**Nyári László**

# ÚJ LEHETŐSÉGEK AZ INTEGRÁLT VÉDELMI RENDSZER FEJLESZTÉSÉRE

**Absztrakt**

Nem kerülhetjük meg! Mai „digitalizált” életünk - minden területén megjelenő – informatikai rendszereinek köréből, nem hiányozhat egy jól átgondolt és felállított Integrált védelmi rendszer.

A közös fejlesztések alapja egy nemrég ismerté vált köz-fogalom is - ami közbeszéd látókörébe is kerül - ez a “HoReKa” Integrált Védelmi Rendszer. Jelentése nem más mint egy találó szórövidítés, fontos szóösszevonás. A Honvédelem, Rendvédelem, és Katasztrófavédelem integrált e-védelmi (igazgatási) rendszer-tervezetének találó szóösszetétele.

A téma feldolgozása nem új keletű, már eddig is több - értékes előzőleg megjelent - cikk és értekezés is foglalkozott vele. Sajnos ezek bár igen fontos de a mai védelmi rendszerek egyes részterületeit dolgozzák csak fel.

Ebben az írásomban az IVR felállításának lehetőségét, esélyeit vizsgálom.

**Kulcsszavak**: új kommunikációs eszközök, átfogó védelem, integrált rendszer, védelmi-informatika

# NEW DEVELOPMENT FOR OVERALL INTEGRATED PROTECTION SYSTEM

**Abstract**

We can not avoid! Nowadays a new notion come into the common-speak, which is the "HoReKa". The meaning as an abridge originated from these Hungarian expressions: Honvédelem, Rendvédelem, Katasztrófavédelem as an integrated protection of these administration systems.

The works on this field are not new, many worthy articles, lectures could be read about. Unfortunately they all work only on some subfield of the protection systems, thou they are important. Impossible to cure out a well taught and well deployed plan for an Integrated Protection System from the informatics systems collection in our digitized life.

In these lecture I would like to show the setting-up possibilities, and chances of Overall Integrated Protection System

**Keywords**: common speek, digitized life, integrated system, protection-informatik,,

## 1. MAGYARORSZÁG VÉDELEMPOLITIKÁJÁNAK ALAPJAI

Nálunk a Minisztériumok sorában hiába keresünk - legfelső szintű védelmi szervezetet - egy Védelmi Minisztériumot. (Ez az alapállás inkább politikai mint szakmai, de talán érdemes a téma kutatása, kapcsán mégis végiggondolni). A különböző veszélyhelyzetek elhárítása több – Honvédelmi, Belügy, Földművelési stb.– minisztérium hatáskörébe is tartozik aminek szinte természetes következménye a széttagoltság az irányításban, a felelősségben 2009. május 1-jétől átalakul a Kormányzati Koordinációs Bizottság (KKB) összetétele is.[1].

[1] A tagok a kijelölt miniszterek (az agrárpolitikáért, az államháztartásért, a bányászati ügyekért, az egészségügyért, az elektronikus hírközlésért, az élelmiszerlánc-felügyeletért, az energiapolitikáért, a gazdaságpolitikáért, a határrendészetért, a honvédelemért, az idegenrendészetért és menekültügyért, az

A KKB Titkársága és a KKB Operatív Törzse a katasztrófák elleni védekezésért felelős miniszter által vezetett minisztérium bázisán, Veszélyhelyzeti Központja pedig az OKF bázisán működik, elnöke a katasztrófák elleni védekezésért felelős miniszter.

A KKB több mint tíz éves története során világosan szétválnak az irányítási és a koordinációs feladatok. A katasztrófák elleni védekezésért felelős miniszter a kormányzati koordinációs szerv véleményének kikérése mellett irányítja „összehangol, javaslatot tesz és kezdeményez" a védekezéssel és a felkészüléssel kapcsolatban a megyei, fővárosi védelmi bizottságok és a megyei, fővárosi védelmi bizottságok elnökei feladatainak végrehajtását.[3] (Ez a felállás esetenként nem segíti elő a szükséges erők és eszközök hatékony rendelkezésre állítását, adott esetben inkább ronthatja a legrövidebb reakció idő elérésének lehetőségét)[2]

***A magyar kormány a biztonság és védelempolitikát a különböző kormányzati intézmények közös feladatának tartja.***

Ennek szellemében különböző veszélyhelyzetek hatékony elhárítására olyan megoldásokat kell alkalmazni, amely képes automatikusan felismerni az incidenseket, rendellenességeket és a különböző behatolási kísérleteket.

