Műszaki Katonai Közlöny

XXVII. évfolyam, 2017. 3. szám

Nyári László[1]

„HOREKA" INTEGRÁLT VÉDELMI RENDSZER KAPCSOLAT-RENDSZERE

„HOREKA" INTEGRATED DEFENCE CONNECTION SYSTEM

A mai globalizált világban folyamatosan új trendek, új kihívások, új kritikus biztonsági fenyegetések jelennek meg nap mint nap. Egyértelművé vált, hogy az új veszélyek kezelésére a fejlett, demokráciák számára ma is nélkülözhetetlen egy hiteles katonai erő fenntartása. Megváltozott, kibővült azonban a védelem tartalma és feladatrendszere. A társ védelmi szervezetek együttműködése nélkül a hatékony megelőzés és kárelhárítás szinte elképzelhetetlen

Gondolkodjunk el azon, hogy az utca rendjének fenntartása, az ismeretlen bűnelkövetők személyének felderítése és elfogása, vagy akár a büntetésüket töltő elítéltek felügyelete, de az országunk biztonságát garantáló információk megszerzése, őrzése milyen összetett tevékenységet és szervezetrendszert igényel

Ez a dolgozat nem más mint, - egy átfogó védelmi veszélyközösségre alapozott integrált védelmi információs rendszer (IVR)2 kapcsolatrendszerének feltérképezése és leírása" - választott kutatási témám második része, szinte alapköve. Különösen fontos tisztázni, milyen alapelvek mentén, milyen előzmények után, milyen kutatások hozhatják meg a felállított célkitűzésekre a tudományosan megalapozott válaszokat..

Kulcsszavak: *védelmi kihívások, jogi környezet, kapcsolat-rendszer, kommunikációs grid, releváns rendszerek*

Today is no longer new notion which 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 system in the defence administration

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 this lecture which is part research, I would like to show the relations of the Overall Integrated Protection System (IPS.) 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 is a part research, I would like to show the Overall Integrated Protection System (IPS.) article relations.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, but they are important..

Keywords: *communications grid,relevant systems, protection-informatik,,digitized life*

BEVEZETÉS: HELYZET VAN!

Napjainkban mikor Európa keleti felén egyre jobban elmérgesedő szörnyű testvérháború dúl, mikor az Unió külső határait fenyegető globális migrációs áradat éri el, nem lehet eléggé hangsúlyozni az Európai Unió vezető szerveinek közös felelősségét, (felelőtlenségét) a fokozatosan romló migrációs helyzet közös, békés politikai és gazdasági megoldására.

Soha nem volt időket élünk. Magyarországot is elérte a XXI. századi újkori népvándorlási hulláma. Minden elképzelhető méreteken túl, háborús menekültek és gazdasági bevándorlók ezrei lépték át naponta nemrég hazánk déli határvonalait. Hiába volt minden figyelmeztetés és tiltás a migrációs áradat folyamatosan duzzadt tovább és tart tovább ki tudja meddig? .

[1] Nemzeti Közszolgálati Egyetem, Doktorandusz
E-mail: lnyari@t-online.hu, ORCID: 0000-0001-9098-1997

[2] Integrált Védelmi Rendszer- Fogalmi leírását bővebben, a „Társadalom és Honvédelem" 2015/2 számában leközölt cikkemben foglaltam össze.

Meggyőződésem szerint, komoly válság-helyzetek megoldási kérdéseire tudományosan megalapozott válaszokkal kell felelnünk, tudományos megoldásokat kell keresnünk és adnunk, mert a különböző veszély-helyzetekre fel kell készülnünk.

Elemezzük a legfontosabb tényeket:

- soha nem volt szükség „békeidőben” a védelmi szervezetek ilyen közös, nagyarányú mozgósítására,
- soha nem volt új fogalmak kerültek be a köztudatba veszélyhelyzetek leírására,[3] (fokozódó terrorveszély, erősödő megélhetési migrációs hullám, stb.)
- soha nem volt ilyen aktív közmegegyezés, (és persze széthúzás is) a rohamosan romló helyzet hathatós megoldására a politikai pártok és civil szervezetek körében,
- soha nem volt ilyen egységes és eltökélt a kormányzat az illegális bevándorlás megfékezésére, Magyarország és Európa „Uniós Schengeni” határainak megvédésére,[1] (műszaki határzár, jogi szigorítások, nyolc pontos javaslat az Európai Unió Tanácsa felé stb.).
- soha nem volt ilyen mértékű, egyértelmű társadalmi támogatás a megoldatlan migránshelyzet sürgető kezelésére.

Összegezve: sohasem volt ilyen időszerű a védelmi erők és szervezetek ilyen szoros összefogására, közös fellépésére, amely mindent félretéve előír a józan megfontolás és a vonatkozó törvények szelleme a nyilvánvaló vészhelyzetek elkerülésére és leküzdésére.

Célkitűzéseim:

Elsőszámú alapvető (fő) célkitűzés a leírtak értelmében:

- a tervezett „IVR” kapcsolatrendszerének feltérképezése, összegezése, rögzítése,
- az alrendszerek funkcionális leírása.

