HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Zsigovits László
zsigovits.laszlo@zmne.hu

AZ ÚJ NEMZETI KÖZSZOLGÁLATI EGYETEM K+F+I ÉS PÁLYÁZATI TEVÉKENYSÉGÉNEK LEHETSÉGES IRÁNYAI

„A tudás az, amely a használat során soha nem kopik”

Absztrakt

E tanulmány röviden összefoglalja az új Nemzeti Közszolgálati Egyetem K+F+I lehetőségeit. Az új egyetem oktatási portfoliója átfogja a honvédelemmel, rendvédelemmel és a közigazgatással kapcsolatos tudományterületeket. Ez lehetővé teszi a komplex biztonság egységes rendszerben történő tudományos vizsgálatát. A széleskörű, nemzetközi együttműködésben végzendő tudományos kutatómunka feltételei az új egyetem számára adottak lesznek. A cikk bemutatja ennek szervezeti, technikai lehetőségeit (kutatói hálózat, HBONE+, szuperszámítógépek, gridek, cloud).

This study summarizes the research, development and innovation opportunities of the newly established University of Public Services. The new university's educational portfolio includes areas of sciences related to the national defence, order protection and the public administration. This makes possible to analyze the complex security in a unified system. The conditions of the wide-ranging, international scientific research work will be provided at the new university. The article presents the organizational, technical opportunities of this (researcher network, HBONE+, supercomputers, grids, cloud).

Kulcsszavak: *Nemzeti Közszolgálati Egyetem, Biztonság fogalma, Információgyűjtés fajtái (módjai), Információszerzés fajtái (módjai), Globális, elektronikai információgyűjtés, Kritikus infrastruktúra, Cloud – felhő, Szuperszámítógép, Grid, Kutatói hálózat, Videotorium*

AZ ÚJ NEMZETI KÖZSZOLGÁLATI EGYETEM ÉS A BIZTONSÁG KAPCSOLATA

Az új Nemzeti Közszolgálati Egyetem megalakulásával létrejön egy olyan kedvező állapot, amelyben a széles értelemben vett biztonság megteremtésének tudományos platformja egy intézményhez kötődik. Ez az új egyetem a honvédségi, rendvédelmi és közigazgatási vezetők képzését végzi és ez a három széles oktatási terület szinte teljes egészében felöleli a biztonság megteremtésének elméletével kapcsolatos témaköröket. Ha, ezen széles értelemben vett biztonság megteremtésének konkrét gyakorlati teendőivel minden tekintetben nem is az említett három nagy társadalmi kategória foglalkozik, de a biztonság elméleti, kutatási, tudományos aspektusai minden vonatkozásban a kompetenciájukat képezik.

Először is körvonalazzuk, hogy mit értünk a széles értelemben vett biztonság fogalmán.

A biztonság fogalma [1]

A biztonság olyan állapot, amelyben a fenyegetések, veszélyhelyzetek feltárásra kerültek és ki lettek dolgozva azok a megelőző, védelmi, elhárító, felszámoló intézkedések, amelyek kizárják, akadályozzák, enyhítik, helyreállítják a bekövetkezett káros hatások következményeit, valamint ezek végrehajtásához rendelkezésre állnak a megfelelő tervek, modellek, felkészült erők, eszközök.

Kiindulásként azt kell megállapítani, hogy a biztonság az egy állapot, egy természetesen kialakuló állapot, amely a veszélytényezők feltárásával befolyásolásra kerül.

Miért van egy természetes állapota a biztonságnak?

A biztonság alanyai lehetnek személyek, természeti képződmények, objektumok, létrehozott alkotások, politikai koncepciók, adatok. Ezek közül legfontosabb a személy biztonsága. A természeti képződmények alatt mindazon környezeti- és természetes értékeinket értjük, amelyek földrajzilag kialakultak, mint például erdők, tavak, folyók, növények, állatvilág. Az objektumok közé tartoznak mindazon létesítmények, amelyeket az ember hozott létre az életkörülményeinek fenntartására. Ezek lehetnek az épületek, gyárak, hidak, utak és még számtalan más műtárgy. A létrehozott alkotások az ember szellemi termékei, illetve szellemi termékének tárgyiasult megjelenési formái, médiumok, kutatási eredmények, gépek, műszerek, könyvek, szoftverek, egyéb tárgyak és művészeti alkotások. Az adatok a fentiekre vonatkozó jellemzők dokumentációit tartalmazzák.

