügyelet feladata, de gyakorlatilag a többi érintett információbiztonsági tudatosságának kialakítása az ellenőrzésére jogosult információbiztonsági szakember feladata.

Ez a rendszer két problémát vet fel: nem egyforma felkészültségű szakemberek különböző szintű felkészítést fognak tartani ezért nem lesz egységes az információbiztonság. Másrészt az információbiztonsági tudatossági felkészítésnek az egyik legfontosabb pillére a bekövetkezett eseményekből levonható következtetések. Ha ezeket a következtetéseket nem országos szinte végezzük el, akkor nagy az esély az incidensek ismétlődésére, ami szintén csökkenti az információbiztonság hatásosságát.

Javaslatom, hogy az mellett, hogy hagyjuk a szervezet információbiztonsági szakembereit a saját szervezetüknél önállóan tevékenykedni, ki kell adni éves szinten azokat a fő kérdéseket, amelyek az elmúlt időszakban különböző problémákat vetettek fel. Saját tapasztalatom azonban az, hogy a legjobban megtartott felkészítő foglakozás is csak részben éri el a célját, ha az nem zárul valamilyen féle számonkéréssel. Ezt a számonkérést a mai technikai fejlettségnél szintén meg lehet oldani központi rendszerben, ezzel is hangsúlyozva a téma komolyságát.

Hivatalos fegyelmi eljárás

Ha valami a közfeladatot ellátó szervek információbiztonságával kapcsolatban ki van dolgozva, az hivatalos fegyelmi folyamat. Ugyanis ha valaki valamilyen kárt okoz az információs rendszerben – ami magában foglalja az információk biztonságának megsértését is - az nem csak a fegyelmi felelősségre vonással néz

szembe, hanem a jog szigorával is. A következő táblázatban összefoglalom, hogy a büntető törvénykönyv és a szabálysértési törvény milyen maximális büntetésekkel fenyegeti az információs rendszert nem megfelelő módon használó személyeket:

Büntetni rendelt cselekmény	Maximális büntetés
Minősített adattal visszaélés	8 év
Információs rendszer felhasználásával elkövetett csalás	10 év
A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény	5 év
Információs rendszer vagy adat megsértése	8 év
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	2 év
Minősített adat biztonságának megsértése	szabálysértési elzárás hatvan nap

3. számú táblázat: büntetési tételek

Alkalmazás megszűnésének feladatai

Alkalmazás megszűnésének célja szintén a szabvány alapján: „annak biztosítása, hogy az alkalmazottak, a szerződő felek és a használó harmadik fél rendezett módon hagyják el a szervezetet vagy változtassanak alkalmazást.
A felelősségeket úgy alakítsák ki, hogy biztosítsák, hogy az alkalmazottak, a szerződő felek vagy a használó harmadik fél távozását a szervezetből úgy intézzék, hogy az összes berendezés visszaküldése és minden hozzáférési jog visszavonása a szervezetben befejeződjék.”
Véleményünk szerint ez a legkevésbé szabályozott terület. Konkrét előírásokat csak a 90/2010. Kormányrendelet tartalmaz a vezetővel, a biztonsági vezetővel, a titkos ügykezelővel és a felhasználóval kapcsolatban. Az információs rendszer többi szereplőjének elszámoltatásával kapcsolatban a feladatok meghatározása a vezető, illetve a biztonsági menedzsment feladata marad.

Összegzés

A közfeladatot ellátó szervezetek információbiztonságának minden területén, így a személyi biztonság megvalósításakor is, szükség az egységes szemlélet kialakítására,

attól függetlenül, hogy a szervezetek minősített vagy nem minősített adatokat, papír vagy elektronikus adathordozókon kezelnek.
Az egységes szemlélet kialakításának alapja a kárelvűség lehet, azaz annak vizsgálata, hogy az adott adatkezelő rendszer biztonságának megsértése milyen kárt okozhat az államnak. A személyi biztonság az egyik legfontosabb feladata az információbiztonság tudatosság kialakítása, amelynek az alappillére a továbbképzési rendszer. A továbbképzési rendszer során azokat a felkészítési kérdéseket, amelyek a képzési ciklusban országos szinten problémákat jelentettek bele kellene építeni a tananyagba, ez azonban csak úgy lehetséges, ha az információbiztonsági hatóságok közösen kidolgoznák, és a továbbképzést végrehajtók számára hozzáférhetővé tennék a tapasztalataikat.

Felhasznált irodalom

[1] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről
[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[3] 2009. évi CLV. törvény a minősített adat védelméről
[4] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről
[5] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól
[6] 27001 szabvány
[7] 2012. évi C. törvény a Büntető Törvénykönyvről
[8] 2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről
[9] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
[10] Pándi Erik – Pándi Balázs: Az elektronikus közszolgáltatások nemzeti szabályozó hatóság részéről történő támogatottságának kérdései, Hadtudományi Szemle I: (1) pp. 106-144., Budapest, 2008. HU ISSN 2060-0437

Pándi, Erik – Pándi, Balázs: Security structure of organizations

Abstract
The steps taken for security may come from two directions. In this publication we provide a comprehensive picture of the structure of NATO information facilities and their brief history, as well as the internal structure of the organizations of the Hungarian Defence Forces.

Absztrakt
A biztonság érdekében tett lépések két irányból érkezhetnek. Jelen közleményünkben átfogó képet nyújtunk a NATO információs létesítményeinek a struktúrájáról és rövid történetéről, valamint a Magyar Honvédség szerveinek egymásra épüléséről.

Introduction

A variety of organizations, companies had reached an agreement to share their experiences in this field, so that specific attack methods can not be applied more than once, once the response mechanism has been developped somewhere, in order to develop an effective information security system. To enable the secure exchange of information a Cross-Domain Solutions (CDS) procedure has been developed, which allows each party to use their own protokolls to share information with other parties. A uniform system is used which monitors data traffic and enables data sharing between the various elements so that it is inaccessible for third parties. This solution is used for linking military communications systems, but in the civilian sector it's also used by major companies to eliminate industrial espionage.

1. NATO Solutions

The association recognizes that the war is not only based on the ground, water and air, but also introduced a new battlefield: the cyberspace. In this area, there are still plenty of undiscovered opportunities: the intention of the attackers is to discover increasingly newer vulnerabilites and to reach their goal by exploiting these.
NATO has incorporated this into their Strategic Concept as a priority, and the recent summits revisited the issue as a point to discuss. Historically NATO has always defended it's IT systems, but as long as there was no major threat in this

area, defense remained at a basic level. The first time when the topic got on the NATO summit agenda was in Prague 2002, and when it became clear that this is a crucial topic to the alliance's future and further measures are needed to create a stronger defense, it was discussed again at 2006 meeting in Riga. Then came the turning point in the views of the alliance: In 2007, a NATO member, Estonia, suffered a cyber-attack that paralyzed the entire infrastructure.

The same year the defense ministers of the Member States got together and adopted a decision to set up a Cyber Security Policy, which they issued in 2008. The cyber activity at the summer of this year used in the Russian-Georgian conflict highlighted that this area should be rightfully called a battlefield, and should be included in the concept of war and the planning processes of operations. The Lisbon Summit in 2010 was another milestone, as the new strategic concept was created here. It declared the establishment of a new, more detailed cyber-defense policy, which also includes the response plan for its implementation. The document was adopted by the defense ministers in June 2011, and it clarifies the risks and the responses to be given to rapidly evolving technological changes. The defense development process began to incorporate the important elements of the area in April next year. In May the same year, at the Chicago summit the leaders of the alliance states have taken further steps to strengthen cyber-defense: centralizing the networks of the alliance, and expanding and enhancing the NATO Computer Incident Response Capability (NCIRC) has led to improved security. The NATO Communications and Information Agency (NCIA) began its operation in July. In February the same year the development of new policy guidelines begun, which was signed at Wales in September. The latest enhanced guidelines, which include an updated response plan were adopted by delegates from the member states at the Welsh Summit held in September 2014. It identifies cyber-security as one of the main points within the framework of collective defense.

In addition, it states that the alliance complies with international laws in cyberspace, and lays the foundation for cooperation between NATO various industries. The agreement emphasizes the importance of continuous control over this area, processes supporting alliance forces, and involving the analysis of battlefield events in operational planning. It identifies the enhancement of readiness, and performing training, and training exercises as an important task, encourages the cooperation with member states and international organizations. By strengthening such relations a defense system based on information exchange between different sectors and organizations can be created. NATO regards the

European Union and the United Nations organization as a major partner. Great emphasis is placed on information flow and processing experience - not only within the alliance – so that recovery from cyber-attacks, prevention and minimization of damage can take place as quickly as possible. Part of the agreement was to develop a response plan that includes the implementation deadlines.

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

Situational awareness

The strategic level of situational awareness implemented by the Allied Command Operations (ACO). This institution has sufficient information to be able to develop long-term plans, which are needed to perceive future threats. Commands subordinate to ACO, such as NATO Allied Joint Force Command Naples (JFC Naples) and the Communications and Information Systems Group (CIS) are responsible for the operational level. Their main task is to analyze the weaknesses of networks and systems – if they have a backup power source, components of the system are properly ventilated and if the employees are appropriately trained. The tactical level is provided by the NATO Communication and Information Agency. It usually uses open-source information provided by software development or anti-virus development companies. These companies often offer a configurations and upgrades suitable for the tactical level. The short term the goal is to apply the widest possible range of products in combination, providing sufficient information for governing bodies to make the appropriate decisions.

Planning

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

Exercises

Exercises are usually designed on the basis of the above scenarios. These are used to assess the preparedness of the troops and determine those areas that still need improvement. There are two kinds of exercises are organized for cyber-security personnel. One is organized by ACT jointly with subordinate commands. These

involve larger scale, extensive simulations that train personnel to perform their tasks within challenging circumstances, in cooperation with other NATO organizations. Another group of exercises only takes place in cyberspace. In these there's more emphasis on tactical level tasks. Such is the annually held Cyber Coalition exercise, which our country helped to organize through the National Security Authority for many years, but this year for the first time experts of the Ministry of Defense also play a role in in the simulations, based on 2013 observer experience.

Continuity

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

2. Domestic tasks

Organizations in the spirit of collective defense providing cyber-security consider the implementation of network security as the task of individual NATO states. The alliance only imposes standards or guidelines on the member states, so that they are always up to date. NATO is responsible for protecting its own networks. It's the responsibility of the NATO Communications and Information Agency to establish and maintain most parts of cyber security systems, but works closely with the Strategic Command, particularly the Allied Command Operations, so that NATOs' cyber-defense is continuously up-to-date and impenetrable. Thanks to the NCIA, the NATO Computer Incident Response Capability (NCIRC) has reached full readiness last year, which is responsible for the security of 51 alliance installations, became part of the process of defense planning, and played a role in the organization and implementation of the yearly Cyber Coalition exercise.
The NCIRC Technical Centre (Technical Centre) is located Mons Belgium, this institution is responsible for technical support of cyber-defense within in NATO, so it plays a key role in responding to cyber-attacks. Its' main tasks is to respond to and report incidents, and to provide information and experience on attacks to end-users and organizations monitoring system-security. The most important role in the field of research played by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), which was set up after the 2007 attack paralyzed Estonia in 2008. As a result of the attack significant investments have been made in the country to develop cyber-defense, so the facility opened its doors in the most

appropriate place, the Estonian capital Tallinn. The goal of the center is to preserve the cooperation, information exchange within the nations of the alliance and to increase capabilities in this field. It tries to reach its' goals by organizing joint exercises, legal and professional conferences and various trainings. To support these they've gathered a group of experts from various NATO member states, including Hungary. They're research results provide the basis of trainings, so that the attendees can learn from an authentic source.
Since NATO does not provide the cyber-defense of individual member states, it also became the task of Hungarian Defense Forces to create their own defense system. In Hungary the National Security Authority (NSA) that operates as part of the Ministry of Interior and the Ministry of Defense is responsible for the national level of military cyber-security. The responsibility of the Ministry is to create the cyber-defense installations of organizations, to control their operation through laws, and to operate the Military National Security Service. While the NSA accredits and oversees the operations of various organizations. The task of the General Staff is planning on the level of the Hungarian Defense Forces, a specific command of this is the Communication and IT and Cyber-Defense Command.

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

of a local security management if a large amount of classified information is handled by the organization.

Summary

In the world of IT the issue of security is constantly changing and increasingly newer trends dictate the direction of change. Keeping track of this constantly changing challenge is hard even for IT security specialists, not to mention average end-users.
It is especially important that not only should the software be always up to date, but also that the users follow the kind of challenges they can encounter on the web and how they can overcome them, and if they discover a new threat, they know who to contact and where they can share their experience. The preparedness of personnel in leading positions in this area is crucial. The application of appropriate security measures is especially important in the military, and also to be familiar with not only our own countries system but also the hierarchy formed by allied forces including their installations and the devices managing them.

References

[1] Phil Breedlove: Attacks from Cyberspace....NATO's newest and potentially biggest threat, http://www.aco.nato.int/saceur2013/blog/attacks-from-cyberspacenatos-newest-and-potentially-biggest-threat.aspx, hozzáférés dátuma: 2014.10.05.
[2] http://www.tempest.hu/index.php?option=com_content&view=article&id=65:mi-is-az-a-tempest-&catid=11:cikk&Itemid=1, hozzáférés dátuma: 2014.09.30.
[3] http://www.nbf.hu/tempestmer.html, hozzáférés dátuma: 2014. 10. 10.
[4] http://www.crossdomainsolutions.com/cyber-crime/, 2014.10.17.
[5] Khawaja Faisal: Global State of Information Security & Standards, PITB - Information Security Conference 2013. 03. 12., https://www.youtube.com/watch?v=ZvukDyve1Ds
[6] Kate Murphy: Web Photos That Reveal Secrets, Like Where You Live, The New York Times, 2010.08.11., http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html
[7] brahambence: Így lopták el a celebek fényképeit az iCloud fiókjukból, http://imagazin.hu/icloud-fiokjukbol-loptak-el-celebek-fenykepeit/, 2014.09.01.
[8] Lieutenant Commander Jim Maher: Warning: Information is Everywhere, http://www.act.nato.int/article-2014-1-13, 2014.04.06.

[9] Microsoft Digital Crimes Unit & IDC & NUS: The Link Between Pirated Software and Cybersecurity Breaches, http://www.play-it-safe.net/, hozzáférés dátuma: 2014.11.10.
[10] WordPress: SaferInternet, https://saferinternet.hu, 2013, hozzáférés dátuma: 2014.10.10.
[11] http://www.nato.int/cps/en/natohq/topics_78170.htm, hozzáférés dátuma: 2014.10.30.
[12] Col. Rizwan Ali: On cyber defence, The Three Swords Magazine, 26/2014, 32. oldal
[13] Kerti András: Az információbiztonsági kockázatkezelés oktatásának buktatói, Kommunikáció 2013, ISBN 978-615-5305-16-0, Nemzeti Közszolgálati Egyetem, 53-60. oldal, Budapest, 2013.
[14] Keri András – Pándi Erik – Töreki Ákos: A vezetési és információs rendszerek elméleti megközelítése, Kommunikáció 2010., ISBN 978-963-7060-21-2, ZMNE, 2010., 39-49. oldal
[15] Kerti András – Pándi Balázs – Rajnai Zoltán: Structure of the command and information system, Hadmérnök 4/3., ISSN 1788-1919, ZMNE, 2009., 303-309. oldal

Nagy Balázs: Információmenedzsment

Absztrakt
Jelen mű egyfajta áttekintést ad az információmenedzsment jelentőségéről. Az üzleti élet minden egyes szereplője tisztában van az információ jelentőségéről, mint egyfajta befolyás eszközéről egyes személyek és szervezetek felett. A tudás hatalom. Az információmenedzsment egy hatékony rendszer az információáramlás kontroll alatt tartására és a döntés előkészítéshez szükséges adatok gyorsabb és pontosabb tálalására. Ebben a rendszerben az adatbázisok jelentős szerepet töltenek be. Válogatott információs csomagokként vannak jelen, mellyel a keresési idő jelentősen lerövidíthető. A keresési láncban az idő egy kulcselem. A technikai robbanásnak köszönhetően bárki számára könnyen elérhetőek az információs bázisok. A kérdés, hogy ki tudja gyorsabban és pontosabban szolgáltatni a megfelelő információkat.
Az adatbázisok és információs rendszerek, mint például a Big Data könnyebbé teheti életünket. Egy jó példa e rendszerekre a Smart City rendszer, mely egy város infrastrukturális rendszerének kontrollját is elláthatja. Ezáltal könnyebbé és kényelmesebbé teheti a benne élő emberek életét. A kulcs elem itt is a hozzá adott emberi tudás. Hatalmas az igény e rendszerekre, mint a privát mind az üzleti életben. Ezen rendszerek fejlődése jelentheti a megoldást e célok elérésében.Jelen cikk összefoglalja a fukusimai atomerőműben történteket.

Abstract
This article gives an overwiev of the databeses importance in the information management system. Everyone in the business life knows that who owns the information owns the leverage that can influence other people or corporations. Knowledge is power. The information management system is an effective way the take the information flow under control and provide faster and more punctual answers for decisions. Databases are an important assests in information management. They store sorted informations which can narrow the time down by each searching prucedure. Time is one key element in the searching chain. Due to our technical bomb everyone can access to a huge amount of infromation. The question is who can sort it and provide it faster.
Databases and information systems such as the Big Data can make our life easier. A good example can be the Smart City system which could control each city infrasturctural system. Due to that it can make people life easer and more convenient. A key element in those systems are the human knowledge. There is a huge amount of need for those systems which makes our personal life and business

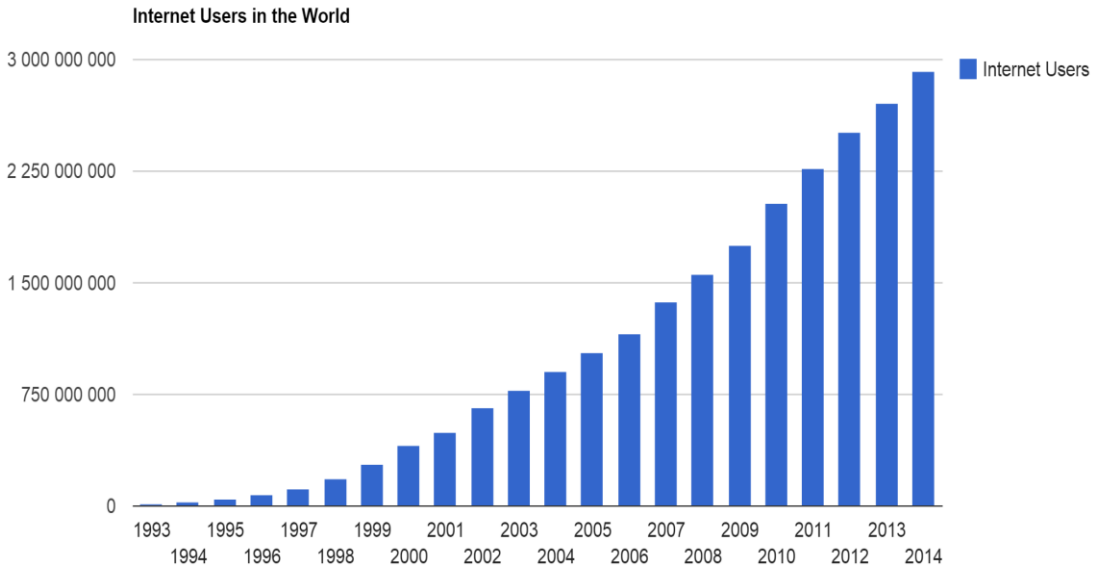
more confortable and effective. The development of these system can achieve the wanted goals.

Bevezetés

Az információ jelentősége a XX. század végére kiemelkedő jelentőséget kapott, szerepe és „tömege" tovább növekszik az egyre komplexebb társadalmunkban. Az információmenedzsment területe széles körben és szerteágazó területen realizálható. A döntés előkészítés folyamatában jelentős szerepe van. Az egyes folyamatok teljes életciklusánál hasznosítható. A technológiák ugrásszerű fejlődésének, forradalmának köszönhetően alakulhatott ki a jelenkor információs társadalma.

1. Adatok menedzselése

E társadalom hatékonyságának mércéje függ az információ koordinált áramlásától és időbeni gyorsaságától. A megnövekedett információmennyiség (adattömeg) kezeléséhez nélkülözhetetlenül szükségesség vált az információk helyes menedzselése. Ennek jelentősége a 80-as évek végére, 90-es évek elejére tehető, ugyanis az internet használat ekkor nyert jelentősebb mértékben teret magának. A következő ábrák az internet használók növekedését és eloszlását szemlélteti:



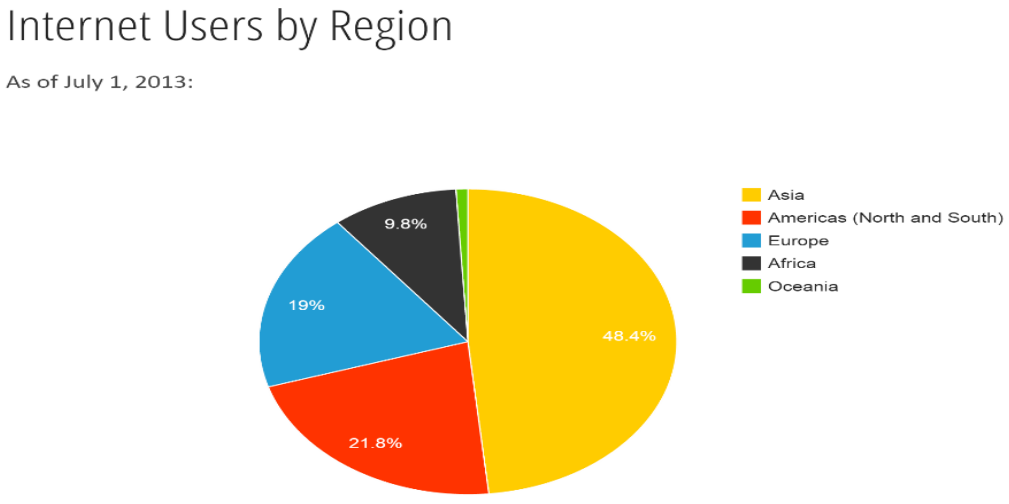
1. számú ábra: Internet felhasználók számának növekedése (grafikon)
(forrás: http://www.internetlivestats.com/internet-users/)

Year (July 1)	Internet Users	Users Growth	World Population	Population Growth	Penetration (% of Pop. with Internet)
2014*	**2,925,249,355**	7.9%	7,243,784,121	1.14%	**40.4%**
2013	**2,712,239,573**	8.0%	7,162,119,430	1.16%	**37.9%**
2012	**2,511,615,523**	10.5%	7,080,072,420	1.17%	**35.5%**
2011	**2,272,463,038**	11.7%	6,997,998,760	1.18%	**32.5%**
2010	**2,034,259,368**	16.1%	6,916,183,480	1.19%	**29.4%**
2009	**1,752,333,178**	12.2%	6,834,721,930	1.20%	**25.6%**
2008	**1,562,067,594**	13.8%	6,753,649,230	1.21%	**23.1%**
2007	**1,373,040,542**	18.6%	6,673,105,940	1.21%	**20.6%**
2006	**1,157,500,065**	12.4%	6,593,227,980	1.21%	**17.6%**
2005	**1,029,717,906**	13.1%	6,514,094,610	1.22%	**15.8%**
2004	**910,060,180**	16.9%	6,435,705,600	1.22%	**14.1%**
2003	**778,555,680**	17.5%	6,357,991,750	1.23%	**12.2%**
2002	**662,663,600**	32.4%	6,280,853,820	1.24%	**10.6%**
2001	**500,609,240**	21.1%	6,204,147,030	1.25%	**8.1%**
2000	**413,425,190**	47.2%	6,127,700,430	1.26%	**6.7%**
1999	**280,866,670**	49.4%	6,051,478,010	1.27%	**4.6%**
1998	**188,023,930**	55.7%	5,975,303,660	1.30%	**3.1%**
1997	**120,758,310**	56.0%	5,898,688,340	1.33%	**2.0%**
1996	**77,433,860**	72.7%	5,821,016,750	1.38%	**1.3%**
1995	**44,838,900**	76.2%	5,741,822,410	1.43%	**0.8%**
1994	**25,454,590**	79.7%	5,661,086,350	1.47%	**0.4%**
1993	**14,161,570**		5,578,865,110		**0.3%**

* estimate for July 1, 2014

Source: ***Internet Live Stats*** (elaboration of data by *International Telecommunication Union (ITU)* and *United Nations Population Division*)

2. számú ábra: az Internet felhasználók számának növekedése



3. számú ábra: Az Internet felhasználók területi eloszlása

Ezen számokon keresztül érezhetővé válik az az információs tömeg mely nap, mint nap áramlik az interneten. Az összefüggés az információmenedzsment és a felhasználók növekedése között az információs mennyiséghez való hozzáférés és annak növekedése. Menedzsment lényege a nagy mennyiségű információk célirányos keresése, majd elemzés értékelése a döntés-előkészítő folyamatok támogatására.
Íme, pár fogalmi meghatározás, a témában jártás néhány szakembertől:
„Az információmenedzsment bármely szervezetben lévő információs források hatékony kezelésével és összehangolásával foglalkozik.” /Mikulás Gábor/
„A szervezet (belső/külső) információs erőforrásainak menedzselésével foglalkozik, biztosítva az elvárható hatékonyságot az információs folyamatokban. Az IM szerep lényege és specifikuma a fenti követelmények alapján a hatékony vállalati, szervezeti információáramlás menedzselése” /Dobay Péter/
Irene Wormell megfogalmazása alapján az információmenedzsment célja „az információs erőforrások hatékony menedzselése és a szervezet képessé tétele arra, hogy gondoskodni tudjon mindarról, amire szüksége van az információs rendszerek alkalmazása, az információhoz való hozzáférés és a végfelhasználók megfelelő segítése tekintetében”
Az információmenedzsment körüli megfogalmazásokból kiderül, hogy e tevékenység az információk gyűjtésében, feldolgozásában nyújt kiemelkedő segítséget. Az egyes szervezetek eredményes működéséhez szükséges elemzett/értékelt adatokat, információkat biztosítja a hírigényeknek alapján, melyeket a szervezet megfelelő részéhez továbbítja és tárolja.
Az eredményes működéshez a teljes életciklusa alatt meg kell valósulni az információk bizalmasságának, sértetlenségének és rendelkezésre állásának. Az információmenedzsment feladatai közé tartoznak tehát a megfelelő minőségű információk gyűjtése, feldolgozása, értékelése, tárolása, visszakeresése, a hozzáférhetőség biztosítása.

2. Adatbázisok

Az információs rendszerek a régi támogató jelleghez képest mára már biztosítják a koncepcionális elképzelések racionálisabb, effektívebb megvalósítását, a folyamatos üzletmentet (Business Continuity Plan – BCP), a piac állandó és gyors változásaira történő azonnali reagáló képességet.
„Az adatbázis azonos minőségű, többnyire strukturált adatok összessége, amelyet egy tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel. Az

adatbázisok célja adatok megbízható, hosszútávon tartós (perzisztens) tárolása, és viszonylag gyors visszakereshetőségének biztosítása."[6]
Az adatbázisok egyes alkalmazási területei:

- Bankszektor;
- Légi társaságok;
- Egyetemek;
- Bankkártya tranzakciók;
- Telekommunikáció;
- Gazdaság;
- Értékesítés;
- Gyártástechnológia;
- Emberi erőforrás.

Az adatbázisok a szervezetek belső működésének támogatására szolgálnak, melyeken keresztül kapcsolatot tarthatnak és adatot gyűjthetnek az ügyfeleikről, a tevékenységre szabott adatok adminisztratív tárolásával.
A technológia és a felhasználók robbanásszerű fejlődésével és növekedésével az adatbázisok mérete és száma is egyre bővült. A Big Data néven ismert kifejezés még nem rendelkezik pontos fogalmi meghatározással, viszont jelentése jól körülhatárolható. A Big Data egy hatalmas adatbázis, melynek hatalmas szerteágazó mennyiségét és feldolgozását különféle hálózatokon lévő gépek és emberek közösen állítanak elő. E hatalmas információmennyiség feldolgozására új módszerek kellett kidolgozni.
Az egyes adatbázisokat a következő paraméterek alapján lehet jellemezni:

- Méret;
- Szerteágazóság;
- Sebesség;
- Változékonyság;
- Megbízhatóság;
- Komplexitás.

Egy 2014. évi felmérés a következő listát állította fel a világ 10 legnagyobb adatbázisait birtokló szervezetek közül[7]:

- Klímaadatok Világközpontja (WDCC);
- Az USA Nemzeti Energiakutató Központja;

[6] http://hu.wikipedia.org/wiki/Adatb%C3%A1zis
[7] http://pandidba.blogspot.hu/2014/01/top-10-largest-databases-in-world.html

- AT&T;
- Google;
- Sprint;
- LexisNexis;
- Youtube;
- Amazon;
- CIA;
- Kongresszusi Könyvtár (USA).

Az adatbázisok implementálásának és felhasználásának a segítéségével az egyes városok, különösen a nagy lélekszámú települések (metropolis) „életét" könnyíthetjük meg. Gondoljunk csak a parkolási rendszerre, a közlekedési zavarokból adódó torlódásokra és egyéb normál működést akadályozó tényezőkre, melyek kontrol alatt tartásával ezek minimalizálhatók lennének nem beszélve a költségcsökkentő hatásairól. Ezen elképzelés alapján született meg a Smart City. Ezt az alkalmazást a városi élet áramlására és egy valós idejű azonnali reagáló képességre fejlesztették ki. „Az okos, vagy élhetőbb város olyan települést takar, mely a rendelkezésre álló technológiai lehetőségeket (elsősorban az információs és kommunikációs technológiát) olyan innovatív módon használja fel, amely elősegíti egy jobb, diverzifikáltabb és fenntarthatóbb városi környezet kialakítását."[8]

Összegzés

A tendenciák, valamint a statisztikai kimutatások szerint az információk mennyisége a jövőben is jelentős méretekben bővülni fog. Az adatbázisok által nyújtott rendszerezett információmennyiség, valamint a szofisztikált keresőprogramok segítségével a döntés-előkészítési folyamatok látványosan megkönnyíthetők. Az információmenedzsment folyamatába beágyazott adatbázisok segítségével a hibázási lehetőség, valamint az információáramlási idő minimalizálható, a produktivitás maximalizálása mellett. A jövőbeni technológia fejlődésével az újabb és újabb keresőmotorok megjelenésével, valamint az adatbázisok bővülésével megfelelő védelmi rendszabályok mellett a döntés-előkészítő folyamatok hatékonysága növelhető lesz.

[8] IBM: „Smart cities" tanulmány, MTA Regionális Kutatások Központja Nyugat-magyarországi Tudományos Intézet, Győr, 2011. május

Felhasznált irodalom

[1] Dobay Péter: Vállalati információmenedzsment, Nemzeti tankönyvkiadó, 1997
[2] Blaise Cronin: Az információmenedzsment alapjai, TMT, 38. évf., 1991. 5/6. sz.
http://infolab.stanford.edu/~ullman/dscb/ch1.pdf
[3] Mikulás Gábor: Menedzsment, Nyíregyháza: "Szabolcs-Szatmár-Bereg Megyyei Könyvtárak" Egyesülés, 1999.
[4] Viktor Mayer-Schönberger, Kenneth Cukier: Big Data, HVG Könyvek, 2014
http://www.internetlivestats.com/internet-users/
[5] IBM: „Smart cities" tanulmány, MTA Regionális Kutatások Központja Nyugat-magyarországi Tudományos Intézet, Győr, 2011. Május
[6] Pándi Erik – Pándi Balázs: Az elektronikus közszolgáltatások nemzeti szabályozó hatóság részéről történő támogatottságának kérdései, Hadtudományi Szemle I: (1) pp. 106-144., Budapest, 2008. HU ISSN 2060-0437
[7] Pándi Erik: A hazai zártcélú hálózatok szerepének átalakulása az elektronikus közigazgatási szolgáltatások bevezetése és kiterjesztése folyamatában Hadmérnök pp. 92-106, Budapest, 2007. ISSN 1788-1919
[8] Kerti András: Az információbiztonsági kockázatkezelés oktatásának buktatói, Kommunikáció 2013, ISBN 978-615-5305-16-0, Nemzeti Közszolgálati Egyetem, 53-60. oldal, Budapest, 2013.
[9] Keri András – Pándi Erik – Töreki Ákos: A vezetési és információs rendszerek elméleti megközelítése, Kommunikáció 2010., ISBN 978-963-7060-21-2, ZMNE, 2010., 39-49. oldal
[10] Kerti András – Pándi Balázs – Rajnai Zoltán: Structure of the command and information system, Hadmérnök 4/3., ISSN 1788-1919, ZMNE, 2009., 303-309. oldal

Sipos, Zoltán – Pándi, Erik: What is cyber security?

Abstract
The present study is using concrete cyber events to present the cyber security and why we have to join the global forces against the cyber attacks. We can see the through the examples that this is a global issue that can concern anybody. It is strongly connected to the 21st century and if we don't pay attention, we may encounter serious problems and damages in the future.

Absztrakt
Jelen cikk a kibertámadások és -védelem témakörében kíván információkat megosztani.

Introduction

The objective of the present study consists of presenting the cyber security and why it is important to handle it properly in the fast 21st century. It is a global threat that may threaten both the individuals and nations if we do not make the necessary steps. The Internet is important for the modern people for many reasons. An average user spends 9 hours / day[9] before the computer and the majority of this time is used for Internet browsing. It is worth considering who is sharing what about himself in the worldwide web because these data can also be sources of abuse. The cyber security includes the protection of the information and the used systems. Referring to ITU-T X 1205[10]: „The cyber security is a collection of cyber security tools, directives, security concepts, security guarantees, risk analysis methods, actions, training, practices that may be used for defence to protect the cyber space, the organisations and the users. The organisations and the users include the IT tools, people, infrastructures, applications, services, telecommunication systems and the sent/received information in the IT environment. The cyber security tries to assure the security features and sustain them for the proper assurance of the assets of the organisation and the users in the cyber space." „The cyber space means the group of the globally interconnected,

[9]The Independent – We now spend more time in front of a screen than in bed, Ofcom study shows http://www.independent.co.uk/life-style/gadgets-and-tech/news/we-now-spend-more-time-in-front-of-a-screen-than-in-bed-ofcom-study-shows-9652631.html (Downloaded: 08/11/2015)
[10] International Telecommunication Union – Overview of cybersecurity http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Downloaded: 08/11/2015)

decentralised, increasing electronic IT systems and the social and economic processes appearing as data and information through these systems."[11]

2. The importance of cyber security

The importance of the cyber security can be proved well with the latest incident that took place in May, 2015. A supposedly Islamic fanatic attacked the website of the Óbuda University[12]. Those who triy to access the university's Internet platform, encountered a video[13] and a message in English. The IT experts of the university tracked down the hacker's IP address and it seemed it was an attack executed by the ISIS. The number of the crimes committed in the cyber space keeps increasing and the events similar to the Óbuda University case is among the smallest. The hackers are not easy to be monitored and they are anonymous. The result is they can act without consequences. The spying, Internet-based money frauds, destruction or disturbing of business systems are among the serious acts. „There is an infected website for every minute at an average company. Every ninth minute there is a risky application. Those using IT systems have to be prepared for facing the danger."[14]
Because of the increasing threatening and the sophisticated attacks the quick steps are important. There are many thousands of contaminated websites appearing every day and there are several hundreds of intrusions offending the average naive users.

[11] The 1139/2013. (III.21) Government decree on the cyber security strategy of Hungary http://www.mysec.hu/download/MK2013_47_M_N_Kiberbiztonsagi_Stratagiaja.pdf (Downloaded: 08/11/2015)
[12] MNO: Islamists may have attacked the website of the Óbuda University http://mno.hu/belfold/iszlamistak-tamadhattak-meg-az-obudai-egyetem-honlapjat-1286998 (Downloaded: 07/25/2015)
[13] Source: youtube.com https://www.youtube.com/watch?v=zcZY401fpP4&feature=player_detailpage (Downloaded: 0/25/2015)
[14] Mihály Zala (chairman, National Security Supervision): Visible and invisible wars – or the threats of cyber space, https://www.youtube.com/watch?v=lw-Z_tHYFgk (Downloaded: 08/11/2015)

3. Reviewing the conflicts of the earlier years

The NATO bombing in Yugoslavia in 1999 can be considered as one of the first cyber war events[15]

After the bombing there were DDoS[16] attacks against the NATO websites. In this case the Yugoslavian army notified its soldiers about the expectable air strikes through data that were collected electronically. They did not manage to get confidential information but they displayed their political messages to several government sites.

Russia launched a cyber war against Estonia"[17]

This was uttered by Jaak Aaviksoo – Estonian defence minister who accused the Russian government that it launched cyber war against the country's websites and through this it is endangering the security of Estonia. At the beginning of the attacks against the website they managed to identify the IP addresses that belonged to Russian government offices but the websites were attacked from more than 1 million computers from all over the world. In April, 2007 there were disturbances in Tallinn during the removal of a WW2 Soviet monument.[18] Then there were regular attacks against the Estonian state administration through the Internet that aimed mostly at hindering the average users in having access to the governmental websites. The centres that manage the country's internet traffic performed several forced stopping because of the data traffic that was almost thousand times bigger than the normal. The system could not handle this huge burden, in this way the banking and financial systems paralysed respectively functioned with interruptions.[19] The SEB Eesti Uhisbank that is Estonia's second

[15] Gergely Szentgáli – Development of the NATO's cyber protection politics http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (Downloaded: 08/01/2015)

[16] Distributed Denial of Service (DDoS) – overstressing attacks

[17] Index.hu – Young Russians launched the Russian-Estonian cyber war http://index.hu/tech/net/2009/03/12/ifjuoroszok_inditottak_az_orosz-eszt_kiberhaborut_/ (Downloaded: 08/10/2015)

[18] Péter Bányász – Ákos Orbók – The NATO's cyber protection politics and the protection of the critical infrastructure in perspective of the social media http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf (Downloaded: 08/07/2015)

[19] Lajos Muha – Cyber war in connection with the Russian-Estonian relationship https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCIQFjAAahUKEwiftfe7_J3HAhXKVRQKHWgpAJw&url=https%3A%2F%2Fhacktivity.com%2Fhu%2Fletoltesek%2Farchivum%2F17&ei=DVDIVd_6DcqrUejSgOAJ&usg=AFQjCNF5I0JqbfgaS9kRv3f3lpMLxTm0nA&bvm=bv.99804247,d.d24&cad=rja (Downloaded: 08/07/2015)

biggest bank, had to suspend its service that assured the access to the foreign bank-systems because of the ongoing Internet attacks. According to the report of another Estonian bank, the Hansabank suffered a traffic loss of more than one million dollar.[20] Due to the Estonian events the NATO announced to investigate the situation but it did not categorise it as a military action. Earlier the Estonian ministry of foreign affairs, Urmas Paet had already accused Russia telling that she attacks Estonia psychologically and physically[21].

Quite recently even Ukraine has faced several negative impacts.

Modification of border, rioting and bloodshed. There is a reason, too, beyond all these that do not require shots but they may also have huge impact on the society. During the DDoS attacks there were communication disturbances and miscommunication that troubled the country.[22] According to the announcement of the BAE System[23] there were 22 computer attacks in 2014 against the Ukrainian systems. These actions were committed by real professionals. The BAE did not determine who is behind the attacks but mentioned that Russian interests may be in the background. This can be concluded from the fact that the coding of the virus was in Russian and the hackers left a logo that can be tracked down to the logo that appeared during the attacks that were committed against the American bases in 2008.

It is worth mentioning a case from year 2008 that concerned the Baku-Tbilisi-Ceyhan[24]

oil pipeline, causing a loss of export income of about USD 1 billion. Before the explosion the system did not signal any alarm and the cameras did not record anything in connection with the break of the fire. During the catastrophe 30 thousand of barrels of oil were spilt, harming the nature. It is assumed that hackers

[20] Prof. Dr. László Kovács - colonel – Security politics http://eiv.uni-nke.hu/uploads/media_items/biztonsagpolitika.original.pdf (Downloaded: 08/07/2015)

[21] Lajos Muha – Cyber war in connection with the Russian-Estonian relationship /Hactivity https://www.youtube.com/watch?v=lkuBtq_jCeo (Downloaded: 08/07/2015)

[22] ZDNet – Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats http://www.zdnet.com/article/ukraines-cyber-warfare-how-nato-helps-the-country-defend-itself-against-digital-threats/ (Downloaded: 08/08/2015)

[23] British multinational defense and security company – http://www.baesystems.com/home (Downloaded: 08/08/2015)

[24] HVG.hu – The blowing up of the oil pipeline is like a crime story http://hvg.hu/gazdasag/20141211_Krimibe_illoen_robbantottak_fel_az_olajve (Downloaded: 07/29/2015)

had attacked the system and they disconnected the emergency alarms of the oil pipeline and cut the communication then they increased the pressure in the pipeline, and by deceiving the workers, they could blow up the pipeline. Although the cameras were stopped successfully before the explosion and 60 hours of footage was removed, it is clear from the records of an infrared camera that was connected to another system, that prior the incident there were two people walking around with laptops along the pipeline who wore black military clothes.