Ezen belül a felállított részcélkitűzések a következők:

- kommunikációs rács (smart grid) mint a tervezett work-flow kapcsolatok továbbfejlesztése, (kétirányú direkt információs útvonalak megtervezése, feltérképezése szervezeti egyeztetése),
- döntéstámogató alrendszer (DTR) elméleti (gyakorlati) kapcsolatai.

1. „IVR” FOGALMI ALAPJAI

Egy tudományos téma feldolgozásának alapvető kritériuma, az egységes, korrekt fogalmak, leírása tisztázása. A hivatkozott fogalmak precíz meghatározása nélkül sem a kitűzött célok és részcélok értelmezése sem az eredmények összegezése nem vezethet tudományosa alátámasztott eredményre.

1.1 Jogi környezet

Az állam egyik alapvető kötelessége e tekintetben a rend védelme. Demokratikus államberendezkedésünk egyik alapelve, a törvények és jogszabályok feltétlen betartása és betartatása. A rend és biztonság megteremtése, fenntartása, mint egy speciális állam által nyújtott szolgáltatás, azonban napjainkra már nem kizárólagos rendőri tevékenység.

[3] Veszélyhelyzet alkalmazása akkor válik szükségessé, ha társadalom életét, az állam működését, az állampolgárok élet- és vagyonbiztonságát fenyegető természeti, vagy társadalmi eredetű veszélyek lépnek fel.

Minden „védelmi”, de különösen a fegyveres rendvédelmi szervek működését, feladatát törvények, más jogszabályok határozzák meg.

Ezeken keresztül szavatolható, hogy e szervek feladataikat a törvényes cél érdekében csak jogszabályokban meghatározott módon láthatják el. A fegyveres jelleg meghatározása érdekében az 1996. évi XLIII. törvény rendelkezései adnak útmutatást.

A 2011. április 25-én elfogadott, 2012. január 1-jével hatályos Magyarország Alaptörvénye kimondja „A Kormány az élet- és vagyonbiztonságot veszélyeztető elemi csapás vagy ipari szerencsétlenség esetén, valamint ezek következményeinek az elhárítása érdekében veszélyhelyzetet hirdet ki, és sarkalatos törvényben meghatározott rendkívüli intézkedéseket vezethet be” (53. cikk (1) bekezdés).

- Magyarország Alaptörvénye,
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról,
- a Kormány 234/2011. (XI. 10.) Korm. rendelete a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény módosításáról,
- 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről,
- 290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény végrehajtásáról.

Rendvédelem

Magyarországon az állam és az állampolgárok biztonságának védelmét elsősorban a belügyminiszter irányítása alá tartozó rendvédelmi szervek végzik, a Kormány irányítása alá tartozó szervekkel együttműködve.[4]

Feladatát tekintve mind az Alaptörvény, mind pedig a rendőrségről szóló 1994. évi XXXIV. törvény tartalmazza. Ellátja a rendkívüli állapot, a megelőző védelmi helyzet, a szükségállapot, a veszélyhelyzet és a katasztrófa vagy katasztrófa veszélye esetén a hatáskörébe utalt rendvédelmi feladatokat.

Katasztrófavédelem

Magyarország lakosságának védelmét egy-egy természeti, vagy ipari katasztrófa esetén a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (továbbiakban: BM -OKF) által vezetett hivatásos katasztrófavédelmi szervek biztosítják.

2010-től egy jelentős szervezeti átalakulás vette kezdetét, melynek csúcsát az új katasztrófavédelmi törvény jelentette (2011. évi CXXVIII. Törvény a katasztrófavédelemről) a hozzá kapcsolódó egyes törvények módosításával összhangban.

Honvédelem

A Honvédség jogállása.

A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény alapján a Honvédség polgári irányítás alatt álló, függelmi rendszerben működő és centrálisan vezetett

[4] a Belügyminisztérium, irányítása alá tartozik a Rendőrség, a Nemzetbiztonsági Szakszolgálat, az Országos Katasztrófavédelmi Főigazgatóság, Nemzeti Védelmi Szolgálat és a Terror-elhárítási Központ

fegyveres állami szervezet. Békében az önkéntességen, megelőző védelmi helyzetben és rendkívüli állapotban az önkéntességen és az általános hadkötelezettségen alapuló haderő.

Rendkívüli feladatait: a 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről[5] határozza meg. [2]
A 2012. január elsejétől hatályos, a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény (Hvt.)
- a Honvédelmi Katasztrófavédelmi Rendszer vonatkozásában is együttműködési kötelezettséget határoz meg a Magyar Honvédség részére, fegyverhasználati jog nélkül. Hvt.: „35. § (2)
- A Honvédség a feladatait a honvédelemben közreműködő más szervekkel együttműködve hajtja végre.”[3]

1.2 Technológiai alapok

Információs rendszernek nevezzük az egymással kapcsolatban álló olyan rendszer-elemek összességét, amelyekben új ismereteket tartalmazó közlések (információk) átadása, feldolgozása, értékelése, történik meg az egyes elemek között.