Ennek alapján egy jól működő átfogó védelmi rendszer a lehető legrövidebb időn belül meg is teszi az alkalmazott automatikus eljárás szerinti szükséges válaszlépéseket. Így amíg a rendszer az emberi beavatkozásra vár, kevésbé okozhat félreértelmezhető adatszivárgást vagy más jellegű kárt a késlekedés, Az esetleges biztonsági események monitorozása már számos szervezetnél alapvető tevékenység.

Az IT-biztonsági szakemberek figyelme azonban az utóbbi időben az események észleléséről az események kezelésének irányába tolódik.

Nem elég ugyanis azonosítani a biztonsági incidenseket, csak akkor teljes a biztonság, ha a szervezet gyorsan és hatékonyan képes reagálni is az adott eseményre.

---

iparügyekért, a kereskedelemért, a kormányzati, közigazgatási informatikáért, a környezetvédelemért, a közlekedésért, a külpolitikáért, az oktatásért, a polgári nemzetbiztonsági szolgálatok irányításáért, a rendészetért, valamint a vízgazdálkodás- ért felelős miniszter),

[2] Lásd 1 sz.. esettanulmány! Mindenkép továbbgondolkodásra érdemes!

# 2. LEGFONTOSABB ÁGAZATOK

## 2.1 Katasztrófavédelem

2012. május 17-től a kormány Katasztrófavédelmi Koordinációs Tárcaközi Bizottságot hozott létre, amelynek elnöke a belügyminiszter, elnökhelyettese pedig az általa kijelölt tag. A KKB tagjai a miniszterek által kijelölt állami vezetők. Az állandó meghívottak köre nem változott. A koordinációs bizottság tevékenységét 1999 óta Tudományos Tanács segíti, amelynek fő feladata a katasztrófák bekövetkezésével, elhárításával, a védekezési munkálatokkal kapcsolatos tapasztalatok tudományos igényű feldolgozása

Ma már más fontos – védelmi stratégiai/taktikai - szempontokat is figyelembe kellene venni nemcsak azt hogy mire jut mire nem és ez a kérdés a gazdasági irányítás közvetlen szervezeti keretén belül aligha kerülhető meg.

Fő feladata a katasztrófák hatósági megelőzése; a bekövetkező polgári veszélyhelyzetekben a mentés végrehajtása; a védekezés megszervezése és irányítása; a káros következmények felszámolása; a helyreállítás-újjáépítés megvalósítása.

*„Széleskörű iparbiztonsági, tűzvédelmi, polgári védelmi hatósági hatásköröket gyakorol: előír, engedélyez, tilt, korlátoz, ellenőriz és szankciókat alkalmaz. Veszélyhelyzetek megelőzése érdekében más hatóságok tevékenységét összehangolja.”*[6]

Országos, megyei, és helyi hivatásos szervezetekkel, önkéntes és bevont- kötelezett polgári védelmi szervekkel, jelentős eszközparkkal, kiépült logisztikai háttérrel rendelkezik. Speciális eszközöket gyártó és javító, országos lefedettségű gazdasági társaságot működtet. Beruházás-tervezést és ingatlangazdálkodást végez. Fontos hatásköröket gyakorol a magyarországi kritikus infrastruktúrák beazonosításában, felügyeletében, valamint a polgári veszélyhelyzeti tervezésben, a védelemigazgatásban, a nemzetgazdaság mozgósításában, az állami tartalékgazdálkodásban.

Szabályozza, irányítja és teljes körűen felügyelet alatt tartja a tűzvédelmi rendszert, helyi készenléti hivatásos szervei végzik a tűzoltást, műszaki mentést, a lakosság védelmét, tájékoztatását és riasztását. Irányítja az önkormányzati, létesítményi tűzoltóságok, bevont önkéntes egyesületek részvételét a tűzoltásban, műszaki mentésben. Megyei bevetési irányítást végez. Fenntartja a területi kiképző bázisokat, a Katasztrófavédelmi Oktatási

Központot, a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézetét, a Központi Zenekart, a Múzeumot, a Kutatóintézetet. Havi újságot, szakmai folyóiratot, kiadványokat, tananyagokat jelentet meg, tudományszervezést végez, sportegyesületet működtet.