In Iran the Stuxnet virus caused huge concern for a machine of the Bushehr plant

„The Stuxnet is a special computer worm that is infecting the machines that are using the Microsoft Windows operation system and it is spreading them and it is exerting its effect through the industrial process-management systems.[25] It is attacking the supervision management of the processes and the data collection and besides spying for the aimed industrial system, it is also reprogramming it."[26] Essentially the virus did not threaten the plant because the Uranium modifying equipment was the target. The code of the virus contained the reference May 9, 1979 and this date is identical with the day when the Jewish businessman, Habib Elghanian was executed in Iran with the charges of spying for Israel. The output of the virus caused that on November 16, 2010 Iran stopped the Uranium enrichment because more than 20% of the centrifuges got damaged during the activity of the Stuxnet. The virus proved that it is possible to cause huge harm from behind the computer.

According to the data of year 2014 Israel has a leading position when talking about cyber defence

The countries realise how important tit is to defend their Internet activities against others and the way they realise, it is worth considering Israel as an example. The country applies astonishing talents and technique to protect and use the software and the services.[27] Israeli experts revealed the deficiencies that concerned the Internet-based[28]. purchasing platform of the Alibaba[29]. This security gap would

[25] David Kushner: The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Downloaded: 07/26/2015)

[26] András Cserháti – The Stuxnet virus and the Iranian atomic program, Fizikai Szemle 2011/5, p. 150-155 http://fizikaiszemle.hu/fsz1105/cserhati1105.html (Downloaded: 07/26/2015)

[27] Israeli Innovation News – Cyber Security Nation: Why Israel Leads The World In Protecting The Web http://nocamels.com/2014/12/cyber-security-nation-israel/ (Downloaded: 08/09/2015)

[28] Israel21c – Alibaba invests in Israeli cyber-security http://www.israel21c.org/alibaba-invests-in-israeli-cyber-security/ (Downloaded: 08/10/2015)

have enabled the external attackers to „deroute" the purchases, to eventually modify the prices, to change the data of the consignments and to even top the purchasing process. Then the Chinese retail company declared that they invest in the Israeli cyber security initiatives in order to get protected against the hackers. The Iranian intelligence service has a unit, namely the unit 8200. Since nowadays the army and the IT sector are in strong connection, they considered it is important to make the proper cyber security steps. Although Israel's IT systems are developed, the country participates as an attacking party and as an attacked party, too, in the cyber war.[30] It stirred great commotion when a few years ago the Anonymous hacker group allegedly attacked two government websites of Israel. Israel denies the events and tells that the breakdown was because of the failing servers. Even the two government websites, the Mossad and the Israel Defence Forces (IDF) also stopped. There was the maintenance announcement on the Mossad site and the IDF was not accessible. The Anonymous hacker group answered to Israel with a youtube video[31] saying that these steps took place on their side because Israeli forces stopped a Canadian and an Irish ship in international waters and they even went aboard those ships. The hacker group considered the sea-blockade of Gaza as illegal and promised ongoing hacker attacks until there are changes in connection with the blockade. The group still tries to attack the various Israeli groups of interest.

Since 2002 several Internet-based intrusions can be connected to China[32]

There is a continuous economic increase in China which is of 7-8% even in the weak periods. China's increasing activity is challenging the countries in various areas. The Chinese cyber activity is proved by the fact that some products were banned from certain countries with the charge of industrial spying. The justification is that the Chinese producers could not explain the origin of some software items and their functions. China and the United States agreed to establish a joint group that is able to liquidate the problems occurring in the cyber security area and simultaneously prevents the hacker attacks that menace the financial sector, the banks or any area

[29] www.alibaba.com – Kína legnagyobb online kiskereskedelmi honlapja

[30] Keri András – Pándi Erik – Töreki Ákos: A vezetési és információs rendszerek elméleti megközelítése, Kommunikáció 2010., ISBN 978-963-7060-21-2, ZMNE, 2010., 39-49. oldal

[31] Anonymus #OpIsrael https://www.youtube.com/watch?v=q760tsz1Z7M&feature=player_embedded

[32] Security politics – Prof. Dr. László Kovács - colonel http://eiv.uni-nke.hu/uploads/media_items/biztonsagpolitika.original.pdf (Downloaded: 08/07/2015)

of life. It is important that each country has to defend its citizens, their rights and the country's infrastructure against the unexpected attacks.

Summary

It is clear through the examples shown in my article that there is need for more attention to the attacks received through the Internet because the current situation shows that there is no need for armed or physical force to cause serious damages. Nowadays even a well-trained hacker and a serious computer can be sufficient. If this hacker finds some support then with this support he can perform things that can seriously damage harm the infrastructure and the personal assets. Many countries realised that the attacks of new type characteristically require lower material expense than the traditional attacks and it is rather simple to spend money on the IT sphere instead of training the soldiers for many years. Following the news we can see an increasing number of cyber events and the big question is whether the world is prepared to react to these attacks. The stake is rather high and the security of paramount importance for every country. The biggest problem is that there is no cooperation between the countries in this regard. The attackers can cooperate in such a way that they don't need to be close to each other physically, they can be at different points of the world. It is difficult to concentrate on the cyber defence because the cyber attacks are unpredictable and difficult to be monitored. It is easy to procure source codes in the „mob's" black market and if it gets in the hands of an expert, they can use it for the development of a new aggressive attacking method. From the Union's perspective Hungary has a good position if we consider the protection of the infrastructure and the parrying of the cyber attacks. In one sentence I can say the cyber security is one of the most important challenges of the 21st century that requires a joint preparation, the goal is the prevention, since the sooner the problem is perceived, the easier is to prevent it.

References

In article.

Paráda István: SNMP alapú hálózat monitoring program fejlesztése és alkalmazása-I.

„A program futtatása az igazi teszt. Megírod a programot, kipróbálod és vagy működik, vagy nem.”

Bill Gates

„Ha nem tanulod meg, semmire sem jutsz, édes Öregem!”

Jobbágy Szabolcs

Absztrakt
Napjainkban az Internet, illetve az informatika körül forog a világ. Felmerül a kérdés, hogy tudják-e az emberek hogy mit is jelent maga az Internet, hogyan is épül fel, milyen elemeket foglal magában és az alkotóelemeiről honnan szerzünk információt?

Abstract
Nowadays life is Internet. What kind of information about information security?

Bevezetés

Napjainkban az Internet, illetve az informatika körül forog a világ. Felmerül a kérdés, hogy tudják-e az emberek hogy mit is jelent maga az Internet, hogyan is épül fel, milyen elemeket foglal magában és az alkotóelemeiről honnan szerzünk információt?
A mai emberek a számítógépet illetve az Internetet mindennapos tevékenységük során folyamatosan használják, igénybe veszik. Ezt a szolgáltatást az emberek többsége alapvetőnek, egyértelmű információforrásnak veszi. Viszont ahogy azt ez előbbiekben is említettem tudják-e mi is áll az lassan létfontosságú szolgáltatásuk, feltételük mindennapos használata mögött. Hiszen az Internet rengeteg eszközből, informatikai elemből épül fel távközlési közegről valamint segéd és illesztő eszközről nem is beszélve. Az Internet szabad megfogalmazás szerint a hálózatok hálózata. Az internet szerverek, számítógépek és hálózati aktív eszközök összessége kábellel illetve rádióhullámmal összekötve. Ezeket az eszközöket felügyelni, menedzselni lehet. Természetesen a különböző eszközök felügyelete és

menedzselése legegyszerűbben egy program, azaz szoftver segítségével történhet. Szoftver alatt a legszűkebb értelemben elektronikus adatfeldolgozó berendezések (például számítógépek) memóriájában elhelyezkedő, azokat működtető programokat értünk. A számítógépes program megmondja egy számítógépnek, hogy mit csináljon, jellemző módon azt, hogy az adatokkal milyen műveleteket végezzen.
Fontos, hogy egy program segítségével a hálózati eszközökről hasznos, illetve az informatikai és távközlési munka megkönnyebbítése érdekében értékes információt kaphassunk. Hisz ez elősegíti az Internet illetve adott Intranetek felhasználóinak igényeinek megfelelő kiszolgálását, a hálózat megfelelő fenntartásán és üzemszerű működésén keresztül.

1. Alapvető hálózati összetevők

A hálózatban számos eszköz és periféria található. A legalapvetőbbekkel, mint a számítógép, nyomtatók, webkamerák stb, nem kívánok foglalkozni, magyarázni működésüket. Egyrészről mindenkinek van alapvető információja ezekről az eszközökről, másrészt a számítógép működése témakör egy nagyobb terjedelmű önálló műnek is remekül beillene. Alapvetően három hálózati eszközzel szeretnék foglalkozni, illetve bemutatni. A router, a switch és hub. Természetesen felépítésük már rendeltetésük révén is különböző, mégis az alapvető hardveres működését, illetve az eszköz felállásának/bekapcsolásának folyamatát bemutatom továbbiakban említett Router szekcióban. A switch bekapcsolási folyamat szinte megegyezik a routeréval, különbségük a működésükben illetve a bővíthető modulok számában és típusában jelentkezik. [1][5][6][7]

Hub
Számítógépek kapcsolódását teszi lehetővé a hálózathoz. A hub az állomások közötti üzenetekhez kapcsolódó dekódoló elektronikával nincs ellátva, így nem tudja kiválogatni melyik üzenet, melyik tagállomáshoz tartozik. Ebből következően egy adatcsomag érkezésekor, regenerálja azt és az összes porton továbbítja. Viszont az Ethernet[33] hálózatok csomagtovábbítási mechanizmusából adódóan az üzenet a keretben mindenképpen tartalmazza a MAC címet[34], így az üzenetet mindegyik a hub-hoz csatlakoztatott állomás megkapja, viszont csak az Ethernet keret cél MAC cím mezőjében szereplő címmel rendelkező állomás veszi

[33] Kommunikációs Szabvány
[34] Media Access Control – hálózati eszköz fizikai címe,azonosítója

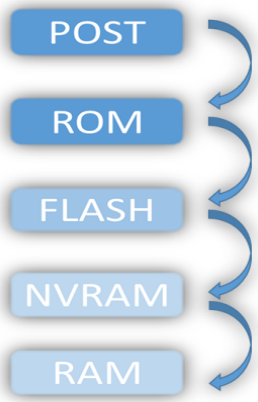
figyelembe. Ezen az eszközön egyszerre csak egy üzenet küldhető, így azonos időben induló adtok esetén üzenetütközési jelenségek lépnek fel. Az ütközött adatok megsérülnek, aminek következtében a feldolgozásuk nem jár eredménnyel. A sérült üzeneteket is észlelik, így amikor nem tudják olvasni azt egy idő után, újraküldik, leterhelve ezzel a hálózatot. Ebből következik, hogy a hubok esetén az ütközési tartományokat korlátozni kell.

Switch

A switch is a hub-hoz hasonlóan több állomást csatlakoztat a hálózathoz. Az eszköz már képes egy adott üzenet meghatározott cél felé továbbítására. Amikor a switch kap, egy adatcsomagot dekódolja, a keretet majd kiolvassa belőle a MAC-címet. Az eszköz fejlettségére utal, hogy fenntart egy táblát is, mely az aktív portok és az ezekhez rendelt MAC-ímeket tartalmazza. Egy adatcsomag elküldésénél a switch összeveti a célt a táblában szereplő adatokkal. Amennyiben a táblában megtalálható a célcím egy áramkörnek nevezett kapcsolatot létesít. Ez a kapcsolat egy dedikált összeköttetés, amelyhez a többi munkaállomás nem csatlakozik. Ez a megoldás lehetővé teszi az azonos időben való üzenetküldést, hisz minden áramkör csak az adott forrás és célállomás között létesül. [1][5][6][7]

Router

Olyan hálózati eszköz, amely összeköttetést biztosít két meghatározott hálózat között. Feladatuk az adatcsomagok forgalmának az irányítása. Ezen felül még egyéb a hálózat hatékony működéséhez hozzájáruló feladatköröket is ellátnak. Az üzenteket dekódolják, viszont switch funkcióin túl a keretbe beágyazott csomagokat is kinyerik. A csomag magába foglalja a forrás és a cél állomás IP-címét[35], ami alapján a router továbbítja az üzenetet. Amikor a forrás és cél IP-címeknek a hálózati részénél eltérés jelentkezik, routerek segítségével lehet eljuttatni a csomagokat a két különböző hálózatba. A router ilyen esetekben fogadja, az üzenetet, kicsomagolja, ezáltal kiolvassa a cél IP-címet. Következő lépésben eldönti a továbbítás irányát, majd a csomagot olyan keretbe ágyazza, amely a csomag célba érkezését lehetővé teszi. A Router összes portja egy adott hálózathoz csatlakozik. [1][5][6][7]



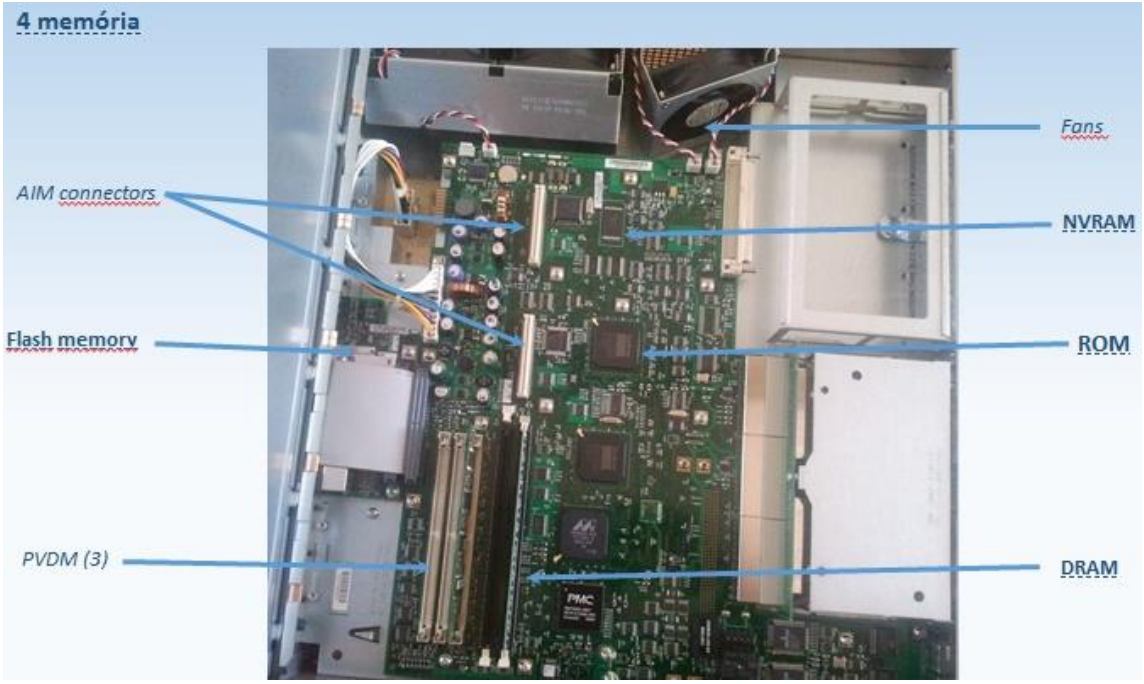
Az eszköz elindításának folyamatát *„boot sequence”*-nek nevezik, az alábbiak szerint:

[35] Internet Protokoll – Hálózati cím

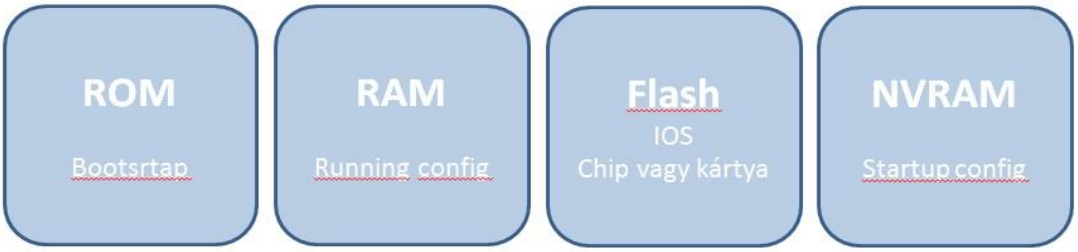
- Az eszköz lefuttatja a POST-ot[36], ez ellenőrzi az alapvető funkciókat, az eszközben található hardvereket, azok működőképességét, és az interfészeket. A ROM[37]-ban található.
- A Bootstrap nevezetű program megkeresi és betölti az IOS[38]-t. Ez is ROM-ban található.
- Az általában a Flash kártyán, vagy Flash chipen található IOS, megkeresi a startup-configot, ami az NVRAM[39]-on van tárolva.
- Ha az NVRAM-on megtalálható a startup-config, akkor az eszköz átmásolja a RAM-ba ami ezáltal már a running-config lesz. A RAM[40] tárolja az ARP[41] táblákat a routing táblákat stb.…;

1. ábra Boot sequence
Forrás: saját

Egy router vagy switch belsejében 4 fő memória található, amelyek segítségével az eszköz a fent említett lépések sorrendjében elindul.



[36] Power on Self-Test – önellenőrző folyamat
[37] Read-Only Memory – Csak olvasható memória
[38] Internetworking Operation System – Cisco hálózati eszközökön futó operációs rendszer
[39] Non-Volative RAM – nem felejtő RAM, kikapacsolás után is megmarad rajta az adat
[40] Random Access Memory
[41] Address Resolution Protocoll – IP cím és MAC cím összerendelésére használt protokoll



2. számú ábra: Router memóriák Forrás: saját

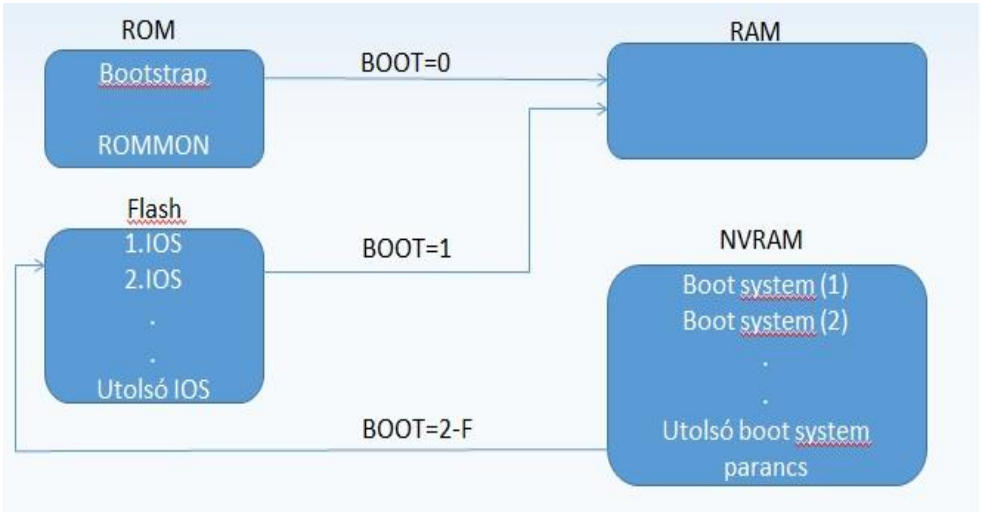
Configuration register

(Router 3 operating system: ROMMON, boot helper, IOS)

Azt irányítja, hogy a router hogyan töltsön (bootoljon) be. Ez az érték a show version parancs utolsó sorában található, alapértelmezett értéke a 0x2102, ami azt mondja, meg hogy az IOS-t a flash memóriából, a config fájlt pedig az NVRAM-ból töltse be az eszköz a console speed-et pedig 9600bps-en hagyja.

A konfigurációs regiszter utolsó hex digit-jét „boot field”-nek nevezik, ezt változtatva?

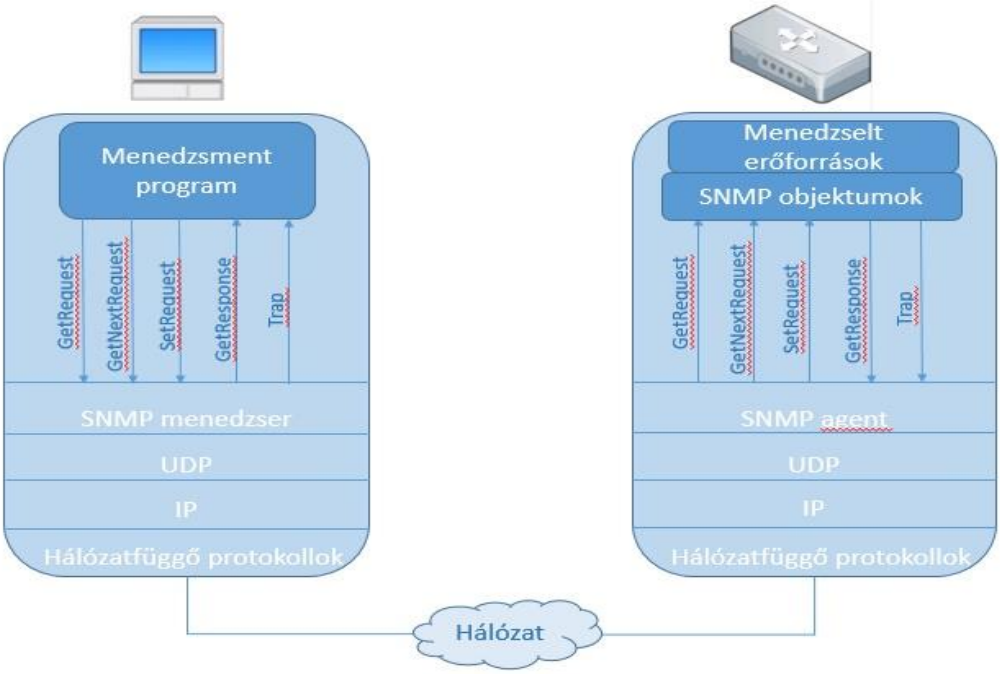
- Bootfield=0, ROMMON OS betöltése;
- Bootfield=1, a Flash memóriában található IOS-ek közül sorrendben az elsőt tölti be;
- Bootfiled=2-F, a startup-config-ból minden boot system parancsot kipróbál addig, amíg valamelyik működik. Ha nincs boot system parancs, vagy egyik se működik akkor az első IOS-t tölti be a flashből.



3. számú ábra: Bootolás folyamata

2. SNMT

Mivel a TCP/IP alapú hálózatokat több komponensek is alkotják, melyeknek vannak ugyanolyan váltózói, adatai, így 1988-ban jött egy ötlet, hogy ezeket a váltózókat kezelhetnék egyszerre (RFC 1065). Belegondolva a PC, a hálózati nyomtató, a router stb. rendelkezik például IP-címmel, interfészekkel, buffer-rel, tehát miért ne csináltak volna egy standard adatbázis ezekről a változókról és egy egyszerű monitorozó és menedzser rendszert.
Az SNMP (Simple Network Management Protokoll) egy application rétegbeli protokoll, amely egy manager és egy agent eszköz közötti kommunikáció formáját biztosítja. Az UDP protokoll alapján kommunikál. Az SNMP manager egy hálózati menedzser program, amelyet a számítógép, azaz munkaállomás futtat. Az SNMP agent szintén egy szoftver amely, azon hálózati eszközön szerepel, melyet felügyelni akarunk. Az agent feladata, hogy lekérje, vagy bizonyos esetekben felülírja, illetve átírja, azokat a változókat, amelyek abban az adatbázisban találhatóak, melyek felelnek az eszköz paramétereinek a beállításáért. Ezt az adatbázist Management Information Base-nek (MIB) hívják. [5][6][7][8]



4. számú ábra: SNMP működése

A folyamatos lekérdezéseken keresztül az SNMP agent begyűjti és analizálja az adatokat a menedzselt eszközről, amelyről statisztika is készülhet. Ezeken a MIB-ben lévő változókon keresztül konfigurálni is lehet az eszközt, persze a megfelelő szintű hozzáférési engedéllyel. Azokat az üzeneteket, amellyel lekérni lehet a változókat az agent szoftverről 'GET message'-nek, amellyel pedig írni lehet 'SET message'-nek nevezzük.
Az SNMP a monitorozást illetően nagy flexibilitást enged. Leggyakrabban a hálózati rendszergazda gyűjti be és tárolja az adatokat, egy menedzsment program segítségével. Majd elemzi a különböző tényeket, adatokat. Az SNMP segítségével például ellenőrizni lehet a router vagy hálózati eszköz CPU kihasználtságát. Először a GET message segítségével lekérdezi a MIB-jéről a paramétereket. Valamilyen probléma megjelenésének esetén az eszköz figyelmeztetni tudja a Manager programot 'trap' üzenetekkel. Ezeket a hálózati eszköz kérés nélkül küldi, szintén a MIB változók listáján szerepelnek, a menedzser program pedig különféle módokon tudja ezeket lereagálni. [5][6][7][8]

2.1. Az SNMP működése

SNMP MANAGER

Feladata hogy kommunkiáljon a SNMP agent-el. Kulcsfunkciói a következők:

- Agent kérdezése;
- Válasz kapása az agenttől;
- Változók beállítása az agenten;
- Aszinkron események nyugtázása.

SNMP AGENT

Egy olyan program, amely a hálózati eszközön található. Az összegyűjtött információt elérhetővé teszi a Manager számára. Funkciói:

- Helyi környezetről gyűjt menedzsment információkat;
- Betölti és tárolja a menedzsment információkat a MIB-be;
- Eseményjelzési funkció a Manager felé [5][8][9][10][11].

SMI

A MIB egy alkalmazott nyelv részhalmazaként van megjelölve. Ez a nyelv az Abstract Syntax Notation One (ASN.1);

ASN.1

Két módon is használva van az SNMP-ben. Az SMI erre alapszik, és a protokollban az üzenetek ez alapján vannak meghatározva.

Példa erre:

sysUpTime OBJECT-TYPE
SYNTAX TimeTicks
ACCESS read-only
STATUS mandatory
DESCRIPTION
The time (in hundredths of a second) since the
network management portion of the system was last re-initialized
:= { system 3 }[5][8][9][10][11]

Managed objects

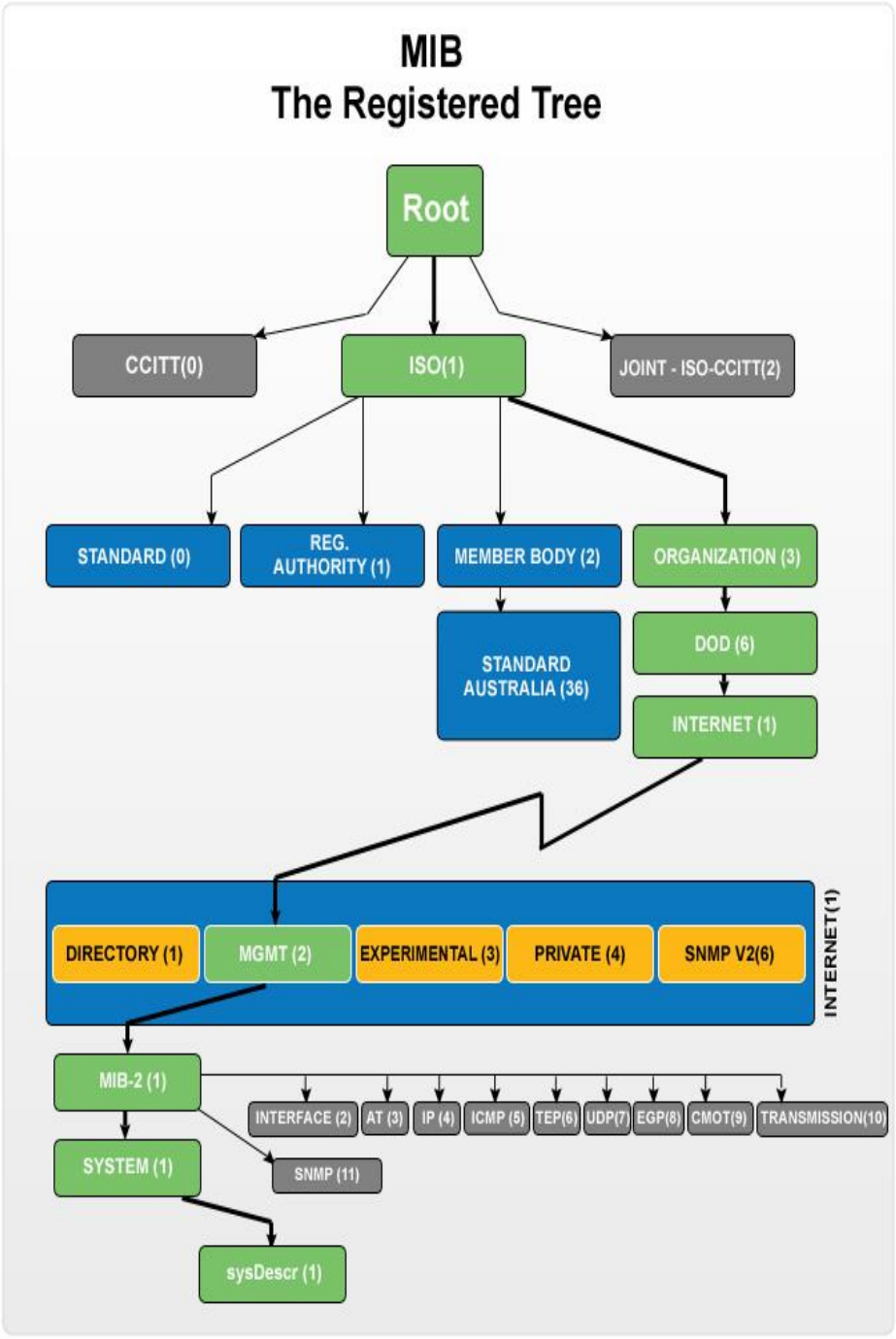
Az erőforrás van menedzselve ezekkel az objektumokkal, amelyek a következők lehetnek:

- Skalárváltozók: amelyeknek csak egy esete van egy kontextben. Ezeknek egyszeri értékük van;
- Táblák: dinamikusan tud nőni;
- Tábla elem: amely egy speciális típusa a skalár változóknak.

MIB Management Information Base

Minden SNMP agent fenntart egy információ adatbázist, amely leírja a menedzselt eszköz paramétereit. Az SNMP Manager ezt az adatbázist használja, hogy információt kérjen le az agenttől és továbbítsa a NMS-nek. A MIB fa struktúrába szervezett elemek halmaza. Ez a fa struktúrájú virtuális adatbázis, melynek egyes csomópontjaira, vagy elemeire számláncokkal, vagy ezt helyettesítő nevekkel hivatkozhatunk ez az OID. [5][8][9][10][11]

- Menedzselt objektumok és a viszony közöttük;
- MIB Management Information Base: menedzsmentra szánt, csoportosított objektumok;
- Minden objektum egy fába van rendezve;
- Egy globális MIB fa része;
- A levelek a rendszer állapotát jelző információkat tárolják;
- MIB-II a legnépszerűbb;
- A gyártók saját MIB-eket definiálnak;



5. számú ábra: MIB fa
Forrás: www.manageengine.com

OID: Object Identifier

A MIB menedzselt objektum azonosítókat tartalmaz, amelyeknek a neve OID. Minden azonosító egy egyedi sajátos tulajdonságát jelenti az eszköznek. [5][8][9][10][11] A szintek pontokkal elválasztva. A szintek a következőket foglalják magukba jobbról balra sorban:

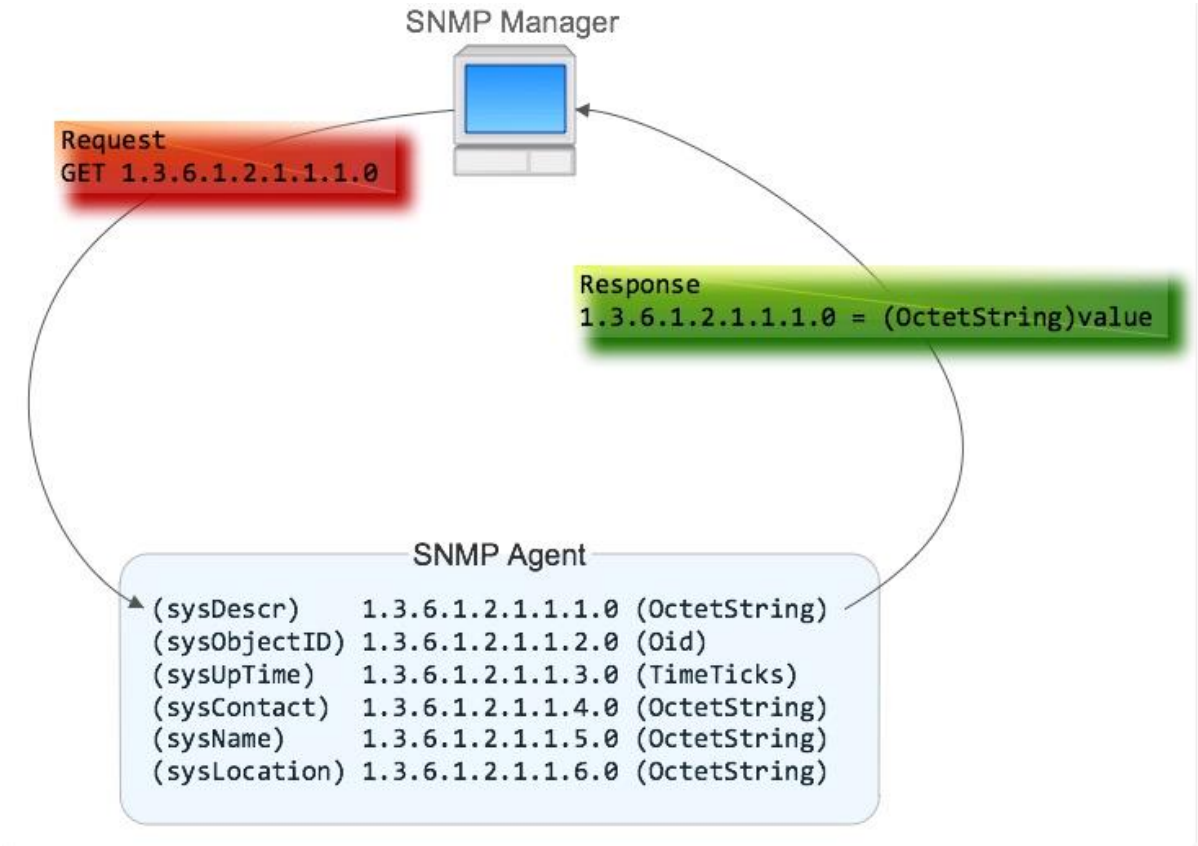
Pl:

1.3.6.1.2.1.2.1.

iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber

2.2 SNMP műveletek:

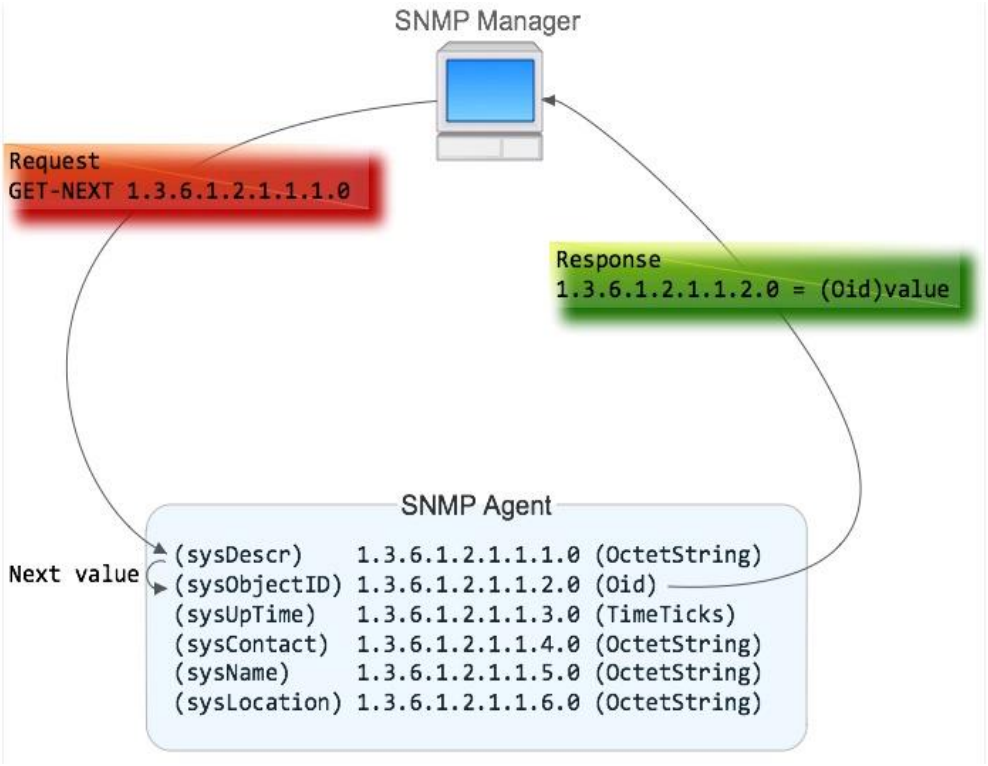
GET REQUEST, egy bizonyos információ lekérése [5][8][9][10][11]



6. számú ábra: GET request
Forrás: www.snmpsharpnet.com

GETNEXT REQUEST

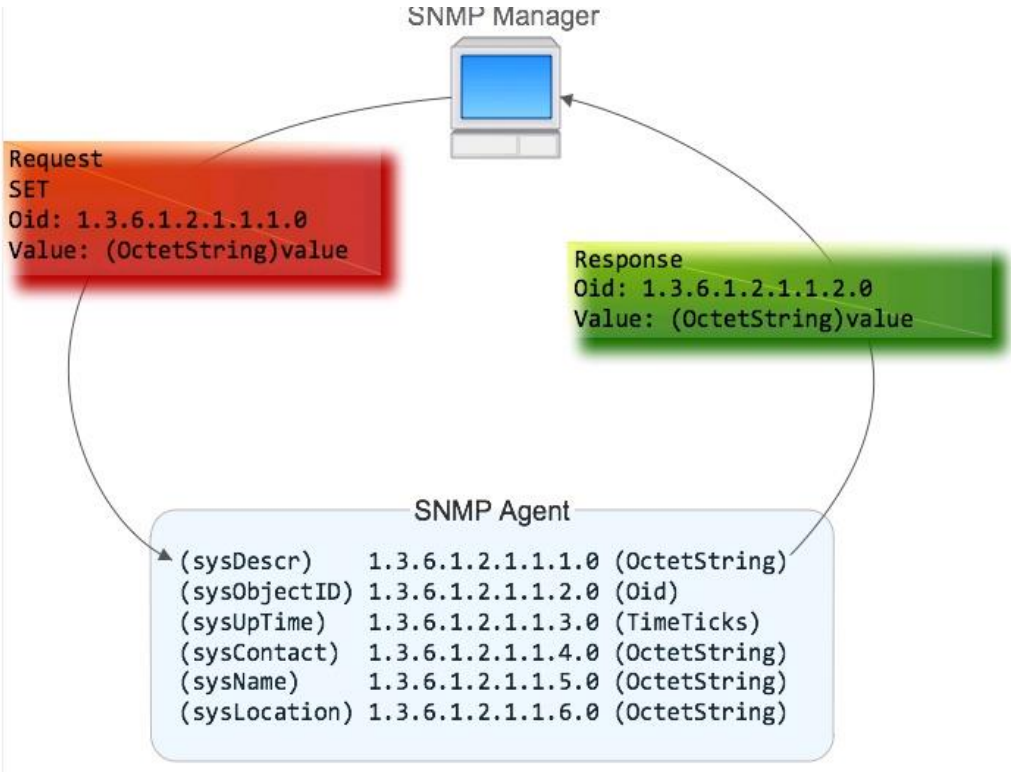
A következő információ lekérése: ennek segítségével végig lehet lépkedni az információkon. [5][8][9][10][11]



7. számú ábra: GETNEXT request
Forrás: www.snmpsharpnet.com

GET RESPONSE, a válasz üzenet

SET, egy objektumnak értékadás (SNMPv1-es protokoll esetében biztonsági megfontolások miatt a legtöbb gyártó kihagyta ezt a protokoll-műveletet) [5][8][9][10][11]



8. számú ábra: SET művelet
Forrás: www.snmpsharpnet.com

TRAP, egy speciális üzenet, akkor jön létre, ha a menedzselt eszközt figyelmeztetés küldésére állították be (például a forgalomszámláló elér egy bizonyos értéket, meghibásodás lépett fel stb. [5][8][9][10][11]

2.3. SNMP verziók

Az első SNMP verzió, amelyet az RFC 1065, RFC 1066, RFC 1067 ír le. Fő hibája a nagyon gyenge biztonság. Az üzenetcsere nem titkosított, jelszó helyett pedig a Community stringeket használja, ami könnyen támadható megoldás. Ennek ellenére nagyon széles körben elterjedt, és a hibáit áthidaló megoldásokkal jól használható.