A jövőkép: A számítási felhő *(Cloud)* egy olyan hatalmas, globális információrendszer, amelyben a szolgáltató a felhasználótól átvállalja a hardver, az operációs rendszer, és az alkalmazott felhasználói alapszoftverek fejlesztési és üzemeltetési - szerződés szerinti egyre nagyobb - igényét. A „felhő” jelentősége nemcsak a költségcsökkentésben mutatkozik meg, hanem a csoportmunka támogatásában is. A tervezett rendszer - pont az ilyen irányú fontos tulajdonságára alapozva - a számítási felhő technológiai alapjaira épülne.
A legújabb fejlesztési és kommunikációs trendek elemzése és figyelembe vétele olyan rendkívül fontos kutatási feladat, mely a tervezett rendszer hatékonyságát alapvetően meghatározza. Az elérhető publikációs és elemző értekezések a ma már a direkt információs utak menedzselése helyett az „okos” megoldások térnyerését igazolja, szinte kizárólagosan a számítási felhő *(Cloud)* technológiára alapozva.

1.3 Infó-kommunikációs fejlődés

Az információtechnológiai fejlődés jóvoltából egyre nagyobb számú és több típusú eszköz és információs csatorna válik alkalmassá az okos hálózatokban történő világméretű (globális) kommunikációra.

Az intelligens hálózatok elemei – szenzor, mérő, szolgáltató központ, (frontpage) – közötti kommunikáció lényege, az egyes elemek közötti biztonságos kétirányú információszolgáltatás megteremtése a valós idejű adatszolgáltatás biztosítása. A mobileszközökről nyomon követhető folyamatok már lakossági és ipari szinten is elérhetővé váltak. Az energiaszolgáltatások mérésére és optimalizálására létrehozott applikációk pedig könnyű kezelhetőséget kínálnak minden felhasználónak.

Az infokommunikációs eszközök használata természetesen nem csupán az energiaszektor kiváltsága. Alkalmazásuk jelentős támogatást nyújthat minden smart grid[6] 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

[5] az Alaptörvény *T)* cikk (1) bekezdése, XXXI. cikk (3) bekezdése, 45. cikk (5) bekezdése, valamint 54. cikk (4) bekezdése alapján
[6] Okos hálózatok

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).

A 3D-s egerek, mobiltelefonok, laptopok, szemüvegek, a mozgás- és érintésérzékelés új alapokra helyezése világosan mutatja az utat az okos hálózatok egyre magasabb szintű kiépítése felé. A cél az „élhetőbb bolygónk”, bízzunk benne, hogy a temérdek és folyamatosan bővülő high-tech megoldások kívánta árammennyiség előteremtéséhez már megújuló energiaforrásokat veszünk majd igénybe. Természetesen az információ biztonsága továbbra is alapvető feltétel. Ennek érdekében alternatív és tartalék útvonalak, kommunikációs eszközök és megoldások is fontos feltételei kell hogy legyenek a tervezett rendszernek.[15]

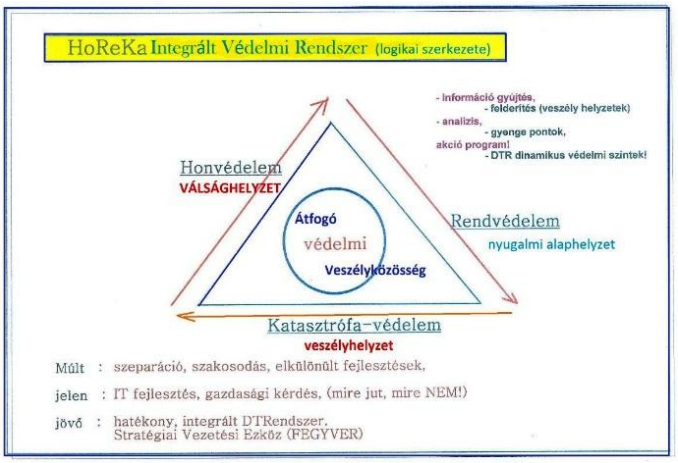
2. AZ INFORMÁCIÓS RENDSZER TERVEZÉSI FÁZISAI, ARCHITEKTÚRÁJA

2.1 jelen és jövő, „stratégiai vezetési eszköz”

A tervezés első fázisa a múlt, a jelen és az elérendő (jövő) funkcionális állapotainak rögzítése, pontosított leírása:

- **alapállapot**, normál esetben rendvédelmi feladat, a nyugalom és az alapvető biztonság fenntartása,
- **veszélyhelyzet**, katasztrófavédelmi eljárások, intézkedések, foganatosítása a különböző veszélyhelyzetek kezelésére,
- **különleges „veszély helyzet”** a különleges jogrend keretei között elrendelhető, eljárások és intézkedések - mindhárom védelmi szervezet egy veszélyközösségbe tömörülve - közös erőfeszítéssel történő elrendelése a vészhelyzet hatékony elhárítása.

A logikai összefüggéseket az alábbi ábrán keresztül értelmezhetjük:



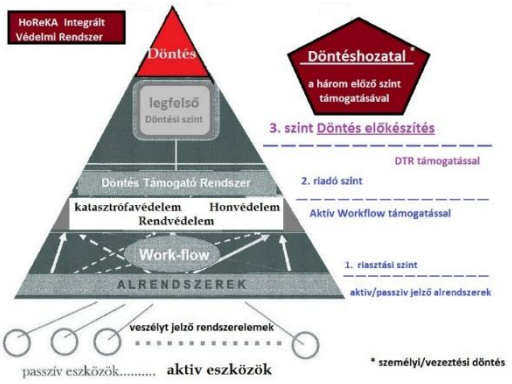
1.ábra: IVR logikai összefüggései[7]

[7] 1. ábra:a szerző saját kutatásának eredményei. (1, 2, 5. sz. ábrák)

- múlt: szeparáció, széthúzó szakosodás, elkülönült fejlesztések,
- jelen: az IT fejlesztés gazdasági kérdés, (mire jut, mire NEM),
- jövő: stratégiai vezetési eszköz, (FEGYVER), hatékony Integrált védelmi információs rendszer alkalmazása.