- Modern távközlési, bevetés-irányítási, informatikai, valamint az egész országot lefedő, mérő-, érzékelő, lakosságriasztó-rendszereket tart fenn.
- Együttműködik a rendvédelmi szervekkel, a Honvédséggel, az önkormányzatokkal, a biztonságot szolgáló hatóságokkal.
- Kapcsolatot tart civil- és karitatív szervezetekkel, azok szövetségeivel, oktatási, tudományos intézményekkel, a magyar médiával." Az elvárt védelmi feladat itt a legkonkrétabb, kötelező együttműködés a rendvédelmi szervekkel, a Honvédséggel, az önkormányzatokkal, a biztonságot szolgáló hatóságokkal.

Előírás szerinti feladata hogy „Modern távközlési, bevetés-irányítási, informatikai, valamint az egész országot lefedő, mérő-, érzékelő, lakosságriasztó-rendszereket tart fenn" (csak a saját keretein belül.)

## 2.2 Honvédelem

A Honvédelmi Minisztérium működteti és fejleszti a Tárca Védelmi Tervezési Rendszerét, amelyben a stratégiai képességcélok és a felhasználható erőforrások kapcsolatát eltérő időtávú tervek teremtik meg. A védelmi tervezés kiindulópontjául Magyarország külpolitikája és biztonságpolitikája alapján megfogalmazott célok szolgálnak.

A képességek fejlesztése a különböző időtávú tervekhez kapcsolódó programok, költségvetések kidolgozásával és végrehajtásával történik. A kormányzati portál így foglalja össze a honvédség feladatait**. A katasztrófák elhárításában csak a „hozzájárulás" a feladata.**

**A Magyar Honvédség legfontosabb feladatai**

Magyarország függetlenségének, területének, légterének, lakosságának és anyagi javaik külső támadással szembeni fegyveres védelme, a szövetségi (pl. NATO) és nemzetközi szerződésből eredő egyéb katonai kötelezettségek – különösen a kollektív védelmi, békefenntartó és humanitárius feladatok – teljesítése..

A honvédelem szempontjából fokozott védelmet igénylő létesítmények őrzése és védelme, közreműködés a fegyveresen vagy felfegyverkezve elkövetett erőszakos cselekmények elhárításában,hozzájárulás a katasztrófavédelmi feladatok megoldásához,[3] részvétel az állami protokolláris feladatok teljesítésében.

A stratégiában foglaltak kiterjednek a Honvédelmi Minisztériumra, a honvédelmi miniszter közvetlen alárendeltségébe tartozó szervezetekre, a Katonai Nemzetbiztonsági Szolgálatra, a honvédelmi miniszter irányítása alatt álló központi hivatalokra, valamint a Magyar Honvédség katonai szervezeteire. Az utasítás kijelöli egyebek mellett a híradó-informatikai szolgáltatások fejlődési irányát, valamint a jövőképet. **[4]**

A stratégia szerint a Magyar Honvédség híradó-informatikai rendszerei és szolgáltatásai 2014-2024 között képessé válnak egyebek mellett a katonai műveletek átfogó támogatására, a szövetségesekkel való teljes körű híradó-informatikai együttműködésre.

További kiemelt feladat az elektronikus iratkezelés és iratnyilvántartás elektronikus megvalósítására, a minősített adatok elektronikus feldolgozása híradó-informatikai feltételeinek biztosítására.

## 2.3 Rendvédelem

A rendvédelmi szervek kötelesek fenntartani közterületek rendjét, védi a kiemelt intézményeket, épületeket. „Katasztrófahelyzetben védelmezi az embereket, **segítséget és felvilágosítást ad** a rászorulóknak és együttműködik a helyi hatóságokkal, intézményekkel”[4]

Az alaphelyzet a feladat minden rendvédelmi szervnél hasonló. A rend védelemének biztosítása minden helyzetben, vészhelyzetekben a segítségnyújtás és kárelhárítás, a

---

[3] Forrás: ***Honvédelmi Minisztérium***, ***Közigazgatási Államtitkárság***, ***letöltve:2017. február 26.***
.