SNMP Version 2

Leírja az RFC 1441 és RFC 1452. Javítottak a biztonságon, teljesítményén, menedzser-menedzser kommunikációt hoztak létre. A GETBULK üzenet létrehozásával több adatot egyszerre lehet lekérdezni, ez sokat javít a v1

hatékonyságán. A bonyolult, és vitatott biztonsági megoldások miatt nem terjedt el, helyette az RFC 1901 és RFC 1908 által leírt SNMP v2c vagy nem hivatalos nevén az SNMP v1.5 terjedt el. Ebben megvannak az SNMPv2 javításai, de a bonyolult biztonsági megoldás helyett maradt a v1 egyszerű Community string alapú megoldásánál. Bár a v1.5 elméletileg csak tervezet, nem elfogadott szabvány, mégis ez a gyakorlatban is elterjedt megoldás.

SNMP Version 3

Az RFC 3411–RFC 3418 által leírt szabvány, a jelenlegi hivatalos SNMP szabvány. A régebbieket az IETF elavultnak nyilvánította.
A gyakorlatban az eszközök általában több SNMP verziót is támogatnak, általában a v1, v2c és v3 szabványokat is. [5][8][9][10][11]

2.4 SNMP tulajdonságai

Az SNMP legfontosabb előnyei:

- Az Interneten használták és tesztelték;
- Egyszerűsége, kis erőforrás igénye megkönnyíti és elősegíti az implementációját a hálózati eszközökbe;
- Az SNMP termékek könnyen hozzáférhetőek;
- A fejlesztő programcsomagok ingyen hozzáférhetőek.

Az SNMP több hátránnyal is rendelkezik:

- Gyenge biztonság (ezen csak az SNMPv2-ben segítenek);
- Nagy tömegű adatlehívás lehetőségének hiánya;
- Az SNMP menedzser-menedzser kommunikáció hiánya;
- A Trap paranccsal felmerülő problémák. [5][8][9][10][11].

3. C#

A programozás elsajátításával rengeteg szakirodalom foglalkozik, amely természetesen megfelel időráfordítás után és rengeteg gyakorlás révén válik hasznossá, illetve használható tudássá.
A C# (sharp) megjelenési éve 2002, a Microsoft fejlesztési környezetével a Visual Studio .NET programcsomag részeként adták ki. Célja a COM alkalmazás szerver technológia leváltása volt.

Elődjének tekinthetjük a C++ nyelvet, hisz szintaktikailag, valamint szervezeti felépítését tekintve is rengeteg hasonlóságot mutat a két nyelv. A programok megírása C++ nyelven, nagyobb időintervallumon került megvalósításra, a nyelv komplexitásának köszönhetően. Ebből az indokból kifolyólag kerestek egy relatív gyorsabb talán nevezhető egyszerűbbnek mondható nyelvet, amely a hatékonyságból nem engedve produktívabb jellemzőkkel bír. Ez lett az objektumorientált C#, amely megteremti azon feltételeket, ami ahhoz kell, hogy viszonylag gyorsan és egyszerűen lehessen .NET keretrendszerű programokat írni. [12][13][14]

.NET keretrendszer

Ez egy Microsoft által kifejlesztett szoftver fejlesztői és futtatói környezet. Ezáltal lehetőség nyílik a programozók számára, hogy könnyen, kényelmesen illetve gyorsan készítsenek alkalmazásokat. Tehát leegyszerűsítve ez egy rendszer, amiben rengeteg programkészlet beépítetten kész van. Számos előnnyel rendelkezik, hisz támogatja a programkód felügyeletét, telepítését és vizsgálatát, ezen felül automatikus memóriakezelést biztosít, egyszerűvé teszi az Internet és adatbázis hozzáférést. Mivel nem kér beállításokat a rendszerleíró adatbázisban, az alkalmazások telepítése a keretrendszeren belül egyszerűbb. Továbbá platformtól független, azaz a programok megírásánál a fájlok egy virtuális gépre készülnek el, ez nem egyenlő azzal, hogy az alkalmazások virtuális gépen futnak, hanem hogy virtuális gépre készülnek, és majd indításkor lefordítódik a használt számítógép által is értelmezhető módra. A .NET keretrendszer fejlesztéséből adódóan magába foglal olyan részelemeket, amelyek csak Windows operációs rendszeren találhatóak, így ha egy megírt program csak azokat a részeket használja, amely minden operációsrendszeren megtalálható akkor a program mindenhol futtatható. Viszont ha olyan réseket is használ, amely csak Windowson érhetőek el akkor, vagy módosítani kell a programot, amely nem minden esetben sikeres, vagy csak Windows rendszeren lesz futtatható az adott alkalmazás. [12][13][14]

A keretrendszer kulcsa a felügyeleti kód, ami a CLR-nek[42] nevezett környezetben fut. Minden fejlesztőeszköz, ami CLR-t használ a kódot a szabványos MSIL[43] nyelvre fordítja le. Ezáltal a különböző nyelvek belső sajátosságai nem jelentenek akadályt, hisz mielőtt a CLR-hez jutnak, eltűnnek. A létrejött MSIL kód még nem alkalmas arra, hogy lefusson, az adott számítógép operációs rendszerén. Ehhez az úgynevezett

[42] Common Language infrastucture
[43] Microsoft Intermediate Language

JIT[44] fordításra van még szükség, amely az operációsrendszerhez kompatibilis, lefuttatható kódot készít belőle. Ezáltal a .NET viszonylag operációs rendszertől független, mivel a JIT fordítót minden rendszerre el lehet készíteni.
A „garbage collection" eljárás segítségével a .NET keretrendszer automatikus memóriakezelést biztosít. A folyamat során a rendszerszál meghatározott időközönként megvizsgálja felügyelt halmon elhelyezkedő objektumokat, és ellenőrzi melyiken található még hivatkozás. Amelyekre már hivatkozás nem irányul azok törlésre kerülnek a felügyelt halomról. Az ott maradó objektumokat tömöríti és javítja a rájuk irányuló hivatkozásokat. Tehát ha a program már nem használja a memóriát, azt a CLR érzékeli és automatikusan újrahasználja azt.
Az erőforrások, adatok és kód tárolására assemblyket használ. A keretrendszer futtatója csak az tárolt kódot hajtja végre, a biztonsági funkciókat, verziókezelést és a név-feloldást is az assemblyk segítségével biztosítja. Az assembly egy .EXE vagy DLL fájlok összessége, amelyek a program kódját és erőforrásait tartalmazzák. [12][13][14]

DLL

A DLL (Dynamic Link Libary) fájlok, mint a nevében is benne van függvénytárak. Magukban nem futtatható programok, amelyek adatokat, programkódokat, sőt még képeket is tartalmazhatnak. Windows operációs rendszerben használatosak, megosztott könyvtárakként definiálhatóak, melyek segédprogramként elősegíti a kompatibilitási problémák kiküszöbölését, illetve a már megírt programkódok alapján egyszerűbbé teszik a programozást. A programokhoz általában több DLL is tartozik, ezek nélkül ugyanis a program nem futna le, nem tudna működni. A dinamikus tulajdonság jelentése, hogy a program meghívja az adott DLL-ben található kívánt programkódot, adatot, amely csak ennek a hívásnak a hatására töltődik be a memóriába. A név könyvtár része az adatok tárolására mutat rá, amit a Windows operációs rendszer igény esetén használatba vesz. A DLL fájlok általában a System illetve a System32 könyvtárakban találhatóak. Elmondható, hogy nagy általánosságban beépülő modulként használják, feldolgozva a bennük tárolt algoritmusokat illetve adatokat. Természetesen, ami segíti a fejlesztői munkát, az jelentős biztonsági szempontból kockázati és stabilitási tulajdonságokkal is felruházza a DLL fájlokat, hisz a külső programok lecserélhetik a sajátjaikra a rendszerfájlokat. [12][13][14]
A program készítésénél DLL használata lett segítségül hívva. A SharpSnmpLib.dll és a SharpSnmpLib.Engine.dll Visual Studio-ba történő betöltésével, amelynek

[44] Just in Time

kezelése így az SNMP GET, SET, TRAP parancsokat felismerve történt. Elősegítette a programozás gyorsaságát, egyszerűségét, illetve optimális munkafolyamatát. A DLL fájlok többsége letölthető az Internetről, valamint felhasználásukat ingyenesen elérhetővé teszik a programozás iránti segítség valamint a fejlődés szellemében.

Összegzés

Jelen publikáció összefoglalja a hálózatok világának alapvető kérdéseit. Megpróbál az első részben beláttatni azokba a mélységekbe, amelyek a felhasználás mögött állnak. Megítélésem szerint a különböző eszközök felügyelete és menedzselése legegyszerűbben egy program, azaz szoftver segítségével történhet, azonban fontos, hogy egy program segítségével a hálózati eszközökről hasznos, illetve az informatikai és távközlési munka megkönnyebbítése érdekében értékes információt kaphassunk. A cikk folytatásaként közlöm további eredményeimet.

Felhasznált irodalom

[1] Paráda István honvéd tisztjelölt: A hálózatbiztonság vizsgálata a hálózati eszközöket érintő támadások gyakorlati szimulációin keresztül 2013
[2] Munk Sándor Hálózatok Fogalma, Alapjai 2010. Szeptember V. Évfolyam 3. Szám
[3] Farkas Éva; A számítógép hálózat 2002; letöltve 2013.01.19-én a következő helyről:http://www.bibl.uszeged.hu/inf/demo/Halozatok/Fogalmak/Fogalmak halozat_fogalma.html
[4] Hálózatok http://www.pollak.hu/static/sanyag/halozat.html (2012.12.09)
[5] Andrew S. Tanenbaum: Számítógép-hálózatok 1992
[6] Todd Lammle: CCNA Routing and Switching 2013
[7] Wendell Odom, CCIE No. 1624 Cisco CCENT/CCNA 2013
[8] http://www.snmpsharpnet.com
[9] http://szabilinux.hu/snmp/index.html
[10] https://www.ietf.org/rfc/rfc1157.txt
[11]Az alkalmazási réteg vizsgálata (SNMP) dr. Tóth Csaba adjunktus Mohácsi János BME Számítógéphálózatok jegyzet. 2000,
[12] Illés Zoltán: Programozás C# nyelven 2005
[13] Reiter István: C# programozás lépésről lépésre 2012
[14] http://csillagpor.hu/remek/fajlkiterjesztes/dll
[15] Pándi Erik: A hazai zártcélú hálózatok szerepének átalakulása az elektronikus közigazgatási szolgáltatások bevezetése és kiterjesztése folyamatában Hadmérnök pp. 92-106, Budapest, 2007. ISSN 1788-1919

Kerti, András – Szabó, Anna Barbara: Auf Dokumentebverwaltung-Software gemachte Erfordernisse in der ungarischen öffentlichen Verwaltung

Absztrakt
A cikk célja az elektronikus iratkezelés egyik eszközével, az iratkezelési szoftverrel szemben állított alapvető követelmények ismertetése Magyarország közfeladatot ellátó szerveinél. Ehhez először a dokumentum-kezelési követelményeket fogom ismertetni, ugyanis az iratkezelési szoftver lényegében egy specializált dokumentumkezelő szoftver.

Abstrakter
Das Ziel des Artikels ist umreissen auf Dokumentebverwaltungsoftware gemachte Erfordernisse in der ungarischen öffentlichen Verwaltung. Ich umreisse die Dokumentenbehandlungsanforderungen zuerst, weil die Aktenverwaltung-Software eine fachkundige Dokumentebverwaltung-Software ist.
Schlüsselwörter: iratkezelés- die Dokumentenverwaltung, irattár- die Registratur, irat- die Akte, dokumentum- das Dokument, ikattni- eintragen

1. Das Dokument, die Akte, die Urkunde

Ich halte den Träger der Informationen für ein Dokument im Artikel, was irgendetwas kann seine Form der Erscheinung als ähnlich betrachten. Das charakteristischdes Dokuemntum, dass beobachtet die Entwicklung der Technik fest, seine vorhergehenden Formen blieb gleichzeitig.
Der Gesetzgeber sieht es als ein Dokument an: jene Dokumente, welches entstand die Funktion von einem der Organe oder von der Tätigkeit der Person auf seiner Reihe, Sie sind dazu, ist feste als eine Einheit zu behandelnde Informationen angekommen, Gruppe der Angaben. Ich ist zu benutzen Begriff der Akte in dieser Bedeutung hierdurch. Das Dokument ist möglicherweise das Papier, das seine Auftrittbasis betrachtet, Sie sind Mikrofilm, magnetisches-, elektronischer Datenträger. Es gibt möglicherweise einen Text, Daten, ein Diagramm, das auf seinem Inhalt, Ton, Bild, oder dieses seine Kombination. [1]
Wir sprechen über die Urkunde: Im Falle der amtlichen Verfahren wenn die Tatsachen, Daten, die Rechtfertigung der Echtheit der Umstände, Pläne, Erklärungen die Funktionen des Dokuments sind. Basis davon ist Polgári perrendtartásról szóló 1952. évi III. Gesetz. [2]
Es ist nicht möglich, das Dokument und die Akte zu unterscheiden viele Male in der Praxis. Zum Beispiel bei der Anwendung: die Daten, die auf dem Umschlag

geschlagen werden können, holen möglicherweise eine ungefähr Rechtsfolge.Der Umschlag kommt in die Ausrichtung diesmal, weil weil das Teil des Datenbandes war.

2. Das Dokument die allgemeinen Gesichtspunkte zu gruppieren

Die elementaren predicamental Standpunkte des Dokuments eine:

- Inhalt z.B.:die Akte, die Zeitung, das Gesetzblatt usw.
- Träger z.B.: das Papier, magnetisches, elektronischer Datenträger usw.
- Konstruktion z.B.: einfach, komplex usw.
- Datenbild z. B.: analog, digital usw. [3]

Die Dokumente können entsprechend Zugang gruppiert werden, ein Dokument ist möglicherweise einzigartiges und kopiertes und kopiertes einzigartiges so.
Einzigartiges Dokument: das dokumentuok mit eingeschränktem Zugriff. Z.B.: die qualifizierte Daten, die Personaldaten.
Kopiertes Dokument: jene Dokumente, welches erlaubterweise für jedes verfügbar, vielleicht im Handelsstrom verfügbar. Z.B.: das Corpus juris, die Veröffentlichung, e Norm, der Standard, Daten von öffentlichen. [3]; [4]
Kopierte einzigartige Dokumente: für die Dokumente, die in einer kleinen Anzahl von Kopien, ein schmaler beruflicher Kreis erscheinen. Z.B.: berufliche Veröffentlichung, Verfahrensauftrag. Zwischen den elektronischen Dokumenten kann die traditionelle Papierbasis die Formen eines Dokumentes gefunden werden. Sie können ihre Bildung vom Anfang auf einer elektronischen Straße als hervorgebracht betrachten, Sie sind auf digitisation, den sie durchgehen. Entsprechend grundlegender Regel im administrativen amtlichen Verfahren bereitete das digitalisierte Papierbasisdokument und vom elektronischen Dokument andere Kopie mit einem einem anderen Format vor, und die elektronische Dokumentenpapierbasis die Beweiskraft seiner geformten Form ist der der Originalurkunde gleich, wenn sie entsprechend den Regeln eines regulierten elektronischen Verwaltungsdiensts die Berechtigung und die Organisation, die von der Regierung zugewiesen wurde, sie vorbereiteten. [5]
Es ist notwendig, einen Unterschied im Hinblick auf eine Verfügbarkeit an den elektronischen Dokumenten das mit lokaler Leistung und Fernzugriff zwischen Dokumenten zu machen.
Dokument mit lokaler Leistung: auf dem Computer, Sie sind ist megmegnyitható auf Datenträger.
Fernzugriff: durch einen Netzkontakt zugänglich.

Die allgemeinen Funktionsregeln der Dokumentenbehandlung
Es ist möglich, die allgemeinen funktionellen Regeln der Dokumentenbehandlung in drei Gruppen zuzuteilen:

1. Mit Benutzern hat Dienstregeln verbunden
2. Von Benutzern unabhängige Dienstregeln
3. Mit einer Suche hat Dienstregeln verbunden
4. Dokumentenfundamentregeln

3. Mit Benutzern hat Dienstregeln verbunden

Mit den Benutzern zwischen dem zusammenhängenden Dienst schulden Regeln ihm persönliche Regeln, die es, das definieren, wer und bis, welches Maß am gegebenen Dokument kommen kann.
Es ist möglich gruppieren die so eine folgenden:

- Die Regel des Erhaltens einer Anforderungsstufe: Die Regel schadet allgemein Maßbasis denkt es, dass die Verletzung des gegebenen Dokumentes, oder, welcher ihn bewirken, unerlaubte Hälften sichernd, auf dem Leben der Organisation hat. Die ungarische Kategorisierung passt sich an Beschluss 2013/488/EU des Rates vom 23. September 2013 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 274 vom 15.10.2013, S. 1).
- Ankunft, Emission, bewegliche Regeln: diese Regeln dem nachweisbaren vom Dokument wird wegen seiner Bildung gedient, sind Sie wegen seiner, in eine Organisation bis seine Vernichtung ankommend.
- Regeln der Beseitigung: wird hier definiert, das das Dokument wie gehört.
- Die Regelung von Bezeichnungen: wird in dieser Regelung, das Kompetenz wie auf die Bildung des Dokuments haben, seine Authentisierung, seine Änderung, auf Einblick, auf Vermehrung, Getriebe, Vernichtung definiert. [4] [6]; [7]; [8]; [9]

4. Von Benutzern unabhängige Dienstregeln

Von den Benutzern zwischen dem unabhängigen Dienst können Regeln mit verwandten formellen Regulierungen der Dokumente aufgezählt werden. Diese in der Allgemeinheit es nachstehend in zerlegbare Gruppen:

- Regulierungen bezüglich mehrerer Kopien: Hier schulden Sie die Funktion der einzelnen Kopien und ihrer die Definition seiner Behandlungsmethode.

- Zeitliche und Ordnungsregulierungen: Die Termine und die offizielle Straße, die der Weg des Dokumentes ist, werden hier formuliert.
- Die Definition der Echtheit: Die Geräte der Echtheit des Dokumentes und seiner Weise werden hier formuliert.
- Es ist möglich, es abzulegen „?”: das erhaltene Dokument, kann oder keiner abgelegt werden. In so viel, um, die Arbeitsabläufe der Organisation sein Blick bereits für ein zu betrachtendes Dokument abgelegt zu werden.

5. Mit Suche verbundener gemeiner Regeln

Zusammenhängende allgemeine Regulierungen helfen dem effizienten wiedergewinnbaren vom Dokument mit der Suche, die Prozesse werden beschleunigt. Hier kann aufgezählt werden:

- Unter Verwendung er für das Register der Schlüsselwörter, Schlüsselausdrücke, mit denen es möglich ist, es zwischen den Dokumenten mit einem ähnlichen Inhalt zu belasten.
- Regelungen auf den Bau der gespeicherten Dokumente: hier ist möglicherweise die Behandlung des elektronischen Dokuments dort Regelungen hinsichtlich einer Größe hinsichtlich eines Formats, im Falle der traditionellen Papierdokumente pl.: ein Verschluss in ihm nicht sein dort gelassen usw.
- Regelungen auf die Speicherung der Dokumente: kann die Erhaltungszeiten und mit den Lagerung bezogenen Anforderungen hier unter anderem aufgezählt werden.
- Regelungen es speichernd auf, die als das genaue Erbringen der Index-Bewegung und des Speicherplatzes getan zu werden Operationen, seine Festlegung. [4]

6. Dokumentenfundamentregeln

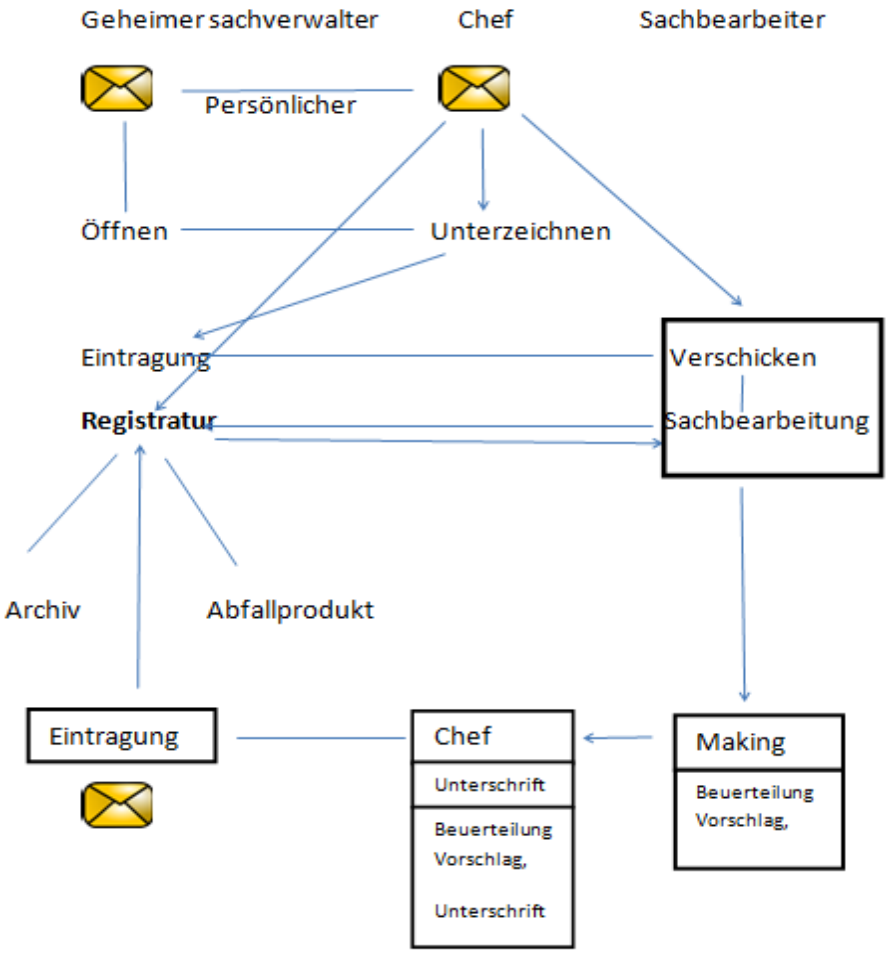
Dokumentieren Sie Grundlagenregeln ebenfalls die leistungsfähigen Dokumentenbehandlungsaufschläge es in der elektronischen Umwelt. Es ist möglich, sie in die unten genannt Hauptgruppen im Allgemeinen aufzuspalten:

- Dokumentenstrukturierung: Machen des Dokuments zu das mit einem vorgeschriebenen Bau.
- Meta- die Anforderung der Koppelung von Daten.
- Die Grundlage eines Dokumententeils ist für das Indexieren passend.

- Auf die typischen Schlüsselwörter des Dokuments Schlüsselausdruckzuordnung. [4]

Ich werde mich mit der Datei Betriebssoftware in zusätzlichen befassen, da sie in ein Register kommen, das mit einer Registrierungsnummer nur von der Menge der Dokumente geliefert ist, die dort entstehen, ins Organ ankommend, welche Funktion von seinem, der Sie im Laufe der Tätigkeit der Person sind, entstanden ist, sind Sie dazu, ist feste Informationen angekommen, die als eine Einheit, Datenband zu behandeln sind.

Die 1. Zahl illustriert die Strasse des Dokuments.



1. Zahl (machte: dr. András Kerti)
Aktenverwaltung-Software

So Informationstechnologielösung, die die Behandlung der Dokumente auf einer elektronischen Straße mit dem Ziel löst, dass er es vereinfachen sollte und ihn die Verwaltungsaufgaben sollte beschleunigen lassen, die mit der Dokumentenbehandlung verbinden werden. Seine Aufgaben schulden das Bilden des elektronischen Rekordbüros.
Der definició aus 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményei:
Aktenverwaltung-Software: die Informatikanwendung wie dieses Unterstützen der Datei Betriebsbasisprozess, dass seine Basisfunktion Sie die Datei als in dieser Ordnung genommene Betriebsoperationen betrachten, bevorzugen sie die Ausführung eines Teils von seinem, unabhängig es, der andere Funktionen neben diesen liefert. Seine Basisfunktionsführer es das elektronische ankommende Register, Register und Archiv. Die Akte, die fogalmaket verwaltet, die 335/2005. (XII. 29.) Verordnung a közfeladatot ellátó szervek iratkezelésének általános követelményeiről definiert.

7. Anforderungen gemacht auf Aktenverwaltung-Software

Grundlegende Erwartung, wie er den Dokumentenbehandlungsregelungen gleich sein sollte, die die effektiven Verwaltungs- und Verwaltungsmaßnahmen eingelassen werden.
In der ungarischen öffentlichen Verwaltung die zwei wichtigsten Regelungen sind 2004. évi CXL. Gesetz a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól, továbbiakban Ket. und 335/2005. (XII. 29.) Verordnung a közfeladatot ellátó szervek iratkezelésének általános követelményeiről.
Wenn es keinen exklusiven legalen Grund gibt, stellt sein einzelnes Verfahren in einer elektronischen Form grafisch dar, die performable ist, die passende Dokumentation der Kontaktaufnahme ist notwendig zu diesem.
Die Unterordnung von verschiedenen Anwendungen und von ihren Einschließungen, die Unterordnung eines Ersatzanrufs und die Ergänzung, untersuchend herein ein Verfahrensdokument ist möglicherweise so, die Erklärung der Veranschlagung, den Antrag einer Rechtfertigungsanwendung, einen Kunden, seine Mitteilung, seine Unterordnungen, die zur Berechtigung gegeben werden, die Kommunikation von einzelnen Anrufen und die Entscheidung.
Vile Dokumenten kommen zu einer Verwaltungsbehörde, aber wir mussen nicht immer eintragen;
z. B.: Bücher, Lehrpläne; Werbematerialien, Führer; Einladungen, einladende Platte; nicht Zeugen mit einer strengen Rechnung.

Ich umreiße die Standpunkte, die mit der Leitungssoftware der wichtigsten Datei in einem Auge im Teil diesbezüglich gestützt werden.
Von der Produkteinführung des Verfahrens müssen die natürlichen Personen, die vom Verwalter vorgewählt werden und die juristischen Personen eine Mitteilung senden. In so vielem geschieht dieses in Form eines Rückscheinbuchstaben, das System muss die Rückscheine automatisch kennen dann, um auszustellen.
Aber muss für die elektronischen Mitteilungsformen passend sein, die digital unterzeichnet werden. Z.B.: E-Mail, Netz auf einer Seite usw.
Lassen Sie denjenigen, der Grundregel ist, zeigen die Termine einem Verwalter die Anwendung auf das Verfahren von einem Tag im Anschluss an seine Ankunft in eine Autorität an, an der Kompetenz und Kompetenz sind, wird gerechnet. Das erste fängt mit dem Tag der Durchführung eines Verfahrensplans im Verlauf eines Verfahrens an, das von einem Büro abfährt. Die Ankunft des Dokuments muss den Tag des Systems deswegen speichern und sein Anfang muss die Gelegenheit zur Verfügung stellen seine Festlegung. Auf der Anforderung oben tragen gemacht auf der Software, dass die Fristenänderung eine Gelegenheit sein sollte. Es ist notwendig, die betroffenen über die Fristenänderung zu informieren, muss eine sein, welches für dieses elektronisch getan werden kann, und muss fähig sein die Frist auf eine Berechnung. Meine praktische Erfahrung, diese Anwendung dort ist ein Anspruch seitlich in dieser Richtung, die den Verfall der Frist die Vorhersage er mit Tagen entsprechend einem Anspruch einstellen gelassen werden lassen, Kundentor and Büro Tor können es in www.mo.hu.
Es ist notwendig, die Ankunft einer Anwendung in der Software und den Namen des Kunden und seines Vertreters, seine Privatanschrift oder seinen Sitz, für den Kunden auf die Entscheidung der Berechtigung zu reparieren die ausgedrückte Anwendung der Wahrheit außerdem wenn er die elektronische Adresse bewilligt, seine Telefonnummer, die Zahl eines Telefaxes.
Lassen Sie ihn die Einschließungen regeln, die zur Anwendung befestigt werden. Lassen Sie ihn gewährt werden, vom System zu sein, zum die Ergänzung heraus fordern zu senden. Die Software kann sie empfangen und lassen Sie sie sie durch ein Kundentor gleichzeitig ankommen lassen, ein Abgesandter unterzeichnete einen Vertrag über eine städtische Webseite elektronisch, Sie ankommen in Form eines elektronischen Buchstaben, der mit Dokumenten einer elektronischen Unterzeichnung geliefert wird. Zur Einreichung der Bewerbungen lassen Sie die elektronischen Formen verfügbar sein.
Zu Suche fachgemäßer Obrigkeiten erlauben Ausgestaltungen zu sein kann ausführen, fixiert zu sein, eins kopiert Angaben quasi automatisch, und erlauben

dieser zu sein möglicher zu senden dieser durch er elektronischer Art, ihr - Postkarte eins zu Abtransport, auf daß zu vorbereiten Dokument.
Zu Suche fachgemäßer Obrigkeiten erlauben Ausgestaltungen zu sein kann ausführen, fixiert zu sein, eins kopiert Angaben quasi automatisch, und erlauben dieser zu sein möglicher zu senden dieser durch er elektronischer Art, ihr - Postkarte eins zu Abtransport, auf daß zu vorbereiten Dokument.
Lassen Sie ihn die Dokumente setzen, die elektronisch in ein Buch des elektronischen Postens ausgesendet werden, von dem ein Verwalter möglicherweise an, wem eine elektronische Unterzeichnung ist nur den Versand schließlich fährt. Lassen Sie den elektronischen Posten Verlegenheit die Tatsache des Versands, seiner genauen Zeit mit dem Versand gleichzeitig buchen und des Aussendens seiner Person.
Entstand lassen Sie ihn die Registernummer auf amtliche Entscheidungen automatisch notieren. Lassen Sie die Arten der gesetzlichen Abhilfe zur Aufnahme in das System kommen, lassen welche es möglich sein, um eine Form mit seiner Auswahl automatisch zu benutzen.
Das Gesetz vom Ziel des Kontaktes es halten definiert die Anforderung einer Zeitreservierung, gleichzeitig eine Dokumentenlenker-Software, die diese Funktion möglicherweise ein Anspruch ist, z.B.: an den Dokumenten mit einzigartigem Zugang.
Die Dokumentenlenker-Software muss den Überwachungsregeln der Dokumentenbehandlung gleich sein. Angekommen ins Organ entsprechend, ist lokal entstanden, Dokument hat identifizierbar, fellelési sein Platz, seine Straße nachweisbar, nachprüfbar vorausgeschickt, und lassen Sie ihn wiedergewinnbar sein. Sein Inhalt nur ließ es, das sie für ihn geeignet waren, ihn erkannt werden lassen werden. Neben der eindeutigen Aussage über persönliche Verantwortung kann behandelt werden. Maßnahmen ist zu ergreifen für seine Berufsbehandlung, seine Register, seine Lieferung, sein Schutz mit notwendigen persönlichen, objektiven, technischen Bedingungen erforderlich. Er muss das unabänderliche und die Erhaltung der Dokumente mit einem aushaltenen Versicherungswert sein.
Zur Verwaltung muss die Vorbereitung der Entscheidung, die richtige Funktion der Organisation einer passenden Unterstützung garantieren. [5]
Von den allgemeinen Anforderungen der Dokumentenbehandlung der Organe, die eine allgemeine Aufgabe in einem Auftrag formuliert die durchführen, Dokumentenverwaltung seine Überwachung, in der das Verwaltungsinformationssystem eine hervorgehobene Rolle empfängt. Von den allgemeinen Anforderungen der Dokumentenbehandlung der Organe, die eine allgemeine Aufgabe in einem Auftrag formuliert die durchführen,

Dokumentenverwaltung seine Überwachung, in der das Verwaltungsinformationssystem eine hervorgehobene Rolle empfängt. Der Führer einer Organisation, die eine allgemeine Aufgabe ebenfalls das verantwortliche durchführt, wird für die Berufs- und sichere Erhaltung der Dokumente für die Formung und den seinen Betrieb eines Archivs gepasst, und objektive, technische und persönliche Bedingungen noch etwas, Geräte sind zur Dokumentenbehandlung für seine Versicherung und seine Überwachung notwendig.
Die Verordnung schafft den verifiability der Datei Betriebstätigkeit, dadurch, das Kapital organisatorische Voraussetzungen einer Datei Betriebssystem formulierend, das, um im Laufe einer elektronischen Dokumentenbehandlung zu gewähren, erforderlich ist:

- Angekommen zum Organ, muss das Dokument, das auf dem beteiligten Entstehen im Organ gesendet wird, identifizierbar sein.
- Der Platz des Dokumentes, seine Straße muss für die nachweisbare für die nachprüfbare und für die wiedergewinnbare sein.
- Das cognizability des Dokuments muss reguliert werden und es wird zu ihm für ihn nur cognizable betitelt möglicherweise.
- Die Aktenverwaltung-Software der Datei kann dieses durch ein mehrstufiges Verteidigungssystem versichern. Dieses reguliert es, entstand das, das der gegebene Verwalter möglicherweise herein nur seine eigenen Dokumente untersucht oder in seine Gruppe, vielleicht in den Dokumentenkreis oder zur ankommenden Organisation, dort alle in ein Dokument.
- Lassen Sie das nachweisbare der persönlichen Verantwortung, die für seine Dokumentenbehandlung existiert, eindeutig zu sein.
- Es ist notwendig, ihn zu versichern: zur Berufsbehandlung des Dokuments, seins Register, seine Lieferung, seine Schutznotwendigen persönlichen, objektiven, technischen Bedingungen.
- Die Versicherung vom unabänderlichen eines Dokuments.
- Regular, der heraus sortieren, und die Versicherung der Erhaltung der Dokumente mit einem aushaltenen Wert.
- Es ist notwendig, die passende Unterstützung für die Verwaltung, die Vorbereitung der Entscheidungen, die richtige Funktion der Organisation zu gewähren.

Die Aufgabe der Person anvertraut mit der Überwachung der Dokumentenbehandlung im Falle der Behandlung des elektronischen Dokuments für die Zugangsbezeichnungen der Leitungssoftware der elektronischen Kartei, für die einzigartigen identifizierenden Merkmale, die Ersatzrechte, den Außen- und

inneren Namen und für Verzeichnisse er Dauern aktuell. Die Operations- und Datensicherheitsanforderungen sicherstellen und sie von ihm muss das Handeln das schmutzige. Sein Betrieb gehört seiner Verantwortung im Verlauf von der regulierten Funktion den halten Beamten und persönliche elektronische Postkästen und von des Kontaktes, auf der elektronischen Straße innerhalb einer Organisation zu geschehen. Auf das Verfolgen der Bewegung des Dokumentes ist es notwendig, das unmittelbare, die Registrierung der Dokumente zur Verfügung zu stellen, die lokal für das System geschehen, ihn mit einem einzigartigen Bezeichner am Tag des Ankunftereignisankommens versorgend. In so viel, wenn berechtigte Person es für ein Dokumentenbehandlungsdokument nicht erhält, schmolz es innerhalb des ersten Werktages im Anschluss an die Ankunft des Dokumentes, das dann ankommt. Das Dokument, das sich innerhalb einer Organisation nachweisbar, nachprüfbar bewegt, und hat seine vorübergehende Einnahme gerechtfertigt sein lassen. Er über angenommenes hat bis the one zu den Benutzer geprüft sein kann, sein Dokumente durch es aufgegeben. In so viel ist es elektronisch Dokument angekommen, Sie sind einzeln seine Elemente können nicht geöffnet werden es ist notwendig, den Absender über die uninterpretable Elemente innerhalb der drei Werktage zu informieren, die von der Ankunft, und von der Ergänzung aufgezählt sind. Es man soll zu informieren dieser über erfolgreicher Beugung des Dokuments gleichfalls Absender einhalbmal. Betriebssoftware der Datei muss es möglich in Übereinstimmung mit den Voraussetzungen der Hauptregistrierung machen, die den Rest der Angestellten der Organisation im Stande sein lassen, Registrierung und Datei Betriebsoperationen gemäß seinem Bezeichnungniveau zu machen. Es ist notwendig, die Ausrichtung von Änderungen und von anderen Dateileitungsoperationen zu der Zeit der Ausrichtung der Dokumente zu versichern. Es ist mit einem Dokument für Änderungen in einem getrennten Tisch verbunden kann beobachtet werden muss sein. In so viel hat sich der Gegenstand des Dokumentes geändert, lassen Sie die Software ihm und in den vorangegangenen Ereignissen tűntesse der ursprüngliche Gegenstand des Dokumentes Zeichen geben. In Bezug auf die Erleichterung der schnellen auffindbaren und statistischen vorteilhaften Informationen, wenn System auf die fähige Sammlerzahl-Registrierung, Sie irgend etwas anderes gemäß Gesichtspunkten auf die Dokumentengruppierung, und für den Benutzer auf die Dokumentation ihrer Arbeit sind, gibt einer Gelegenheit ihre Tätigkeiten auf ihn, ein Tagebuch behaltend. Die Software muss die schnelle Datensuche auf der Straße von unmittelbaren Datenergebnissen versichern. Es ist notwendig im Stande zu sein, die Integration mit den Informatikanwendungen anderer Spezialitäten die

erfolgreichen Informationen, das Dokument im Interesse einer vorübergehenden Einnahme zu vollbringen. [9]

Zusammenfassung

Wir haben die allgemeinen Gesichtspunkte des Dokumentes, eines Dokumentes, eines Dokumentes entworfen, das sein Konzept und die Dokumente in der ersten Hälfte des Artikels gruppiert. Im Anschluss daran haben wir gemachte grundsätzliche Voraussetzungen gegen die Datei Betriebssoftware ausgedrückt, die an Organen verwendet sind, die eine öffentliche Aufgabe in der zweiten Partei des Artikels durchführen, mit der Anwendung praktischer Erfahrungen und 2004. évi CXL. Gesetz a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól, továbbiakban Ket. und 335/2005. (XII. 29.) Verordnung a közfeladatot ellátó szervek iratkezelésének általános követelményeiről.

Literatur

[1] 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről
(http://njt.hu/cgi_bin/njt_doc.cgi?docid=23938.287218, 2015.03.10.)
[2] 1952. évi III. törvény a polgári perrendtartásról
(http://njt.hu/cgi_bin/njt_doc.cgi?docid=305.287365, 2015.03.10)
[3] Éva Farkas: Bevezetés a könyvtári információkeresés technikájába
(http://www.bdf.hu/konyvtar/informaciokereses/index.htm, 2014.12.02.)
[4] Géza Gaul: Irodaautomatizálás
(http://www.sze.hu/~gaul/tszhonlap_public/iroda/irodaut1.pdf, 2015.03.10.)
[5] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól
(http://njt.hu/cgi_bin/njt_doc.cgi?docid=85989.290128, 2015.03.10.)
[6] 2009. évi CLV. törvény a minősített adat védelméről
(http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.287593, 2015.03.10)
[7] 2013. évi V. törvény a Polgári Törvénykönyvről
(http://njt.hu/cgi_bin/njt_doc.cgi?docid=159096.239298, 2015.03.10.)
[8] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
(http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.287254, 2015.03.10.)
[9] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

(http://njt.hu/cgi_bin/njt_doc.cgi?docid=96458.290541; 2015.03.10.)
[10] Pándi, Erik – Pándi, Balázs: Structural changes among domestic closed-purpose networks, Kommunikáció 2007. 511 p. ISBN 978-963-7060-31-1
[11] Tóth András – Farkas Tibor – Pándi Erik: A válságreagáló műveletek híradó- és informatikai rendszerének megszervezése, Hírvillám, ISSN 2061-9499 1/1. 13-31., 2010.
[12] Tóth András- Farkas Tibor – Pándi Erik: A válságreagáló műveletek híradó és informatikai támogatásának elméleti alapja, Hadmérnök 5. pp. 425-436. (2010), ISSN 1788-1919

Répás Sándor: Kritikus infrastruktúrák interdependencia vizsgálata hálózati szimulátor alkalmazásával

Absztrakt
A súlyos természeti katasztrófák, a terrorizmus fenyegetése, valamint a kiberhadviselés fejlődése mind egyre fontosabbá tették a kritikus infrastruktúrák üzembiztonságának vizsgálatát, melynek fontos területe az interdependencia vizsgálat. Ennek a vizsgálatnak egy lehetséges módszere, az eseményvezérelt diszkrét idejű hálózat szimuláció kerül bemutatásra.