2.2 A megcélzott jövő

A cél egy olyan „információs döntési piramis” logikai felállítása, amely biztosítani képes a megcélzott átfogó veszélyközösségre épülő Integrált Védelmi Rendszert.
Rendszertechnikailag értékes, (iránymutató), lehet az IEW (elektronikus hadviselés), és az IVR alrendszereinek összehasonlítása. A kiinduló helyzet analízisénél azt feltétlen figyelembe kell venni.
A pontosított döntési piramis logikai felépítését az alábbi ábra szemlélteti.



2. ábra: döntési piramis szintjei [8]

2.3 Információs szintek (a döntés előkészítés lépcsői)

A piramist három alapvető szinten kell és lehet átgondolni, a szükséges logikai és irányítási lépcsőket megtervezni, a minél hatékonyabb védelmi eljárások indítása érdekében.

1. szint: veszélyjelző információs alrendszerek,
2. szint: irányított forró „riasztási” workflow alrendszer,
3. szint: döntéstámogató vezetői alrendszer.

A felmérések és a kutatásaim szerint is az első szint szervezetei, aktív/passzív eszközei a védelem mindhárom területén már megbízhatóan működnek sőt folyamatosan fejlődnek. A rendszertervezés fő iránya ezért a második szint elemzésével, kapcsolati rendszerének feltérképezésével indul.

A második szint: irányított forró „riasztási” workflow[9] alrendszer:

A workflow rendszer minden résztvevője jogosultságának megfelelően szinte valós időben, gyors és megbízható információkat kap a veszélyforrások jelzéseiről az elvégzendő feladatokról és határidőkről.

[8] 2. ábra: a forrásmegjelölés nélküli ábrák, a szerző saját kutatásának eredményei.
[9] Az ICT rohamos fejlődése meghaladta a workflow rendszert

Minden fontos információ az előírt legrövidebb úton jut el a felelős szervezeti egységekhez (vezetőihez). A rendszer - a folyamat dedikált résztvevőhöz - azonnal továbbítja az összes szükséges adatot, és információt a döntés előkészítés minél hatékonyabb támogatása érdekében.

A tevékenységek végrehajtásában nem csak a workflow rendszer saját eszközei (pl. az információs ablakok, útirányítási felületek) adnak támogatást hanem lehetőségük nyílik további (egyedi) alkalmazások indítására, illetve a szükséges paraméterek átadására is.

Harmadik szint: döntéstámogató vezetői alrendszer:

Döntés-előkészítői „vezetői” információs rendszereket elsősorban azért alkalmazunk, hogy minden releváns (feldolgozott, kiértékelt adatot) információt elérhetővé tegyük a felelős döntéshozóknak, akkor és amikor, éspedig olyan formában, ahogy szükségük lehet rá.

Nem az információ hiányával van gond. Hiába van ugyanis a védelmi szervezetnek különböző irányítási rendszere, az azokban tárolt információkhoz a döntés-előkészítők, döntéshozók, vagy nem férnek hozzá, vagy nincs megfelelő jogosultságuk, vagy nincs meg hozzá a megfelelő informatikai tudásuk.[13]

3. A TERVEZETT IVR KAPCSOLATRENDSZERE

3.1 A hon és ország-védelem jelenlegi rendszere

Egy jól (korrekt módon) feltérképezett kapcsolatrendszer ismerete nélkül nem tervezhető semmilyen hatékony információs rendszer. Egy pontatlan kapcsolat-térkép nem teremhet biztos alapot sem a rendszer megbízható működésre – a szükséges információ gyors, irányított áramlásra – sem a továbbfejlesztési lehetőségekre!

3. ábra: az ország védelem rendszere[10]

[10] 3. ábra: Hon és Ország-védelem rendszere, forrás: http://www.kormany.hu/download/9/68/20000/Magyarorszag_Vedelmi_Igazgatasa_a_Kozigazgatas_Uj_Kornyezeteben_2014_n.pdf, letöltve: 2016.04.12

A honvédelemre való felkészülésben és a honvédelmi feladatok végrehajtásában a Honvédelmi törvényben (Hvt.-ben) meghatározott keretek között, a törvény alapján létrehozott jogalanyok vesznek részt. Magyarország védelmi igazgatása a közigazgatás új környezetében mentén Magyarország minden tagja és szervezete képességei szerint köteles részt vállalni.

„A honvédelem komplex rendszerként értelmezhető. Ennek a rendszernek civil elemeit a védelmi igazgatás, a polgári védelem, a katasztrófavédelem, a katonai elemeit a Magyar Honvédség és a rendvédelmi szervek alkotják.”[11]

Meggyőződésem hogy - nemcsak különleges helyzetekben[12] - „békeidőben is” nemcsak a határainkat elérő migrációs áradat kapcsán kellene egy átfogó veszélyközösséget alkotni a három alapvető védelmi ágazat (honvédelem, rendvédelem, katasztrófa-védelem) vezető szerveinek és beosztott állományának.