A biztonság eme alanyai valamilyen környezetben élnek, funkcionálnak, léteznek, tárolódnak és ez az a környezet, amely a természetes állapotot kialakítja. Valamelyik alany a tengerparton, másik folyók mellett, harmadik hegyes területen vagy nagyvárosban él, települt, található. Ez a helyhez való kötődés határozza meg alapvetően a biztonsági állapotot, mivel minden helynek mások az objektíve kialakult veszélytényezői.

A tengerparton veszélyforrás lehet a cápatámadás vagy a szökőár. A hegyes területen a lavina vagy szakadékba zuhanás. A nagyvárosban a bűnözők. Számítóközpontban a hackerek. Folyóparton az árvíz. Törésvonalak mentén a földrengés. Gazdaságilag stabil térségekben az illegális migráció és a drogeladás. Politikailag feszült térségekben a háború, terrorizmus.

Ezért egy természetes állapot a biztonság, hiszen a veszélyforrások a biztonság alanyaitól függetlenek, objektíve léteznek.

De ez az állapot befolyásolható a veszélytényezők feltárásával. Ha a veszélytényezők feltárásra kerülnek, akkor az állapot minősége javítható, azaz a biztonság növekedni fog. A jól beazonosított veszélytényezők alapján lehet a fogalomban lefektetett alapvetések (megelőző, védelmi, elhárító, felszámoló intézkedések / tervek, modellek, felkészült erők, eszközök) megvalósítása. Ezen alapvetések arra hivatottak, hogy egyrészt kizárják a veszélytényezők hatásait, de legalábbis mérsékeljék azokat, másrészt pedig a bekövetkezett káros hatások felszámolása szervezetten, hatékonyan kerüljön levezetésre.

Csak két egyszerű példa a biztonság állapotának növelésére. Ha egy útvonal jelentősen kanyarog, ez természetes állapot a terep adta lehetőségek miatt. A biztonság ezen útvonalon, a veszélytényezők helyes feltárásával, sebesség korlátozással és előzési tilalommal fokozható. Másik példa, ha a turista útvonal szakadék mellett halad el, akkor korlátot kell építeni az útvonal mentén a biztonság fokozására.

Tudományos kutatók a biztonságot sok szempont alapján másként és másként értelmezik. [2] Én azokkal értek egyet, akik komplex értelemben közelítik meg a biztonságot, azaz a széles értelemben vett biztonságtartalmat vizsgálják.

Általában a biztonság szűkebb értelmezése során a kritikus infrastruktúrák védelmét tekintik sok esetben a vizsgálat tárgyának.

Ha biztonságot a komplex értelmében vizsgáljuk, megállapítható, hogy az nagyon széles területet ölel fel.

Ezek közül, a teljeség igénye nélkül, néhány fontosabb elem felsorolása is jól mutatja a bonyolultságát, összetettségét: pénzügyi- gazdasági biztonság, katonai biztonság, államhatárok biztonsága, rendvédelem biztonsága, katasztrófák elleni biztonság, tűzvész elleni biztonság, élelmiszer biztonság, ökológiai biztonság, egészség biztonság, egyéni biztonság, információbiztonság, jogbiztonság és még hosszan sorolható lenne a biztonság elemrendszere.

A komplex biztonság ezen elemei szorosan összefüggnek egymással, hatnak egymásra, feltételezik egymás érvényesülését. Például, pénzügyi- gazdasági biztonság nincsen katonai biztonság, államhatárok biztonsága, rendvédelem biztonsága, információbiztonság, jogbiztonság nélkül. De az államhatárok biztonsága sem tartható fenn a pénzügyi- gazdasági biztonság, katonai biztonság, rendvédelem biztonsága, információbiztonság, élelmiszer biztonság, jogbiztonság nélkül. Az összefüggések szinte megszámlálhatatlan kombinációban érvényesülnek.