Abstract
Serious natural disasters, threats of terrorism, cybercrime and the spread of cyberwarfare are all forced the analysis of critical infrastructures by the aspect of secure operation. The interdependences of the different critical infrastructures are critical parts of such examinations whereby one possible method could be the event-driven discrete-event simulation. Discussing further this solution.

Bevezetés

A modern társadalmak működéséhez elengedhetetlenül szükség van különböző infrastruktúrák szolgáltatásaira, melyek folyamatosan biztosítják az emberek életének és a gazdaság működésének feltételeit. Ilyen infrastruktúra lehet például az energiaellátás, az infokommunikáció, a közlekedés, de a pénzügyi rendszer is. Könnyen belátható, hogy a felsoroltak közül bármelyik elégtelen működése komoly károkat okoz a társadalomban, így ezen infrastruktúrák kielégítő működése kritikus fontosságú. Az Amerikai Egyesült Államok (USA) elnökének 1998-ban megjelent irányelve szerint: a kritikus infrastruktúrák olyan fizikai, vagy kiber alapú rendszerek, melyek létfontosságúak a gazdaság és az állam működéséhez [1]. Ezen rendszerek rendkívül komplex felépítésűek és egymással függőségi kapcsolatban állnak, a technológia folyamatos fejlődése következtében pedig a rendszerek komplexitása is folyamatosan nő, ráadásul egyre nagyobb mértékben informatikai eszközökkel automatizált. A súlyos természeti katasztrófák, a terrorizmus fenyegetése, valamint a kiberhadviselés fejlődése mind egyre fontosabbá tették a kritikus infrastruktúrák üzembiztonságának vizsgálatát, melynek fontos területe az interdependencia vizsgálat is, azaz annak meghatározását, hogy a kritikus infrastruktúrák milyen hatással vannak más kritikus infrastruktúrákra, működésük, vagy épp meghibásodásuk, hogyan befolyásolja más infrastruktúrák működését.

Egy ilyen számtalan rendszerből álló rendkívül komplex rendszer vizsgálatára az analitikus módszerek nem alkalmazhatóak hatékonyan, azonban a szimuláció, a modellezés segítségével sok felmerülő kérdésre választ kaphatunk.
A cikk a következő témákat veszi sorra: elsőként a kritikus infrastruktúrák meghatározása, majd az interdependencia fogalma és annak vizsgálata következik.
Ezután az aktuális kutatási eredmények rövid bemutatása, majd a szimulációs módszer alkalmazásának ismertetése, végül pedig a konklúzió következik.

1. Kritikus infrastruktúrák

Annak érdekében, hogy a kritikus (másképpen létfontosságú) infrastruktúrák egymásra hatását vizsgálni lehessen, először meg kell határozni a kritikus infrastruktúrákat, azonban már ez a meghatározás is nehézségekbe ütközik, meghatározásuk nem egységes [2].
Az USA Patriot Act [3] 1016/e. pontja a következőképpen határozza meg a kritikus infrastruktúrákat: olyan fizikai vagy virtuális rendszerek vagy eszközök, amelyek annyira létfontosságúak az USA számára, hogy bármelyikük működésképtelensége vagy megsemmisülése végzetes hatással lehet a biztonságra, a nemzetgazdaság biztonságára, a lakosság egészségére vagy biztonságára, vagy az előbbiek bármilyen kombinációjára.
Az Európai Bizottság közleményének [4] meghatározása a következő: olyan eszközök, illetve azok részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, ideértve az ellátási láncot, az egészségügyet, a biztonságot, valamint az emberek gazdasági és társadalmi jólétét is. Az Európai Tanács irányelve [5] alapján: azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.
A 2012. CLXVI. létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján a következő ágazatok tartoznak a kritikus infrastruktúrák közé [6]:

- Energia
- Közlekedés
- Agrárgazdaság
- Egészségügy

- Pénzügy
- Ipar
- Infokommunikációs technológiák
- Víz
- Jogrend – Kormányzat
- Közbiztonság – Védelem

A következőkben mi is ezt a felosztást alkalmazzuk, mert némileg eltérő csoportosításban ugyan, de nagyrészt más források is ezen ágazatokat tekintik kritikus infrastruktúráknak [7].

2. Interdependencia

Az egyes infrastruktúrák működtetéséhez szükség van más infrastruktúrák igénybevételére. Talán a legjobb példa erre az energiaellátás, hiszen szinte minden tevékenység elvégzéséhez szükség van energiafelhasználásra.
Rinaldi és társai az elsők közt végeztek fontos kutatásokat a kritikus infrastruktúrák interdependenciájával kapcsolatban. Minden kritikus infrastruktúra közös jellemzője, hogy egymással kölcsönhatásban lévő komponensekből áll, és egy tanulási folyamat során gyakran változik, azaz komplex adaptív rendszer (CAS). A hatékony vizsgálat érdekében a CAS-ok, tehát a kritikus infrastruktúrák egyes elemeit intelligens ágensekként kezelték. [8]. Definíciójuk szerint: „Az interdependencia egy kétirányú kapcsolat két infrastruktúra között, melyen keresztül mindkét infrastruktúra állapota hatással (vagy korrelációban) van a másik állapotára. Általánosabban megfogalmazva, két infrastruktúra interdependens, ha mindkettő függ a másiktól.” Kutatásuk során négy interdependencia típust határoztak meg:

- Fizikai: két infrastruktúra fizikailag interdependens, ha mindkettő állapota függ a másik kimenetétől. Más szavakkal, ha az infrastruktúra működéséhez szükség van a másik infrastruktúra által előállított árucikkre.
- Kiber: egy infrastruktúra kiber interdependenciával rendelkezik, ha állapota függ az információs infrastruktúrán átvitt információktól.
- Földrajzi: infrastruktúrák földrajzilag interdependensek, ha egy helyi környezeti esemény képes mindegyik állapotában változást előidézni.
- Logikai: két infrastruktúra logikailag interdependens, ha mindkettő állapota függ a másik állapotától, de nem fizikai-, kiber-, vagy földrajzi- kapcsolat által.

A fentiektől kissé eltérő interdependenica típusokat határoztak meg

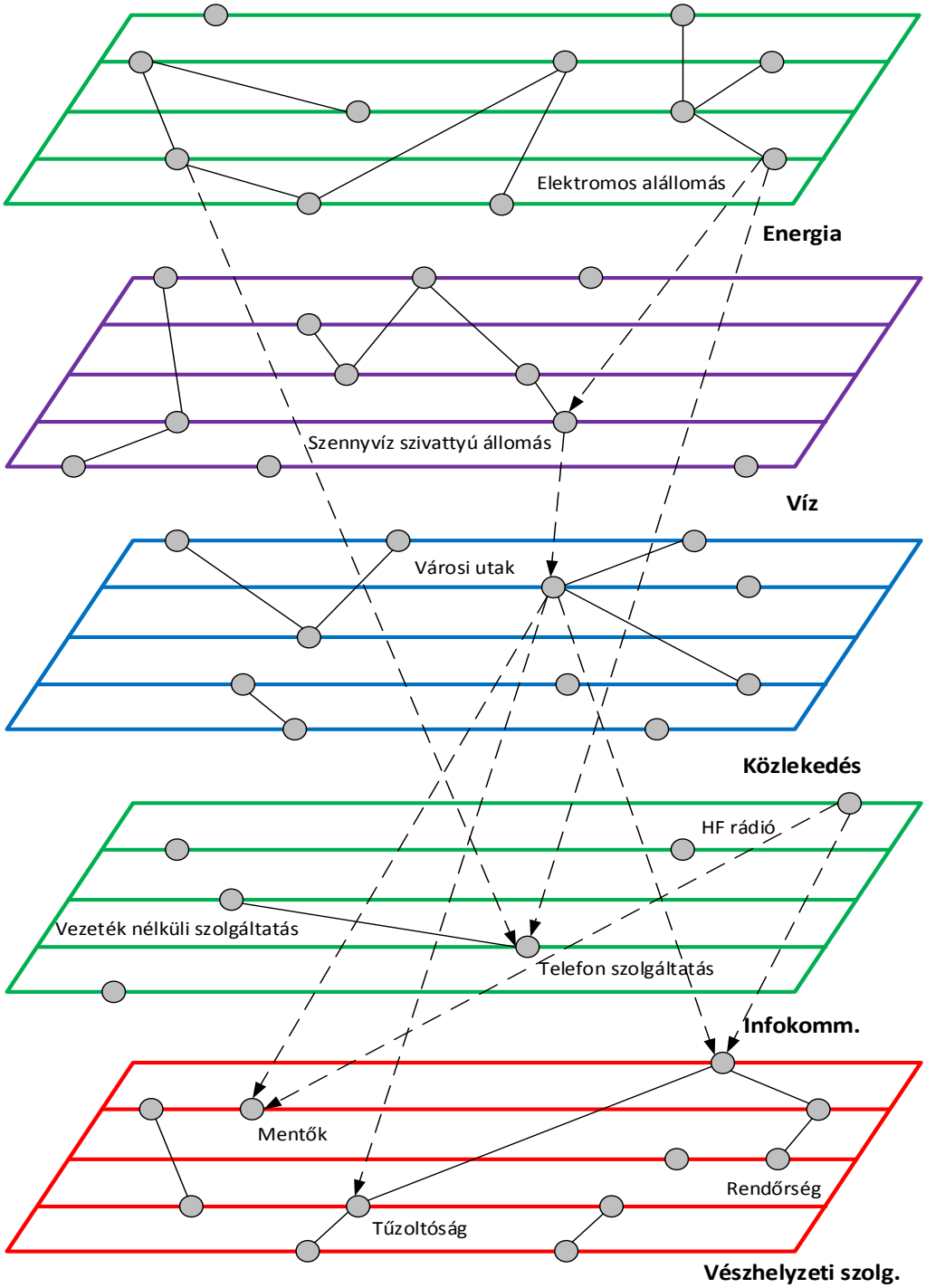
Dudenhoeffer és társai [9]:

- Fizikai: direkt összeköttetés az infrastruktúrák között, olyanok, mint szállítói, fogyasztói, termelési.
- Térinformatikai (gaospatial): infrastruktúraelemek azonos helyen kerülnek elhelyezésre.
- Politikai: infrastruktúraelemek kötődése politikai vagy magas szintű döntéshozatal által.
- Információs: infrastruktúrák közötti kötődés vagy bizalom az információáramlásban.

Porcellinis és társai ezen kívül bevezették még a szociális interdependencia típusát is [10]. A [13] alapján az interdependenciák ábrázolására látható példa az 1. ábrán, valamint egy, a függőségek mértékét is mutató, ábrázolásra az I. táblázatban. A függőségek matematikai formalizálására kidolgozott módszer található [9]-ben, a formalizálás során 9 definíció került alkalmazásra. Az 1. ábrán látható egy nagyon leegyszerűsített árvízi esemény, valamint a rá adott válaszok. Minden egyes sík egy infrastruktúrát jelképez. Egy síkon belüli vízszintes vonal egy-egy szektort, vagy az adott infrastruktúra egy részhalmazát jelzi. A szürke pontok pedig a kulcsfontosságú elemeit jelölik az infrastruktúrának. Az ágazatokon belüli interdependenciákat az összekötő vonalak, míg az ágazatok közöttieket a szaggatott nyilak jelölik.

Egy infrastruktúra elégtelen működésének hatása egy másik infrastruktúrára lehet első, vagy többed rendű. Első rendű, ha meghibásodása közvetlenül befolyásolja a másik infrastruktúra működését, ugyanakkor többed rendű, ha áttételesen befolyásolja azt.

Az interdependenciák megnövelik a meghibásodásokból eredő sebezhetőséget, valamint ezáltal a kockázatokat [11]. Minél több interdependencia van egy infrastruktúra elemei közt, valamint az infrastruktúrák között, annál komplexebb az infrastruktúrák rendszere, aminek következtében egy kisebb meghibásodás is könnyen továbbgyűrűzhet, ezáltal pedig lényegesen nagyobb hatással lehet a rendszer egészének működésére. Éppen ezért az interdependenciák pontos meghatározása, vizsgálata nagyon fontos terület, melynek fontos, jól alkalmazható eszköze a modellezés, a szimuláció.



1. számú ábra: Infrastruktúrák interdependenciája

TÁBLÁZAT I. FÜGGŐSÉGI MÁTRIX MINTA [13]

Ágazat		Energia és közmű					Szolgáltatások		
	Elem	Villamos energia	Víztisztítás	Szennyvíz	Földgáz	Olaj	Vám és bevándorlás	Korház és egészségügy	Élelmiszeripar
Energia és közmű	Villamos energia		L			M			
	Víztisztítás	H				M			
	Szennyvíz	M	H			H			
	Földgáz	L				L			
	Olaj	H	L						
Szolgáltatások	Vám és bevándorlás	H	L	L	L	L		L	
	Korház és egészségügy	H	H	L	H	H	M		H
	Élelmiszeripar	H	H	H	L	M	M	L	
Függőség mértéke:	L: alacsony, M: közepes, H: magas								

1. számú táblázat: Függőségi mátrixminta

3. Aktuális kutatási eredmények rövid áttekintése

Rengeteg nemzetközi publikáció jelent meg, mely a kritikus infrastruktúrák interdependenciájának vizsgálati lehetőségeit tárja fel különböző modellek és szimulációk alkalmazásával. A téma fontossága ellenére azonban, csak elenyésző számú magyarországi publikációt sikerült fellelni.

Rinaldi már 2004-ben hangsúlyozta a modellezés és szimuláció kiemelt jelentőségét a kritikus infrastruktúrák vizsgálatában [12]. Munkájában a lehetséges modellezési megoldásokat 6 nagyobb kategóriába sorolta a következők szerint:

- Aggregate Supply and Demand Tools
- Dynamic Simulations
- Agent-Based Models
- Physics-Based Models
- Population Mobility Models
- Leontief Input-Output Models

A különböző számítógépes modellezési lehetőségekről nagyon jól összeállított

áttekintés található [13]-ban, sajnos azonban mára már több a publikációban ismertetett modell nem lelhető fel.
Chunlei és társai a komplex rendszerek elméletének alapján vizsgálta modellezés és elemzés lehetőségét [14]. Véleményük szerint a kritikus infrastruktúrák modellezésen és szimuláción alapuló vizsgálata az egyik legfontosabb módszer a kritikus infrastruktúrák jellemzőinek vizsgálata során.
Gyarmati döntéselmélet és játékelmélet segítségével modellezi a kritikus infrastruktúrát üzemeltető és támadó viselkedését [15], valamint a kockázatokat [16].
Varga és Illési a kritikus infrastruktúrák hatás alapú modellezését vizsgálta [17]. Eredményeik alapján a modellben szerepelnie kell a kritikus infrastruktúra hierarchiának, tehát a kritikus infrastruktúra elemeknek, a szervezeteket, valamint felépítésében követnie kell a jogszabályi ágazati struktúrát. Ezen kívül a modellnek tartalmaznia kell az egyes kritikus infrastruktúrák elvesztésének:

- hatókörét,
- nagyságrendjét,
- időbeni hatását.

4. Hálózati szimuláció alkalmazása kritikus infrastruktúrák interdependencia vizsgálatára

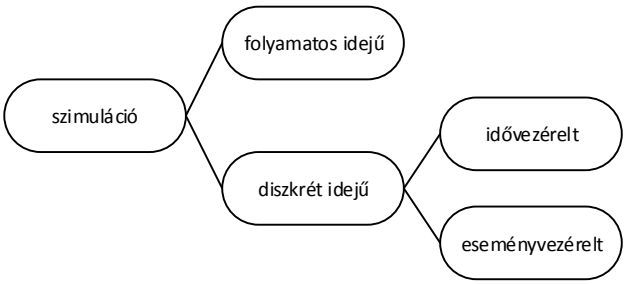
Szimuláció

A következőkben a diszkrét idejű hálózat szimuláció alkalmazási lehetőségeit vizsgáljuk meg. Anélkül, hogy a szimulációk működésébe részletesen belemennénk, néhány alapfogalom [18] alapján:
A szimuláció számítógép által végrehajtható modellen végzett kísérlet. A 2. ábrán látható a lehetséges szimulációfajták egyfajta osztályozása.
Diszkrét idejű szimuláció (Discrete Event Simulation, DES) esetén a rendszer állapotváltozásai csak egymástól elkülöníthető időpontokban történhetnek.
Eseményvezérelt szimuláció (Event-driven) esetén csak azokkal az időpontokkal foglalkozunk, melyekben olyan események történnek, melyek a rendszer állapotát megváltoztatják.
Az Eseményvezérelt diszkrét idejű szimulációk (event-driven discrete-event simulation) alkalmazása széles körben elterjedt módszer az infokommunikációs hálózatok teljesítményének vizsgálata során [19]. Egy sokoldalú, moduláris ED-DES eszköz az OMNeT++ [20], mely elsődlegesen hálózatok szimulációjára készült.

A kritikus infrastruktúrák mindegyike leírható egy-egy hálózatként. A hálózatokon belül, valamint az egyes hálózatok között is folyamatos kommunikáció zajlik. Az infrastruktúra normál működése esetén ez a kommunikáció zavartalanul folyik, míg zavar, meghibásodás esetén a kommunikáció folyamatában zavarok lépnek fel, mely zavarok más hálózati elemek működését is befolyásolják, ezáltal az intra-, valamint az interdependenica vizsgálatára jól alkalmazhatóak.
Kétség kívül minden szimuláció esetében a megfelelő modell elkészítése a legnehezebb és legtöbb erőforrást igénylő feladat. A modell részletességétől, valamint kidolgozottságától függően több kérdésre is választ kaphatunk szimulációk segítségével. [13] alapján, ilyenek lehetnek:

- Bizonyos események bekövetkezése milyen hatással van egyes infrastruktúra elemekre (csomópontok).
- Adott hálózat, valamint kívánt végállapot esetén, milyen események vezethetnek egy következményhez.
- Adott események és következmények alapján milyen interdependenciák állapíthatóak meg.
- Adott hálózat esetén, melyek a legkritikusabb funkciók, és elemek (csomópontok), melyek a legnagyobb hatást váltják ki direkt, vagy indirekt módon.

Egy egyszerű példával megvilágítva: Vizsgálható, hogy milyen hatása van egy elektromos alaphálózati vezeték (400kV) meghibásodásának a teljes elektromos energiaellátásra (intradependencia), valamint, a mobil távközlésre, közlekedésre, stb. (interdependencia).



2. számú ábra: szimuláció típusok

Modell elkészítése

A [21] eredményeit felhasználva, valamint [22] alapján egy OMNeT++ rendszerben, valamint [22] alapján egy OMNeT++ rendszerben történő szimulációhoz szükséges számítógépes modell elkészítésének lépései:

a) A modellezni kívánt infrastruktúrák összegyűjtése.
b) Az egyes infrastruktúrák topológiájának elkészítése.
c) Az infrastruktúra elemek funkcióinak meghatározása.
d) Az egyes elemek sérülékenységeinek meghatározása.
e) Az egyszerű modellek (modules) elkészítése a szimulációs rendszerben.
f) Az összetett modellek (modules) elkészítése a szimulációs rendszerben.
g) Az egyes infrastruktúrák topológiáinak elkészítése a szimulációs rendszerben.

Problémák

A számítógépes szimuláció alkalmazásának is vannak hátrányai, és korlátai. A legnagyobb problémát a pontos, és kellően részletes modell elkészítése okozza. Fontos, hogy egy modell minden esetben a valós rendszernek csak leegyszerűsített mása lehet. A modell elkészítése során meg kell hozni a döntést, hogy mennyire részletes legyen az elkészült modell, mert ez befolyásolja az egyszerű modellek elkészítését, melyekre az egész modell épül. Egy egyszerűbb modell elkészítése rövid idő alatt, alacsony költségráfordítással elkészülhet, azonban segítségével a szimuláció eredménye csak távolról közelíti egy esetleges valós esemény kimenetelét. Egy részletes modell elkészítése nagyon időigényes és sok információt igényel a valós kritikus infrastruktúrák rendszeréről, ráadásul az egyes szimulációk elvégzése nagyon időigényes lehet, mely alkalmatlanná teszi a modell alkalmazását, annak ellenére, hogy léteznek módszerek a szimulációk végrehajtásának gyorsítására [23].

Összegzés

A kritikus infrastruktúrák organikus fejlődése során egyre komplexebb rendszerek alakulnak ki, melyek egymásra hatása analitikus módszerekkel csak nagyon nehezen vizsgálható. A számítógépes szimulációk fejlődésével azonban nagyon fontos eszköz áll rendelkezésre az interdependencia vizsgálatok elvégzésének elősegítésére, a különböző lehetséges forgatókönyvek vizsgálatára. Ugyanakkor egy megfelelően pontos eredményeket produkáló, kellően pontos modell elkészítése nehéz és költséges feladat, de nem elkerülhető a megfelelő szintű kritikus infrastruktúravédelem számára.

Felhasznált irodalom

[1] Presidential Decision Directive/NSC-63, Elérhető: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
[2] Z. Précsényi és J. Solymosi, "Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé," Hadmérnök, vol 2. no. 1, pp. 65-76, 2007. Elérhető: http://hadmernok.hu/archivum/2007/1/2007_1_precsenyi.pdf
[3] USA PATRIOT Act (H.R. 3162), https://epic.org/privacy/terrorism/hr3162.html
[4] COM(2006) 787 final 2006/0276 (CNS) Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Elérhető: http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=kCs9Jn7SPNLsXgYnTvnTsSQ18rTrGb6DhMWcQnQsTCsd1Bqzk02Q!-895171320?uri=CELEX:52006PC0787
[5] A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, Elérhető: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:HU:PDF
[6] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=155940.287727
[7] E. A. M. Luiijf és M. H. A. Klaver, "Protecting a nation's critical infrastructure: the first steps," in *Proc. 2004 IEEE International Conference on Systems, Man and Cybernetics*, The Hague, 2004. pp. 1185-1190. doi: 10.1109/ICSMC.2004.1399785
[8] S. Rinaldi, P. Peerenboom és T. Kelly, "Identifying, understanding and analyzing critical infrastructure interdependencies," IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, 2001.
[9] D. D. Dudenhoeffer, M. R. Permann és M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," in *Proc. 2006. WSC 06. Winter Simulation Conference*, Monterey, 2006. pp. 478-485. doi: 10.1109/WSC.2006.323119
[10] S. D. Porcellinis, R. Setola, S. Panzieri és G. Ulivi, "Simulation of heterogeneous and interdependent critical infrastructures," International Journal of Critical Infrastructures, vol. 4, no. 1/2, pp. 110-128, 2008. doi: 10.1504/IJCIS.2008.016095
[11] L. Xiao-Juan és H. Li-Zhen, "Vulnerability and interdependency of critical infrastructure: A review," in *Proc. Third International Conference on*

Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA 2010), Shenzen, 2010. pp. 1-5. doi: 10.1109/INFRA.2010.5679237

[12] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in *Proc. 37th Annual Hawaii International Conference on System Sciences (HICSS-37)*, Island of Hawaii, 2004. doi: 10.1109/HICSS.2004.1265180

[13] P. Pederson, D. Dudenhoeffer, S. Hartley és M. Permann, "Critical infrastructure interdependency modeling: A survey of U.S. and international research," Idaho National Laboratory, 2006.

[14] W. Chunlei, F. Lan és D Yiqi "National critical infrastructure Modeling and analysis based on complex system theory," in *Proc. First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, Beijing, 2011. pp. 832-836. doi: 10.1109/IMCCC.2011.211

[15] J. Gyarmati, "Kritikus infrastruktúra modellezése döntéselmélet és játékelmélet segítségével," Hadmérnök, vol. 8. no 1, pp. 65-78. 2013. Elérhető: http://hadmernok.hu/2013_1_gyarmatij.pdf

[16] J. Gyarmati, "Kritikus infrastruktúra kockázatának modellezési lehetőségei," Bolyai Szemle, vol. 22. no. 1, pp: 51-62, 2013. Elérhető: http://uni-nke.hu/downloads/bsz/bszemle2013/1/bszemle_2013_1.html

[17] P. Varga és Zs. Illési, "Kritikus infrastruktúrák hatás alapú modellezése," Hadmérnök, vol. 4. no 4, pp. 390-399. 2009. Elérhető: http://hadmernok.hu/2009_4_vargap_illesi.pdf

[18] G. Lencse. Számítógép-hálózatok. Universitas-Győr, pp. 173-178. 2008.

[19] G. Lencse, I. Derka és L. Muka, "Towards the efficient simulation of telecommunication systems in heterogeneous distributed execution environments," in *Proc. 36th International Conference on Telecommunications and Signal Processing (TSP 2013)*, Rome, 2013, pp. 304-310. doi: 10.1109/TSP.2013.6613941

[20] OMNeT++, http://omnetpp.org/

[21] M. Ouyang, L. Hong, Z-J. Mao, M-H. Yu és F. Qi, "A methodological approach to analyze vulnerability of interdependent infrastructures," Simulation Modelling Practice and Theory, vol. 17. no. 5, pp. 817-828. 2009. doi: 10.1016/j.simpat.2009.02.001

[22] A. Varga, OMNeT++ User Manual Version 4.6, 2014. Elérhető: http://www.omnetpp.org/doc/omnetpp/Manual.pdf

[23] G. Lencse és I. Derka, “Testing the Speed-up of Parallel Discrete Event Simulation in Heterogeneous Execution Environments,” in Proc. 11th Annual Industrial Simulation Conference (ISC'2013), Ghent, 2013, pp. 101-107.
[24] Pándi, Erik – Pándi, Balázs: Structural changes among domestic closed-purpose networks, Kommunikáció 2007. 511 p. ISBN 978-963-7060-31-1
[25] Tóth András – Farkas Tibor – Pándi Erik: A válságreagáló műveletek híradó- és informatikai rendszerének megszervezése, Hírvillám, ISSN 2061-9499 1/1. 13-31., 2010.
[26] Tóth András- Farkas Tibor – Pándi Erik: A válságreagáló műveletek híradó és informatikai támogatásának elméleti alapja, Hadmérnök 5. pp. 425-436. (2010), ISSN 1788-1919

Szabó Gergő: Stratégiai kommunikáció I.

Absztrakt
Jelen cikk összefoglalja a startégiai kommunikáció jelentőségét.

Abstract
This article shows relevance of startegic communication.

Bevezetés

A katonai berkekben tapasztalt izgalom a „stratégiai kommunikáció" és a „befolyásolás" körül jelzi annak a ténynek az újra felfedezését, hogy a háború sikeressége szubjektív. Általában nem vezet közvetlen út a győzelemhez, sokkal inkább alacsony intenzitású konfliktusokkal [45] és a média által okozott reflektorfénnyel szegélyezett kacskaringós útvesztőben kell megtalálni a győzelemhez vezető ösvényt. De mi számít győzelemnek? A győzelem talán, hogy meggyőzzük az embereket, hogy azt tegyék, amit akarunk és, hogy azt higgyék, amit akarunk. Ha ezt elértük, megtettük az első és legfontosabb lépést a végső siker felé.
Ebben a tudományos cikkben a stratégiai kommunikációt övező kérdésekre igyekszem választ találni:

- Mi is a stratégiai kommunikáció?
- Különbözik-e az eddig megszokott kommunikációs eljárásoktól?
- Miért van szükség új fogalomra?
- Milyen elméleti igény miatt született az eljárás?
- Mennyiben érinti a katonák mindennapi életét?
- Mennyiben érinti ez a híradó szakcsapat mindennapi életét?

A kutatásom alapját szolgáló elveket és eljárásokat elsősorban a nyugati hadikultúra irányából vizsgálom. Egyrészt a nyelvi korlátok miatt más irányba nem tudok kitekinteni, másrészt Magyarország és a Magyar Honvédség is a nyugati hadikultúrához tartozik.
NATO tag lévén a jövőben is lesz példa arra, hogy több nemzeti, szövetségeseinkkel együtt, missziós műveletekben fog részt venni a Magyar Honvédség. Ezért kiemelten fontosnak tartom, hogy a kutatáshoz kapcsolódó NATO dokumentumok

[45] Low Intensity Conflict; hagyományos fegyverekkel vívott konfliktus.

vizsgálata szerepeljen a dolgozatban, a megértése és feldolgozása ezeknek a dokumentumoknak elengedhetetlen feltétele a hatásos együttműködésnek.

A dolgozat során külföldi, elsősorban angol forrásokkal dolgoztam. A téma újszerűsége miatt, nagyon kevés hazai publikáció jelent meg a stratégiai kommunikációval kapcsolatban.

1. Stratégiai kommunikáció

A tudományos írásművem első fejezetében igyekszem bemutatni, hogy hogyan alakult ki az igény a stratégiai kommunikációra (SC). Ehhez meg kell vizsgálni a hadviselés generációit és a generációk közötti összefüggéseket. Az elméleti háttér áttekintése után példákat hozok, hogy elsősorban a nyugati szövetségeseink hogyan is kezelték a képesség kialakulását. A fejezet végén bemutatom, hogy hol is helyezkedik el a katonai műveletekben a SC, hogyan épül fel, és mi a módszertana.

Generációk a hadviselésben[46]

Ebben az alfejezetben bemutatom a hadtudomány által általánosan elfogadott három generációt, valamint a szakértők körében megosztó „negyedik generáció”[47]-t. Az alfejezet végén a generációkban megjelenő hasonló elemeket fogom elemezni. Ezek az elemek mind a három (négy) generációban felfedezhetőek és egyre nagyobb hangsúllyal jelennek meg.

A hadművészet, hadtudomány fejlődését egy folyamatos evolúciós folyamatnak tekinthetjük, melynek gyökerei a támadó és védő harcászati eljárások, valamint az emberiség gazdasági, technológiai, demográfiai, kulturális stb. fejlődésében lelhetőek fel. Minden az akció-reakció elvére vezethető vissza, hiszen a védelemben lévő fél reagál a támadó által alkalmazott harcászati eljárásra[48]. Ennek ellenére a modern hadviselés három vízválasztót élt meg.

Az első generációs hadviselést a XVII. század közepétől egészen a napóleoni háborúkig tartjuk számon. Ez egy állandó hadseregek – és így államok – közötti konfliktus, ahol a hadviselő felek szigorú szabályok szerint küzdöttek. A hadseregek felállítása és kiképzése igen költséges volt, így a parancsnokok kerülték a döntő

[46] Kiss Álmos Péter: A negyedik generációs konfliktusok jellemzői és tapasztalatai, Somkuti Bálint: A negyedik generációs hadviselés – az érdekérvényesítés új lehetőségei

[47] A létezése elfogadott az ilyen típusú hadviselésnek, a szakértőket a generációként emlegetése osztja meg. Sokak szerint ez a harmadik generáció egyik alfaja, mások külön generációként emlegetik. A dolgozatnak nem célja, hogy besoroljon valamelyik táborba, viszont a szerző az aszimmetrikus hadviselés létezését elfogadottnak tartja.

[48] Természetesen ez megfigyelhető a magasabb, hadműveleti és a hadászati szinteken is.

ütközeteket. Ha csatára került a sor, akkor is elsősorban a nehezen, lassan manőverező gyalogság fejlődött vonalba. A kiképzés során a katonákba belesulykolták a fegyelmet, így azok az ellenség golyózáporát is fegyelmezetten állták, jobban féltek a saját kiképzőiktől, mint az ellenségtől.
A korszak hadviselésének szigorú és megváltoztathatatlannak hitt szabályaiba hozott forradalmi változást Napóleon, habár neki is a kényszer adta helyzettel kellett megküzdenie, semmint saját újításait alkalmazta volna a harctéren. Napóleonnak a környező államok támadása miatt (és előtte az éppen hatalmon lévő kormánynak) nem volt ideje arra, hogy a besorozott újoncokat kiképezzék olyan szinten, ami a kor szabályai szerint megfelelő fegyelmet biztosított volna a harctéren. Így, ezek az újoncok olyan 'címeres ökörségeket' csináltak, mint például a fedezék keresés. Ez teljesen szembe ment a korszak elveivel.
Ezt a kort más néven a muskéta- és vonalharcászat néven illetjük. A hadseregekre jellemző volt a mobilitás totális hiánya. Az arcvonalak nagyon lassan alakultak ki, hiszen a parancsnokok célja az volt, hogy minél hosszabb arcvonala legye, így nagyobb tűzerővel rendelkezzenek. A harcok csak akkor kezdődtek el, amikor az arcvonal minden katonája elfoglalta a helyét. Ez a hadviselési forma abszolút elavultnak tekinthető.
A generációk között nincs éles határvonal, a hadászati változásokat sok tényező befolyásolta. Nagyon sok példát lehetne hozni, hogy egy egyértelműen későbbi generáció „virágkorában" egy korábbi generációs hadviselést alkalmaznak. Az I. Világháborúban, de még a Koreai- és Vietnámi háborúkban is jellemző volt a szuronnyal vívott közelharc, ahogy a magyar lovasság az egyik legfelemelőbb győzelmét a II. Világháborúban aratta.[49]
A második generáció körülbelül a XIX. század második felében kezdett elterjedni. Az változás már látható volt mind az amerikai polgárháborúban, mind a krími háborúban. A változást elsősorban az ipari forradalom ki- és elterjedése okozta, hiszen ekkorra már az összes államban beindult a tömegtermelés.
A generáció virágkorának az I. világháborút tekintjük. A kor frappánsan jellemezhető a *tüzérség legyőz, gyalogság elfoglal* szószerkezettel. Az új hadviselési forma, valamint az ipari forradalom új „találmányai", a közvetett irányzású tüzérség és a sorozatlövő fegyverek, elsősorban a géppuska, olyan mértékű károkat okozott az élőerőnek – mindkét fél részéről –, hogy az I. világháború első időszakát követően a hadviselő feleknek át kellett gondolniuk ezt a hadviselési formát.

[49] http://www.ng.hu/Civilizacio/2008/06/A_szovjet_frontot_is_attortek_a_huszarok?action=print&back=%2FCivilizacio%2F2008%2F06%2FA_szovjet_frontot_is_attortek_a_huszarok pp. 2. (letöltés dátuma 2014.11.10)

Ezért került át a fókusz az ellenség stratégiai mélységének pusztítására, a hátország kifárasztására. Az ipari potenciál határainak tesztelése, az ellenség felmorzsolása, az utánpótlási vonalak elzárása vált a fő céllá, gondoljunk csak az anyagcsatákra[50] vagy a tengeri blokádokra.

Ebben a korszakban jelentek meg az új fegyvernemek is, elég csak az angolszász erők által 1916-ban bevetett „tank"-ra, a repülőgépekre vagy a mélységi tengeralattjárókra gondolni. Az ipari forradalom civil vívmányainak alkalmazása, például a vasút, lehetővé tette a gyors csapatmozgatásokat, így a hadszíntér térben kibővült, időben felgyorsult.

Az I. világháború végére jelentek meg az olyan alakulatok, amelyek már előre vetítik a következő generáció jellemzőit, gondolok itt a kommandós egységekre vagy a páncélosok tömeges alkalmazására.

Tehát az I. világháború végére megjelent az ellenség hátországának pusztítására irányuló törekvések, más szóval az ellenség **belső összeomlasztása** lett a fő célkitűzés, az élőerő pusztítása helyett. Ezeket a törekvéseket **gyorsan** és az ellenfél elől **rejtetten** kellett végrehajtani. Mivel bizonyos alakulatok a saját erőktől távol hajtották végre a feladataikat, ezért szükségessé vált, hogy nagyobb önállósággal, de mégis a **parancsnoki elképzelés** alapján hajtsák végre a feladatokat.

Ezen elképzelések végrehajtására láthattuk számtalan példát a II. világháború során. A németek előálltak a *„blitzkrieg"* elképzelésükkel, mely a páncélosok és a deszant alakulatok stratégiai mélységbe juttatását jelentette. A cél ugyan az volt, amit már az I. világháború végén megfogalmaztak a háborúzó felek, az ellenfél hátországának elfoglalása, így a **morál pusztítása**, a harci kedv megtörése.

Rommel szavaival: „Következésképpen az állóharcnak mindig az emberek megsemmisítése a célja, ellentétben a mozgóharccal, amely elsősorban az ellenség anyagi erőinek felmorzsolására irányul."[51]

A harmadik generációs hadviselés hattyúdala a Sivatagi Vihar[52]. Ennek a műveletnek a tanulmányozása külön, önmagában megérne egy ilyen dolgozatot. Mivel a dolgozatnak a generációk nem fő része, csupán a téma elhelyezésében és szükségességében játszanak szerepet, ezért a teljesség igénye nélkül írok pár gondolatot a Sivatagi Viharról. A légierő, a haditengerészet és a különleges erők olyan műveleteket hajtottak végre, amelyek az ellenség irányítási pontjait, C2 (Command and Control = Vezess és irányíts) központjait pusztították. Fontos megemlíteni a szárazföldi erők által végrehajtott átkaroló műveletet, a *Hail Mary*-

[50] Az anyagcsata alatt a nagy befektetéssel járó, kis hasznú csatákat értem.

[51] ROMMEL, Erwin: Háború gyűlölet nélkül, P. 37.

[52] 1991.01.16-1991.02.28.

t[53], amelyben 250.000 gyalogos kerülte meg a felderítési információk nélkül maradó iraki erőket.
A negyedik generációs hadviselés, mint elnevezés, és mint köztudatba bekerülő fogalom, az elmúlt évek eredménye. Maga a hadviselési forma a hidegháború ideje alatt kezdett elterjedni. Bizonyos tekintetben a hidegháborúra tekinthetünk egy hatalmas sakk játszmaként az USA és a Szovjetunió között. Ezen időszakban a két szuperhatalom és a tábora úgy próbálta a stratégiai célokat megvalósítani, hogy abba ne húzza bele a másik szuperhatalmat. Ezért olyan eszközökhöz nyúltak, amivel a feladatot gyorsan és rejtetten végre tudták hajtani.
Manapság a fogalom kibővült. A II. világháború után a nemzetközi politika és jog, a globalizáció és a számítástechnika – internet – elterjedésével a média egyre jobban befolyásolja a hadviselést. Gondoljunk csak arra, hogy a médiában megjelent hírek, képek Vietnámról, milyen gyorsan hangolták a közvéleményt a kormány ellen.
Megfigyelhető, hogy a II. világháború után lévő konfliktusokban már nem csak állami résztvevők vannak, hanem megjelentek az államon belüli csoportok, milíciák, törzsek, lázadók, valamint a nem állami szervezetek (NGO = 'Non-governmental organisations') is.
Az előzőeken felül fontos megemlíteni, hogy az egész negyedik generációra jellemző egy aszimmetria, a hadviselő felek erejét, és az általuk alkalmazott eljárásokat tekintve. A legjobb példa erre a 2001. szeptember 11-i terrortámadás a WTC ellen. Ez egy kis befektetéssel, de hatalmas pusztítással járó művelet volt az al-Kaida részéről. Akkora kárt okoztak, amire korábban csak más államok voltak képesek, kisebb szervezetek nem. Az anyagi kár nagysága azonban eltörpült a kultúrára mért csapás mellett. Az amerikai polgárháború óta egyedül a pearl harbor-i csata volt az egyetlen, amely komolyabb károkat okozott volna az USA-nak, amerikai területen. Az al-Kaida a terrortámadással figyelmen kívül hagyta a hadviselés eddigi szabályait és az USA egyik szimbólumát pusztította el.
A negyedik generációs elméletek legfőbb összetevőit le is vonhatjuk ezekből: n**incs meghatározott ellenség**. Nem csak egyenruhások vívják most már a harcokat, hanem olyan harcosok, akik valamilyen eszméért küzdenek, de emellett lehet, hogy a mindennapos „civil" életüket is folytatják. Így előfordulhat az, hogy a nap közben békésen földjét művelő parasztember fog az éjszaka során ránk lőni. Mivel az aszimmetria jelen van, ezért az ellenség képtelen a fegyverek útján elérni a célját, így a célpontok áthelyeződnek a kultúrára, az eszmei célokra. Röviden, hatványozottan igaz, hogy nem a tényleges, fizikai pusztítás a cél, hanem a belső összeomlasztás, a nép támogatásának megszüntetése.