Alapesetben: a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság irányítja a védekezést. Nemzeti Veszélyhelyzet kezelési Központot (KKB NVK) működtet, mely a védekezés idején 0 -24-ben koordinálja a közreműködők tevékenységét.

4. ábra: az új védelmi ernyő is a veszélyközösségre épül. [13]

Az alapkérdés a következő: ha már az alapelvekben (átfogó veszélyközösség) egyetértés van, hogyan legyen tovább? Melyik irányba, - minden szinten vagy szintenként integrálva- fejlesszük az információs rendszert? Két lehetőség (módszer) közül kell választanunk:

- első változat: a már (önállóan) működő IT alrendszereket integrálva fejlesszünk a védelmi rendszert tovább vagy,
- második változat: a már meglévő/működő szervezeti/személyi kapcsolatok alapján fejlesszünk ki egy teljesen új IT rendszert?[14]

A végeredmény a fontos! Mindkét módszer kötelező talán legfontosabb alapja, a pontos kapcsolatrendszer feltérképezése, még a fejlesztések előtt. Az előzőekben leírtak szerint[15] szinte megkerülhetetlen a második „riasztási” szint újragondolása. jelenlegi ismereteim és a

[11] forrás: Magyarorszag_Vedelmi_Igazgatasa_a_Kozigazgatas_Uj_Kornyezeteben_2014_n.pdf
[12] A rendkívüli állapot a *különleges jogrend szerinti időszakok* közül az Alaptörvény által előírt állami rend létét leginkább veszélyeztető szituációk kezelésére szolgál.
[13] 4. ábra: Az új védelmi ernyő, forrás: https://prezi.com/ure_jrwckgpp/a-katasztrofavedelem-feladat-es-szervezetrendszere-ppt/ letöltve: 2016-05-02
[14] régi bölcsesség: sokszor többe kerül egy régit megjavítani, mint egy újat építeni
[15] 1.2 fejezet, technológiai alapok

kutatások alapján egy „okos védelmi kommunikációs szint” (SDCG) felállítása és alkalmazása lenn az optimális megoldás.[12]

Újabban jelentősen terjednek az ún. Grid rendszerek,[16] ahol nagyszámú, vagy nagyteljesítményű erőforrásokat kapcsolnak össze komplex feladatok megoldása érdekében. A Web sikere mindannyiunk által jól ismert. Nemcsak személyes életünket teszi jelentősen kényelmesebbé, de az egész társadalom felépítésére és az üzleti életre is óriási hatással van. Sokak szerint a Webhez hasonló forradalmi változás előtt állunk, amit az információs rendszerek egy új ágának a kifejlődése, a Grid rendszerek megjelenése fog elindítani. A Web sikerét az okozta, hogy forradalmasította és társadalmasította az információ elérését az Internet segítségével, azaz bárki bármilyen információt bárki számára könnyen és gyorsan elérhetővé képes tenni és ez az információáramlás soha nem látott mértékű felgyorsításához vezetett.

A Webhez képest a továbblépést az jelenti, hogy a Grid rendszerekben nemcsak az információt tehetjük nyilvánossá, hanem bármilyen más erőforrásunkat, szolgáltatásunkat (pl. pillanatnyilag szabad processzor és diszk kapacitásunkat, speciális programjainkat, számítógéphez csatlakoztatott műszereinket, stb.) és azt mindenki elérheti (bizonyos konvenciók és megállapodások alapján) az Interneten keresztül.[17]
Cserében mi is elérhetjük mások erőforrásait és szolgáltatásait, amikor arra éppen szükségünk van. Ily módon a rendelkezésre álló erőforrások kihasználtsága és a szolgáltatások elérhetősége jelentősen javul, ami az információfeldolgozás hatékonyságának és gyorsaságának ugrásszerű növekedéséhez fog vezetni a tudományos kutatásokban, az üzleti életben és össztársadalmi szinten is.[14]

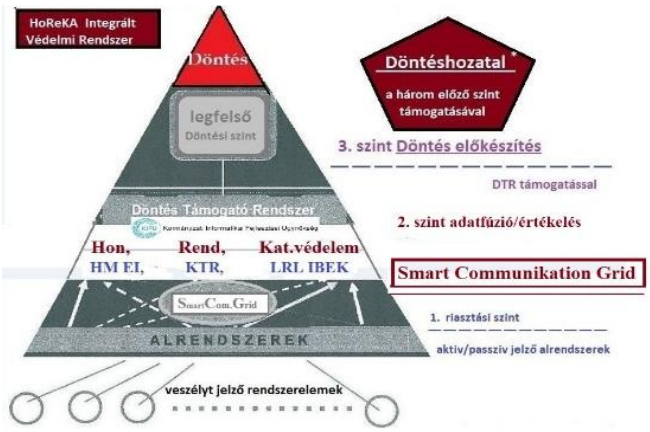
A továbbiakban részletes fel kell dolgozni:

- mitől lesz okos egy információs rendszer,
- hogy kell felépülnie az új riasztási „grid” szintnek,
- rendelkezésre állnak-e a megvalósítás feltételei?