[4] A rendőrség feladatai katasztrófa helyzetekben forrás: http://www.kormany.hu/hu/mo/rendvedelem/rendvedelmi-szervek-es-a-buntetesvegrehajtas letöltve: 2016. október 5.

szervezetek kiemelt feladata. **[5]**

# 3. ÁTFOGÓ VÉDELMI VESZÉLYKÖZÖSSÉG

A védelem biztosításának egyik legfontosabb fogalma a veszélyközösség. Célja a tagok közös védekezése a veszélyhelyzetek elhárítására, a – közösségi, emberi, gazdasági – károk következményeinek közös felszámolása, helyreállítása.

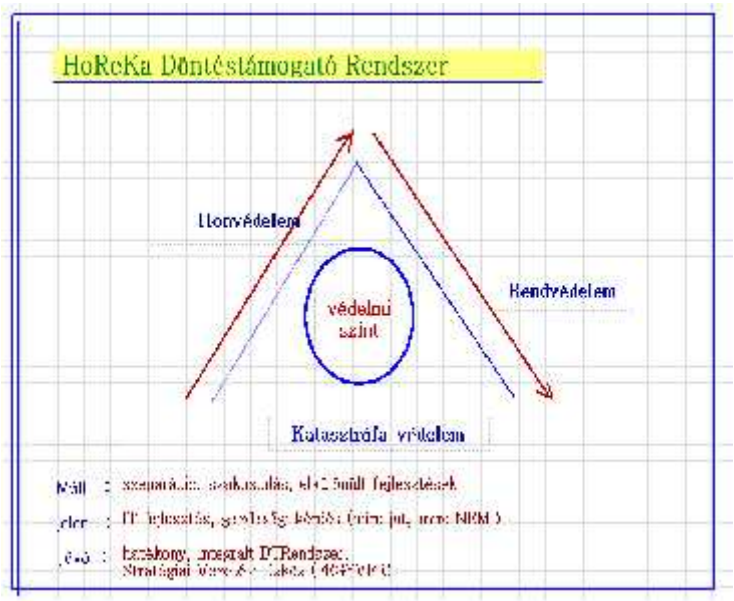
Veszélyközösségeket már a történelem során nagyon korán kezdtek szervezni. Egy régi történet szerint már az egyik folyón felhajózó ókori kínai kereskedők is alkalmazták a veszélyközösség szervezésének módszerét.

A kereskedők problémája az volt, hogy a folyam mentén rablók tanyáztak, akik rendszeresen fosztogatták a kereskedők bárkáit. Ha valamelyik bárkát elfogták, akkor annak teljes árukészlete veszendőbe ment.

A legrosszabb a dologban nem a veszteség ténye, hanem annak bizonytalan és katasztrófaszerű jellege volt.

Ezért fél legjobban ma is napjaink legtöbb embere a váratlan katasztrófa jellegű veszélyektől még akkor is ha tudja – vagy úgy gondolja – a közeljövőben nem fog ilyen helyzet nagy valószínűséggel bekövetkezni

A HoReKa Döntéstámogató Rendszer az elképzelések szerint egy közös (Honvédelmi/rendvédelmi/katasztrófavédelmi) integrált Informatikai rendszer felállításának alapját képezné.




1.ábra: „HoReKa” rendszerelképzelése (saját szerkesztés)

A jelenlegi rendszer továbbfejlesztésének általam is javasolt alapja az a védelmi veszélyközösség amiben a mindhárom védelmi ágazat – egymást erősítve, kiegészítve a saját speciális erőforrásaival - egy átfogó Integrált Védelmi Rendszert alkot.

Az újra gondolt védelmi informatikai rendszer három szinten:

– riadó,

( a telepített aktív/passzív/smart érzékelők jelzései alapján) lép működésbe)

- riasztás,

az információk hiteleségének ellenőrzése után a megfelelő riasztási protokoll aktivizálása, döntés-előkészítés indítása,

- döntés támogatási szint – egymást kiegészítve és egymásra épülve hatékony támogató eszköze lehetne a döntéshozó szerveknek.