[53] Finlan, A (2003): The Gulf War 1991

Az aszimmetriából adódóan a gyengébb hadviselő fél nem vállalhatja fel a frontális, hagyományos csatákat. Az élőerő pusztítására sokkal inkább improvizált eszközöket vetnek be, például a nyugati világot sokkoló improvizált robbanó eszközöket (IED = Improvised Explosive Device), melyek detonációjakor az elhelyező talán már több száz kilométerre van. A gerillák a céljaik elérése érdekében, illetve a „hit and run" taktika érdekében a tűzerő elé helyezik a mozgékonyságot és a rejtett mozgást.
Az államokon belüli konfliktusokban az ellenállók, a *gerillaharcosok* olyan eszmékért küzdenek, amik megnyerőek a nép számára. Ők a romantikus szabadságharcosok, így az összes tettük jogos és megalapozott, legyen akármilyen szörnyű is az. Így egy állami hadviselő, aki lehet az adott állam kormánya, ahol a polgárháború dúl, vagy egy külső megszálló, például a NATO Irakban és Afganisztánban, hátrányban van. Kis túlzással lehetne mondani, hogy ha a két fél ugyanazt követi el, akkor a gerillák hősök, a kormányerők meg barbárok, hogy meg merték lépni ezt a lépést.
Miért fontos ez? Mao-ce Tung[54] leírta a gerilla hadviselés általános szabályait, ami elsőre légből kapott volt, de a történelem zseniálisan igazolta az ő elméletét. Ezen értekezésében fogalmazta meg, hogy lényegében a harcok a lakosság támogatásáért folynak, a cél a saját támogatói bázis növelése. Hiába van valaki hatalmas túlerőben, ha a lakosság nem áll mellettük a túlerő mit sem ér. Az **információ** értéke felértékelődött.

Hasonlóságok a generációkban, avagy olyan jellemzők, amelyeket tovább viszünk magunkkal

A generációkat vizsgálva négy, nagyon fontos tulajdonságot jegyezhetünk le, amik egyre nagyobb hangsúllyal jelennek meg a későbbi generációkban.

1. Az első a **parancsok most már inkább küldetésnek számítanak**. Minden generációs váltás azzal járt, hogy a hadszíntér térben kibővült és ezen a haderők szétszóródtak. Így, a legkisebb harcászati egységnek is flexibilisen, a főparancsnoki elképzelés szerint kell cselekednie, miközben végrehajtja a művelet célját. Ezt sokszor úgy, hogy mindenféle kommunikáció tiltott, például különleges műveletek esetén, vagy amikor a terep nem engedi az összeköttetés megvalósulását. Ilyenkor is tisztában kell lenni azzal, hogy mi az elképzelése a főparancsnoknak. Látni fogjuk, hogy most már nem csak az a lényeg, hogy a feladatot végrehajtsák, hanem, *hogyan* hajtják azt végre.
2. A második a **manőverezhetőség**. A legélesebb váltás a második és harmadik generáció között vehető észre, a légierő és a páncélos alakulatok

[54] Mao tse Tung,(1961) On guerrilla warfare.

megjelenésével új eljárások jelentek meg. A negyedik generáció ezt megfejelte még a rejtett mozgással is, hiszen mind a két fél rá van kényszerítve a rejtett és gyors mozgásra. Ahogy láttuk a második generáció esetén, az élőerő hatalmas pusztításának elkerülése érdekében inkább a hátország támadása került előtérbe.

3. A harmadik a **központosított logisztika háttérbe szorulása**. A kis harcászati egységek előtérbe kerülésével, a gyors és rejtett mozgás korában nincs lehetőség az utánpótlás folyamatos biztosítására. Így e harcászati egységek számára szinte kötelezővé vált, hogy túléljék mind az ellenséget, mind a földet, ahol a feladatot végrehajtják.
4. A negyedik az **ellenség összeomlasztása**, a fizikai elpusztítás helyett. A célok most már nem az élőerő és a haditechnikai eszközök pusztítása, hanem az ellenség hadműveleti, hadászati és stratégiai központjainak pusztítása. A cél, hogy a nép ne támogassa a háborús elképzeléseket. Az esettanulmányok során ki fogok térni rá, hogy az orosz katonai felső vezetés már most kijelentette, hogy a hadszíntér a fizika síkról az elméleti síkra, **az emberek elméjébe** helyeződött át.

Az ellenség összeomlasztása belülről és a média szerepe

Minden fegyveres konfliktusban megfigyelhető, hogy a világ, akár az érintett országok lakossága, akár a nemzetközi közösség, morális ítéletet hoz a résztvevők fölött és valamelyik oldalára állnak. Ezért minden résztvevő megpróbálja befolyásolni és a saját javára fordítani ezt a folyamatot, így fel tudja használni a lakosságban rejlő tartalékokat, meg tudja győzni az egyéneket, hogy a harcuk jogos, a szövetségeseket pedig arról, hogy továbbra is megéri támogatni őket. Ezekkel az eszközökkel az ellenség harci kedve elvehető, valamint a semlegesek a saját oldalra állíthatóak.

A média az egyik, ha nem a legkétélűbb fegyver a mai világban. Okos és hatékony felhasználásával meg lehet nyerni a tömegeket az ország ügyének, így az adott fegyveres konfliktus támogatásának. Elhanyagolása épp az ellenkezőjét eredményezi; a közvélemény elkezdi megkérdőjelezni a kormány és a haderő által hozott döntéseket.

Az információs környezet befolyásolása fontos minden háborúban, de különösen fontos egy aszimmetrikus konfliktus során, ami sokkal inkább egy kegyetlen verseny az állami résztvevő és az ellenállók között, mintsem tényleges háború; a lakosság megnyerése a cél. Ebben a helyzetben az üzenet közvetítése fontosabb, mint a tényleges katonai műveletek. A nem állami résztvevő ezt sokkal jobban megérti és ki is használja az előnyét.

Mao-ce Tung a gerilla hadviselésről[55] írt értekezésében kifejti, hogy miért fontos, hogy a felek megnyerjék maguknak a lakosság támogatását. A nyugati világ, így a NATO számára ez különösen fontos kérdés. Egy politikai vezetés számára veszélyes és elkerülendő, hogyha a közvélemény ellenük fordul, ez veszélyezteti az újraválasztásukat, rosszabb esetben olyan belső nyomást gyakorol, hogy kénytelen kilépni egy fegyveres konfliktusból (lásd Vietnám esetében).
Mi is a stratégiai kommunikáció? Talán a jól ismert propaganda másként? Álláspontom szerint itt többről és másról van szó. A propaganda alkalmazásáról temérdek példát láthatunk a múltban és jelenben, elég csak az I. és II. világháborús toborzó plakátokra, vagy a győzelmet hirdető plakátokra gondolni. Azonban a definíciókat és eljárásokat vizsgálva bebizonyosodik, hogy eltérő fogalmak, sőt a propaganda csak egy része a stratégiai kommunikációnak.

Stratégiai Kommunikáció

Korunk világában egyre többet kell foglalkozni a kommunikációval. Az internet elterjedésével lecsökkentek a távolságok a Földön, egy Afganisztánban végrehajtott művelet eredményéről akár pár percen belül, a világ másik felén is olvashatnak az emberek. Az internetes cikkek és főleg a hozzászólások félrevezethetik az átlag polgárt, és a választók olyan véleményt formálhatnak, amelyek szembefordítják őket a kormányzattal. Ezért kiemelten fontos manapság, hogy a kormányzat és a hozzá kapcsolódó szervezetek információval lássák el a polgárokat.
A kommunikációs folyamatok során **információval** látjuk el a célközönségeket. Fontos megkülönböztetni, hogy nem adatokat, hanem információkat nyújtunk, hiszen az információ már feldolgozott adat. A **kommunikáció** egy olyan tevékenység mely során az információt eljuttatjuk a feladótól a fogadóig. Kiemelten fontos kihangsúlyozni, hogy nem csak verbális kommunikációról van szó, a **non-verbális** kommunikáció ugyanúgy jelen van, és az is elképzelhető, hogy nagyobb hatásfokkal.
A kommunikációs folyamatok nem stratégiai **érvényűek**. Magát az üzenetet a stratégiai szinten fogalmazzák meg a vezetők, de nem egy, általános célközönségünk van. Az afganisztáni misszió esetében például meg kell különböztetni legalább négy célközönséget; az afgán populációt, a koalíciós erők otthoni lakosságát, a nemzetközi közösséget és az ellenálló tálib erőket. Minden

[55] Mao tse Tung,(1961) On guerrilla warfare. A témával és a hozzá kapcsolódó COIN stratégiákról sok értekezés és kézikönyv készült. Porkoláb Imre alezredes 2008-as doktori értekezése, A különleges műveleti erők szerepe az aszimmetrikus kihívásokból adódó katonai feladatok tükrében, különös tekintettel a nemzetközi terrorizmus elleni küzdelemre, és a FM 3-24.2 átfogóan felöleli, hogy a lakosság megnyerése miként segíti a gerilla hadviselés elleni harcot.

célközönségnek más és más üzenetet kellene szánni, hiszen más az adott közösség érdeke. Az afgán populáció számára sokkal közelibb a konfliktus, nekik a két, szembenálló fél közül kell választani, őket meg kell győzni arról, hogy az ISAF (International Security Assistance Force = Nemzetközi közreműködő biztonsági erő) oldalára álljanak. Az otthoni lakosság számára a fő kérdés, hogy miért is van a koalíció Afganisztánban, számukra erre kell választ adni. A nemzetközi közösséget is ez a kérdés foglalkoztatja, valamint a jogi háttere a missziónak. A tálibok számára szánt üzenet pedig, hogy a harc felesleges, túlerőben vagyunk, adják fel.
Ebből látható, hogy a nincs stratégiai érvényű kommunikáció, nem lehet egy üzenettel az összes célközönséget megszólítani és az oldalunkra állítani. Bármelyik célközönség kihagyása hátrányt jelent. Vietnám esetében láthattuk, hogy milyen eredménnyel jár, hogyha a közvélemény kihátrál a kormányzat és a haderő mögül. A helyi lakosság elveszítése esetén a szembenálló erőnek kedvezünk, hiszen őket látják el információval, nyersanyaggal vagy akár élőerővel. A nemzetközi közvélemény elveszítése politikai nyomást helyez a hadat viselő államokra, ez szankciókat, akár újabb hadviselő felet is eredményezhet. Az előző fejezetből láthatjuk, hogy a modern kori hadviselés egyik alappillére lett az ellenség belső összeomlasztása, így a nekik szánt megfélemlítő, elrettentő üzenetek elengedhetetlenek.
Ezt koránt sem könnyű megvalósítani, hiszen minden egyén elfogult, senkinél sem indulhatunk tiszta lappal. Mindenki a számára hitelesnek tartott forrásból érkező információkat fogadja el igaznak, és cselekszik aszerint. Ezért a sikeres kommunikációhoz kiemelten fontos megérteni a célközösség kultúráját, gondolkodásmódját, összetételét, politikai rendszerét, nyelvét és vallását, hogy ezeknek megfelelően lehessen módosítani az üzenetet.
A cél az, hogy a célközönséget úgy befolyásoljuk, hogy a cselekedeteik az elképzelésünknek megfelelő legyen, nem az, hogy elfogadjanak, kedveljenek minket.
A feladat nem egyszerű, ezt még nehezebbé teszi, hogy a kormányzati szervek, melyek a haderőt is irányítják, egyre több ügynökségre, központra osztódik fel. A szervezetek tevékenységét össze kell hangolni, így a stratégiai kommunikációval kapcsolatban is születtek stratégiák, eljárások, iránymutatások definíciók.
Az Egyesült Államok 2007-es stratégiai kommunikációs stratégiája[56] nem tartalmaz definíciót, inkább irányelvekkel operál:

[56] Strategic Communication and Public Diplomacy Policy Coordinating Committe: U.S. National Strategy for Public Diplomacy and Strategic Communications, 2007 június, p 2.

- Megerősíteni a kötődésünket a szabadsághoz, emberi jogokhoz és a becsületességhez, valamint az emberi egyenlőséghez.
- Azokhoz szólni, akikkel azonos az ideológiánk.
- Támogatni azokat, akik küzdenek a szabadságért és a demokráciáért.
- Szembeszállni azokkal, akik a gyűlölet és elnyomás ideológiájában hisznek.
- Az USA-nak pozitív reményképet és lehetőséget kell kifelé sugároznia, ami az alapértékei között gyökerezik.
- A partnereivel karöltve céljuk, hogy elkülönítsék és elszigeteljék az erőszakos szélsőségeket, akik fenyegetik a szabadságot és a békét.
- Médiumok: televízió, rádió, internet és nyomtatott sajtó.
- Személyek, akik hitelesek: papok, oktatók, újságírók, női vezetők, vállalkozás vezetők, politikusok, tudósok és katonák.
- Kiket kell befolyásolni?
  - Fiatalok, hiszen ők lesznek a jövő szavazói és vezetői.
  - Nők és lányok, a dokumentum egy kutatásra hivatkozik[57], mely szerint a fejlődő országokban a nők oktatása lendíti előre a közösség fejlődését.
  - Kisebbségek.

A NATO a 2010-es Public Affairs Kézikönyvben[58] viszont konkrét definícióval állt elő, amiben közrejátszott az afganisztáni tapasztalat is. Eszerint a stratégiai kommunikáció „A NATO kommunikációjának és képességeinek koordinált és megfelelő használata, mely magában foglalja a Nyilvános Diplomáciát[59], a Közügyeket[60], a Katonai Közügyeket[61], az Információs Műveleteket és a Pszichológiai Műveleteket, hogy támogassa a Szövetség politikáját, műveleteit és tevékenységeit és hogy a NATO közelebb kerülhessen céljai teljesítéséhez.”[62]

A NATO Allied Command Operations (ACO; Szövetséges Műveleti Parancsnokság) már műveleti szinten próbálja megfogalmazni, hogy mi is a stratégiai kommunikáció: „Együttműködve a NATO főparancsnoksággal, a koordinált és megfelelő használata a Katonai Közügyeknek, Információs Műveleteknek és

[57] Uo. p. 4
[58] ACO/ACT (2010): Public Affairs Handbook
[59] Public Diplomacy
[60] Public Affairs
[61] Military Public Affairs
[62] ACO/ACT (2010): Public Affairs Handbook

Pszichológiai Műveleteknek, összehangolva más katonai eljárással és betartva a katonai utasításokat és szabályokat (…).”[63]
Az USA 2010-es Stratégiai Kommunikáció Kézikönyve[64] viszont nem ad konkrét definíciót, ami már nem is probléma, hiszen az előző elvekből, definíciókból már látható a stratégiai kommunikáció sava-borsa.
Összegezve az amerikai és a NATO által kiadott elveket és definíciókat, a stratégiai kommunikáció egy összetett, legfelsőtől a legalsó szintig átívelő folyamat, amely arra irányul, hogy a fontos célközönségek úgy cselekedjenek, ahogy szeretnénk. Ez főleg a NATO esetében problémás, a nyelvi különbségek már önmagában megnehezítik az egységes végrehajtást, az eltérő politikai érdekek pedig tovább bonyolítják a helyzetet.
A stratégiai kommunikáció fontos elemei:

- **Public Diplomacy** (PD = Nyilvános Diplomácia): olyan tevékenység, amely informálja a külföldi célközönséget.[65]
- **Public Affairs** (PA = Közügyek): olyan tevékenység, mely a média segítségével befolyásolja a célközönséget.[66] A legfontosabb különbség a PD és a PA között, hogy míg a PA reaktív és informatív, elsősorban órák, maximum napok állnak rendelkezésre az eljárásokra, addig a PD proaktív és hosszú távú, akár évtizedek is szükségesek a siker eléréséhez.
- **Military Public Affairs** (MPA = Katonai Közügyek): az amerikai szakterminológia különbséget tesz a katonai ügyekben, de ugyanazok az alapelvek, mint a civil PA esetében.[67]
- **Information Operations** (IO = Információs Műveletek): sokan úgy gondolják[68], hogy az információs műveletek a stratégiai kommunikáció hadműveleti szintje, de ez nem igaz, az IO csak egy része az SC-nek. Az amerikai szakterminológia szerint: „Az elektronikai hadviselés, hálózati hadviselés, pszichológiai hadviselés, megtévesztés és műveleti biztonság központi képességeinek integrált bevetése, hogy befolyásolja, megzavarja,

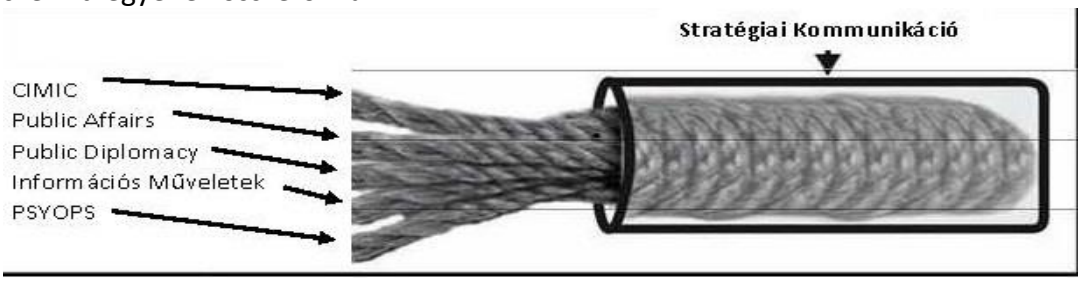
[63] Supreme Headquarters Allied Powers Europe (2012): AD 95-2, ACO Strategic Communications
[64] US Joint Forces Command Joint Warfighting Center (2010): Commander’s Handbook for Strategic Communications and Communication Strategy
[65] Martemucci, M. G. (2007): Regaining the High Ground: The challenges of Perception Management in the National Strategy and Military Operations. P. 4.
[66] Uo. p. 4.
[67] Uo. p.5.
[68] Kiss Álmos Péter (2011): A negyedik generációs konfliktusok jellemzői és tapasztalatai

megfertőzze és megakassza a tanácsadó emberi és automatizált döntéshozó képességeket, amíg a sajátunkat megvédi."[69]

- **Psychological Operations** (PSYOPS = Pszichológiai műveletek): „Olyan megtervezett hadműveletek, amelyek a kijelölt információk és jelzések segítségével képes befolyásolni a külföldi közönségek, kormányok, szervezetek, csoportok és egyének érzéseit, motivációit, cél megállapítását és végezetül a viselkedésüket."[70] PSYOPS műveletekre a legjobb példa, a hatalmas szórólap dobálás, amit az amerikaiak Afganisztánban végrehajtottak, ezzel értesítették az afgán lakosságot a bin-Ladenre kitűzött vérdíjról.[71]
- **Civilian Military Cooperation** (CIMIC = Civil Katonai Együttműködés):" A CIMIC a katonai és a civil oldal kormányzati és nem kormányzati szervezetek, a nemzeti hatóságok, nemzetközi szervezetek, valamint a helyi lakosság között kiépített és fenntartott koordináció és együttműködés a támogatott A fentebbi definíciókban akad némi átfedés, de külön-külön nagy területet ölelnek fel.

Fontos kihangsúlyozni, hogy ezeket az eljárásokat párhuzamosan és sokszor egymástól függetlenül kell végrehajtani. Mivel sokszor nincs idő az egyeztetésre, ezért félő, hogy egymással ütköző üzenetek kerülnek kiosztásra, ami elkerülendő. A következő táblázat bemutatja, hogy hány helyen lehet ütközés és a műveletet tervezőknek, illetve a parancsnoknak mire kell odafigyelnie, amikor a stratégiai kommunikációval kapcsolatos eljárásokat tervezik.

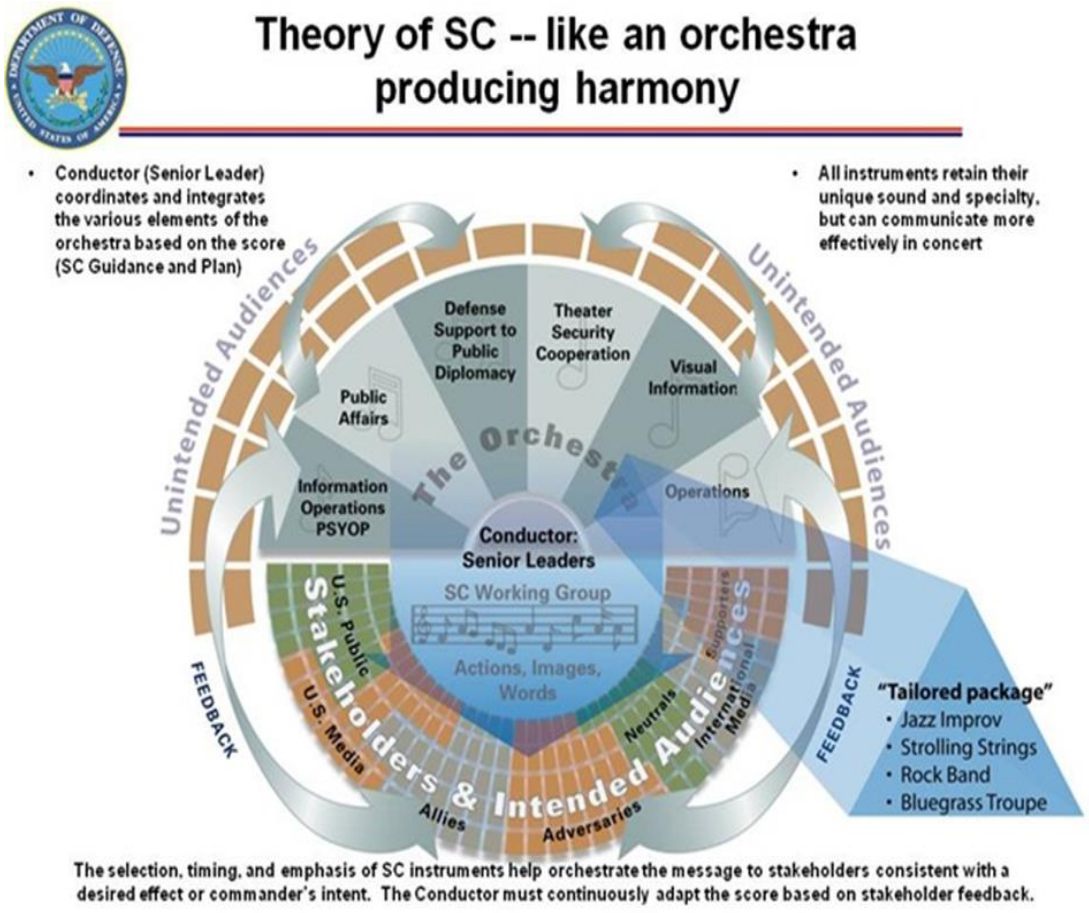
Az SC-t így leginkább egy sok szálból font kötélhez lehetne hasonlítani. A kötélnél elengedhetetlen, hogy minden szál ugyanolyan erős legyen és ugyanazon eljárás szerint legyenek összefonva.



2. számú ábra Kötél hasonlat

[69] Martemucci, M. G. (2007): Regaining the High Ground: The challenges of Perception Management in the National Strategy and Military Operations. P. 8.
[70] DoD : Joint Pub 1-02, "DOD Dictionary of Military and Associated Terms," 2006. augusztus 8.
[71] Uo. p.10

Ennél azonban többről van szó. Szakértők szerint a stratégiai kommunikáció egy zenekarhoz hasonlítható. A karmestere a zenekarnak általában a nemzeti kormánya a megszálló hatalomnak. A hangszerek a kommunikációs terv. A zenekar maga a különböző közösségek és kommunikációs utak, melyek a művelet részét képzik. A zene az üzenet. A zene tempója változtatható a karmester által elérni kívánt hatás függvényében.



3. számú ábra A stratégiai kommunikáció, mint zenekar[72]

[72] http://mountainrunner.us/images/c7f4ec0a6185_9A32/orchestrawtriangle24Jun08.jpg (letöltés ideje: 2014.9.20)

A műveleteinket minden síkon egységesen és azonos hatásfokkal kell végrehajtani, hogyha sikeres stratégiai kommunikációt szeretnénk:

- Fizikai síkon elsődleges a nyilatkozatok és a hozzá kapcsolódó tettek közötti időeltolódás irányítása, valamint a hitelességet aláássa, ha a **tettek** meghazudtolják a szavakat.
- Az információs síkon olyan médiumokat kell megszólítani, melyeket a célközönség elfogad és hitelesnek tart.
- A szociális síkon kell megvizsgálni, hogy az adott célközönség milyen tálalásban fogadja legjobban az üzeneteket.
- A kognitív síkon lehet befolyásolni az üzenet értelmezési lehetőségét.

Milyen módszertant ajánlatos használni az üzenetek tervezésekor?[73]

- Meg kell határozni a politikai célokat.
- Be kell azonosítani a célközönségeket.
- Meg kell határozni, hogy milyen viselkedést kívánunk elérni.
- Végre kell hajtani a célközönség vizsgálatát:
    - Milyenek előítéleteik, a hozzáállásuk és a viselkedési normák?
    - Milyen kívánt hatást szeretnénk elérni az előítéleteikkel, hozzáállásukkal és viselkedésükkel kapcsolatban?
- Be kell azonosítani a témákat, melyeken keresztül meg tudjuk szólítani a közönséget.
- Meg kell formálni a célokat és üzeneteket, tetteket, hogy azok megfelelőek legyenek a célközönség számára.
- Harmonizálni kell a tetteket, szavakat és az irányvonalakat.
- Szinkronizálni kell a médiumokat és az időbeni hatásokat.
- Meg kell jósolni, előzni és akadályozni az ellenség reakcióját.
- Össze kell gyűjteni, frissíteni és elemezni a közönség reakcióját és ennek megfelelően módosítani az üzeneteket.

A módszertan bármelyik lépését meg kell állítsa és felül kell írnia a folyamatos megfigyelésből szerzett új információknak. A stratégiai kommunikáció megtervezésének mindig hamarabb kell megtörténnie, mint a hadműveleti tervezésnek.

2. Esettanulmányok

Ebben a fejezetben két részben, esettanulmányokon keresztül fogom bemutatni a stratégiai kommunikáció működését, és eredményeit. A prezentálás érdekében úgy

[73] Goldman, Emily (2008): Strategic Communication Theory and Application

választottam meg az esettanulmányokat, hogy az egyik sikertelen, a másik sikeres legyen. Így demonstrálható, hogy mi a haszna, ha sikeres és hogy mi a hátránya, ha nem. Az első esettanulmány a NATO afganisztáni missziója, a második a Krími-válság.
Mielőtt belekezdenék a két esettanulmány tárgyalásába, fontos előzetes párhuzamot vonni a két hadművelet között. Először is, fontos kiemelni, hogy a két környezet, Afganisztán és Ukrajna, merőben eltér kulturálisan. A két megszálló hatalom, Oroszország és NATO, viszonylatában ki kell emelni, hogy az előbbinek valószínűleg könnyebb dolga volt, hiszen egy sajátjukkal egyező múltú, kultúrájú így elfogadóbb környezetben hajtotta végre a műveletét.
Másodjára, amikor az Egyesült Államok, később a NATO megszállta Afganisztánt a stratégiai kommunikáció gyerekcipőben járt, Oroszországnak viszont már kész stratégiák, doktrínák és eljárások álltak rendelkezésére, amit jól tudott alkalmazni mankónak.
Harmadjára, a nyugati kultúra közel sem gyakorol akkora nyomást a médiára, mint Oroszország. Az előző fejezet rávilágított, hogy a média segítsége mennyire fontos a teljes hadművelet végrehajtása érdekében. Sőt, ahogy később látható lesz, a NATO-nak és az ISAF-nek meg kellett küzdenie az otthoni médiával is.
Továbbá fontos kihangsúlyozni, hogy Afganisztán közel sem rendelkezik akkora telekommunikációs és infokommunikációs infrastruktúrával, mint Ukrajna. Ez nyilvánvalóan sokkal nehezebbé teszi a kommunikációt a célközönséggel.

Első esettanulmány: A NATO afganisztáni stratégiai kommunikációs veresége

Úgy gondolom, hogy mindenféleképpen foglalkozni kell Afganisztánnal és a NATO ottani kommunikációjával, hiszen ez az legfrissebb, 2014-15 év végére lezáruló missziónk, melyben kulcsfontosságú szerepet kap a kommunikáció.
A sikertelen kommunikáció talán ott kezdődik, hogy az ISAF képtelen volt megindokolni a „Miért vagyunk Afganisztánban?" kérdést. David Betz által készített interjúkban egy amerikai tiszt azt mondta, „9/11 után jöttünk Afganisztánba, azzal az egyetlen céllal, hogy elkapjuk és megbüntessük bin Ladent és az őket védőket és elrejtőket. És ezt követően…. mi csak úgy… itt maradtunk."[74] De a háborúnak komolyabb indok kell, e nélkül, minden más, politika, stratégia, akció megalapozatlan.
Ahogy később majd látni fogjuk, az afganisztáni misszióból hiányoztak a célok és irányelvek, valamint a misszió szenvedett a sokrétű célközönség miatt, hiszen

[74] David Betz (2011): Communications Breakdown: Strategic Communications and defeat in Afghanistan

egyszerre kellett megszólítani az anyaországi lakosokat, Afganisztán szomszédjait, a teljes muszlim világot valamint az afganisztáni lakosokat, akik szintén megosztottak. Ezen túl a misszió maga sem volt egységes, hiszen az USA-nak az elsődleges célja az al-Kaida felszámolása, a koalíciós országoknak, valamint a NATO egységességének biztosítása, bizonyítása és az Egyesült Államokkal való kapcsolat ápolása.
Ebből már lehet látni, hogy miért is nehéz megállapítani a közös, egységes stratégiai irányelveket és célokat; hiszen borzasztóan nehéz, ha nem lehetetlen egy olyan közös kommunikációt folytatni a különböző célokkal, érdekekkel rendelkező célközönségekkel, főleg ha maga a kontingens is megosztott. Ahogy egy ISAF kommunikációs tiszt megjegyezte: „Ez olyan, mintha egy filmet forgatnál húsz rendezővel. Ha sikerül befejezni a filmet, ami már önmagában csoda, unalmas lesz.”[75]
A stratégiai kommunikáció alap gondolata, hogy egy felső szinten megszületett politikai elképzelés, egységesen, egybehangzóan megy végig a rendszeren, egészen a taktikai szintig. De az ISAF erőknél ez nem teljesülhet teljesen, hiszen nem egy ország, vagy akár egy szövetségi rendszer elképzeléséről van szó, hanem több különálló szervezetről. Mindenki arra figyel, hogy hol és mikor fog szerepet kapni, és hogy a kommunikációjával hogyan tudja ezt minél jobban megtámogatni. Hogyan fog az ISAF parancsnok ebből egy mindenkinek megfelelő, célokkal és irányelvekkel is rendelkező stratégiai elképzelést készíteni?
A koalíciós erők afganisztáni kommunikációját időben célszerű három részre bontani, hiszen nagyobb politikai döntések születtek, stratégiai célok teljesültek és ezek merőben megváltoztatták a kommunikációt

2001-2003 időszaka

Ezt az időszakot elsősorban a támadó kommunikáció kísérte. Az Amerikai Egyesült Államok pozitív talajjal rendelkezett a kommunikációt illetően, hiszen a televíziókban folyamatosan sugárzott füstölgő ikertornyok képek a sok baráti országot szimpátiával töltött el az USA irányába.
Ám Bush elnök szavai; „Amit Afganisztánban tenni fogunk egy jelzés lesz a többi ország számára, hogy mennyire is komolyan gondoljuk a terrorizmus elleni háborút”[76], először meghökkentette a nemzetközi közvéleményt és megijesztette a muzulmán világot. Bush retorikája, amelynek során a civilizációk ütközetéről beszél valamint, hogy a terrorizmus elleni háború egy keresztes hadjárat és a „Aki nem

[75] Uo.
[76] Woodward, B. (2003). Bush at war. London: Simon & Schuster

velünk van, az ellenünk."[77] kinyilatkozása nagy kommunikációs hibának bizonyult. A szavai elsősorban az amerikai nemzetnek szóltak, mellyel inspirálni akarta honfitársait és ezek valóban azt az eredményt is váltották ki a lakosságból, melyet az elnök elvárt.

A beszédéről készült felvételek azonban bejárták a világot és természetesen eljutottak az USA ellenségeihez is. Ez hatalmas lehetőséget biztosított az al-Kaida számára, hiszen ez azt jelentette, egy barlangból legyőzheti a világ legnagyobb kommunikációs képességekkel rendelkező nemzetét. Bush üzenetét sokan, köztük a semleges, haladó gondolkodású muszlimok is úgy értelmezték, hogy az Amerikai Egyesült Államok hadat üzent az Iszlám ellen. Később az amerikai kormány próbálta ellensúlyozni a nyilatkozatok által okozott kárt, de nem lehetett meg nem történté tenni.

Habár számos kommunikációs és befolyásoló művelet volt az afganisztáni misszió első két évében, nem volt egy meghatározott stratégiai kommunikációs elv mögöttük. A koalíciós erők nem követték a kommunikációs stratégiai irányelveket – hiszen nem is voltak – a véletlenszerű befolyásoló műveletek pedig elsősorban az éppen aktuális katonai művelet támogatásául szolgált.

Fontos megemlíteni, hogy a Public Affairs csoportok, akik az afganisztáni művelet előtt aktívan részt vettek az akciókban és aktívan kommunikáltak az anyaországgal, ebben az időszakban nagyon ritkán voltak a csapatok közelében, és akkor sem a közvetlen érintkezés környékén. Ez megnehezítette a kommunikációt az anyaországi lakossággal, az otthoniak nem tudták, hogy a misszió hogyan teljesít, egyáltalán sikeres-e?

A befolyásoló tevékenység is nehezen – vagy egyáltalán nem – ért el arra a szintre, ami szükséges lett volna. A műveleteket önállóan, mindenféle stratégiai elképzelés és iránymutatás nélkül, hajtották végre az amerikai PSYOPS csoportok. Ők elsősorban temérdeknyi szórólappal és egy EC 130J Commando Solo[78]-val végrehajtott rádiós üzenetszórást végeztek. Ezzel a műveletek támogatását hajtották végre, valamint próbálták elérni, hogy az afganisztáni lakosok ne támogassák a tálib erőket. A helyi lakosság azonban másodlagos szerepet játszottak a művelet céljaiban, a fő irányvonal továbbra is a terrorista fenyegetés megszüntetése volt. Sajnos bármilyen, az ISAF irányába, pozitív eredményt is értek el a PSYOPS csapatok, ezt ellensúlyozta, ha nem tovább rontotta, a masszív bombázás, ami félelmet keltett a lakosságban. Ez közvetlenül a tálibok és az al-

[77] White House Office of the Press Secretary. (2001 Szeptember). Remarks by the President upon arrival. {online} http://georgewbushwhitehouse.archives.gov/ (letöltés dátuma: 2014.10.30.)

[78] Leginkább egy légierődhöz lehetne hasonlítani, fedélzetén rádiók voltak az üzenetszórás céljából.

Kaida kezére játszott, utóbbi nem is volt rest kihasználni és elferdíteni a tényt; az amerikaiak vallási okokból támadják az országot.

A kezdeti hadműveletek és eljárások totális összhangban voltak az *amerikai* elképzeléssel. A Bush adminisztráció a terrorizmus elleni harc jegyében küldte oda *harcosait,* akiknek célja a „rossz fiúk célbavétele és feltakarítani a tálib rezsim után”[79] volt. Már a hadművelet megkezdése előtt nyilvánvaló volt, hogy a katonákat nem az ország építése érdekében, a lázadás ellen vagy békefenntartó céllal küldik oda. Ezért teljesen érthető a helyi lakosság reakciója, akik aggódtak az országukba érkezett külföldi katonák miatt és, hogy a támadó hadjárat érdekében a koalíciós erők nem fektettek hangsúlyt a szavakra és a kommunikációra.

A sikeres offenzívát követően az ISAF a terrorizmus elleni harc mellett a béke és a nyugalom helyreállítását tűzte ki céljául Afganisztánban. Ekkor kezdtek megjelenni az *információs műveletek*, de csak a partvonal mentén, ugyanis csak ott került alkalmazásra, ahol a legmagasabb szintű törzstisztek is bevonásra kerültek.[80] A konkrét iránymutatások, elvek, stratégiák hiánya miatt ezeket következetlenül, pontatlanul hajtották végre. Az alsó szinteken a PSYOPS csapatokat is bevonták az információs műveletekbe.[81] Elsődleges feladatuk a helyi lakosság informálása volt, nehogy belekeveredjenek a harcokba. Néha kiegészítésre kerültek a Civil Affairs csapatokkal, a cél a helyi lakosok bizalmának elnyerése volt. Ezeket az eljárásokat egész Afganisztán területén folytatták, de csak ideiglenes eredménye volt, a helyi lakosság folyamatosan visszatért az elfogadott sorsához.[82] Amerikának és NATOnak se a képessége, se az igénye nem volt meg arra, hogy a megtisztított területeket úgy is tartsák.

A 2003-as év közepétől az előny újra a tálib erőknél volt. Elsősorban Dél- és Kelet-Afganisztánban értek el sikereket, hiszen a terroristák elleni hajtóvadászata az amerikaiaknak éppen a tálibok hatalmát erősítette. Lassan, de biztosan kezdett megérni a gondolat a felső-vezetőkben, hogy a győzelmet nem a katonai erővel, hanem sokkal inkább a helyi lakosság megnyerésével lehet kivívni. Ami szükség volt az elsősorban egy biztonságra és fejlődésre alapozott irányvonal, melynek egy effektív kommunikációs stratégia az alapja.

---

[79] Jones, S. (2009). In the graveyard of empires: America’s war in Afghanistan. New York: W.W. Norton & Company

[80] Cox, J. L. (2006). Information operations in operations enduring freedom and Iraqi Freedom—What went wrong? Fort Leavenworth, KS: United States Army Command and General Staff College pp. 32-40

[81] Uo pp. 55

[82] Giustozzi, A. (2008). Koran. In Kalashnikov and laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007. New York: Columbia University Press

2003-2006 időszaka

2003-ra a koalíciós erők is megértették, hogy a terrorizmus és a belső lázadás elleni háborút nem csak a fizika síkon, a fegyverek erejével, hanem mentális síkon is kell megvívniuk. Ez elsősorban a tálibok kommunikációs sikerének volt köszönhető, hiszen az előző időszakból, kommunikációs értelemben, egyértelműen ők kerültek ki győztesen.

A tálibok sokkal fontosabbnak tartották a kommunikációs, ezzel együtt a mentális síkon szerzett fölényt. A parancsnokok hajlandóak voltak olyan akciókat végrehajtani, ahol nyilvánvaló volt számukra, hogy harcászati és hadműveleti szinten is vereséget fognak szenvedni. Ennek ellenére ezeket a vereségeket képesek voltak kihasználni; nincs biztonság Afganisztánban, az akció a tálib erődemonstráció része. És sajnos az ilyen akciók általában civil áldozatokkal jártak, ezt a tényt sem voltak restek a koalíciós erők szemére vetni.

Az előző kommunikációs üzenetekkel, és az elmúlt évek eredményeivel a tálib bázis elhitette a nemzetközi közösséggel, hogy Afganisztán a **birodalmak temetője**, és egyik külföldi szuperhatalom sem képes uralni.

Azonban nem csak a nemzetközi közösség megnyerésében léptek előre, a helyi lakosságot is saját maguk felé terelték. Ezt elsősorban a durva eszközökkel, fenyegetéssel, manipulációval és a fegyveres propagandával összehangolt megfélemlítés eredményezte. Rengeteg helyi lakos kapott úgynevezett „éjszakai levelet", melyben finoman figyelmeztetik őket a koalíciós erőkkel való együttműködés veszélyeire.

Azonban a legerősebb üzenetet a „harcászati sikereik" hordozták; hiszen amelyik területet a koalíciós erők megtisztítottak, oda a tálib ellenállók szinte azonnal újra bevonultak.