Az első szint változatlan hagyása mellett a már működő alrendszerek alapján fejlesztett IVR kapcsolati térképet az alábbiak szerint rajzolhatjuk fel.

[16] Tároló alrendszer, (EU DataGrid), demo grid (SZTAKI), monitorozó alrendszer(PROVE

[17] A grid alkalmazások esetén a nagy adatmennyiségek mozgatása lényeges szempont de nem a legfontosabb.. Itt olyan elosztott cache technikák kidolgozása a cél, melyek jelentős mértékben képesek (hitelesség megőrzése mellett) csökkenteni a mozgatandó adatok mennyiségét



5. ábra: a módosított fejlesztési változat kapcsolat térképe

3.2 Releváns IT. alrendszerek

Honvédelem:

Elektronikai és Informatikai Igazgatóság célja, hogy a Honvédelmi Minisztérium kiemelkedő informatikai szolgáltatója legyen

6. ábra HM EI, Informatikai Alkalmazási Divízió[18]

A ZRT. munkatársai nagy gyakorlattal rendelkeznek speciális, katonai és minősített informatikai megoldások tervezésében és kivitelezésében. Teljes körű szolgáltatást biztosít a - tervezésétől a fejlesztésig - a rendszerek komplett megvalósításáig,

Rendvédelem:

A Rendvédelem feladatainak hatékony ellátását, saját (helyi) elektronikus információs rendszerek támogatják. Ugyanakkor a védelem megteremtése kormányzati felelősség is és ez a rendőrség oldaláról csak koordináltan történhet. Furcsa ellentmondás, a koordinációt pedig - a hatékonyság maximalizálása érdekében - centralizálni kell,

[18] 6. ábra HM EI, Informatikai Alkalmazási Divízió forrás: http://www.kormany.hu/download/9/68/20000/Magyarorszag_Vedelmi_Igazgatasa_a_Kozigazgatas_Uj_Kornyezeteben_2014_n.pdf, letöltve: 2016-05-04

Katasztrófa védelem:

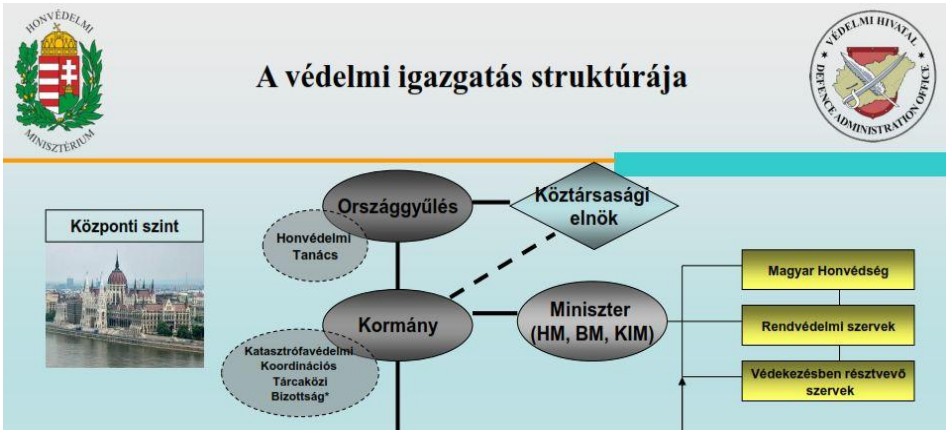
A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság hálózatbiztonsági feladata körében, a honvédelmi szempontból létfontosságú rendszerek és létesítmények kivételével, nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátása érdekében eseménykezelő központot működtet[19].

7. ábra: LRI, BEK központ[20]

Létfontosságú rendszerek és létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRL IBEK) biztos alapokat szolgáltathat a tervezett kommunikációs grid - katasztrófavédelmi hálózat rendszerpontjainak - belépő információi számára.

4. DÖNTÉSTÁMOGATÓ ALRENDSZER ÉS KAPCSOLATAI

A feladat – az előzőekben megfogalmazás szerint - Döntés-előkészítői „vezetői” kapjanak meg minden releváns (feldolgozott, kiértékelt adatot) információt akkor és amikor, éspedig olyan formában, ahogy szükségük lehet rá. A kapcsolati rendszert ennek érdekében kell feltérképezni, működtetni.



8. ábra: Védelmi igazgatás struktúrája[21]:

[19] Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő központ)
[20] 6. ábra: LRI, BEK központ, forrás: http://www.kormany.hu/download/9/68/20000/Magyarorszag_Vedelmi_Igazgatasa_a_Kozigazgatas_Uj_Kornyezeteben_2014_n.pdf, letöltve: 2016-05-04
[21] 7. sz. ábra: belbiztonsági szervezetek és feladatai, forrás: http://www.slideserve.com/rowdy/a-rendv-delmi-szervek-helye-a-kiberv-delemben, letöltve: 2016-04-09 8/11 oldal

Világosan kell látni: a sikeres együttműködés feltétele - egy minden politikai erővel egyeztetett, és elfogadott – konszenzus a cél elérése érdekében.