# 4. MEGVALÓSÍTHATÓSÁGI LEHETÓSÉGEK

## 4.1 Intelligens hálózati eszközök.

A jövő kutatói szerint körülbelül 20 év múlva „egy szabványos méretű joghurtos pohárban annyi intelligencia elfér, mint az összes európai ember fejében” – kezdte előadását Ian Pearson Londonban a Global Security Summit konferencia és kiállításon, amelyet 2012. október 11–12-én rendeztek meg. Előadása eléggé bizarr volt, amelyet gondolatébresztőnek szánt, és például egyik figyelmeztetése szerint a zombik átveszi bolygónk irányítását, de említésre méltó a retina méretű iPad-ekről szóló előre jelzése is. Manapság már nem járunk messze ezektől a futuristáknak látszó eszközök mindennapi alkalmazásától.

2. ábra: smart érzékelő eszközök[5]

A dolgok internete „Internet of Things” irányzat aktuális fejleményei (fejlesztései) mentén olyan új „okos” mérési eszközök jelennek meg, amelyek folyamatosan továbbítják az adatokat az az ellenőrzött terület bármely pontjáról.

[5] www://okos megoldások smart grid és smart metering.htm,
letöltve: 2017.04.12

A Big Data infrastruktúra heterogén, hektikusan érkező, nagy mennyiségű adat tárolására, feldolgozására, az adatokra épülő analitikus algoritmusok valós idejű futtatására alkalmas.

E technológián alapulva lehetővé válik, hogy az információn alapuló beavatkozások a lehető legrövidebb időn belül pozitív eredményt hozva épüljenek be az ellenőrzött folyamatokba.

3. ábra: smart közlekedési érzékelők[6]

A digitalizáció három egymástól függetlenül zajló fejlődési folyamat találkozásában új lehetőségeket hoz a védelmi ipar számára is. A folyamatok automatizálása lehetővé teszi, hogy a folyamat minden lépése mérhetővé váljon. Az adatátviteli technikák fejlődése mind fix, mind mobil területen biztosítja a gyors és pontos adattovábbítást. Az informatika az adattárolás, a feldolgozás és adatelemzés területén lehetővé teszi, hogy a veszélyhelyzetek korai felismerése, a kárelhárítási folyamatok irányítása, - a keletkező adatok kiértékelése után - a legjobb döntések szerint történjen.

## 4.2 Workflow és csoportmunka

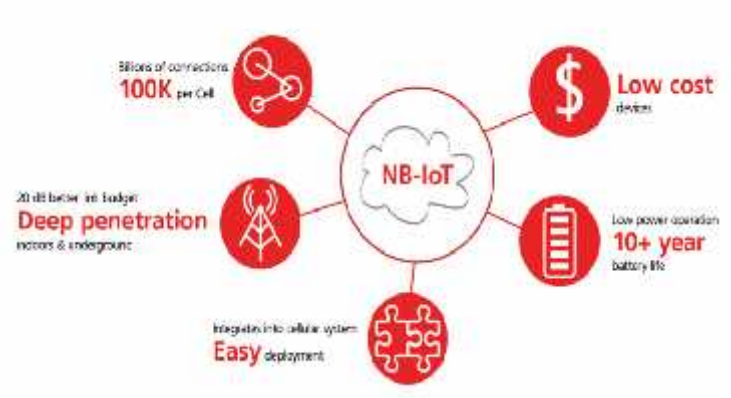
A workflow nem forradalmian új dolog, csupán a szabványos vagy szokványos szoftveralkalmazások olyan kapcsolatrendszerrel való ellátása, amely hatékonyan biztosítja az egész szervezet működtetését. A workflow rendszerek feladata a nevében is jelzett

[6] http://www.redicecreations.com/specialreports/smartdustmatrix.html

letöltve: 2017.03.22

munkafolyamat vezérlés, azaz az egyes munkafázisok elektronikus úton történő irányítása, nyilvántartása, összefogása. Az általános meghatározásokon túl a csoportmunka: - felhasználó aktív/passzív – elképzelésein túl még egy lényeges különbség fedezhető fel Az ilyen típusú rendszerekre az jellemző hogy a felhasználók jogosultságtól függően természetesen, olyan minősített közös erő- (információ-) forráshoz férnek folyamatosan hozzá, aminek alapján hatékonyan szervezhetik meg az együttműködést.[6]

Fejlesztési alapfeltétel: bármikor a lehető legrövidebb időn belül, jusson el minden elérhető (releváns) információ a döntéshozók részére Az ilyen rendszerek jellemzője, hogy a résztvevők egymással nemcsak azt az információt osztják meg, ami a következő tevékenység elvégzéséhez feltétlenül szükséges, hanem az utat is kijelöli amely szerint muszáj mindenkinek a közös információforrás struktúrát követni. A rendszer garantálja, hogy a munka elvégzéséhez szükséges és elégséges információhoz automatikusan mindenki – arra felhatalmazott vezető vagy felelős irányító - biztosan hozzájut. Az intelligens hálózatok elemei az „okos” szenzor, mérő, szolgáltató központok (frontpage) közötti kommunikáció lényege, az egyes elemek közötti nagy biztonságot garantáló információ szolgáltatással. [9].