Hatalmas előnyt jelentett számukra, az amerikaiak szabadesése a nemzetközi megítélésben, amely betudható az iraki háború elindulásának, valamint az emberi jogok megsértésének Guantánamóban, Bagramban és Abu Ghraibban. Ez helyi szinten tovább erősítette a koalíciót övező ellenszenvet.

Az fentebbi eseményekről az Al Jazeera[83] vitte el a hírt a muzulmánoknak. Az Al Jazeera folyamatos hatását próbálta egyensúlyozni az amerikai Public Diplomacy. Létrehozták az Al-Hurra[84] televíziós csatornát és az Al Sawa[85] rádiót, de a kárt nem lehetett meg nem történtté tenni.

[83] www.aljazeera.com , az oldal látogatottsága körülbelül 35-40 milliós napi szinten.
[84] http://www.alhurra.com/info/about-us/112.html
[85] http://www.radiosawa.com/info/about-us-en/108.html

2004 áprilisában, amikor az Al-Hurra televízió létre lett hozva, a Jordan Times élesen bírálta a döntést, szerintük ugyanis „amire az Egyesült Államoknak szüksége van, az nem egy új média stratégia, hanem a változás a politikájában”[86]. A szakadék még sosem volt ennyire mély az USA és az EU között, a közeledés helyett még távolodtak az egyes államok stratégiai irányelvei, céljai és kommunikációi. A nyugati kritikusok elkezdték megkérdőjelezni a misszió legitimációját.

2003-ban az amerikai kormány tudomásul vették, hogy vesztésre állnak a kommunikációs háborúban. Egy 2003-as kritikus belső jelentésben, amely a befolyásoló műveletekről íródott, a Védelmi Minisztérium észlelte, hogy a PSYOPS csapatok kommunikációja nincsenek összhangban a nemzeti témákkal és iránymutatásokkal, és elsősorban reakció az ellenség propagandájára.[87] Donald Rumsfeld később folytatta ezt a gondolatot: „Az ellenségeink ügyesen alkalmazkodtak ahhoz, hogy hogyan vívják meg harcaikat korunk modern, média világában…”[88]

A Védelmi Tudományos Bizottság (Defense Science Board) 2004-es jelentése kulcsfontosságú volt a stratégiai kommunikációról a politikai és katonai szférában. A jelentés szerint, a probléma nem elsősorban a helyes üzenet és médium kiválasztása, sokkal inkább a hitelesség hiánya, ami a politika gyakorlati alkalmazásából fakad.[89] A probléma nem az üzenetek voltak, hanem, hogy a tetteink hangosabban beszélnek, mint a szavaink.[90] Sok politikai döntéshozó meg volt győződve arról, hogy nem a folytatott politika a hibás, hanem ahogyan az prezentálva van a közönség számára.

A 2003–2006 közötti időszak Afganisztánba is elvitték a változás szelét. David Barno tábornok érkeztével, aki átvette az ISAF parancsnoki beosztását Kabulban, a terrorizmus ellenes harc átalakult lázadás ellenivé. Utóbbiban a lakosság megnyerése kulcsfontosságú, ezért a befolyásoló eljárások is célt váltottak, elsősorban a lakosság felé fordították figyelmüket, mintsem az ellenség felé.

---

[86] Kuttab, D. (2004, February 2). America’s Clumsy Reach, Jordan Times. {online} http://www.jordantimes.com/ (letöltés dátuma 2014. október. 29)

[87] United States Department of Defense. (2003 October). Information operations roadmap. Washington, DC: Government Printing

[88] Council on Foreign Relations (2006 February). New realities in the media age: A conversation with Donald Rumsfeld. {online} http://www.cfr.org (letöltés dátuma 2014.11.10.)

[89] Defense Science Board. (2004). Report of the Defense Science Board Task Force on strategic communication. Washington, DC: Government Printing Office pp 3. 41.

[90] Fenton, T. (2009). Thoughts on journalism and the military. In G. J. David Jr. & T. R. McKeldin III (Eds.), Ideas as weapons, influence and perception in modern warfare (pp. 87–92). Dulles: Potomac Books, Inc. pp 92

Megtörtént a publikációja és a szétosztása az amerikai Counterinsurgency Field Manualnak, melyben az alapvető iránymutatások kellő pontossággal le lettek írva. Ez hozzájárult, hogy az információs műveletek, a pozitív cselekedek és szavak legyenek az új stratégia központjai. Sajnos a képzett állomány, a szükséges tudás és tapasztalat hiány miatt ez a harcászati szinten még mindig nem teljesült.
Azonban a földi csapatok ekkor már belátták, hogy az úgynevezett kinetikus műveletek, melyek a rengeteg civil áldozatot okoztak, vagy melyekben rengeteg házat pusztítottak el, milyen reakciót is váltanak ki a helyi lakosságból. A legtöbb parancsnok tisztában lett azzal, hogy a nem-kinetikus műveletekkel talán pozitívabb hatást tudnak kiváltani a helyi erőkben. A tevékenységek viszont még nem voltak összehangolva egy központi stratégiai kommunikáció által mutatott irányelvek és útmutatások alapján.
A PRT (Provintial Reconstruction Teams = Tartományi Újjáépítési Csoportok) nagyon jó példák a nyitásra, hiszen ezen csapatok mutatják a misszió humanitárius oldalát az otthoniaknak és a nemzetközi közösségnek valamint meggyőzhetik a helyi lakosságot a koalíció jó szándékáról. De sajnos ebből kevés realizálódott akkoriban.
Azonban az információs hadműveletek még mindig támogató elemként jelentek meg a katonai akciókban és nem fordítva – mint ahogy majd látni fogjuk Oroszország és Ukrajna vonatkozásában. Ez egészen 2006 végéig nem valósult meg.

2006-2010 időszaka

A NATO 2007-ban publikálta az első stratégiai kommunikációval foglalkozó dokumentumát. A SHAPE (Supreme Headquarters Allied Powers Europe; A Szövetséges Erők Európai Főhadiszállása) által, 2007 október 31-én kiadott dokumentum a „NATO stratégiai kommunikáció képességének fejlesztése" címet viselte. A dokumentumban megvizsgálták és bebizonyították, hogy a nemzetközi közösség megnyerése elengedhetetlen az afganisztáni misszió sikeréhez. A legfontosabb következtetés, hogy a NATO-nak folyamatos és egybehangzó irányelveket és célkitűzéseket kell megfogalmaznia, melyet az összes hadművelet alátámaszt.[91]
2007-ben jelent meg az első ügynökségek közötti dokumentum az USA-ban, melyet a Strategic Communication and Public Diplomacy Policy Coordinating Committee adott ki, Karen Hughes vezérletével. Azóta egyre gyakrabban látnak napvilágot a témával foglalkozó dokumentumok és elképzelések, de nem mindegyik járt sikerrel.

[91] ISAF (2008 October) Theatre strategic communications strategy

Az eddig végrehajtott befolyásoló műveletek elsősorban az afgán lakosság és az ellenség reakcióján alapult és nem vették figyelembe a nemzetközi közösség véleményét, vagy az anyaországban élőkét. Ez 2008 közepére változott meg. 2007 végén az Amerikai Védelmi Minisztérium tervezetet adott ki az afganisztáni stratégiai kommunikációról melyben 12 darab, különböző célközösséget különböztettek meg. Ezt követte az ISAF stratégiai kommunikációs stratégiája 2008-ban. Ebben a dokumentumban fogalmazták meg a koherens stratégiai létszükségletét és a Public Affairs, PSYOPS, információs műveletek és a Key Leader Engagement szükséges ahhoz, hogy megnyerjék maguknak a helyi lakosságot és az afgán kormányt. Hogy ezt elérjék alapvető szabályokat kellett lefektetniük, mint például az 'Egységes Hang' és a 'Szavak és tettek egyezősége'.

Azonban az új iránymutatások ellenére, nem volt semmiféle koordináció a végrehajtó állomány és a Public Affairs erők között. A gyakorlatban a Public Affairs csapatok féltek attól, hogy az éles elhatárolása a célközönségeknek hitelességvesztéssel jár és az egységes kommunikáció bánja. Másodjára, hiába voltak tökéletes irányelvek és útmutatások, a harcászati szinten ezeknek nem volt eredménye. A PA csapatok közvetlenül a NATO-tól kapták meg az utasításokat, ehhez nekik kellett hozzátenni a terepen tapasztaltakat, kultúra, vallás, népcsoportok, helyi politikai érdekek, otthoni politikai érdekek, mind saját és különböző tartalommal. Továbbá ezek az útmutatások csak és kizárólag a PA legénysége között lettek szétosztva, az ISAF útmutatása soha nem érte el a terepen műveletekben részt vevő csapatokat és nem vették figyelembe őket, amikor hadműveleteket terveztek.

Az ISAF életébe a legnagyobb változást McChrystal[92] tábornok érkezése hozta. Az új elvek, melyeket meghonosított Afganisztánban nem voltak újak, sőt ezeket elsősorban az elődjeitől vette át. Nagyobb hangsúlyt fektetett a belső lázadás elfojtására és a helyi lakosságot helyezte középpontba. Nem voltak forradalmiak az ötletei, csak könnyebben lehetett a gyakorlatba helyezni az elvi iránymutatást. A beosztásba helyezésekor mondott beszédében, 2009 augusztus 30-án, már előre vetítette, hogy milyen politikát is szeretne követni; „az ISAF erők következetlenül hajtják végre a lázadás elfojtásához szükséges tevékenységet. A koncepció nem új. De ha ezeket a koncepciókat agresszívan alkalmazzuk, forradalmian fognak hatni a misszió sikerességére."[93]. Véleménye szerint, a stratégiai kommunikáció egy „elengedhetetlen hozzájárulás az általános cél elérése érdekében."[94]

[92] http://www.biography.com/people/stanley-mcchrystal-578710 (letöltve 2014.11.10)
[93] McChrystal, S. (2009). Commander ISAF's initial assessment. Kabul: ISAF p 7
[94] Uo, p. 9

Másodjára, fontosnak érezte, és nyomást is gyakorolt igaza bizonyításának érdekében, hogy a tettek többet jelentenek a helyi lakosság számára, mint a szavak. Ezt gyakorlatba is helyezte, a cél érdekében csökkentette a légi csapások számát, az erőszakos és agresszív éjszakai rajtaütéseket. A gyakorlatban is követte a saját szabályait, tárgyalásoknál sosem viselt repeszálló mellényt és nem vitt magával fegyvert. Véleménye szerint ez bizalmat sugárzott és azt kommunikálta a lakosok felé, hogy nem becsüli többre a saját életét az afgánokénál.
Harmadjára, sikerült elérnie azt, amit az elődjeinek sosem, hogy a PSYOPS és PA csapatok együttműködjenek a kabuli főhadiszálláson. Azóta, minden kommunikáció a kulcsfontosságú vezetőkkel és minden szétosztott üzenet adatbázisban rögzítettek. Ezzel minimalizálta az ellentétes jelentésű üzenetek esélyét.
2007 óta rohamosan fejlődött a NATO kommunikációja, aktívak lettek a Twitter, Facebook, Flickr és YouTube közösségi portálokon, rendelkezik saját weblappal és televíziós csatornával és elkezdődtek a munkák az iPhone alkalmazásokon is. Videók és képek a NATO hadműveletekről meg lettek osztva a nemzetközi közösséggel, hogy ellensúlyozzák a tálib propagandát.

Az első rész összegzése

Steve Tatham, nemzetközi szinte az egyik legelismertebb tanulmányozója a stratégiai kommunikációnak, úgy definiálta azt, hogy: „Olyan szisztematikusan felépített, koherens és fenntartható tettek sorozata, melyeket a stratégiai, műveleti és harcászati szinten hajtanak végre és melynek segítségével sikerül megérteni a kijelölt közönséget, azonosítani lehet hatásos kommunikációs csatornákat és kifejleszthetőek és előtérbe hozhatóak olyan ötletek és eszmék, melyek segítségével elérhető bizonyos típusú viselkedés a célközönségnél”.[95]
Ehhez mérve az ISAF stratégiai kommunikációs teljesítményét megállapítható, hogy nagyon gyenge és erőtlen lett. Nehéz olyan periódusokat keresni, ahol az egységesség legapróbb jele is megtalálható lenne, nem is említve a folyamatosságot. A kapcsolat a stratégiai és harcászati szint között akkor jött létre, amikor a miniszterek rá lettek kényszerítve, hogy magyarázatot adjanak, gyakorlatilag nem létezett.
A célközönségek aggályai és céljai, legyen helyi, nemzetközi vagy otthoni, nem kerültek felderítésre és főleg nem lettek megértve. A kommunikációs csatornából, az afgánok esetében, kihagyták a telekommunikációs eszközöket, mely szektor a

[95] Steve Tatham (2008) Strategic Communication: A Primer, Advanced Research and Assessment UK Defence Academy, p. 3.

leggyorsabban növő része az afgán gazdaságnak[96]. Ezek után nem okozhat meglepetést, hogy a lakosság hozzáállása a tálibok és az ISAF felé nem változott.
A stratégiai kommunikáció elképzelésének elmagyarázásakor gyakran hozzuk a zenekar hasonlatot. A karmestere a zenekarnak általában a nemzeti kormánya a megszálló hatalomnak. A hangszerek a kommunikációs terv. A zenekar maga a különböző közösségek és kommunikációs utak, melyek a művelet részét képzik. A zene az üzenet. A zene tempója változtatható a karmester által elérni kívánt hatás függvényében. [97] Hagyjuk figyelmen kívül azt a problémát, hogy nincsen egyedüli kormány bevonva és, hogy a NATO nem áll készen arra, hogy a politika szemszögéből is biztosítsa azt a bizonyos egységes hangot.
Ehhez hozzájön, hogy az Egyesült Államok, aki vezető szerepet játszott a misszióban és ráerőltette a saját irányelveit a többi résztvevő államra, 7 évig elfoglalt volt Irakban és nem foglalkozott az afganisztáni helyzettel. A gyakorlatban, egyik ideális elem sem volt jelen, úgy, ahogy jelen kellett volna lennie. Ez nagyon érdekes, annak tükrében meg főleg, hogy mekkora hangsúlyt helyeztek rá a parancsnokok és az ő politikai vezetőik. Miért történhetett ez? Az általános betegségei a bürokráciának és az anyagi érdekeltségnek, valamint a 'stratégiai kommunikációs hős' hiánya és az időeltérés a hadműveleti tapasztalatok feldolgozása és a képesség kialakulása között.[98]
A missziós során felmerülő legnagyobb probléma, a stratégiai kommunikációval kapcsolatban, az elv mögé helyezett stratégia csekélysége. A forrásaim feldolgozása közben, a beszámolókat, személyes véleményeket olvasva, arra a következtetésre jutottam, hogy a misszió során egy pozitív érzés vette körül a résztvevőket, úgy érzeték, hogy a misszióval jót cselekednek. Habár ez nem nevezhető győzelemnek, mégis egy pozitív eredmény. Viszont tovább olvasva ezeket az interjúkat, sajnos továbbra is szomorú tény marad az, hogy jelenleg sincs észrevehető politikai stratégia a kommunikáció mögött, a saját zsákutcájába szorult az ISAF és így a NATO is, hozzákötve egy olyan afgán kormányhoz, melynek nem érdeke úgy kormányozni, ahogy az ISAF érdeke kívánná, és továbbra sincs semmi lehetőség arra, hogy a tálibokkal is eredményes kommunikációt folytassanak.
Az esettanulmány végére visszaérkezünk oda, ahonnan elindultunk. Minden kampány, legyen az politikai, marketing vagy katonai, sikeressége attól függ, hogy

[96] David Betz (2011): Communications Breakdown: Strategic Communications and defeat in Afghanistan
[97] Steve Tatham (2008) Strategic Communication: A Primer, Advanced Research and Assessment UK Defence Academy, p. 3.
[98] Michael Flynn (2010): Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan (Washington, D.C.)

mennyire adható el a termék. Tisztában kell lenni azzal, hogy mit szeretnék eladni – mi legyen a végállapot, mi a misszió célja más szavakkal-, feltételezve, hogy a szituáció még menthető egyáltalán. És ha menthetetlen? Akkor levonjuk az angolszászok által annyira szeretett 'Lessons learned'-öt és a következő alkalommal próbáljuk alkalmazni.
Talán a probléma maga az elv volt, melyet kommunikálni szerettünk volna, mely tiszta és világos, de olyan magasságokban van, hogy egy normál ember nem érheti el. A tény az, hogy nincsenek sziklaszilárd résztvevői a stratégiai kommunikációnak; nincs biztos célközönség, nincs biztos üzenet, nincs biztos kommunikációs csatorna. Mindig mozgásban van, mindig változik, ahogy láthattuk Afganisztán esetében is.
A háború színház. Ez a megállapítás keveseket kell, hogy meglepjen. Richards tábornoknak igaza van, amikor azt mondta, hogy most már a digitális médián keresztül folynak a harcok, melynek köszönhetően, sajnos vagy szerencsére, eltűntette a szakadékot az egymástól távol lévő műveleti területek és a különböző célközönségük között. De a háború mindig színház volt – egy improvizáló színház. Talán ez a legnagyobb probléma a parancsnok karmesterként történő azonosításával. Működik, egészen addig, amíg az a kérdés, hogy „Kinek is a sora ez?". Viszont már nem működök, amikor egy olyan színdarabról beszélünk, mint Shakespeare Tévedések Vígjátéka. Az improvizációhoz olyan „színészekre" van szükség, akik képesek figyelni, megfelelő önbizalommal rendelkeznek, tisztán látnak és ösztönszerűen, spontán cselekednek a történetnek megfelelően, amely folyamatosan fejlődik a szereplők és a közönség kölcsönhatásának köszönhetően. Ez totális ellentéte az előre megírt, irányvonal mentén végrehajtott, begyakorolt előadásoknak.
Ezek azok a képességek, amelyekkel a legjobb kommunikálók rendelkeznek – és a legjobb katonák is. Talán a leckét, amelyet meg kellene tanulnunk az afganisztáni szereplésünkkel kapcsolatban az az, amit el sem kellett volna felejteni. Az esettanulmány végére had módosítsam, Helmuth von Moltke tábornagy, aki 30 éven át volt a porosz hadsereg vezérkari főnöke és a 19. század egyik legnagyobb stratégája, idézetét: egyik forgatókönyv sem éli túl a kapcsolatfelvételt a közönséggel.

Felhasznált irodalom

A szövegben.

Répás Sándor – Rajnai Zoltán: SCADA, Rendszerek, mint Kritikus Információs Infrastruktúrák Biztonsága

Absztrakt
A kritikus infrastruktúrák működtetésében az ipari irányítási rendszerek (ICS, SCADA) alkalmazása általánossá vált. Életünk szinte minden területe tőlük függ. Ezek a rendszerek biztosítják az energia, az ivóvíz ellátását, irányítják a közlekedést. Nélkülözhetetlenségük kiváló célponttá tette őket a számítógépes bűnözők és a kiberterroristák számára, valamint rendkívül fontos szerephez jutottak a kiberhadviselés során is. Biztonságuk kiemelt fontosságúvá vált, azonban fejlődésük során elsődleges szempont a hatékony, gazdaságos és megbízható működés volt, nem a támadásoktól való védelem. Ismertetésre kerülnek a lehetséges kritikus infrastruktúrák, majd azok interdependenciái, a SCADA rendszerek általános felépítése, valamint működése. Végül ezen irányítási rendszerek sebezhetőségei kerülnek bemutatásra.

Abstract
The industrial control systems are commonly used to the operation of critical infrastructures. They are essentials in our everyday life by ensuring power supply, drinking water supply and traffic control. Therefore, they are popular and perfect targets of hackers, cyber terrorists and play important role in the cyber warfare, too. However, it is essential to provide high level of security for these systems, they were originally designed as an effective, stable and economical system with small attention on safety. Further introducing the different types of critical infrastructures with interdependences, then presenting the structure and operation of SCADA systems and finally demonstrating the vulnerabilities of them.

Bevezetés

A modern társadalmak működéséhez elengedhetetlenül szükségesek a különböző infrastruktúrák szolgáltatásai, melyek folyamatosan biztosítják az emberek életének, valamint a gazdaság működésének feltételeit. Ilyen infrastruktúra lehet például az energiaellátás, az infokommunikáció, a közlekedés, és az egészségügy rendszere is. Könnyen belátható, hogy a felsorolt infrastruktúrák bármelyikének elégtelen működése komoly károkat okozhat a társadalomban, így ezen infrastruktúrák kielégítő működése kritikus fontosságú. Az Amerikai Egyesült Államok elnökének 1998-ban megjelent irányelve szerint: a kritikus infrastruktúrák

olyan fizikai, vagy kiber alapú rendszerek, melyek elengedhetetlenek létfontosságúak a gazdaság és az állam működéséhez [1]. Ezen rendszerek rendkívül komplex felépítésűek és egymással függőségi kapcsolatban állnak, a technológia folyamatos fejlődése következtében, a rendszerek komplexitása is folyamatosan nő, ráadásul egyre nagyobb mértékben informatikai eszközökkel automatizált.
A terrorizmus fenyegetése, a kiberhadviselés fejlődése egyre fontosabbá tették a kritikus információs
A cikk a következő témákat veszi sorra: elsőként a kritikus infrastruktúrák meghatározása, majd az interdependencia fogalma következik. Ezután a SCADA rendszerek bemutatása, majd biztonságuk ismertetése, végül pedig a konklúzió következik.

1. Kritikus infrastruktúrák

Annak érdekében, hogy a kritikus (másképpen létfontosságú) infrastruktúrákat vizsgálni lehessen, először meg kell határozni a kritikus infrastruktúrák körét, azonban már ez a meghatározás is nehézségekbe ütközhet, mert meghatározásuk nem egységes [2].
Az USA Patriot Act [3] 1016/e. pontja a következőképpen határozza meg a kritikus infrastruktúrákat: olyan fizikai vagy virtuális rendszerek vagy eszközök, amelyek annyira létfontosságúak az USA számára, hogy bármelyikük működésképtelensége vagy megsemmisülése végzetes hatással lehet a biztonságra, a nemzetgazdaság biztonságára, a lakosság egészségére vagy biztonságára, vagy az előbbiek bármilyen kombinációjára.
Az Európai Bizottság közleményének [4] meghatározása a következő: olyan eszközök, illetve azok részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, ideértve az ellátási láncot, az egészségügyet, a biztonságot, valamint az emberek gazdasági és társadalmi jólétét is. Az Európai Tanács irányelve [5] alapján: azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.
A 2012. CLXVI. létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény (Lrtv) alapján a következő ágazatok tartoznak a kritikus infrastruktúrák közé [6]:

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

A következőkben mi is ezt a jogszabályi felosztást alkalmazzuk, ugyanakkor megjegyzendő, hogy kismértékben eltérő csoportosítások alkalmazása is előfordul a szakirodalomban [7], 0.

2. Kritikus információs infrastruktúrák

Az Lrtv. 3. melléklete alapján az Infokommunikációs technológiák ágazati felosztása a következő:

- információs rendszerek és hálózatok
- eszköz-, automatikai és ellenőrzési rendszerek
- internet-infrastruktúra és hozzáférés
- vezetékes és mobil távközlési szolgáltatások
- rádiós távközlés és navigáció
- műholdas távközlés és navigáció
- műsorszórás
- postai szolgáltatások
- kormányzati informatikai, elektronikus hálózatok

Az Lrtv. végrehajtási rendelete 0 tartalmazza a következő definíciót: „létfontosságú információs rendszer és létesítmény: a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.”

3. Interdependencia

Az egyes infrastruktúrák működtetéséhez szükség van más infrastruktúrák igénybevételére. Két nagyon fontos kritikus infrastruktúra az energiaellátás, valamint az információs infrastruktúrák. Ennek oka, hogy, szinte minden infrastruktúra működéséhez elengedhetetlenül szükséges e kettő megfelelő működése.
Rinaldi és társai az elsők közt végeztek fontos kutatásokat a kritikus infrastruktúrák interdependenciájával kapcsolatban. Minden kritikus infrastruktúra közös jellemzője, hogy egymással kölcsönhatásban lévő komponensekből áll, és egy tanulási folyamat során gyakran változik, azaz komplex adaptív rendszer (CAS). A hatékony vizsgálat érdekében a CAS-ok, tehát a kritikus infrastruktúrák egyes elemeit intelligens ágensekként kezelték. [8]. Definíciójuk szerint: „Az interdependencia egy kétirányú kapcsolat két infrastruktúra között, melyen keresztül mindkét infrastruktúra állapota hatással (vagy korrelációban) van a másik állapotára. Általánosabban megfogalmazva, két infrastruktúra interdependens, ha mindkettő függ a másiktól.” Kutatásuk során négy interdependencia típust határoztak meg:

- Fizikai: két infrastruktúra fizikailag interdependens, ha mindkettő állapota függ a másik kimenetétől. Más szavakkal, ha az infrastruktúra működéséhez szükség van a másik infrastruktúra által előállított árucikkre.
- Kiber: egy infrastruktúra kiber interdependenciával rendelkezik, ha állapota függ az információs infrastruktúrán átvitt információktól.
- Földrajzi: infrastruktúrák földrajzilag interdependensek, ha egy helyi környezeti esemény képes mindegyik állapotában változást előidézni.
- Logikai: két infrastruktúra logikailag interdependens, ha mindkettő állapota függ a másik állapotától, de nem fizikai-, kiber-, vagy földrajzi- kapcsolat által.

A fentiektől kissé eltérő interdependenica típusokat határoztak meg Dudenhoeffer és társai [9]:

- Fizikai: direkt összeköttetés az infrastruktúrák között, olyanok, mint szállítói, fogyasztói, termelési.
- Térinformatikai (geospatial): infrastruktúraelemek azonos helyen kerülnek elhelyezésre.
- Politikai: infrastruktúraelemek kötődése politikai vagy magas szintű döntéshozatal által.
- Információs: infrastruktúrák közötti kötődés vagy bizalom az

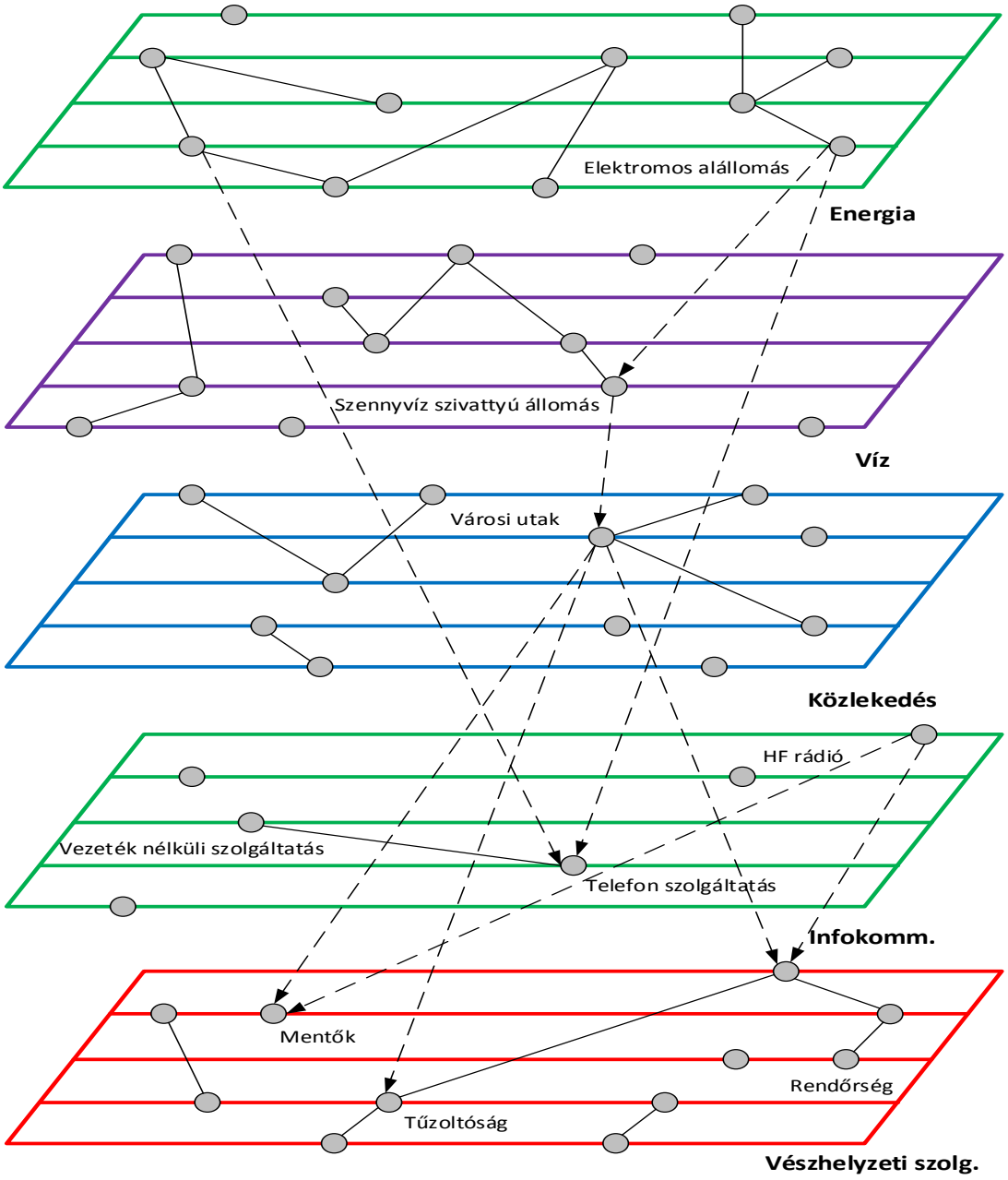
információáramlásban.
Porcellinis és társai ezen kívül bevezették még a szociális interdependencia típusát is [10].
[13] alapján az interdependenciák ábrázolására látható példa az 1. ábrán. Minden egyes sík egy infrastruktúrát jelképez. Egy síkon belüli vízszintes vonal egy-egy szektort, vagy az adott infrastruktúra egy részhalmazát jelzi. A szürke pontok pedig a kulcsfontosságú elemeit jelölik az infrastruktúrának. Az ágazatokon belüli interdependenciákat az összekötő vonalak, míg az ágazatok közöttieket a szaggatott nyilak jelölik.
Az interdependenciák megnövelik a meghibásodásokból eredő sebezhetőséget, valamint ezáltal a kockázatokat [11]. Minél több interdependencia van egy infrastruktúra elemei közt, valamint az infrastruktúrák között, annál komplexebb az infrastruktúrák rendszere, aminek következtében egy kisebb meghibásodás is könnyen továbbgyűrűzhet, ezáltal pedig lényeges hatással lehet a rendszer egészének működésére. Az információs infrastruktúrák fontossága már Rinaldi és társai meghatározásában is megfigyelhető, hiszen a négy típus egyike a kiber interdependencia. Az információtechnológia, az automatizálás folyamatos fejlődése pedig egyre inkább csak fokozza az egyes infrastruktúrák függését az információs infrastruktúráktól, így védelmük kiemelten fontos terület 0.

4. SCADA rendszerek

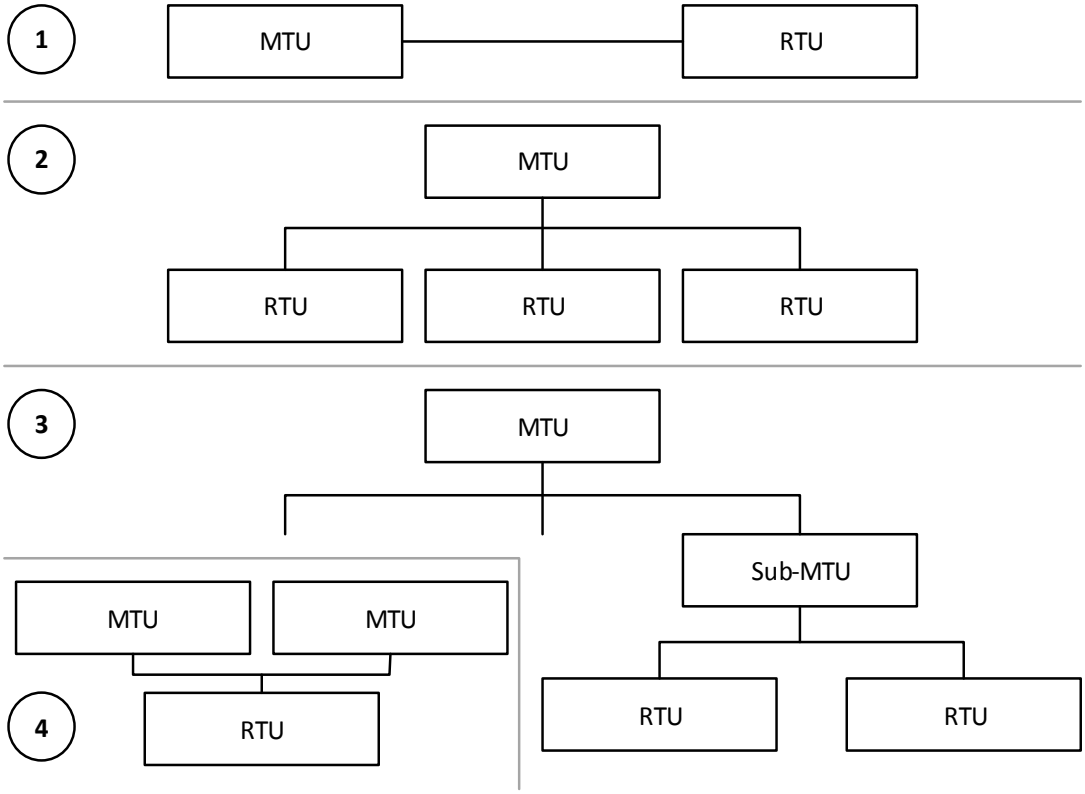
A felügyeleti, irányító és adatgyűjtő (Supervisory Control and Data Acquisition, SCADA) rendszerek ma már nagyon sok területen nélkülözhetetlenek. Az energiaellátás területén segítségükkel vezérlik a teljes villamos energiaellátó rendszert, a kőolaj és a földgázipar berendezéseit. Fontos feladatokat látnak el a közlekedés különböző területein, de nélkülözhetetlenek az ivóvíz ellátásban, az élelmiszer ellátásban, valamint az ipari termelésben is. Alkalmazásuk szinte mindegyik kritikus infrastruktúra ágazatban nélkülözhetetlen.

SCADA rendszerek felépítése

A SCADA rendszereket eredetileg csak kisebb távolságokon, telephelyen belül, helyi hálózatokat felhasználva, alkalmazták. Az infokommunikációs technológiák fejlődésével azonban, a SCADA rendszerek által vezérelt rendszerek földrajzi kiterjedése is megnőtt, ezen túlmenően egyre több rendszer felhasználja az internetet is az adatok továbbítására 0.



4. számú ábra: Infrastruktúrák interdependenciája [13]

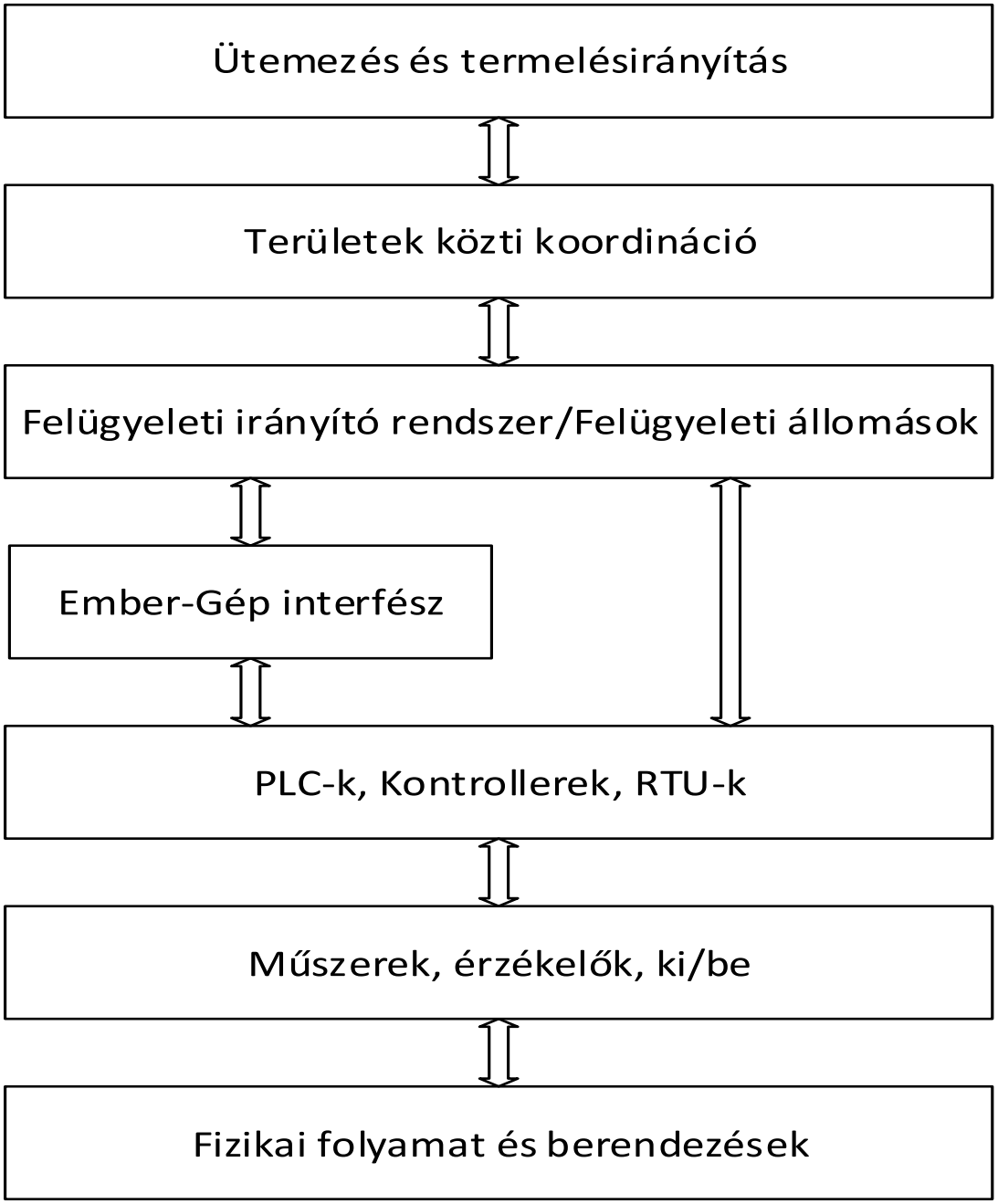


2. számú ábra: SCADA rendszerek kommunikációs alaptopológiái 0

Egy SCADA rendszer három alapvető összetevőből áll:

- Központi vezérlő egység (Master Terminal Unit, MTU);
- Távoli vezérlő egység (Remote Terminal Unit, RTU);
- Valamint az őket összekötő kommunikációs hálózat.

A SCADA rendszerek esetében alkalmazott kommunikációs alaptopológiák a 2. ábrán láthatóak, melyekből a leginkább alkalmazott a 2. és a 3. A magyar villamos energiarendszert irányító MAVIR ZRt. is általában a 3. megoldást alkalmazza, bár az üzembiztonság növelése érdekében több MTU-s (multi master) kialakításban 0.



3. számú ábra SCADA rendszerek vezérlési szintjei 0

A 3. ábrán láthatóak a SCADA rendszerek vezérlési szintjei 0 alapján. A SCADA

rendszerek réteges felépítésűek, ahol az egyes rétegek közt kerülnek továbbításra az adatok.

SCADA protokollok

A SCADA rendszerek kezdetben zárt, gyártófüggő, monolitikus rendszerek voltak, azonban elterjedésükkel párhuzamosan egyre inkább nyílt, szabványos megoldások alkalmazása került előtérbe, megjelent az IP protokoll alkalmazása 0.

A SCADA rendszerek fejlődése során több száz kommunikációs protokollt fejlesztettek ki a rendszer egyes elemei közti kommunikációra, melyekből néhány széles körben elterjedt:

- DNP 3.0
- Ethernet+TCP/IP
- Fieldbus
- IEC 60870-5
- IEC 61850
- MODBUS
- PROFIBUS
- SPA-bus
- UCA

RTU és PLC

A SCADA rendszerek beavatkozó és adatgyűjtő eszköze az RTU és a PLC (Programmable Logic Controller). Az RTU és a PLC feladata, hogy adatokat gyűjtsön, adatokat aggregáljon, valamint azokat továbbítsa az MTU irányába. Szükség esetén beavatkozzon, valamint az MTU felől érkező utasításokat végrehajtsa, végrehajtassa a hozzá kapcsolódó eszközökkel.