A biztonság megteremtéséhez információkra van szükség, amely információk első sorban az állapot szintjéről, minőségéről adnak tájékoztatást, illetve a fenyegetettségeket tárják fel. [3]

Az állapot szint és a minőséget leíró információ egyrészt a biztonság alanyainak körülményeiről ad tájékoztatást, másrészt a védekező, elhárító, megelőző, következmény felszámolási erők és eszközök képességeit, lehetőségeit veszi számba.

A fenyegetettségek feltárására számtalan módszer és modell (PTA - Practical Threat Analysis – Gyakorlati Fenyegetés Elemzés, SWOT, PEST, Hibafa, Fenyegetés mátrix, Sérülékenység és kockázatértékelés, Realistic Threat Scenario – Várható Fenyegetés Forgatókönyv, Real-Time Vulnerability Analysis – Valós-idejű Sebezhetőség Elemzés, RISK – Monte Carlo szimuláció stb.) áll rendelkezésre, amelyeknek az alapja szintén az információ. Az információgyűjtés (információszerzés) fajtái (módjai)[1] a hagyományos értelemben két fő csoportra oszthatók, a titkos információgyűjtésre és a nyílt információgyűjtésre.

Napjaink technológiai fejlődése, az internet térhódítása, a világ digitalizálódása, a robottechnológia fejlődése kitermelte a harmadik információgyűjtési módot, a globális elektronikai információgyűjtést.

Ez az információgyűjtési mód (fajta) nem sorolható sem a titkos, sem a nyílt információszerzési módhoz (fajtához), mivel mindkét hagyományos információgyűjtési mód (fajta) jellemzőt magán hordozza, illetve nincsen tér- és időbeli korlátja.

A titkos információgyűjtés általában jogellenes cselekmények felderítésére valamint államérdek szavatolására irányul titkosszolgálati eszközökkel, azaz rejtve folyik úgy a célszemélyek, mint az egész társadalom tekintetében. [4]

[1] A szakirodalom módot és fajtát is említ.

A nyílt információgyűjtés a publikus adatok összegyűjtését jelenti nyilvános módon. Nem sérti a személyiségjogokat. Köztudott úgy a célszemélyek, mint a társadalom előtt.

A globális elektronikai információgyűjtés nyílt abban a vonatkozásban, hogy mindenki előtt ismert az a tény, hogy vannak műholdak, amelyek kamerái olyan felbontással rendelkeznek, hogy a gépkocsi rendszáma is látható a műholdképen, mindenütt biztonsági- és térfigyelő kamerák pásztázzák a terepet, objektumok környékét és rögzítik a történéseket.

Titkos olyan formában, hogy nem tudjuk, ki, mikor, milyen célból készít rólunk videofelvételt és azt mire használja fel. Mindenki életében lehetnek kényes pillanatok, amelyeknek a közzététele sértheti a személyiségjogokat, erkölcsi kárt okozhat a számára. Az a rövid ruhában, fehérnemű nélkül előrehajoló hölgy, - akiről egy élelmiszerüzlet biztonsági kamerája készített hátulról felvételt és az kikerült az internetre, mint jó sztori, - nem biztos, hogy hozzájárult volna a nyilvánossá tételhez. A kétezres évek elején, amikor a Határőrség technikai korszerűsítése kapcsán a határőr járőrrádiókba GPS nyomkövető került beépítésre, azt az adatvédelmi biztos aggályosnak találta, mivel a járőr tartózkodási helye így állandóan követhetővé vált és ez véleménye szerint sértette a személyiség jogokat.

Globális, mert térben, időben határtalan, a korszerű automatizált eszközök az egész földet átfogva, a nap minden másodpercében képesek az események rögzítésére.

A műholdak az egész földfelszínt látják, az internet behálózza az egész világot, ha egyszer valaki fellép a világhálóra, akkor annak az összes virtuális kalandozása nyomon követhető, a hackerek mindent megtudhatnak róla, bankszámlája virtuális rablás áldozatává válhat. A mobiltelefonok figyelésével a használó személy mozgása, fizikai tartózkodási helye rögzíthető, a bankkártya használata megint csak helyszíni nyomot hagy maga után. A video- és infrakamerák bárhol elhelyezhetők, éjjel nappal képesek figyelni, elektronikusan rögzíteni a történteket. Más számtalan mozgásérzékelő és felfedő szenzor is használható az emberek tevékenységének figyelemmel kísérésére. A 2010-es influenzajárvány kapcsán napvilágot láttak olyan híresztelések, hogy a védőoltással mikrocsipet ültetnek az emberekbe. Ez technikailag lehetséges, hiszen a kutyák, macskák nyilvántartására már alkalmazzák az ehhez hasonló módszert.