4. ábra: frontpage előnyök[7]

A mobileszközökről nyomon követhető folyamatok már lakossági és ipari szinten is elérhetővé váltak. Az energiaszolgáltatások mérésére és optimalizálására létrehozott applikációk pedig könnyű kezelhetőséget kínálnak minden felhasználónak.

[7] forrás:http://frontpage.hu/hu/frontpage , letöltve: 2017.02.14

Az infokommunikációs eszközök használata természetesen nem csupán az energiaszektor kiváltsága. Alkalmazásuk jelentős támogatást nyújthat minden smart grid[8] megoldással bíró ágazatban, legyen az oktatás, egészségügy vagy akár turizmus.

A bennük rejlő potenciál – akárcsak a smart grid hálózatok által hordozott lehetőségek – egy olyan új területet nyitott meg globális szinten, amely jelentős mértékben alakíthatja a hétköznapi felhasználói, a vállalati – ipari vagy akár mezőgazdasági – területen is a működés folyamatait. Az eszközök fejlődésében ma már elérhető 3D technológia, nemcsak a nyomtatásban, de a virtuális 3D világban történő együttműködésben is (virtuális labor).


5. . ábra: a Horeka IT döntéspiramisa. (saját szerkesztés)

Az elgondolás lényege a következő: a védelem komplexitása csak olyan módon gyűrhető le, ha a biztonság több szinten, de az egyes rétegek közötti hatékony együttműködéssel és kommunikációval valósul meg. (Mindez nemcsak a teljes védelmi infrastruktúrára igaz)

[8] Az okos hálózatok elterjedésével az ITC technológiák is lépést kell tartaniuk

# 5. ÚJ M2M TECHNOLÓGIA NARROW BAND

A Narrow Band-IoT[9] egy új, szabványosított mobil technológia, amely a szolgáltatók jelenleg meglevő hálózatain fog futni az Internet of Things-re optimalizálva. Egyedülálló képességeinek köszönhetően nagyszámú, olcsó, és alacsony energiaigényű eszköz beltéri környezetben való használatára is kitűnően alkalmas amellett, hogy a jelenlegi mobil hálózat lefedettsége ezzel a szolgáltatással lényegesen megnő.

Így elérhetővé válhatnak a mezőgazdasági művelésben lévő mobil hálózattal részlegesen lefedett területek is, illetve a jelenleg gyengébben lefedett beltéri helységek is.[10]

Az alacsony energiaigény és nagy területi lefedettség az NB-IoT/LPWA hálózat két legfontosabb alaptulajdonsága. Ezen igények teljesítése érdekében az M2M moduloknak külső áramellátástól függetlenül is működőképesnek kell lenniük. Ezért nagyon fontos jellemzője ezeknek az okos eszközöknek a minél kedvezőbb, alacsonyabb energia felvétel. A legújabb fejlesztések már szinte önellátók a napenergia hatékony felhasználásával.

Mivel többnyire csak kis mennyiségű adatot továbbítanak, az alkalmazásnak megfelelően akár óránként vagy naponta egyszer, az NB-IoT modulok kis fogyasztásúak így megfelelő elemmel és adatkommunikációs gyakorisággal, akár 10 évig is működhetnek és nem igényelnek karbantartást. Az alacsony költséggel beszerezhető, M2M hálózatot használó NB-IoT eszközök kis-, és közepes méretű vállalkozások számára is jól hasznosíthatók. Számos területen és módon felhasználhatók:

Mindemellett nagyon jó terjedési tulajdonsággal kell rendelkezniük, hogy a jelek kellő mélységben vagy csatornák mentén is eljussanak a rendeltetési helyükre. (a GPS koordináták nem mindenhol elérhetőek) A jelek biztonságos továbbítása akár párhuzamos csatornákon is elképzelhetőek ma már.