Nagyobb távolságok esetén általában RTU kerül alkalmazásra, míg kisebb távolságok, és kevesebb mérő és beavatkozó eszköz illesztése esetén PLC-k alkalmazása az elterjedt. Az RTU sok esetben egy speciálisan kialakított PC kompatibilis számítógép, amely akár Linux alapú is lehet. A PLC-k leginkább olyan hibatűrő mikrokontrollerekként képzelhetőek el, melyek saját nyelvükön programozhatóak, és speciális ki/bemeneti interfészekkel rendelkeznek. Magyarországon széles körben elterjedt a Siemens által gyártott Simatic Step 7 PLC, valamint a Prolan által gyártott ProField-RTU alkalmazása, de ezen kívül rengeteg más gyártó termékei is használatban vannak.

A MAVIR ZRt. összes alállomásán is megtalálható a ProField-RTU, mely az MTU irányában az IEC 60870-5 protokoll segítségével kommunikál 0 0.

5. Biztonság

Az első SCADA rendszerek megjelenésekor elsődlegesen a rendszer elemeinek fizikai megsemmisítése ellen védekeztek a fizikai hozzáférés korlátozásával, izolált rendszerek kialakításával 0. A rendszerek tervezése és kialakítása során csak lényegesen később kerültek előtérbe a biztonsági szempontok. A rendszerek fejlődésével, azok egyre komplexebbekké váltak, egyre nagyobb mértékben kapcsolódtak más rendszerekhez, sőt sok esetben az internetet is valamilyen módon igénybe veszik működésük során.
A már meglévő rendszerek cseréje, frissítése rendkívül költséges, és időigényes. Ennek következtében a legtöbb SCADA rendszerben túlsúlyban vannak a régi, még jól működő, de nem biztonságos eszközök és protokollok. Egy ilyen rendszer szinte minden pontján támadható. A rendszerek (költséges) frissítése mellett, egyedüli megoldásként a külső védelmi eszközök alkalmazása jelenthet megoldást. Olyanok, mint a hálózat szegmentálása VLAN-ok alkalmazásával, tűzfalak és IDS/IPS eszközök alkalmazása, IPSec bevezetése, stb.
Az utóbbi években egyre több SCADA rendszereket célzó informatikai támadás történt. Számtalan publikáció foglalkozott az iráni atomprogramot hátráltató Stuxnet-tel 0 0 0, mely a Siemens Step 7 PLC-ket támadta, majd 2012 májusában felfedezték a Flame (más néven sKyWIper) malwaret 0, mely célzottan az energetikai SCADA rendszerekkel kapcsolatos adatokat gyűjtött. 2014 júniusában pedig megtalálták a Havex trojant, mely szintén energetikai irányító rendszereket támadott 0.
0 a következőképpen csoportosítja a SCADA rendszerek sebezhetőségeit:

- SCADA hardver
- SCADA szoftver
- SCADA adatintegritás
- SCADA hálózat
- Egyéb számítástechnikai sebezhetőségek

Ezen területek részletes vizsgálata alapján, mind az öt esetben alkalmazhatóak külső eszközök a biztonság fokozására. Nagyon fontos ugyanakkor, hogy ne kerüljön a rendszerbe egy újabb támadási pont, vagy meghibásodási lehetőség, mely végső esetben még kiszolgáltatottabbá teheti az irányítási rendszert. Ehhez

elengedhetetlen a megfelelő eszközökre épülő megoldások alkalmazása, valamint a minden részletre kiterjedő tervezés és implementáció.

Összegzés

A kritikus infrastruktúrák organikus fejlődése során egyre komplexebb rendszerek alakulnak ki, melyek több generációból származó, eltérő biztonsági képességekkel rendelkező eszközökből állnak. E rendszerek elemeit jellemzően csak nagyon ritkán frissítik, így külső eszközökkel történő védelmük kiemelkedő fontosságú terület. A védelem kialakítását azonban gondos tervezésnek kell megelőznie. Ennek a tervezésnek figyelembe kell vennie a lehetséges fenyegetéseket, ugyanakkor arra is figyelemmel kell lennie, hogy milyen új sebezhetőségek kerülhetnek a kritikus infrastruktúrát irányító információs rendszerbe.

Felhasznált irodalom

[1] Presidential Decision Directive/NSC-63, Elérhető: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
[2] Z. Précsényi és J. Solymosi, “Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé,” Hadmérnök, vol 2. no. 1, pp. 65-76, 2007. Elérhető: http://hadmernok.hu/archivum/2007/1/2007_1_precsenyi.pdf
[3] USA PATRIOT Act (H.R. 3162), https://epic.org/privacy/terrorism/hr3162.html
COM(2006) 787 final 2006/0276 (CNS) Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Elérhető: http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=kCs9Jn7SPNLsXgYnTvnTsSQ18rTrGb6DhMWcQnQsTCsd1Bqzk02Q!-895171320?uri=CELEX:52006PC0787
[4] A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, Elérhető: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:HU:PDF
[5] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=155940.287727
[6] E. A. M. Luiijf és M. H. A. Klaver, “Protecting a nation's critical infrastructure: the first steps,“ in *Proc. 2004 IEEE International Conference on Systems, Man and Cybernetics*, The Hague, 2004. pp. 1185-1190. doi: 10.1109/ICSMC.2004.1399785

Report on interdependence of infrastructures Deliverable 5.2, Ingeniería de Sistemas para la Defensa de España, S.A., pp. 17, 31. 2012. Elérhető: http://www.focusproject.eu/documents/14976/21546ecc-5018-46e2-9291-a1875c8a77c5

[7] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159312.269526

[8] S. Rinaldi, P. Peerenboom és T. Kelly, "Identifying, understanding and analyzing critical infrastructure interdependencies," IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, 2001.

[9] D. D. Dudenhoeffer, M. R. Permann és M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," in *Proc. 2006. WSC 06. Winter Simulation Conference*, Monterey, 2006. pp. 478-485. doi: 10.1109/WSC.2006.323119

[10] S. D. Porcellinis, R. Setola, S. Panzieri és G. Ulivi, "Simulation of heterogeneous and interdependent critical infrastructures," International Journal of Critical Infrastructures, vol. 4, no. 1/2, pp. 110-128, 2008. doi: 10.1504/IJCIS.2008.016095

[11] P. Pederson, D. Dudenhoeffer, S. Hartley és M. Permann, "Critical infrastructure interdependency modeling: A survey of U.S. and international research," Idaho National Laboratory, 2006.

[12] L. Xiao-Juan és H. Li-Zhen, "Vulnerability and interdependency of critical infrastructure: A review," in *Proc. Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA 2010)*, Shenzen, 2010. pp. 1-5. doi: 10.1109/INFRA.2010.5679237

[13] D-J. Kang, J-J. Lee, S-J. Kim és J-H. Park, "Analysis on cyber threats to SCADA systems," in *Proc. Transmission & Distribution Conference & Exposition: Asia and Pacific*, Seoul, 2009, pp. 1-4. doi: 10.1109/TD-ASIA.2009.5357008

[14] T. Bencsik, "A MAVIR ZRt. hálózat távkezelésének kialakítása (1)," MEE 56. Vándorgyűlés, Balatonalmádi, 2009. Elérhető: http://www.mee.hu/files/images/5/A4_5_1.pdf

[15] R. E. Johnson, "Survey of SCADA security challenges and potential attack vectors," in *Proc. 2010 International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2010, pp. 1-5.

[16] F. Haji, L. Lindsay és S. Shaowen, "Practical security strategy for SCADA automation systems and networks," in *Proc. Canadian Conference on Electrical and Computer Engineering*, Saskatoon, 2005, pp. 172-178. doi: 10.1109/CCECE.2005.1556903

[17] ProField-RTU, http://www.prolan.hu/uzletagak/villamosenergia-ipar/profield/

[18] E. Chikuni és M. Dondo, “Investigating the security of electrical power systems SCADA,” in *Proc. AFRICON 2007*, Windhoek, 2007, pp. 1-7. doi: 10.1109/AFRCON.2007.4401531

[19] T.M. Chen és S. Abu-Nimeh, “Lessons from Stuxnet,” Computer, vol 44. no. 4, pp. 91-93, 2011. doi: 10.1109/MC.2011.115

[20] R. Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” Security & Privacy, vol 9. no. 3, pp. 49-51, 2011. doi: 10.1109/MSP.2011.67

[21] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” in *Proc. 37th Annual Conference on IEEE Industrial Electronics Society (IECON 2011)*, Melbourne, 2011, pp. 4490-4494. doi: 10.1109/IECON.2011.6120048

[22] Z. Sami, ”The middle east under malware attack dissecting cyber weapons,” in *Proc. 33rd International Conference on Distributed Computing Systems Workshops (ICDCSW 2013)*, Philadelphia, 2013, pp. 11-16. doi: 10.1109/ICDCSW.2013.30

[23] Advisory (ICSA-14-178-01) ICS Focused Malware, https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01

[24] B. Zhu, A. Joseph és S. Sastry, ”A taxonomy of cyber attacks on SCADA systems,” in *Proc. 2011 International Conference on Internet of Things (iThings/CPSCom), and 4th International Conference on Cyber, Physical and Social Computing*, Dalian, 2011, pp. 380-388. doi: 10.1109/iThings/CPSCom.2011.34

Szegedi Péter: Kriptoeszközök előállításának és felhasználásának lehetőségei

Absztrakt
Tudományos Diákköri Konferenciára készült munkám során szembesültem a kriptoeszköz elkészítésének sajátosságaival. Dolgozatom az eszköznek mind a gyakorlati megvalósítását, mind a felhasználhatóságát vizsgálja, ennek eredményeit szeretném röviden áttekintve bemutatni.

Abstract
While preparing my work for the Scientific Student's Conference, I found myself dealing with the unique of creating a crypto device. My thesis examines the problem of both realization, and usage of the device, which results I would like to summarize shortly

Bevezetés

Akik napjainkban foglalkoznak az információ biztonság témakörével, azok számára nem lehet ismeretlen fogalom a kriptográfia, vagy magyarul rejtjelezés. Ez a témakör előkerült tanulmányaim során is, mivel olyan szerencse ért, hogy a méltán híres varsói Katonai Műszaki Akadémián (WAT) hallgathattam erről a témáról. A dolog hamar érdekessé vált számomra, ehhez párosult, hogy megismertem a szakmában alapműnek számító Simon Singh: Code Book-ját [99]. Innentől nem volt megállás, és sorban kezdtem megoldani a könyv hátulján kiadott egyre nehezedő feladatokat (aki olvasta, ismeri az érzést). Végül pedig érdeklődésem a gyakorlati megvalósulás felé kezdett terelődni. Egyre több feladatot oldottam meg gépen, apróbb algoritmusok megírásának segítségével (amelyek bevezető gyakorlatok is lehetnének egy programozói kurzus során, de legfőképp a folyamatot gyakorolni volt hasznos). Ennél továbbmenve, szerettem volna hálózatban kiépítve megvalósítani egy kezdetleges titkosított kapcsolatot, ezáltal is megközelítve napjaink gyakorlati kripto alkalmazásait, pl. SSL/TLS[100] (természetesen csak elvi szinten, nem állítom, hogy bármilyen forradalmian új titkosított csatornát hoztam volna létre). Így jutottam el a TDK dolgozatom projektjéhez, és ennek megvalósítását mutatom most be, lépésről lépésre.

[99] Simon Singh: The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor, 2000. ISBN-13: 978-0385495325
[100] Transport Layer Security (TLS) és elődje a Secure Sockets Layer (SSL)

1. Első lépések

Először mindenképp szükségem volt egy hardver eszközre (egészen pontosan kettőre), hogy kapcsolatot hozzak létre, hálózatot építsek ki. Választásom a népszerű, sokak által kedvelt Raspberry Pi („Málna PC") bankkártya méretű számítógépre esett. Alapvető rendeltetése a lelkes programozóknak platformot biztosítani a kísérletezésre, tanulásra. Piaci forgalomban lévő, ezáltal könnyen beszerezhető eszközről van szó. A készülék fizikai paraméterei nyilvánosan elérhetőek[101], saját céljaim szempontjából több, mint elegendőek. A gépre többféle operációs rendszer is elérhető, de az ajánlott (és legelterjedtebb) a Raspbian OS, amely a népszerű Debian Linux disztribúciónak egy kifejezetten a Raspberry-hez kialakított változata. Jómagam is ezt használtam, mivel teljes mértékben megfelel az általam kitűzött célokhoz.

2. Hálózati megvalósítás

Adott a két eszköz, de ahhoz, hogy bármiféle titkosítást alkalmazzunk, először hálózati kapcsolatot kell kialakítani. Az egyszerűség és a demonstrálhatóság érdekében a TCP/IP alapú kapcsolatot építettem ki, standard Ethernet kábel alapú csomagátvitellel. Maguk a rejtjelezett csomagok UDP formában kerülnek elküldésre, de elméletben nincs akadálya a TCP protokoll használatának sem. A kapcsolat felépítése socket alapú, amely az IP cím és a port szám alapján különbözteti meg a feleket. Az IP címek adottak, port számot pedig kellőképp magasat választottam (1000-64000 tartományban), hogy véletlenül se legyen interferencia egy népszerűbb port-on futó csomagküldéssel (pl. FTP, 21-es port). Másik fontos tulajdonsága a socket alapú kapcsolatnak a master-slave alárendeltség, vagyis kialakítottam, hogy ez egyik eszköz legyen kiszolgáló (server), azaz csomagfogadó, a másik pedig user (felhasználó), azaz csomagküldő szerepkörben. Végezetül, a Raspberry gépek sajátosságaiból adódóan (nincsen gyári periféria: monitor, billentyűzet, egér, stb..) úgy kellett kialakítanom a hálózatot, hogy legyen vezérlő PC, amely irányítja a csomagküldést a két eszköz között. Ezen okból kifolyólag nem crosslink kábel segítségével oldottam meg az összeköttetést, hanem egy switch-re csatlakoztattam mindhárom eszközt. Innentől kezdve minden adott volt a hálózati kapcsolat kialakításához.

[101] http://www.raspberrypi.org/documentation/hardware/raspberrypi/README.md

3. Szoftveres megvalósítás

Megvolt tehát a működő hardver, és hozzá a logikailag működő hálózat. Ideje volt kialakítani a megfelelő szoftveres környezetet, és ami a legfontosabb, belevinni a kriptográfiát.
Mielőtt rátérek a konkrét megvalósításra, röviden összefoglalnám a titkosítás folyamatát, hogy érthetőek legyenek a következő lépések. Minden rejtjelezés esetén feltételezzük, hogy Alice és Bob (jelen esetben a két eszközünk) próbál egy nyílt csatornán egymásnak üzenni oly módon, hogy ha lehallgatják őket, akkor se tudják meg az üzenet tartalmát. Erre a legelső példa Julius Caesartól származik, aki a latin ABC betűit 0-tól 25-ig listázta, majd elfoglalt helyüket bizonyos értékkel eltolja (eredetileg 3-mal). Amint megérkezik az üzenet Bobhoz, már tudni fogja, hogy egy előre megbeszélt értékkel kell visszatolni a karaktereket, hogy visszakapja az eredeti üzenetet, egyébként érthetetlen betűsorozatot olvas. A titkosítás párhuzamosan megjelent a kriptanalízis is, amely a titkosított üzenet megfejtését, feltörését hivatott elérni. Ezzel kialakult egy mai napig tartó macska-egér játék, ahol újabb és újabb titkosításokat alakítanak ki, és próbálják azokat megfejteni.
A kriptográfia napjainkra szerteágazó tudományággá vált, és többféle vonalon indult el fejlődése, felhasználásának jellegétől függően. Dolgozatomban, egy napjainkban is használt és biztonságosnak ítélt (legalább 2048 bites kulcs esetén) eljárást, az RSA-t használtam fel. Nevét megalkotóiról kapta, (**R**ivest, **S**hamir, **A**dleman), 1977-ben találták ki, és azóta is használatban van. Maga a metódus az aszimmetrikus titkosítás kategóriájába tartozik, ugyanis rejtjelezéshez és visszafejtéshez különböző kulcsot használunk (nyilvános és privát kulcs). Ennek alapjait két úriember (Diffie, Hellman) fektette le egy évvel korábban, ezt nevezik nyilvános kulcscserének. Korábbi példával élve, ez egy olyan módszer, amivel Caesar az üzenetet fogadó tábornok tudomására juttathatja, hogy mennyivel kell tolni az ABC értékéit (a kulcs értékét), anélkül, hogy a futárt esetlegesen foglyul ejtő ellenség értelmezhetné (lehallgatná). Szerencsénkre napjainkban fejlettebb titkosítási eljárás párosult az egyébként zseniális kulcscseréhez, és ennek eredményeként jött létre az RSA. Alapvetően három részből áll (mindhárom egyébként jelen van a programomban), a kulcscsere, a titkosítás (nyilvános kulcs segítségével), és a visszafejtés (privát kulcs segítségével). Mind ennek, mind a Diffie-Helmann eljárásnak a matematikai háttere elérhetőek publikusan.[102][103]

[102] The Original RSA Patent as filed with the U.S. Patent Office by Rivest; Ronald L. (Belmont, MA), Shamir; Adi (Cambridge, MA), Adleman; Leonard M. (Arlington, MA), December 14, 1977, U.S. Patent 4,405,829

Adott elméleti háttérrel rá is térek a konkrét programozási megvalósításra. Mint említettem a socket alapú kapcsolatnál, két félből, különböző programból épül fel (server-client), így voltak némi eltérések a két program között. Fontos kiemelni, hogy én a Python nevezetű nyílt forráskódú programozási rendszert használtam, mivel rendkívül sokrétű, és erős támogatói bázissal rendelkezik (fórumok, leírások). A hálózat kiépítésével kezdtem, importálva a Python megfelelő folyamatát (import socket). Megadva a beállításokat, a szoftver folyamatosan figyelte és listázta az átmenő csomagokat (extraként beállítottam, hogy egy log file-t is készítsen). Van tehát egy csatornánk, amely alkalmas az üzenetek küldésére és fogadására, ehhez jönnek a titkosítási folyamatok. Én egy, a Python-hoz nyilvánosan, bárki számára elérhető toolkit-et alkalmaztam, a PyCrypto-t. Ezt ugyanúgy importálni kell, megfelelő beállításokat meg kell adni (pl. kulcs méret), és véletlen szám generátorral elkészíteni a kulcspárokat. Innentől kezdve a megfelelő eljárásokkal megtörténik az üzenetek (amiket raw_input segítségével a felhasználó ad meg a programnak) titkosítása, és a socket folyamatok segítségével küldése is.
A szoftver leírása nem teljes, ugyanis dolgozatommal (és vele együtt programommal) jelenleg a XXXII. Országos Tudományos Diákköri Konferenciára készülök. Természetesen a Konferencia után mind a dolgozatom, mind a forráskódom nyilvánosan elérhetővé válik.

4. Felhasználhatóság

Elkészülvén a működőképes projekttel, felmerült bennem a kérdés, hogy mi lehet a gyakorlati alkalmazhatósága. Nyilvánvaló, hogy valós, elfogadható biztonságú titkosított csatornák létesítésére alkalmatlan, ehhez rendkívül sok szabályzónak és előírásnak kell megfelelni.
A fentiekkel ellenben kifejezetten alkalmas az eszköz egy másik feladatkörre, méghozzá az oktatás kérdésében. Felmerült ugyanis az igény, hogy a hallgatók korszerű kriptográfiai, információ biztonsági képzésben részesüljenek. Ennek okán kifejezetten alkalmas lehet az eszköz demonstrációs jelleggel. Egyértelműen látványos és életszerű példát mutat be a kriptográfia gyakorlati alkalmazására, emellett DIY (Do It Yourself) jellege izgalmassá, esetleg kihívást jelentővé teszi. Sokkal könnyebb megnyerni a hallgatók érdeklődését, ha egy valós, működő eszközön bemutatva látja a tananyagot. Emellett a programozási nyelv és az operációs rendszer sajátosságai lehetővé teszik a kísérletezést, hogy esetleg a

[103] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". IEEE Transactions on Information Theory 22: 644–654.

lelkes érdeklődök célirányos változtatásokkal próbálgassák ki az eszközök működését (megváltozott kulcs erősség, változatos plaintext-ek, új csatornák kialakítása, stb…).

Összegzés

Zárásként szeretném összegezni munkám és az elért eredményeket. Úgy vélem a saját magammal szemben kitűzött célokat maradéktalanul elértem. Fontos kiemelni, hogy valóban működő eszközt alakítottam ki, gyakorlatban is megvalósítottam a feladatot. Azon túlmenően, hogy saját magam számára rendkívüli tapasztalat szerzési lehetőségnek bizonyult, ahogy fentebb rátértem, hosszú távú oktatási lehetőségeket biztosít. Munkámmal az Intézményi Tudományos Diákköri Konferencián is eredményesen szerepeltem, és remélem a jövőben lesz lehetőségem jobban beleásni magam a témakörbe és további eredményeket elérni.

Felhasznált irodalom

Szövegben.

Szanyi Sándor – Jobbágy Szabolcs – Pándi Erik: A minden a hálón biztonsági aspektusai

Absztrakt
Jelen cikk az Internet térhódításával foglalkozik.

Abstract
This article shows the conquest of Internet.

Bevezetés

A milliárdnyi eszköz, amely felcsatlakozik a minden a hálón világában, döbbenetes mennyiségű adatot generálhat pár nap lefolyása alatt. Az óriási adathalmaz létrejötte nagymértékben megnöveli a hálózat biztonságával kapcsolatos megoldások jelentőségét, hiszen napjainkban, az információ jogosulatlan megszerzésére, módosítására és az adat jogosult hozzáférésének megakadályozására tett kísérletek szinte napi gyakorisággal előfordulnak. Következésképpen, egyetlen egyén és szervezet sem kerülheti el a minden a hálón megvalósításának folyamatában a szükséges információvédelmi tevékenységek végrehajtását, valamint a biztonság szüntelen naprakészen tartását.

1. Biztonság

A biztonság egy objektum állandóan fennálló, komplex védelme. Ez az objektum lehet egy személy, egy épület, vagy például egy számítógépes rendszer. Az informatikai rendszerekre nézve, a biztonság kiterjed a rendszer fizikai (környezet, épület, helyiség, szoba, hardver elemek), illetve a nem fizikai komponenseire (adat, információ, alkalmazások). A hálózat esetén, amely alapvetően egy elosztott számítógépes rendszer, a védelem tárgya magába foglalja a hálózatot felépítő erőforrásokat, mint például a kommunikációs csatornákat, a hálózati eszközöket (forgalomirányító, kapcsoló, ismétlő) és végberendezéseket, valamint a rajtuk tárolt adatokat és alkalmazásokat. A minden a hálón lényegében egy hatalmasra duzzadt, a fizikai világunkat teljesen átható intelligens hálózat, egy elosztott informatikai rendszer, amely eddig nem látott képességeket és előnyöket rejt magában a felhasználói számára. Mivel alapvetően összekapcsolt információ technológiai eszközök halmaza, így leginkább a hálózati biztonság témakörébe tartozik a minden a hálón erőforrásainak védelme.

A biztonságnak alapvetően három fő elve van, amelyekre a védelmi mechanizmusoknak épülniük kell. Ez a *bizalmasság*, *sértetlenség* és a *rendelkezésre állás*. Az elvek az informatika területén a következőket foglalják magukba: [38] [39]

- A *bizalmasság* elvének célja az információ vagy egyéb erőforrás jogosulatlan hozzáférésének megelőzése. Ez azt jelenti, hogy csak az a személy férhet hozzá egy adathoz, vagy eszközhöz, aki arra jogosult. Ide sorolható a szükségesség elve („need to know”), amely alkalmazásával lehetővé válik, hogy adott munkakörben csak a munka elvégzéséhez szükséges erőforrásokhoz történjen hozzáférés.
- A *sértetlenség* célja az információ és egyéb erőforrás jogosulatlan módosításának elkerülése, az adat integritásának és eredetének megőrzése.
- A *rendelkezésre* állás elve pedig lehetővé teszi, hogy az információ vagy egyéb erőforrás a megfelelő személy számára, a megfelelő időben és formában elérhető legyen.

Az elvekhez mérten alkalmazott védelmi mechanizmusok az informatikai rendszert célzó *fenyegetések* minimalizálására törekednek annak érdekében, hogy az információ és az egyéb erőforrások bizalmassága, sértetlensége, rendelkezésre állása minél inkább megvalósuljon. A fenyegetés a biztonság potenciális megsértése vagy annak a lehetősége, így lehet egy erre irányuló cselekedet, egy számítógépes rendszer elleni támadás (e-mail fiók feltörése, adatok lopása, szolgáltatás megtagadása, vírusok, stb.) vagy a biztonsági rendszer megsértésének kockázata, a rendszer sebezhetőségének kihasználása. (lejárt szoftverfrissítés, véletlen jelszókiadás, stb.

Az informatikai rendszereket célzó fenyegetések több forrásból származtathatóak:

- A sebezhetőségek eredhetnek *a hálózati infrastruktúra és a kommunikációs protokollok gyenge pontjaiból*. Biztonsági résnek számít, a TCP protokoll által használt három-utas kézfogás során, a szerverek által félig-nyitva hagyott socket - k problémája, amelyek utat biztosítanak a hackerek [104] tevékenységének. Továbbá, az alkalmazási réteg protokolljaihoz köthető jól ismert portok használata, valamint a csomagkapcsolt hálózati infrastruktúrának az a jellemzője, hogy az üzeneteket több kis csomagra lebontva továbbítja a hálózaton keresztül véletlenszerű útvonalakon, nagy bizalmat helyezve a hálózatot felépítő eszközök megfelelő működésébe. Ezeket kihasználva a támadó speciális módszerek segítségével (pl. port szkennelés, az épp nyitott

[104] Hacker: olyan személy, aki különböző célok által vezérelve számítógépes rendszerekbe tör be. Napjainkban a „hacker” kifejezésnek leginkább negatív vonzata van (feketekalapos hacker), azonban vannak olyan szakemberek, akik a rendszer biztonsági réseinek kiküszöbölése miatt próbálják kijátszani a védelmi mechanizmusokat (fehérkalapos hacker).

portok keresésére) a hálózaton áramló csomagokat elfoghatja, a tartalmukat, a forrás és a cél IP címüket megváltoztathatja (IP hamisítás), az adott szervereket hamis csomagokkal túlterhelheti (SYN elárasztás), sőt kiaknázva a gyengeségeket akár bejuthat a kommunikáló felek informatikai rendszerébe is egyaránt.

- A támadási felületek származhatnak *szoftver hibákból*, főleg az *operációs rendszerek gyengepontjaiból,* illetve a *nem megfelelő működésükből*. Egy operációs rendszer (OS) alapvető szerepet játszik az eszközök megfelelő működésében, hiszen lehetővé teszi, hogy a rendszeren futó programok hozzáférjenek a végrehajtásukhoz szükséges erőforrásokhoz. Egy informatikai rendszerbe történő behatolás után, az OS gyengepontjait kihasználva a támadó átveheti az adott számítógép feletti irányítást; adatállományokat módosíthat, törölhet, vírusokat futtathat és akár felülírhatja a merevlemez tartalmát is.
- A *globális hálózat exponenciális növekedése* biztonsági szempontból egyre meghatározóbb problémát jelent. A kibertér[105] megállás nélkül nagyobbá és átláthatatlanabbá válik, hiszen több - és több eszköz csatlakozik fel a hálózatra, ami által sokkal többen élvezik az internet nyújtotta lehetőségeket. Minél több a felhasználó, annál több olyan lesz köztük, akik fenyegetést jelentenek a hálózatra nézve, hiszen rossz szándékkal, jogosulatlanul akarnak hozzáférni az információkhoz és egyéb erőforrásokhoz.
- Biztonsági réseket jelentenek az informatikai rendszerekre és a rajtuk tárolt adatokra nézve a házon belüli (szervezeten belüli) *megbízhatatlan munkatársak jelenléte*, akik hozzáférhetnek, módosíthatják, a jogosultak számára elérhetetlenné, illetve jogosulatlan személy számára hozzáférhetővé tehetik a rendszeren tárolt bizalmas információkat és egyéb erőforrásokat.
- A fenyegetések meghatározó része az *emberek naivitásának kihasználásból (social engineering)* származik. Az ember a leggyengébb láncszem a biztonság vonatkozásában. Számos módszer létezik (adathalászat, bizalom megszerzése, stb.), amely által a támadó hozzáférést szerezhet a hálózati erőforráshoz, vagy bizalmas, a szervezet vagy egyén számára kulcsfontosságú információhoz juthat hozzá.

[105] Kibertér: egy képzeletbeli, virtuális környezet, ahol a hálózati eszközök kommunikációja zajlik. Pontos definíciója nem létezik. Az elnevezés William Gibson sci-fi írótól származik. [58]

- Az *eszközöknek az ellopása*, illetve *elhagyása* sem elhanyagolható a biztonság szempontjából, mivel ennek következtében a rosszindulatú támadók fizikailag hozzáférhetnek az eszközökhöz, a rajtuk tárolt adatokhoz, valamint az elérhető erőforrásokhoz.

A támadásokat végrehajtó egyén vagy csoport motivációja szerteágazó, a bosszútól a kémkedésen át a terrorizmusig bármi lehet.

Az előbb felsorolt hálózati sebezhetőségeket kihasználva a hackerek számtalan támadást indíthatnak az összekapcsolt számítógépek ellen. A támadásoknak alapvetően két típusa van, amelyek a következők:

- Az egyik típus a *betörés*, vagy *beszivárgás (penetration).* Ebbe a csoportba tartoznak azok a cselekedetek, amelyek az információ és a hálózati erőforrásokra vonatkozó sértetlenség és bizalmasság elvét megszegik. Az informatikai rendszerhez történő jogosulatlan hozzáférés után a behatoló teljes irányítása alá tudja vonni a hálózati erőforrásokat, következésképpen a kezelt adatokat módosíthatja, ellophatja, kártevő programokat telepíthet a számítógépekre. Ide tartoznak a különböző vírusok, férgek, szimatoló programok (sniffers). A támadások lehetnek helyiek (egyazon LAN-ból eredőek), illetve származtathatóak a publikus, nyílt hálózatokról is egyaránt.
- A támadások másik csoportja a *szolgáltatás megtagadás (denial of service; DoS)*. Itt a cél az informatikai rendszer szolgáltatásainak zavarása, illetve megszakítása, amely az információra és az erőforrásokra vonatkozó rendelkezésre állás elvét sérti meg. A hálózatra vonatkozóan az *elosztott szolgáltatás megtagadás (distributed denial of service)* módszerei a meghatározóak, amely a felcsatlakoztatott számítógépeket veszik célba. IP hamisítás, SYN elárasztás, halálos ping támadás, DNS hamisítás, stb., mind ebbe a csoportba sorolhatóak. A hálózati betörésekhez hasonlóan a támadások lehetnek helyiek és külső hálózatból is eredeztethetőek.

A hálózati fenyegetések ellen irányuló biztonsági lépéseknek három fő, egymásra épülő típusa van. Mechanizmusok, amelyek a fenyegetések *megelőzésére*, az *észlelésére*, valamint a biztonsági eseményre való *reagálásra* hivatottak.

- A *megelőzést szolgáló biztonsági lépések* feladata, hogy megakadályozzák a fenyegetések bekövetkezését. (biometrikus beléptető rendszerek, kriptográfia, jelszavak, tűzfalak, hozzáférési listák, IPS.)
- A *detektáló mechanizmusok* célja a rendszer folyamatos vagy rendszeres ellenőrzése, a támadások felismerése, és a reagáló mechanizmusok riasztása. (elektronikus riasztó rendszerek, IDS, vírusok elleni védelem, tűzfalak, stb.).
- A *reagáló biztonsági lépések* célja egyrészt a folyamatban lévő támadások megakadályozása, valamint a biztonsági esemény utáni helyreállítás. (vírusok

elleni védelem, port letiltása, biztonsági másolatok, naplózások, stb.) Másrészt a támadás ideje alatt a rendszer működésének fenntartása (redundáns komponensek).

A hálózat biztonságának megvalósítása a fenyegetések minimalizálása (esetleg megszüntetése) érdekében a háromfajta biztonsági lépés együttes alkalmazásával lehetséges. Az információ és az egyéb hálózati erőforrás bizalmasságának, sértetlenségének, valamint rendelkezésre állásának biztosítása azonban nehéz feladat. Egy átlagos asztali számítógép megfelelő biztonságának elérése sem egyszerű. Komplex, több szintű védelmet kell létrehozni és folyamatosan karbantartani, valamint az idő múlásával keletkező fenyegetéseket megfelelően kezelni. Egy több milliárdnyi eszközből felépülő számítógépes hálózat biztonságának megteremtése és fenntartása pedig szinte emberfeletti feladat a végberendezések és a kapcsolatok sokszínűsége miatt. A minden a hálón elképzelésben konkrét biztonsági megoldások még nem születtek erre, sőt irányelvek is csak elvétve vannak, ami nem meglepő a feladat nehézségének, valamint a rendszer kiforratlanságának köszönhetően.

A következő alfejezetek, a minden a hálón alappilléreinek biztonsági oldalát elemzik. Annak következtében, hogy az egész rendszert átható megoldások még nem születettek ezen a területen, olyan, a kutatásaim során összegyűjtött fenyegetések és biztonsági lépések kerülnek bemutatásra, amelyek megalapozhatják a hálózatot célzó támadásokat, illetve megoldást jelenthetnek biztonsági problémákra, továbbá valamilyen formában szorosabban köthetőek az egyes alappillérekhez.

A dolgok biztonsága

A dolgok pillérén belül alapvetően két terület kerül bemutatásra a biztonság vonatkozásában. Ezek az *otthoni hálózatok*, valamint a *szenzorok védelme*.

Az otthon védelme

A minden a hálón elképzelésben az *otthon dolgai*, a viselhető intelligens eszközöktől a hűtőkön, termosztátokon át az elektronikus monitorozó- és riasztórendszerekig, valamennyi felcsatlakozik majd a globális hálózatra, így új terület nyílik a biztonság és a sebezhetőség szempontjából is. Az otthon biztonságának megteremtése pedig minden ember számára kiemelkedő fontosságú. A nagyfokú digitalizációnak köszönhetően azonban az otthoni, komplex, több komponensből álló hálózat jobban kiszolgáltatottá válik a rosszindulatú támadók számára.

Az otthoni hálózatot érintő támadások és fenyegetések szerteágazóak.

- Az elektromos hálózaton keresztüli adattovábbítás (Powerline technológiák) újszerű sebezhetőséget hordoz magában, hiszen ezt a rendszert kihasználva a támadó távolról hozzáférést szerezhet az otthoni hálózathoz, és teljes irányítása alá veheti az eszközöket, mint például a világítást, elektronikus zárakat, fűtő- és légkondicionáló rendszereket, amelyeket átprogramozva kénye kedve szerint alakíthatja át az adott ház arculatát. Továbbá a viselhető egészségügyi és monitorozó eszközökhöz is hozzáférést szerezhet, amellyel szélsőséges esetben akár a hordozójának életét is veszélybe sodorhatja. Végül pedig a vezeték nélküli hálózatok gyenge pontjait is kiaknázhatja a rosszindulatú, amely szintén szabad utat biztosíthat az otthoni rendszerekhez, beleértve a hagyományos, hálózati kapcsolatra képes számítógépeket.
- Az otthoni hálózat leggyakoribb fenyegetései közé sorolhatóak a trójai vírusok, hátsó kapu programok, e-mail vírusok és hamisítás, csomagok szaglászása (packet sniffing), valamint a szolgáltatás megtagadás támadások.

Az ajánlott biztonsági lépések a fenyegetések minimalizálása érdekében a következőek:

- Vírusvédelem és tűzfalak használata;
- Ismeretlen eredetű, gyanús e-mailek és csatolmányai megnyitásának mellőzése;
- Ismeretlen eredetű alkalmazások letöltésének és futtatásának mellőzése;
- Valamennyi program, az operációs rendszert is beleértve, rendszeres frissítése;
- Vezeték nélküli otthoni hálózat biztonsági beállításainak alkalmazása;
- Biztonsági másolatok készítése.

A szenzor hálózatok biztonsága

A több milliárdnyi eszköz nagy része érzékelőkkel kiegészített intelligens berendezés. A *beépített szenzorok*, ahogy a dolgok pillérénél már kifejtettem, az élet különböző területein a fizikai világról gyűjtenek adatokat. Az összegyűjtött adatmennyiséget elküldhetik elemzésre vagy akár maguk az eszközök is feldolgozhatják, következésképpen értékes információhoz juttathatják az embereket az adott területtel kapcsolatban. A hálózatban lévő szenzorok biztonsága, az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása így kiemelkedővé válik.

Az érzékelőkhöz számos fenyegetés, sebezhetőség kapcsolható.

- A *szenzorok telepítése* sok környezetben véletlenszerűen történik. Nincs előretervezett topológia, sőt bizonyos esetekben a fizikai védelem sem valósul meg. Ennek következtében az érzékelő számítógépek könnyen elfoghatóvá válnak. A támadók egyrészt fizikailag hozzáférhetnek az szenzorokhoz, valamint hálózaton keresztül is akár egy vírussal átvehetik az eszköz felett az irányítást.

- Az érzékelők alapvetően *korlátozott mennyiségű energia és számítási kapacitással* rendelkeznek. Az energiát főleg az adatok gyűjtésére és a hálózati kapcsolatok fenntartására fordítják. A szűk erőforrás akadályozza a hatékony biztonsági megoldások (pl. erős titkosítás) megvalósítását.
- A *szenzorok típusa* szerteágazó, alkalmazási környezettől függő, amely tovább bonyolítja az érzékelők biztonságának megvalósítását.

A jogosulatlan személy a felsorolt, illetve az egyéb hálózati biztonsági réseket kihasználva támadhatja a szenzorokat. A támadások a következők lehetnek.

- *Lehallgatás (eavesdropping)* esetén a támadó elfogja az érzékelőktől származó hálózati forgalmat, és megnézi a csomagok információtartalmát. Két típusa van, az egyik a passzív lehallgatás, amikor a támadó jelenléte inaktivitása miatt a szenzor hálózaton nem érzékelhető, a másik az aktív módszer, amikor tevékenyen hajtja végre a csomagok lehallgatását.
- *Megszakítás (disruption)* során a támadások célja, a szenzorok működésének zavarása, megakadályozása. Itt is két típust különböztetünk meg. Lehet szó szoftveres vagy hardveres megszakításról. Az előbbihez sorolhatóak például a szolgáltatás megtagadások, vagy útvonal hurkok, amelyek hamis irányító címzést alkalmazva irányítási hurkokat hozhatnak létre. A hardveres támadás csoportjába tartozhat az érzékelők környezetének fizikai manipulálásai, például az eszköz környezetének felmelegítése, amely által hibás adatok kerülhetnek továbbításra.
- *Eltérítés (hijacking)* csoportjába tartozó támadásokkal a rosszakaró elfoghatja a hálózati forgalom csomagjait és megváltoztathatja az összegyűjtött adatok tartalmát.

Átfogó megoldás nem létezik a szenzorok védelmére, csupán irányelvek vannak, amelyek konkrét megvalósulásai elősegíthetik a biztonság létrejöttét. Ennek az oka, a szenzorokhoz köthető, az előbbiekben már felsorolt sebezhetőségek, amelyek a tradicionális számítástechnikában elvétve vannak jelen. Az irányelvek körébe tartoznak a különböző *hozzáférést szabályzó mechanizmusok* létrehozásának, a kommunikációs csatorna valamilyen mértékű *titkosításának*, az érzékelők *fizikai védelmének* megvalósítására tett lépéseknek a megalkotása.

Adatok biztonsága

A minden a hálón hatékonysága nagyban támaszkodik a felhő alapú számítástechnika által nyújtott technológiákra. A nagy adat kezelése, elemzése és tárolása legfőképp a felhő infrastruktúrák használatával valósul meg, amelyek adatközpontokban kerülnek kiépítésre. Az adatok pillérének vonatkozásában a *felhő alapú számítástechnika biztonsági oldala* kerül bemutatásra.