4.1 HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség:

„A Honvédelmi Minisztérium rendeltetése kettős.[8] Egyrészt, mint a honvédelem közigazgatási funkcióját ellátó szerv, gondoskodik az ország honvédelemi, védelempolitikai illetve védelemgazdasági céljainak formálásáról.”

Feladatai:

A honvédelmi tárca informatikai stratégiájának, híradó és informatikai doktrínájának kidolgozása, a megvalósítással kapcsolatos döntések előkészítése, a stratégiához és doktrínához kapcsolódó oktatási, felkészítési követelmények kidolgozása, a szükséges szabályozók kiadása.[15]

HVK csapatkar jelzés[22]

4.2 Rendvédelem: NBSZ

A Nemzetbiztonsági Szakszolgálat feladata Magyarország nemzetbiztonsági védelmének, a bűncselekmények megelőzésének és feltárásának, valamint az igazságszolgáltatás hatékonyságának elősegítése. Az Elemző és Értékelő Osztály a Nemzeti Védelmi Szolgálat Főigazgatójának közvetlen irányítása és felügyelete alatt álló önálló szervezeti egység, melynek fő feladata a védelmi tevékenység, a védelmi tisztek munkájának a támogatása. Az osztály a rendelkezésére bocsátott információk felhasználásával, feldolgozásával értékelő-elemző jelentéseket készít.

Az NBSZ folyamatos fejlődésre törekszik a tudományos, valamint az önálló kutatás-fejlesztési eredmények adaptálásával, munkatársai szakismereteinek bővítésével, teljesítőképességének, szolgáltatásai és szakértői tevékenysége színvonalának javításával.

[22] Honvéd Vezérkar Tudományos kutatóhely, támogatója a kutatásnak

9. ábra: belbiztonsági szervezetek és feladatai[23]

4.3 Katasztrófa védelem: KKB, OKF

Katasztrófavédelmi Koordinációs Tárcaközi Bizottság (KKB) elnevezésű szervezet a belügyminiszter vezetésével, az ágazati miniszterek által kijelölt vezetőkkel, valamint a központi államigazgatási szervek (pl. Rendőrség, Nemzeti Adó- és Vámhivatal, Országos Meteorológiai Szolgálat stb.) vezetőivel látja el feladatát. [9]

A **BM Országos Katasztrófavédelmi Főigazgatóság** irányítása alatt létezik már „döntéstámogató Rendszer”[24] ennek országos szintű integrálása fontos lenne. de még messze nem megoldott. Alapvető rendeltetése a magyar lakosság élet- és vagyonbiztonságának, a nemzetgazdaság és a kritikus infrastruktúra elemek biztonságos működésének védelme.

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

- **Kapcsolatot tart** civil- és karitatív szervezetekkel, azok szövetségeivel, oktatási, tudományos intézményekkel, a magyar médiával.

- Együttműködik a rendvédelmi szervekkel, a Honvédséggel, az önkormányzatokkal, a biztonságot szolgáló hatóságokkal. [7]

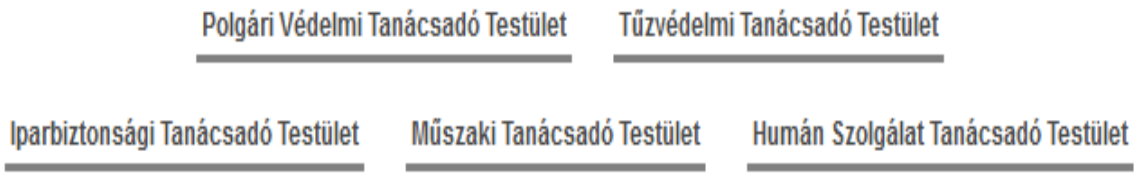
OKF működési támogatói:

Katasztrófavédelmi **TUDOMÁNYOS TANÁCS**

A katasztrófavédelem szerepe az utóbbi években megnőtt, ez jól tükröződik mindennapjainkon is – a szervezet tevékenységével nap mint nap találkozhatnak az állampolgárok. Ahhoz, hogy a katasztrófavédelem tagjai megalapozott tudással és rutinnal tudják végezni felelősségteljes munkájukat, elengedhetetlen a jelen tudományos eredményeinek összegzése.

[23] Forrás: É/3468/2012. számú főigazgatói utasítással kiadott BM OKF Szervezeti és Működési Szabályzat.
[24] területi védelmi igazgatási szervek döntéstámogató rendszere: Fejlesztő: Szentes László (Fejér MVB) és az InFenToth Bt.

Polgári Védelmi Tanácsadó Testület:



forrás:http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_mtt_index

Az OKF főigazgatója arra kérte a megalakuló testület 17 tagját, hogy ki-ki a maga szakterületén mérje fel a polgári védelmi szakma helyzetét a megelőzés, a beavatkozás és a helyreállítás tekintetében is. A testületet azzal a feladattal bízta meg, „tekintse át a más hatóságokkal, társszervekkel, kormányzati szervekkel való együttműködés terén szükséges elképzeléseit”

5. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Meggyőződésem hogy - nemcsak különleges helyzetekben - „békeidőben is” nemcsak a határainkat elérő migrációs áradat kapcsán kellene egy átfogó veszélyközösséget alkotni a három alapvető védelmi ágazat (honvédelem, rendvédelem, katasztrófa-védelem) vezető szerveinek és beosztott állományának.