Ezek a berendezések, eszközök mind elektronizáltak, intelligensek, emberi felügyelet nélkül képesek folyamatosan működni és elektronikusan, többnyire digitalizáltan rögzítik, tárolják az általuk begyűjtött információkat. Ez a digitalizált információ az adatátviteli hálózatokon gyorsan, torzításmentesen továbbítható a világ bármely pontjára.

Amíg a két hagyományos információgyűjtési fajta nagyrészt analóg módszerekre épül (dokumentum elolvasása, élő beszéd, fénykép, hangfelvétel, telefon lehallgatás stb.), a megszerzett információ is analóg információhordozóra kerül, addig a globális elektronikai információ már eredendően digitalizált formában keletkezik. A hagyományos módon megszerzett információt a gyors továbbításhoz, a számítógépi tároláshoz a hatékony feldolgozás érdekében először digitalizálni kell, amely időbe kerül, korszerű és drága eszközöket igényel.

A globális elektronikai információgyűjtés adathordozója már digitális eszközökön és módszereken alapul, így azonnal feldolgozható és továbbítható elektronikus hálózatokon. Egy videokamera által rögzített személy arcképe azonnal lefuttatható egy arcfelismerő programon és találat jelezhető ki, ha ezen személy valamilyen célból szerepel az ellenőrzést végző szervezet arckép archívumában.

A fentieket alapul véve, célszerű az információgyűjtés módjait (fajtáit) az alábbiak szerin meghatározni.

Információgyűjtés módjai (fajtái):

- nyílt;
- titkos;
- globális elektronikai.

A biztonság szintje emelésének egyik fontos eszköze lehet a globális elektronikai információgyűjtés. Természetes, e mellett a nyílt és titkos információgyűjtés jelentősége sem csökken. A globális elektronikai információgyűjtés egyrészt irányulhat a védendő objektum állapotának figyelésére, másrészt a veszélyteményezők feltárására. A globális jellegnél fogva időben szakadatlanul lehet a védendő objektumról a szükséges adatokat gyűjteni és elektronikusan feldolgozni. Ha a vörös iszap tározó folyamatosan ellenőrizve lett volna valamilyen videokamera rendszerrel, akkor a gáton fellépő repedés időben észlelhető lett volna. Vannak olyan intelligens kamerák, amelyek változás észlelésekor automatikusan riasztó jelzést adnak. A kialakuló veszélyhelyzetek szintén időben felfedhetők a globális elektronikai információgyűjtő eszközökkel. Ilyenek is már számtalan helyen üzemelnek, mint például a szökőár előrejelző rendszer, a különböző meteorológiai mérőállomások, vulkántevékenység felmérő berendezések, hő-kamerák a határőrizetben stb.

AZ ÚJ NEMZETI KÖZSZOLGÁLATI EGYETEM K+F+I LEHETŐSÉGEI

A biztonság és az információgyűjtés alapvetésekből kiindulva, az új Nemzeti Közszolgálati Egyetem K+F+I tevékenysége elméleti szinten a biztonság széles értelemben vett területeire irányulhat, amíg gyakorlati téren csak a kritikus infrastruktúra védelmének kutatását célszerű művelnie.

Mi indokolja a biztonság széles értelemben vett körére irányuló elméleti kutatómunka felvállalását?