---

[9] Új kis energia igényű (alacsony fogyasztású) Iot eszközök

[10] Az elemzők szerint 2023-ig körülbelül 3 milliárd LPWA eszköz hálózatra kapcsolódása várható világszerte. Az olcsó, NB-IoT megoldás nagy területi lefedettséget és hatékony beltéri használatot kínál a felhasználók számára.

# 6. ÖSSZEFOGLALÁS

A NetIQ, a Novell és a SUSE tapasztalat szakértői is – többek között – az integrált védelmi irányítás kérdésköreit tartják 2016-ban a legégetőbbeknek, amelyekre fókuszálva átfogó megoldásokat kínálnak a naprakész biztonság érdekében.

A legújabb infokommunikációs eszközök használata természetesen nem csupán az energiaszektor kiváltsága. Alkalmazásuk jelentős támogatást nyújthat minden smart megoldással bíró ágazatban, legyen az oktatás, egészségügy vagy akár turizmus. A bennük rejlő potenciál – a smart grid hálózatok által hordozott lehetőségek – egy olyan új területet nyitottak meg melyek jelentős mértékben alakíthatják át a hétköznapi felhasználói, vállalati, ipari vagy akár egészségügyi – területen is a korszerű működés folyamatait.

A jó pap holtig tanul… a védelmi irányítás ezen belül az irányítás informatikai szakemberei szintén. A technológia fejlődésével és a korral haladva időről időre célszerű megvizsgálni, hogy a szervezet IT infrastruktúrája megállja-e helyét a legújabb körülmények között is. [8] Az alkalmazott védelmi közös rendszerben az IT alrendszereinek aktuális állapotára történő rálátás, az esetleges riasztásokra történő azonnali reakció kiemelten fontos.

Ma már. a legkülönbözőbb rendszerfejlesztési eszközök és módszerek széleskörű lehetőségeket kínálnak a grid alapú ICT fejlesztésekhez. Alkalmazásuk a védelmi rendszereken belül több mint időszerű, megkerülhetetlen stratégiai kérdés!

Egy megbízható és jól működő döntéstámogató információ-technológiával alátámasztott „Átfogó Integrált Védelmi Rendszer” (IVR) mindenképen alapja, sőt vezérfonala lehet egy egységes aktív vezetésnek egy jól átgondolt és hatékony védelmi stratégának.

# IRODALOMJEGYZÉK


[1]forrás:file:////BMVg.de%20%20Das%20Bundesministerium%20der%20Verteidigung.htm letöltve: 2015.10.04

[2]forrás::http://2010-2014.kormany.hu/hu/honvedelmi-miniszterium/elso-allamtitkarsag/felelossegi-teruletek letöltve:2015.10.04

[3].forrás:http://nit.uni-nke.hu/uploads/media_items/magyar-biztonsagpolitika_-1989-2014.original. letöltve: 2017.05.05

[4] Megjelent a Magyar Honvédség 2014-2024 időszakra vonatkozó informatikai stratégiája.
forrás: H I V A T A L O S É R T E S Í T Ő • 2014. évi 46. szám letöltve: 2015.09.11

[5]forrás:http://www.kormany.hu/hu/mo/rendvedelem/rendvedelmi-szervek-es-a-buntetesvegrehajtas letöltve: 2015. október 5.

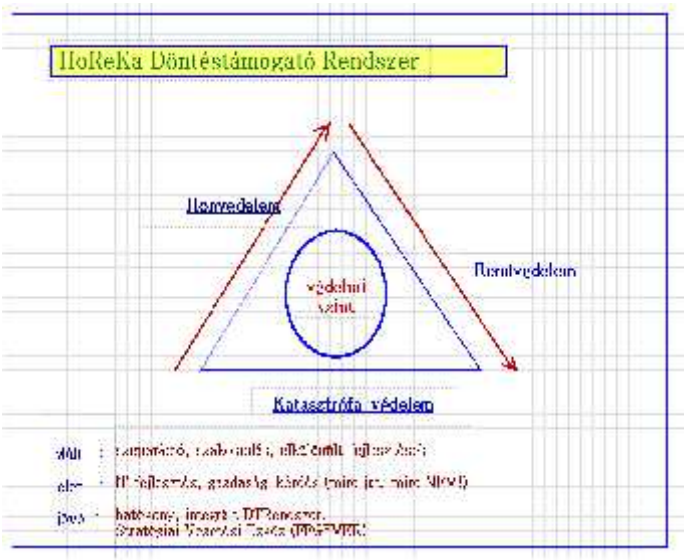
[6] Nagy Rudolf, Halász László: **Monitoring és lakossági riasztó rendszer és a kritikus infrastruktúra-védelem összefüggései,** Hadmérnök III. Évfolyam 2. szám - 2008. június -OKF RODOSZ informatikai rendszer,