A védelmi szervezetek kapcsolati rendszerének korrekt feltérképezése során egy egész sor körülményt is számon kell tartanunk. Feltétlenül figyelembe kell vennünk, hogy az egyes döntéshozó testületek, szervezetek, ill. azok vezetőinek adatai – éppen biztonsági okokból nem mindig publikusak. Sőt néhány „dedikált”[25] kapcsolat értelemszerűen titkos is lehet.

Azt azonban biztosan állíthatom: napjainkra egyértelművé vált, hogy a fejlett, demokráciák számára még ma is nélkülözhetetlen egy hiteles katonai erő, az új veszélyek hatékony kezelésére

„Megelőző védelmi helyzetben vagy rendkívüli állapot időszakában sor kerülhet akár a hadkötelezettség bevezetésére is Az esetleges biztonsági események monitorozása már számos szervezetnél alapvető tevékenység”

Nem volt rá példa, nem volt rá szükség a magyar védelmi rendszerek ilyen szoros összefogására mint napjainkban!

Napjainkban szinte magától értetődő, hogy az állam garantálja minden polgárának, és a területén legálisan tartózkodó más személyeknek nemzetközi szerződésekben és hazai Alaptörvényünkben megfogalmazott jogainak érvényesülését. [4]

Ma már egyértelmű (migráns, menekült áradat, fokozott terrorhelyzet stb.) a társ védelmi szervezetek együttműködése nélkül a veszélyhelyzetek szakszerű megelőzése, hatékony kárelhárítása szinte elképzelhetetlen.

Nem kétséges, hogy egy új szellemben (átfogó veszélyközösségben) irányított, - a tervezett Integrált Védelmi Rendszer, megfelelő döntés-előkészítő támogatásával - ***egységes védelmi vezetés minden tekintetben hatékonyabb, ütőképesebb lehet*** mint a jelenleg működő keretek

[25] különleges hozzáférési jogokkal felruházott vezetési kapcsolatok

között. A társ védelmi szervezetek szoros együttműködése nélkül a szakszerű, hatékony megelőzés és hatékony kárelhárítás szinte elképzelhetetlen.

Utóirat:

10. ábra: egy „átfogó veszélyközösségben” van az erő![26]

FELHASZNÁLT IRODALOM:

1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről,

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról,

É/3468/2012. számú főigazgatói utasítással kiadott BM OKF Szervezeti és Működési Szabályzat. BM OKF: Nemzeti Katasztrófa Kockázat Értékelés, összeállította: Dr. Gyenes Zsuzsanna, 2011. A BM OKF főigazgatójának beszédei különböző fórumokon;

KKB határozatok: 3/2015. (XII. 30.) http://www.katasztrofavedelem.hu/index2.php?pageid=vedelemig_kkb_index letöltve: 2016. február 12.

Megújult rendszer, megújult környezetben http:// http://www.katasztrofavedelem.hu, letöltve: 2016. március 12.

Hivatkozások:

[1] Magyarország és Európa „Uniós Schengeni” határai http://magyarhirlap.hu/cikk/33841

[2] A honvédelmi ágazat katasztrófák elleni védekezésének irányításáról és feladatairól szóló 23/2005. (VI. 16.) HM rendelet 23/2005. (VI. 16.) HM rendelet 2. § (2);

[3] „A Honvédelmi Katasztrófavédelmi Rendszer napjainkban” című, MH szintű szakmai konferencián elhangzott HM TKF előadásból, 2012. 09. 19.;

[26] 9. ábra: összefogásban van az erő! forrás: https://prezi.com/ure_jrwckgpp/a-katasztrofavedelem-feladat- es-szervezetrendszere-ppt/ letöltve: 2016-06-19

[4]Magyarország Alaptörvénye;

[5] Tokovicz József, Kádár Pál, Süle Attila, Borsos József, Juhász László: A Magyar Honvédség képességei és a katasztrófa-elhárítás kihívásai, 2000–2011. Zrínyi Kiadó, 2011. 95 -96. oldal.

[6] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

[7] 2011. évi CXXVIII. törvény
a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[8] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról;

[9] 1150/2012. (V. 15.) Korm. határozat a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság létrehozásáról, valamint szervezeti és működési rendjének meghatározásáról a témakörben megjelent szakfolyóiratok, értekezések, alapján

[10] **A** BM Országos Katasztrófavédelmi Főigazgatóság alapvető rendeltetése
http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_bemutatkozas

[12] Péter Egri, József Váncza: Efficient mechanizm for Aggregate Demand Prediction in Smart Grid. Electronic Edition BibteX, Page: 250 263

[13] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi Szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal, HU ISSN 2060-0437);

[14] Négyesi Imre: COTS rendszerek alkalmazási lehetőségeinek vizsgálata (Hadtudományi szemle on-line, IV. évfolyam (2011) 4. szám, 111-116. oldal, HU ISSN 2060-0437)

[15] Négyesi Imre: DIE ÜBERPRÜFUNG DER VORAUSSETZUNGEN VON COTS SYSTEMEN (COTS RENDSZEREK KÖVETELMÉNYEINEK VIZSGÁLATA) (Hadmérnök on-line, VII. évfolyam (2012) 2. szám, 371-376. oldal, ISSN 1788-1919).