Első sorban a hadtudomány tágabb értelemben való felfogása, vizsgálata, másod sorban az új Nemzeti Közszolgálati Egyetem tudomány művelő területeinek összetétele. [5]

A három ősi mesterség egyike a harc, a másik az ezzel szorosan összefüggő kémkedés, a harmadik a „rosszlánykodás”. A harc az ember kifejlődésével együtt jelent meg, hiszen az ember harcot folytatott a természettel, harc volt a vadászat, harc volt a saját védelme más támadókkal szemben. A fejlődés során a harc tudománya a hadtudomány lett. A harcot nem biztos, hogy le kell szűkíteni a fegyveres küzdelemre, sok fegyverek nélküli küzdelem is folyik az emberi tevékenységek során. Példaként nézzük a biztonságot.

Bármely elemét vizsgálva is a biztonság megteremtésének, azt kell megállapítani, hogy az egy küzdelem, harc folyamán valósul meg. Ezen harc, küzdelem alatt nemcsak a fegyveres harcot és küzdelmet kell érteni, hanem a szellemi, jogszabályi, politikai, gazdasági, rendfenntartási, emberi viszonyalakítási, feltétel megteremtési, objektum-, eszköz- és létesítményalkotási szinten folytatott harcot, küzdelmet is. Ha tovább folytatjuk a nem fegyveres harc és küzdelem megvívásának elemzését, akkor azt kell megállapítanunk, hogy mindegyikben fellelhető a klasszikus fegyveres harc megszervezésére és megvívására irányuló úgynevezett „parancsnoki munka” folyamata és elemrendszere, csak az más szavakkal történik kifejezésre.

Azt senki nem tagadhatja, hogy bármely, nem fegyveres jellegű tevékenység során is meg kell érteni, hogy mit akarunk végrehajtani, szükség van időütemezésre, a körülmények, lehetőségek feltárására, a feltételek megteremtésére, tervezésre, szervezésre, a folyamatok irányítására, a szükséges beavatkozásokra anomáliák esetén. Különböző módszertanok láttak napvilágot a nem fegyveres folyamatok megszervezésére, irányítására. A teljesség igénye nélkül, csak párat említve, léteznek különböző projekttervezési és -levezetési módszertanok (PRINCE, SSADM, PCM, LFA, TOGAF), időütemezési eszközök (Gantt diagram), SWOT,

FMEA, HAZOP, HRA, QRQ, ETA, PEST elemzés, hibafák (FTA), kockázati tényező mátrix, folyamat gráfok, különböző számítógépi elemző, modellező programok.

Az is nyilvánvaló, hogy a hadtudomány az a tudomány, amely a legrégebb idők óta tárja fel a harc megvívásának általános és specifikus törvényszerűségeit, dolgozza ki a harc előkészítésének, megvívásának elveit, gyakorlatát, emberi és technikai feltételeit.

Ezek alapján célszerű a hadtudományt a legszélesebb értelemben felfogni, és ebből leszármaztatni a nem fegyveres küzdelem megvívásának tudományos megalapozását, így a rendvédelem, rendészet, államigazgatás területeken is. A hadtudomány foglalkozhat a fegyveres és a nem fegyveres harc általános törvényszerűségeivel, elméletével, a fegyveres harc specifikus törvényszerűségeivel, elméletével, az egyes kialakuló tudományok, mint például a rendvédelem tudomány az adott terület specifikus törvényszerűségeit kutathatja és elméletét dolgozhatja ki.

A létrejövő új Nemzeti Közszolgálati Egyetem képzési portfoliója folytán teljes egészében képes a fenti alapvetés mentén a hadtudomány általános és specifikus területeinek művelésére. Gondozhatja a fegyveres harc tudományát, a kialakulóban lévő rendvédelemmel kapcsolatos tudományt, valamint az állam működtetéséhez kapcsolódó tudományokat. Ha ezt a három területet vesszük vizsgálat alá, akkor azt a következtetést kell levonnunk, hogy a komplex biztonság összes elemét elméleti szinten magában foglalják ezen tudományok. A biztonság egyetemes voltából adódik, hogy tudományos megalapozottságát is egyetemes módon kell felfogni.