7] Dr. Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (Dunaújvárosi Főiskola Közleményei (2010), XXXI. évfolyam, ISSN 1586-8567);

[8] Miért jobb az Ipv6, Magyar Telekom:, forrás: file://Miért jobb az IPv6.html, letöltve: 2017.02.14,

1. sz. melléklet:

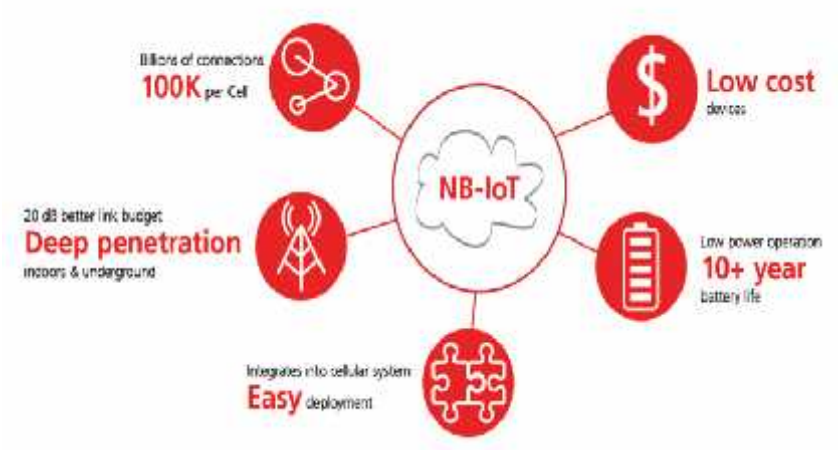
Ábrajegyzék



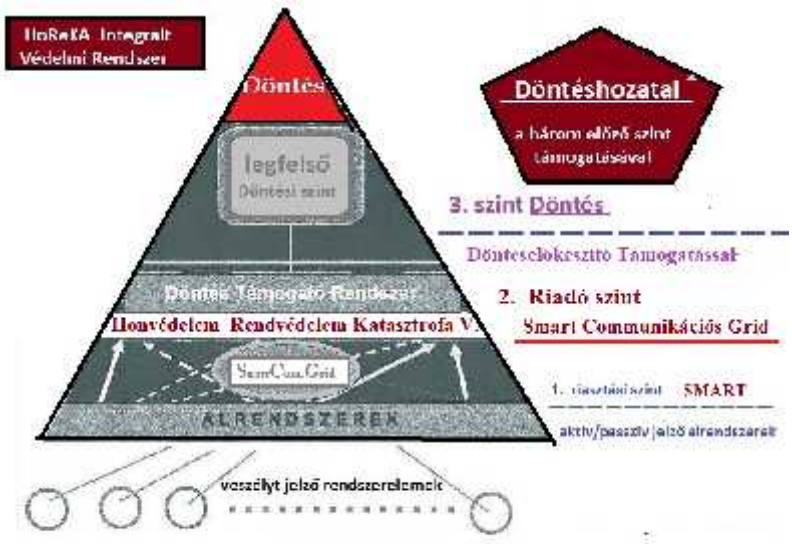

1.ábra: „HoReKa” rendszerelképzelése (saját szerkesztés)

2. ábra: „smart” okos  érzékelő eszközök

3. ábra: „smart” okos közlekedési érzékelők




4. ábra: frontpage rendszer előnyei




5. . ábra: a Horeka IT döntéspiramisa. (saját szerkesztés)

2. sz. melléklet: A biztonság átfogó értelmezése


Biztonság és veszélyhelyzetek szintjei

**Nyári László**, doktorandusz Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, e-mail: lnyari@t-online.hu

A kézirat benyújtása: 2017.05.03.
A kézirat elfogadása: 2017.06.14.