2. A felhő alapú számítástechnika biztonsága

A virtualizáció kulcsfontosságú szerepet tölt be a felhő alapú szolgáltatások biztosításában. A virtualizált környezet valósítja meg a felhő technológia sokoldalúságát és skálázhatóságát. A felhő alapú számítástechnika által használt virtualizáció középpontjában pedig a VM szoftverek (hypervisor) állnak. A programoknak köszönhetően létre lehet hozni igény szerint virtuális gépeket, és elosztani közöttük a fizikai erőforrásokat. Mivel a VM programok felelősek az összes virtuális gép megfelelő működéséért, így ha egy támadó bejut és átveszi a VM szoftverek irányítását kénye kedve szerint létrehozhat, törölhet vagy manipulálhatja a már meglévő virtuális környezeteket, amely által veszélybe kerülnek a felhő alapú szolgáltatások biztosítása. Ennek következtében, a felhő alapú szolgáltatások biztonságánál kiemelkedő szerepet kap a *VM szoftverek védelme.*

A virtuális gép szoftvereknek két típusa van, az első közvetlen a hardverre van telepítve (*1. típus*), a másik már egy adott operációs rendszeren fut (*2. típus*). Mind a két típushoz kapcsolhatóak biztonsági fenyegetések, amelyek a következők:

- Az *1. típus* esetén, ha bejut a támadó a rendszerbe, akkor az egész infrastruktúra felett, beleértve a virtuális gépeket, átveheti az irányítást. Olyan kártevő programok (VMBR, Virtual Machine Based Rootkit) léteznek, amelyek álcázva magukat virtuális gép szoftvereknek telepíthetőek a hardver platformra, s alapbázist adhatnak további rosszindulatú programok telepítésére és használatára. Ilyen támadásokkal az egész felhő infrastruktúra használhatatlanná tehető, amely a vállalkozások és egyének számára felbecsülhetetlen értékű károkat okozhat. A VMBR - k nehezen detektálhatóak, mivel a teljes megfertőzött rendszert ők irányítják, így a rendszeren belül futó védelmi mechanizmusok elől rejtve tudnak maradni.
- A *2. típusra* vonatkozóan nem áll fenn az 1. típusnál lévő fenyegetés, mivel a virtuális konténerek a hardverre telepített operációs rendszeren belül futnak. Így a támadás nem az egész virtuális környezetre lehet káros, hanem egy-egy logikailag elkülönített gépet tud csupán tönkre tenni.

Minden VM szoftver *terheléselosztást* végez. A programok a létrehozott felhő infrastruktúrában a virtuális gépek között optimálisan szétosztják a beérkező forgalmat, amely által a felhő alapú számítástechnikai rendszerek megfelelően ki tudják szolgálni a felhasználóikat. Következésképpen, a VM programokon belül, ez a terheléselosztás az elsődleges célpontja a támadók nagy részének, mivel ha hozzáférést szereznek ehhez a funkcióhoz, akkor az adatforgalom kiszolgáltatottá válik számukra. (DoS; betöréses támadások megvalósíthatóak lesznek).

A fenyegetések minimalizálása érdekében nagyon fontos az *erős titkosítás és hitelesítés* alkalmazása a szolgáltatások hozzáféréséhez, illetve az adminisztratív feladatok (pl. VM programok menedzselése) ellátásához. A felhő alapú szolgáltatások eléréséhez leginkább web alapú hozzáférési pontok vannak, amelyek további biztonsági mechanizmusok (pl. biometrikus védelem, több lépcsős beléptetési rendszerek) alkalmazását igénylik. A VM programoknál felsorolt fenyegetések minimalizálására és a támadások detektálására léteznek anti- VMBR szoftverek is már. A virtuális gép programok terheléselosztásának védelme pedig főleg a *megfelelő konfiguráción*, illetve a funkció optimális működésének *folyamatos ellenőrzésén* múlik, amely a rendszeradminisztrátorok feladata. Az infrastruktúra és az általa nyújtott erőforrások biztonsága az *adatközpontok fizikai védelmén* is alapszik, így a komplex védelem kialakítása nem könnyű feladat, amely ellátásához *megfelelően képzett szakemberekre* van szükség.

Emberek biztonsága

Az ember a központi és egyben leggyengébb láncszem minden gazdasági rendszerben. Számos érzelmi állapot, valamint viselkedési forma sebezhetővé és támadhatóvá teszi őket. A kíváncsiság, naivitás, aggodalom, stressz, figyelmetlenség, gondatlanság és egyéb emberi gyengeségek kihasználása a rosszindulatú támadók kedvelt módszerei közé tartoznak az információ és egyéb erőforrások megszerzésére

A támadási fajták lehetnek *humán*, valamint *számítógép alapúak*.

- Az elterjedtebb humán alapú támadások közé tartozik a *váll- szörfing (shoulder surfing), a kukaátvizsgálás (dumpster diving), különböző megszemélyesítési technikák*. A váll-szörfing a jelszavak megszerzésére irányuló támadás, amely során a rosszakaró közel kerülve az áldozatához, valamilyen ürüggyel rákényszerítve a rendszerbe történő belépésére, a jelszavát megláthatja, megszerezheti. A kukaátvizsgálás az irodai szemetes átkutatását foglalja magába. Humorosnak tűnhet elsőre, de rengeteg olyan információ található a kukákban, amely egy esetleges támadás megalapozásához kell; jelszavas cetlik, személyes adatok, amelyek segítséget nyújthatnak az illető személyazonosságának felvételéhez, vagy olyan információ, amely birtokában a támadó az adott alkalmazottat zsarolni tudja. A megszemélyesítési technikákkal a támadók megbízható személyeknek adják ki magukat, s megvezetik az áldozatukat az információ megszerzése érdekében. Ebbe a csoportba tartozik például az ügyfélszolgálatok átverése, vagy felsőbb vezető megszemélyesítése.
- A számítógép alapú technikák alkalmazásával a támadók a hálózaton keresztül próbálják kihasználni az emberek sebezhetőségét. A támadások lényege, hogy a

rosszakarók elhitetik az áldozataikkal, hogy egy valódi, biztonságos rendszerrel kommunikálnak. Ide sorolhatóak az *ál-weboldalak, különböző adathalászati technikák*, illetve a *trójai programok* alkalmazása. Ál-weboldalak esetén olyan oldalak használatát értjük, amelyek valamilyen csábító, legtöbbször ingyenes ajánlatot kínálnak regisztráció ellenében. Ezzel a módszerrel több e-mail és jelszó is megszerezhetővé válik. Az adathalászati technikák a hamis weboldalaktól és elektronikus üzenetektől kezdve az SMS-eken keresztül a reklámok alkalmazásával bezárólag változóak, de a cél közös, az áldozat megtévesztése, átverése, valamint a különböző adatok megszerzése a felhasználó együttműködésével. A trójai programok, olyan rosszindulatú szoftverek, amelyek kedvesnek és hasznosnak tűnnek, azonban az álca mögött rossz szándék húzódik. Így a potenciális áldozat a haszon érdekében, rákattintva az alkalmazásra elindítja a rejtett kártékony kódot, ami hozzásegíti a támadót a rendszerhez történő illetéktelen hozzáféréshez, és különböző adatok megszerzéséhez.

A támadások elleni védelem körébe tartozik a sebezhetőségek feltérképezése, a releváns biztonsági szabályzat, irányelvek, politikák létrehozása az adott szervezeten belül, a fenyegetések minimalizálása érdekében. Ezeket a biztonsági előírásokat be kell tartani és tartatni, valamint folyamatosan ellenőrizni. Továbbá, ami a legfontosabb, az alkalmazottak, munkatársak képzése (biztonságtudatossági oktatás) és továbbképzése, amelynek tárgya a felsorolt támadások és fenyegetések, és az ellenük végrehajtható biztonsági megoldások alkalmazása.

Folyamatok biztonsága

Ez a pillér nagyban befolyásolja a többi hatékonyságát, hiszen az adatmennyiség, amely a különböző dolgoktól származik és információt hordoz az ember számára, a megfelelő helyre, a megfelelő időben és formában az optimális folyamattal képes eljutni. Következésképpen a különböző folyamatok, illetve a kommunikációs csatornák védelme kiemelkedő fontosságú a minden a hálón biztonsági vonatkozásában.

A folyamatok pillérrel összefüggésben a *virtuális privát (VPN)* valamint a *vezeték nélküli helyi hálózatok (WLAN) biztonsági mechanizmusai* kerülnek bemutatásra, amelyek megvalósíthatóak mind a háromfajta kommunikációs forma (M2M, M2P, P2P) esetén.

Wi-Fi hálózatok biztonsága

A vezeték nélküli hálózatok használata az utóbbi időben népszerűvé vált, hiszen nagyfokú mobilitást nyújt a felhasználói számára. Ezeknek a technológiáknak köszönhetően az emberek (és eszközök) bárhonnan és bármikor fel tudnak csatlakozni a hálózatra, következésképpen nem meglepő, hogy a minden a hálón elképzelés is előnyben részesíti a vezetékes csatlakozási lehetőségekkel szemben, sőt a modern intelligens hálózat meghatározó részét képezik. Biztonság szempontjából a legelterjedtebb és a szinte mindenki által használt technológia, a vezeték nélküli helyi hálózatok (Wireless Local Area Network, WLAN) kerülnek ismertetésre.

A WLAN technológiák az IEEE[106] 802.11-es szabványokat foglalják magukba, amelyeket összefoglalóan Wi-Fi hálózatoknak nevezünk. Ezeket a hálózatokat leggyakrabban otthon, irodákban, illetve egyéb publikus helyeken, mint például egyetemek, repülőterek és éttermek területén használják. A Wi-Fi hálózatok mindenki számára elérhetőek és mivel egyre hangsúlyosabb szerepet kapnak az informatika világában, a WLAN – ok biztonsága kulcsfontosságú tényezővé válik.

Egy Wi-Fi hálózatot bárki elérhet az adott hozzáférési pont (Access Point, AP) hatótávolságán belül, ami az előnyén kívül egyben a sebezhetőségét is adja a vezeték nélküli hálózatnak, hiszen a rosszindulatú hackereknek még csak fizikailag sem kell hozzáférni az AP-hoz, hanem leegyszerűsítve elég egy vezeték nélküli hálózatra felcsatlakozni képes eszköz, és már végre is hajthatja a támadásokat. [41]

A Wi-Fi hálózat elleni támadások leginkább a szolgáltatás megtagadás (DoS) típusába tartoznak. Ezek közül pedig a meghatározóbbak a következők:

- A *nem megfelelően konfigurált* hozzáférési pontból kifolyólag a támadó bejuthat a rendszerbe és átállíthatja az eszköz beállításait, amellyel megbéníthatja az egész hálózatot. Helytelen konfiguráció a gyenge jelszó használata, vagy például a megfelelő titkosítás hiánya.
- *Interferencia* is okozhat szolgáltatás megtagadást. Ez azt jelenti, hogy olyan eszköz van használatban, amely ugyanabban a rádió frekvencia sávban működik, mint a Wi-Fi AP, és így a két eszköz zavarja egymás működését. (mikrohullámú sütő, különböző telefonok, stb.) Természetesen a jelenség véletlenszerűen és szándékosan is előidézhető.
- A *megtévesztő szétkapcsolás (spoofed disconnect attack)* olyan DoS támadás, amellyel a rosszakaró hamis „szétválasztó” üzeneteket küld az összes vezeték

[106] IEEE (Institute of Electrical and Electronics Engineers): a világ egyik legnagyobb nemzetközi szervezete, amely informatikusokból, mérnökökből áll és célja a technológia fejlődésének támogatása; továbbá vezető szabványosító szerv az információ technológia területén. [56]

nélküli állomásnak (Station, STA). Ennek következtében a végberendezések lekapcsolódnak a hálózatról, majd újra megpróbálnak felcsatlakozni, ami nagymennyiségű adatforgalmat generál. Ezt többször ismételve, a támadó megbéníthatja az egész hálózatot.

- A *CTS áradás* akkor történik, ha a támadó a CSMA/CA módszert használja ki. A hacker folyamatosan elárasztegy hamis állomást CTS üzenetekkel, ami által a többi, valódi állomás visszatartja a csomagok továbbítását. [107]

Wi-Fi hálózatok esetén is jelen vannak az adatok és egyéb erőforrások jogosulatlan hozzáférésére és módosítására tett kísérletek. A behatolásos támadások közül a legjellemzőbbek a *hamis hozzáférési pontok* használatával az úgynevezett „man-in-the-middle" (MITM) offenzívák.

- A hamis AP, olyan, nem engedélyezett vezeték nélküli hozzáférési pont, amely telepítése sebezhetőséget okoz a már felépített biztonsági rendszerben, hiszen kaput nyit a támadóknak a rendszer erőforrásaihoz. A rosszakaró ezzel a módszerrel elfoghatja a felhasználók üzeneteit (MAC és IP címeket; adat tartalmát), módosíthatja azokat, illetve hozzáférhet a hálózaton található többi eszközhöz, továbbá MITM támadásokat is végrehajthat.
- A vezeték nélküli MITM támadások közül a legnépszerűbb az „evil twin AP", amely során a rosszakaró az engedélyezett hozzáférési pontnak megfelelő SSID[108] - t állítja be a hamis AP - nak. Ennek következtében, a felhasználók két ugyanolyan WLAN – t látnak és azok, akik közelebb helyezkednek el a támadó hozzáférési pontjához, nagyobb jelerősséget fognak érzékelni a hamis AP SSID - nél az eszközükön, így a rosszakaró AP - ra csatlakoznak majd fel. A forgalom, amit a becsapott felhasználók generálnak a támadó eszközére érkeznek, és a hamis AP a valódi hozzáférési pont felé irányítja a csomagokat és fordítva. Ennek következtében a támadó megszerezheti az egyes kliensek felhasználó nevét, jelszavát és egyéb, a céljainak megfelelő információkat.

A Wi-Fi hálózatokat érhető fenyegetések megelőzése és minimalizálása érdekében a következő biztonsági lépések hajthatóak végre.

- *SSID elrejtése.* Ezzel lehetővé válik, hogy csak az a személy tudjon felcsatlakozni a vezeték nélküli hálózatra, aki ismeri az adott SSID-t.
- *MAC- cím szűrése.* A metódussal megvalósítható egy MAC- cím alapú hozzáférési lista elkészítése, amellyel a rendszer adminisztrátora meghatározhatja, hogy ki kapcsolódhat fel az adott hálózatra.

[107] CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance): az IEEE 802.11- es szabványú hálózatoknál használt protokoll, amelynek a feladata a csomagok ütközésének a megelőzése. A CTS (Clear To Send) pedig egy jel arra, hogy az üzenet a hálózaton keresztül továbbítható.

[108] SSID (Service Set Identifier): Az adott vezeték nélküli helyi hálózatnak az azonosítója (neve).

- *Megfelelő hitelesítés és titkosítás beállítása.* Biztonság szempontjából a megosztott kulcsú hitelesítés és titkosítás közül a WEP, WPA és WPA2 mechanizmusokat választhatjuk. A WEP (Wired Equivalent Privacy) olyan védelmet biztosít, mintha a kommunikációs csatorna vezeték alapú lenne. Azonban a kulcs, amit a mechanizmus használ állandó, így könnyű feltörni, azaz alkalmazása nem ajánlott. WPA (Wi-Fi Protected Access) és WPA2 vagy IEEE 802.11i már olyan titkosító algoritmusokat használnak,[109] amelyek a kulcsokat az egyes csomagok továbbításánál megváltoztatják, így alkalmazásukkal magasabb fokú biztonság érhető el. A WPA/WPA2 metódusoknak további két típusa létezik, amelyek közül lehet választani. Ez a személyes (Personal) és a vállalati (Enterprise) WPA – k, attól függően, hogy a Wi-Fi hálózatot milyen környezetben akarjuk kiépíteni. A különbség a kettő között, hogy az Enterprise[110] a hitelesítés végrehajtására külön, erre a feladatra kijelölt szervert használ.[111]

A biztonsági beállítások alkalmazása, és a hálózat megfelelő és folyamatos monitorozása minimalizálhatja a sebezhetőségből fakadó különböző támadások sikerességét. Azonban, olyan publikus vezeték nélküli hálózatok (étterem, üzletek, repülőterek, stb.) esetén, amely beállításai csupán az internetre történő felcsatlakozást teszik lehetővé, mellőzve mindenféle biztonsági lépést, a fent említett támadások könnyebben kivitelezhetőek, így, ha tehetjük, ne csatlakoztassuk eszközünket a hálózathoz, vagy ha mindenképpen szükséges, akkor használhatjuk a *virtuális privát hálózatokat*, amely további, magasabb szintű biztonság megteremtésére hivatottak.

Virtuális privát hálózatok

A minden a hálón világában az eszközök, és általuk az emberek különböző helyszínekről csatlakozhatnak fel a szervezetek hálózataira. A vállalatoknak szükségük van biztonságos, megbízható, valamint költséghatékony megoldásokra, hogy ezek a kapcsolatok eredményesek legyenek. A virtuális privát hálózatok által a publikus hálózatokon keresztül vándorló adatmennyiség biztonságban van. Köszönhetően a létrehozott privát csatornáknak, amelyek erős titkosítást és

[109] WPA által használt titkosító algoritmus a TKIP (Temporary Key Integrity Protocol). A WPA 2 pedig az AES (Advanced Encryption Standard) metódust alkalmazza, amely az egyike mai létező legerősebb titkosító módszereknek.

[110] A vállalkozásoknak ajánlott a WPA típusok közül az Enterprise-t választani, amely erősebb hitelesítést valósít meg a RADIUS (Remote Authentication Dial In- User Service) szerverek által.

[111] Megjegyzés: a felsorolt algoritmusok és hitelesítések részletes kifejtése túlmutat a dolgozat témáján.

hitelesítést valósítanak meg, az adat bizalmasságának, sértetlenségének biztosítása megvalósul.

A virtuális privát hálózatoknak következő két típusa létezik.

- *Helyszínt- helyszínt összekötő VPN (Site-to-site VPN)*. Ez a megoldás két privát hálózatot tud összekötni biztonságosan az interneten vagy bármilyen publikus hálózaton keresztül. Ez egy állandó kapcsolat, a kommunikáló felek nincsenek tudatában a virtuális privát hálózatnak. A megvalósítás úgynevezett VPN forgalomirányítók által történik. Ezek az eszközök felelősek a hálózatokból kimenő forgalom megfelelő keretekbe történő beágyazásáért, valamint az adatok titkosításáért, az üzenet továbbításáért. Továbbá, az üzenet fogadása során a csomagok dekódolása, illetve a megfelelő végberendezéshez történő eljuttatása is a forgalomirányítók feladata. Ez a típus egy WAN megoldásnak felel meg; régebbi Frame Relay kapcsolatok vagy bérelt vonalak helyettesítésére szolgálhat.
- *Távoli hozzáférés VPN (Remote access VPN)*. Ez a típus az egyének és a vállalatok közötti biztonságos kapcsolat létrehozására szolgál. Dinamikus kapcsolat, így igény szerint építhető ki, valamint kliens-szerver modellt alkalmaz, következésképpen egy VPN kliens program szükséges az adott személy eszközén, hogy a privát, titkosított csatorna a szervezet hálózatának határán lévő VPN forgalomirányítójával felépítésre kerüljön. A működése a csatorna kiépülése után megegyezik a helyszínt-helyszínt összekötő virtuális privát hálózatéval, annyi különbséggel, hogy az egyén eszközén telepített kliens szoftver veszi át az egyik VPN forgalomirányító titkosító és hitelesítő funkcióit.

A virtuális privát hálózatok megvalósításához a legelterjedtebb keretrendszer az *IPSec*.

Az IPSec (Internet Protocol Security) egy nyitott, IETF[112] szabvány, amely az IP alapú virtuális privát hálózatok biztonsági mechanizmusait biztosítja. Ez a protokoll a hálózati rétegben működik, és az IP csomagok hitelesítésért, valamint titkosításáért felelős. A védelmi mechanizmusok kiterjednek a harmadiktól a hetedik rétegig, következésképpen minden alkalmazás forgalma egy biztonságos kommunikációs csatornán kerülhet lebonyolításra.

IPSec három kritikus funkciót nyújt a biztonság vonatkozásában:

[112] IETF (Internet Engineering Task Force): hálózati szakemberek, kutatók nemzetközi szervezete, akiknek célja az internet infrastruktúrájának fejlődésének támogatása és az optimális működésének biztosítása. A szervezet feladata olyan minőségi szabványok, dokumentumok kiadása, amelyek szabályozzák az internet infrastruktúrájának tervezését, kezelését.

- Az *adatok bizalmassága (confidentality)* biztosítja, hogy csak a jogosult személy férhet hozzá az elküldött üzenet tartalmához. A megvalósítás erős titkosító algoritmusok által történik (AES, RSA)
- Az *adatok sértetlensége (integrity)* által megvalósul, hogy az adatok tartalmát a hálózaton keresztüli vándorlásuk során jogosulatlan személy nem módosítja. (Keretvégi ellenőrző összegek, hash függvények, MD5, SHA-1) [113]
- Az *adatok hitelesítése (authentication)* biztosítja, hogy a kommunikációs csatorna mindkét végén a megfelelő személyek vannak (IKE, PSK, digitális aláírások). [114] Ez a kommunikációs felek identitását védi a támadók megszemélyesítő támadásai ellen.[115]

A keretrendszernek két fő protokollja van, amelyre épülhetnek a biztonságot megvalósító algoritmusok.

- Az *Authentication Header (AH)* olyan protokoll, amely nem biztosítja az adatok bizalmasságát, csupán az IP csomagok hitelesítését és integritását. Minden üzenet nyíltan kerül továbbításra a hálózaton. Egyedül alkalmazva nem nyújt megfelelő biztonságot a kommunikációs csatornáknak.
- Az *Encapsulated Security Payload (ESP)* protokoll lehetővé teszi az adat titkosítását, valamint a hitelesítés megvalósítását.

Az IPSec beállításánál legelőször a megfelelő keret protokollt (AH és ESP kombinálható) kell kiválasztani, majd az ahhoz kapcsolódó és engedélyezhető biztonsági algoritmusokat, amelyek a kerettől függően az adat bizalmasságát, integritását, valamint a kommunikáló felek hitelesítését valósítják meg.

A négy alappillér és a közöttük lévő kölcsönhatás együttesen adja a minden a hálón elképzelésében rejlő értékeket. Következésképpen, a harmadik fejezetben felsorolt, és bemutatott biztonsági fenyegetések, illetve az ellenük megléphető védelmi mechanizmusok, valamint biztonsági irányelvek természetesen az egész rendszert áthatják, függetlenül a dolgozatban leírt csoportosítástól.

A fejezetből látható, hogy a biztonság, úgy, ahogy maga az egész elképzelés meglehetősen képlékeny még. Jelenleg átfogó megoldás nem létezik a milliárdnyi eszköz, valamint az általuk generált adatmennyiség védelmére, pusztán egy-két terület biztonsága valósítható meg, de ezek is inkább a már meglévő megoldásokra

[113] A hash függvény (hasító függvény): olyan függvény, amely egy tetszőleges hosszúságú karaktersorozatot egy rövidebb, fix méretű karaktersorozattá alakít át. IPSec esetén a használt hasító eljárások az MD5 (Message Digest 5) és a SHA-1 (Secure Hash Algorithm).

[114] Az IPSec által használt hitelesítés az IKE (Internet Key Exchange). Ez a hitelesítő módszer jelszavakat, digitális aláírásokat, PSK (Pre-Shared Key) algoritmust használja a feladat végrehajtására.

[115] Megjegyzés: a felsorolt algoritmusok és eljárások részletes kifejtése túlmutat a dolgozat témáján.

hagyatkoznak. Így mérhetetlenül nehéz feladat áll a szakemberek előtt, hogy a minden a hálón elképzelésben rejlő értékeket a világ valóban megtapasztalhassa, hiszen a nem megfelelően felépített biztonság akár a megálmodott, korlátok nélküli intelligens hálózat összeomlását is eredményezheti.

Összegzés

A változás az egyetlen, ami állandó a világunkban. Ez hatványozottan igaz az információ technológia világára nézve, hiszen közel egy emberöltő alatt az internet egy katonai célra szánt apró hálózatból egy világméretű informatikai rendszerré alakult át. Napjainkra behálózta a fizikai világunkat, valamint a mindennapi életünket egyaránt. Internet nélkül az élet már szinte elképzelhetetlen lenne a mai ember számára.
A globális hálózat fejlődése természetesen nem állt meg, hiszen megszületett a minden hálón, a mindent és mindenkit átható intelligens hálózat, amely új szintre emeli az internetet és annak képességeit. Ez az elgondolás, ahogy láthattuk, egy mérhetetlenül nagy változást hoz az életünkbe. A több milliárd eszköz, az elképzelhetetlen mennyiségű adat, a megfelelő folyamatok és a mindig középpontban álló ember; a négy alappillér és az őket támogató két fő informatikai trend (virtualizáció és a felhő alapú számítástechnika), amelyet a dolgozat bemutat, meghatározza, de pillanatok alatt le is rombolhatja a megálmodott intelligens hálózatot.
A modern globális hálózat jelenleg a megvalósítás fázisánál tart. A korlátokat nem ismerő optimizmus, ami átjárja a minden a hálón elképzelést, azonban könnyedén a visszájára fordulhat. A hálózat elgondolása még képlékeny, így a megismert pillérek sem állnak elég stabilan a megálmodott lehetőségek teljes mértékű kiaknázásához. A megvalósítás előtt álló akadályok egy része könnyedén, a többi nehezebben küzdhető le. Meglátásom szerint, a legnagyobb problémát a nagy adat kezelése, és a minden a hálón biztonságának megteremtése okozza. Ez a két terület sorsdöntő a modern hálózat kiteljesülésének szempontjából. A hatalmas eszközpark óriási méretű adathalmazt generál, amelynek nagy része mozgásban van, így a legtöbb esetben valós vagy közel valós időben kell az értékes információt kinyerni és adott pillanatban azt felhasználni. Ráadásul az adat a rendszer alkalmazási területétől függően hordoz információt magában, hiszen ami egyik területnek értékes információ a másiknak messziről sem az. Ennek a megvalósítása pedig óriási feladat. A biztonság megteremtése megint csak egy vízválasztó akadály, amelyre a dolgozat jól rámutat, hiszen nincs átfogó megoldás, és a megfelelő védelmi mechanizmusok alkalmazása egy olyan rendszernél, amelyre a mindennapi

ember hétköznapjainak és az üzleti életének nagy része támaszkodik, nem valósul meg, annak súlyos következményei lehetnek, és az egész rendszer összeomlását vonhatja maga után.
Rengeteg kérdés marad nyitva a témával kapcsolatban, amelyek megválaszolása bőven túlmutat e tanulmányon. A dolgozat elején kitűzött céljaimat azonban elértem, mivel egy átfogó képet nyújtottam a modern globális hálózatról, annak képességeiről, továbbá a lehetőségeimhez mérten megvizsgáltam a rendszert a biztonság vonatkozásában is egyaránt.
Összefoglalva, a jövő hálózata kitárta kapuit. Az emberek tudásán múlik csupán, hogy sikerül-e belépni és teljes mértékben megtapasztalni a minden a hálón, a mindent és mindenkit átható intelligens hálózat képességeit vagy sem. Ez a legjelentősebb nyitott kérdés, amelyre pár év, illetve évtized múlva meg fogjuk kapni a megfelelő választ.

Felhasznált irodalom

[1] J. M. Kizza, Guide to Computer Network Security Third Edition, London: Springer- Verlag , 2015.
J. E. Canavan, Fundamentals of Network Security, Norwood, MA: Artech House, Inc., 2001.
[2] M. Bishop, Computer Security: Art and Science, Boston, MA: Pearson Education, Inc., 2003.
[3] O. E. Diána, Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője, Budapest: Budapesti Corvinus Egyetem, Gazdálkodástudományi Kar, Számítástudományi Tanszék, 2008.
[4] http://borg.uu3.net/cisco/inter_arch/pic/01-01.jpg. [Letöltés ideje: 2015.02.15.].
[5] http://www.techopedia.com/definition/5899/advanced-research-projects-agency-arpa. [Letöltés ideje: 2014.12.14.].
[6] Kerti András: Az információbiztonsági kockázatkezelés oktatásának buktatói, Kommunikáció 2013, ISBN 978-615-5305-16-0, Nemzeti Közszolgálati Egyetem, 53-60. oldal, Budapest, 2013.

Paráda, István – Pándi, Erik: Network monitoring program development based on SNMP protocol

Abctract
Nowadays Information Technology is the most popular profession, which plays a huge role of our everyday life. In the recent years technical development has been tremendously fast paced, and produced interesting solutions. Consequently, one of the basic knowledge to explore and recognize which elements a network consists of, and how these devices are work?

Absztrakt
Az IT ágazatban dolgozni napjainkban igen remek, egyebek iránt is nagy szerepe van mindenenpi életünkben. Jelen cikk ezen kérdéskör néhány aspektusát kívánja röviden feldolgozni.

Preface

A simple network consists of some which communicate with other networking devices such as switches, routers and other PCs. The switches main task is to ensure the communication at Layer2, so they forward the frames, based on the MAC-address and port number comparison process. Routers operate at a higher layer, that is, layer 3, where packet-forwarding occurs. This is Layer 3 where the device forward packets. The packet-forwarding process utilizes IP addresses in conjunction with next-hop addresses or outgoing interface numbers to route the information appropriately.

1. SNMP

Networking devices have become extremely complicated over time. To suffice the necessities of administrators, developers had to find a way to control and manage these devices. There are lots of software to use and maintain devices properly. These software's use protocols to reach their purpose. One of the most popular and easiest is the SNMP- Simple Network Management Protocol.
SNMP is a protocol which is located at the Application layer. It ensures a communication format between a manager and one or more agent devices. The manager is a software can has been installed on a PC, the agent is also a software but it can be found on the network devices as well router or switch. The SNMP uses UDP protocol to build up a connection between the agent and the manager device.

These UDP segments collect several data and attribute about the agent device. This collection depends on the MIB (Management Information Base).

The process of data collect consists of some operation:

- Get request
- Get Next Request
- Get Response
- Set
- Trap

2. DLL files, .NET framework

If we want to write a program, first of all we need to know a program language. My advice for the preparation of the program is the C#, and Visual Studio.
There is an essential thing which is the usage of DLL files, because they make the program writing process much easier, and faster. DLL (Dynamic Link Library) is a collection of files, which are actually pieces of programs, but they are not able to run independently. Usually these are located in the System and System32 directories.
.NET Framework (pronounced *dot net*) is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It includes a large class library known as Framework Class Library (FCL) and provides language across several programming languages. Programs written for .NET Framework execute in a software environment (as contrasted to hardware environment), known as Common Language Runtime (CLR), an application virtual machine that provides services such as security, memory management, and exception handling. FCL and CLR together constitute .NET Framework.

3. Programming

First of all, I have to clear up I use Windows 8.1 operating system with 4.5 .NET Framework and Visual Studio 2010 Ultimate software to write the program. Furthermore there were two necessary DLL files: SharpSnmpLib.dll and SharpSnmpLib.Engine.dll
Then I create a new Windows Form Application, refer to the above sentences it is very important to load the proper DLL files, because these help to write the right commands. Next one I have to make three *String* variables. These were the IP address, SNMP Community and the OID. The *String* makes these properties static,

so the programmer can change them, but not dynamically. Thereafter I made a button which sends a *GET-Next Request* message to the network device. This message depends on which IP address and Community are given. It checks the OID number and start the query. There is a MIB structure, so when the first query was successful, it jump to the next OID according to the MIB. The *GET-Next Request* message was written inside a *for cycle*, which generates a top-down running process, so my message runs many times in a row. Every request message has an answer which was defined by a *var variable*. Because of the *var variable*, these data packets were dynamically changeable.

```
namespace WindowsFormsApplication1
{
   public partial class Form1 : Form
   {
      String IPcim = "192.168.1.2";
      String Community = "public";
      String OID = "1";
      public Form1()
      {
         InitializeComponent();
      }

      private void button2_Click(object sender, EventArgs e)
      {
         String JelenErtek = "1.3.6.1.2.1.1.0";
         listView1.BeginUpdate();
         for (int i = 0; i <= 1000; i++)
         {
            GetNextRequestMessage message = new
GetNextRequestMessage(0,
                  VersionCode.V1,
                  new OctetString("public"),
                  new List<Variable> { new Variable(new
ObjectIdentifier(JelenErtek)) });
            ISnmpMessage response = message.GetResponse(60000,
new IPEndPoint(IPAddress.Parse(textBox1.Text), 161));
            if (response.Pdu().ErrorStatus.ToInt32() != 0)
            {
            }
```

```
var result = response.Pdu().Variables;
string tmp = result[0].ToString();
```

So I had a big data stream from the network device. Then I wanted to write the data to a list, so I created *a listview* table and added to the values to the *Subitems* of the List. There were lots of ineffectual data, so I made a decision to cut the unavailing data and write just the appropriate data to the list. I made this with the correct use of *Substring* and the *INDEXOF*. Because of the overwhelming data the program worked too hard, and sometimes got frozen, so I had to make a sleep process, which is helped to the software to the right time exploitation.

```
            ListViewItem row = new
ListViewItem(tmp.Substring(tmp.IndexOf("Id") + 5, tmp.IndexOf(";
D") - tmp.IndexOf("Id") - 5));
            row.SubItems.Add(tmp.Substring(tmp.IndexOf("Data") + 5));
            string tmp2 = tmp.Substring(tmp.IndexOf("Data") +
5).Trim();
            if ((tmp2 != "0") && (tmp2 != ""))
               listView1.Items.Add(row);

            int beginnum = result[0].ToString().IndexOf("Id:") + 5;
            int endnum = result[0].ToString().IndexOf("Data") - 2;
            int length = endnum - beginnum;
            String NewResult = result[0].ToString().Substring(beginnum,
length);
            JelenErtek = NewResult;
            if (i % 500 == 0) { System.Threading.Thread.Sleep(100); }
         }
         listView1.EndUpdate();


         listView1.AutoResizeColumns(ColumnHeaderAutoResizeStyle.Colum
         nContent);
```

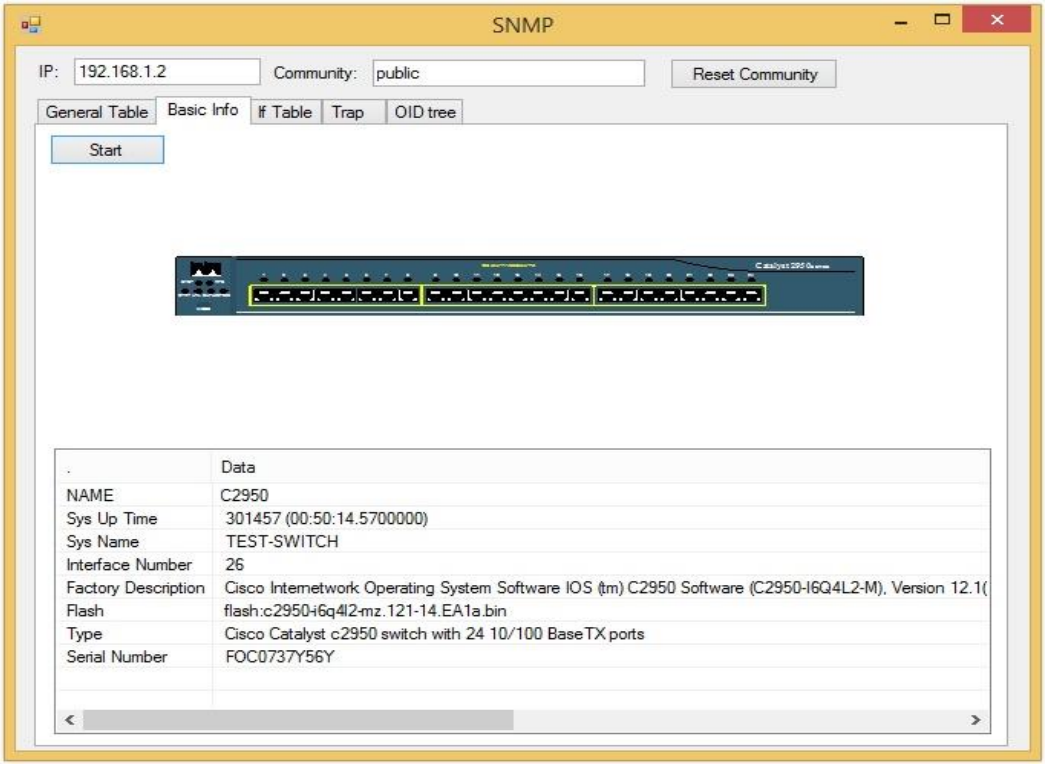
Furthermore I wanted some graphical feedback so I made a copy from my first List, and pasted it a second list. The mass of information had to be treated carefully, so only the most important data had been chosen, for example the device name, up time, serial number, port number, IOS type, etc. Also I made a collection of pictures about the network devices, if the system name is contains of the first five letters

from the device, then it paste a picture whit a *bool* function. So the user can see how the network device looks like. The next step was a new list which produces a table about the interfaces, MTU, Speed and Status characteristics.

```
            copy_row(find_row(listView1, "1.3.6.1.2.1.1.3.0"), 0, "", false,
"Sys Up Time",listView2);
            copy_row(find_row(listView1, "1.3.6.1.2.1.1.5.0"), 0, "", false,
"Sys Name",listView2);

        private void listView2_SelectedIndexChanged(object sender,
EventArgs e)
        {
        }
        private int find_row(ListView lw, string search_text)
        {
            int row = 0;
            for (int i = 0; i < lw.Items.Count; i++)
            {
                if (lw.Items[i].SubItems[0].Text.Contains(search_text))
                {
                    row = i;
                    break;
                }
            }
            return row;
        }
        private void copy_row(int row_index, int substring_length,
string device_type, bool load_image, string row_title, ListView
targetListView)
        {
            string smt = listView1.Items[row_index].SubItems[1].Text;

            if (substring_length == 0)
                substring_length = smt.Length;

            if (smt.Contains(device_type))
            {
                ListViewItem lvi = new ListViewItem();
                ListViewItem lvi2 = new ListViewItem();
```

```
                    lvi.Text = row_title;
                    lvi2.Text = row_title;
                    targetListView.Items.Add(lvi2);
                    lvi2.SubItems.Add(smt.Substring(smt.IndexOf(device_type),
            substring_length));
                    if (load_image)
                       pictureBox1.Image = new Bitmap("IMG\\" + device_type
            + ".bmp");
targetListView.AutoResizeColumns(ColumnHeaderAutoResizeStyle.ColumnContent
);
                }
        }
```

Design



Summary

My main goal was to write a program, which collect important information from the active networking devices. These informations support the Information

Technology job and tasks. Otherwise there is another type of this manager information, it is called trap. Trap messages are sent automatically. This feature is necessary, if you would like to troubleshoot a network.
The program what I made is a manager program, which helps maintaining the computer network, and supports the IT personal with necessary information, to mitigate control and troubleshooting all over the network

References

[1] Paráda István hadnagy (2013): A hálózatbiztonság vizsgálata a hálózati eszközöket érintő támadások gyakorlati szimulációin keresztül 2013
[2] Paráda István hadnagy (2015): SNMP alapú hálózatmonitoring program fejlesztése, alkalmazása
[3] Andrew S. Tanenbaum (1992): Számítógép-hálózatok
[4] Todd Lammle (2013): CCNA Routing and Switching
[5] http://www.codeproject.com/Articles/468892/An-introduction-to-sharpSNMP-an-Open-Source-SNMP
[6] http://www.snmpsharpnet.com/?page_id=30
[7] Kerti András – Pándi Balázs – Rajnai Zoltán: Structure of the command and information system, Hadmérnök 4/3., ISSN 1788-1919, ZMNE, 2009., 303-309. oldal

Jelen számunk szerzői

Farkasné Hronyecz Erika	NKE HHK PhD hallgató
Fődi Gábor	ÓE PhD hallgató
Dr. Horváth Zoltán mk. alez.	NKE HHK adjunktus
Jobbágy Szabolcs szds.	NKE HHK tanársegéd
Dr. Kerti András mk. alez.	NKE HHK adjunktus
Nagy Balázs hdgy.	NKE PhD hallgató
Paráda István hdgy.	MH BHD IFK
Pausits Péter	ÓE PhD hallgató
Dr. Pándi Balázs	közgazdasági programozó matematikus
Dr. Pándi Erik r. ezds.	NKE HHK főiskolai tanár
Prof. Dr. Rajnai Zoltán	ÓE BDGBK dékánhelyettes
Répás Sándor	ÓE
Sipos Zoltán hdgy.	MH KDK
Szabó Anna Barbara	ÓE PhD hallgató
Szabó Gergő htj.	NKE HHK hallgató
Szanyi Sándor htj.	NKE HHK htj.
Szegedi Péter htj.	NKE HHK htj.
Szögi Gábor	okl. biztonságtechnikai mérnök

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 (29-358 mellék)
hhk_hirado_szakcsoport@uni-nke.hu