Az élet bármely területét vizsgálva azt kell megállapítani, hogy a hadtudomány szinte minden tudományból merít, interdiszciplináris tudomány is, a konkrét fegyveres küzdelem megvívásának tudománya mellett. Bármelyik más tudományt tekintjük át, az a hadsereg, rendvédelem, közigazgatás területén sajátos formában megjelenik. Csak pár példa a szemléltetés kedvéért. Az egészségtudomány elengedhetetlen a harctéri gyógyításban, az élelmiszer- és vízbiztonság a hadseregek, rendvédelmi szervezetek, állami és önkormányzati intézmények élelmezésében, a meteorológia, fizika, aerodinamika a repülésben, az építő- és gépészmérnöki tudás az erődítésben, harcjárművek, fegyverek gyártásában, alkalmazásában, a vegyi, biológiai tudományok a tömegpusztító fegyverek kifejlesztésében, illetve az ellenük való védekezésben, a rádióelektronikai, informatikai tudományok az összeköttetés és információbiztonság megteremtésében. De még véget nem érően lehetne sorolni az összefüggéseket.

Az egyetemes szemléletből fakad, hogy az új egyetemnek célszerű lenne kialakítania egy akadémiai kutatócsoportot a komplex értelemben vett biztonság elméleti téziseinek kutatására, törvényszerűségeinek feltárására, tudományos megalapozottságának megteremtésére.

A biztonság gyakorlati megvalósítása számos más tudományhoz, intézményhez kapcsolódik, amelyek a biztonság egy-egy részével, szeletével foglalkoznak, ezeknek a részterületeknek tudna az akadémiai kutatócsoport egységes koncepciót, egységes célkitűzést meghatározni.

Ha áttekintjük a kritikus infrastruktúra elemeit, akkor arra a megállapításra kell jutnunk, hogy az új Nemzeti Közszolgálati Egyetem képzési portfoliója szinte teljes egészében lefedi azokat a biztonsági területeket, amelyek a kritikus infrastruktúra védelmét szolgálják. [6]

Ebből fakad az a következtetés, hogy az új egyetem gyakorlati kutatási irányait a kritikus infrastruktúra védelem mentén célszerű felépíteni.

A kritikus infrastruktúra értelmezése is sokszínű, de abban minden kutató egyetért, hogy az állam működőképességét, a biztonságot szavatoló létesítmények, erőforrások, energiaforrások, információtechnológiák tartoznak a kritikus infrastruktúrák közé. [7]

Magyarországon a 2112/2004. (V.7.) kormány határozat a következő területeket sorolja a kritikus infrastruktúrák közé:[2]

- energiaellátás;
- közművesítés;
- közlekedés és szállítás;
- távközlés, elektronikus adatforgalom és informatikai hálózat;
- bankrendszer;
- szolgáltatások;
- média;
- ivóvíz es élelmiszer alapellátás;
- egészségügyi biztosítás.

Ha megvizsgáljuk a hon-és rendvédelem aktuális problémáit, akkor több olyan markánsan körvonalazódó kutatási területet lehet fellelni, amelyben az összes katonai- és rendvédelmi szervezet érintett.

Egyik ilyen terület a környezetvédelem és a vele szoros összefüggésben lévő katasztrófavédelem, amelyben a hon-és rendvédelem, valamint az államigazgatás egyrészt, mint környezetszennyező, másrészt, mint környezetvédő vesz részt. Említett szervezetek járműveket használnak, rengeteg energiát fogyasztanak, veszélyes anyagokkal dolgoznak, amelyek szennyezik a környezetet. Ha sikerül új technológiákat, alkalmazási eljárásokat és eszközöket kifejleszteni, akkor a környezetkárosítás, a környezetszennyezés nagymértékben csökkenthető, ezáltal az egyes katasztrófákat kiváltó okok is mérsékelhetők. De a felsorolt szervezetek hatáskörébe tartozik több tekintetben a környezetkárosítás felfedése, intézkedések meghozatala annak megszüntetésére. Szintén új technológiák, eljárások kutatásával, létrehozásával a felfedés hatékonysága jelentősen fokozható. [8]

Másik általános terület az informatikai védelem. A hon-és rendvédelemi szervek, az államigazgatási apparátus azok közé a célobjektumok közé tartozik, amelyek a támadások középpontjába kerülhetnek úgy a hackerek, mint a terroristák vagy az ellenséges hírszerzés tekintetében. Az egyéb célobjektumok (bankok, energiaellátás stb.) elleni támadás felfedésében, a bekövetkezett támadás elkövetőinek felfedésében a rendvédelmi szervek alapvető szerepet játszanak. Létező veszély, ha még látens állapotban is van az elektronikai harc, a kybertámadás, robothadviselés. [9], [10]

Szintén jelentős veszélyforrás az illegális migráció, a fegyver-, drog-, hasadóanyag- és emberkereskedelem. Ez a veszélyforrás kategória az egész társadalmat érinti, amelynek felfedésében, akadályozásában szintén a hon-és rendvédelemi szervek, az államigazgatási apparátus az, amelyek a fő szerepet játsszák.

A rendvédelem minden területén előtérbe kerül a biztonság fokozásának egyik eszközeként az automatikus terep- és létesítményfelügyelet.

A rendőrség a schengeni külső határok őrizetében alkalmaz mobil és telepített hő-kamerákat, repülőkre szerelt kamerákat az EU határőrizeti akciók során vet be, illetve az egyéb rendezvények biztosítása és a közlekedési jogsértések felderítése során térfigyelő kamerákat vesznek igénybe. Több rendőrjárőr autó el lett látva eseményt rögzítő kamerával. Ezen kívül más érzékelőket is alkalmaznak a tevékenységek során az objektumok védelmére, zárt területre való behatolás felfedésére, mint lézerkerítést, hang- és mozgás érzékelő

[2] 2080/2008 (VI. 30.) Korm. Határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

berendezéseket. Történtek kísérletek felfüggesztett léggömbre szerelt kamerákkal való terep- és esemény felügyeletre is.

A NAV szállítmányok, földbe rejtett tárgyak felfedésére alkalmaz különböző szenzorokat.

A BVI objektumvédelemre és fogvatartott követésre használ, illetve tervez használni szenzorrendszereket.

A rendvédelmi kutatás tárgyát képezhetné olyan átfogó térinformációs rendszer kiépítése is, amelyben az esemény bekövetkezése időpontjától kezdve az automatikus szenzorrendszerek felfednék az eseményeket, majd rögzítenék digitális térképen azok helyszínét, GPS rendszeren keresztül követnék és időbélyeggel ellátnák minden beavatkozó mozgását, ezzel biztosítva hatékony együttműködésüket, a rendszer az automatikus szenzorrendszerek folyamatos információközlése alapján térinformációs elemzéssel bevetési célszerűség, együttműködési és hatásmodellezést végezne.

Az egységes térinformációs rendszer alapját a határrendészeti, közterület felügyeleti, bevetés irányítási jelenleg működő térinformációs rendszerek, valamint a Robotzsaru képezné.

A katonai, rendvédelmi és államigazgatási szervek is nagy energiafogyasztók, ezért fontos lenne az alternatív és megújuló energiaforrások alkalmazási lehetőségeinek kutatása.

A parafa granulátum nanotechnológiai elegyítése a szénnel olyan hő-, hang szigetelő, korrózió gátló, kopásálló, infrasugár- és rádióhullám elnyelő anyagot képez, amelynek számtalan előnye kihasználható lenne a kritikus infrastruktúrák védelmében.

Ha áttekintjük a kritikus infrastruktúra védelem EU –ós megítélését, azt láthatjuk, hogy a fent nevesített kutatási területek jól illeszthetők az EU –s elképzelésekhez.[11]

A kutatói hálózatok és a klaszterek lennének azok a kapcsok, amelyek az egyetemi elméleti alapvetéseket és az egyes részterületek gyakorlati kutatómunkáját, tudomány alkalmazását harmonizálnák, a kutatási eredményeket közkinccsé tennék.

A KUTATÓI HÁLÓZATOK LEHETŐSÉGEI

A felsőoktatási intézmények számára a kutatói hálózatok hatékony működéséhez az infrastrukturális feltételek rendelkezésre állnak. A NIIF (Nemzeti Információs Infrastruktúra Fejlesztési Intézet), MIT (Magyar Internet Társaság) és a HUNGARNET Egyesület (Magyar Felsőoktatási, Kutatási és Közgyűjteményi Számítógéphálózati Egyesület) közreműködésével létrehozásra került egy nagy sávszélességű hibrid adathálózat, a HBONE+[3].[12]

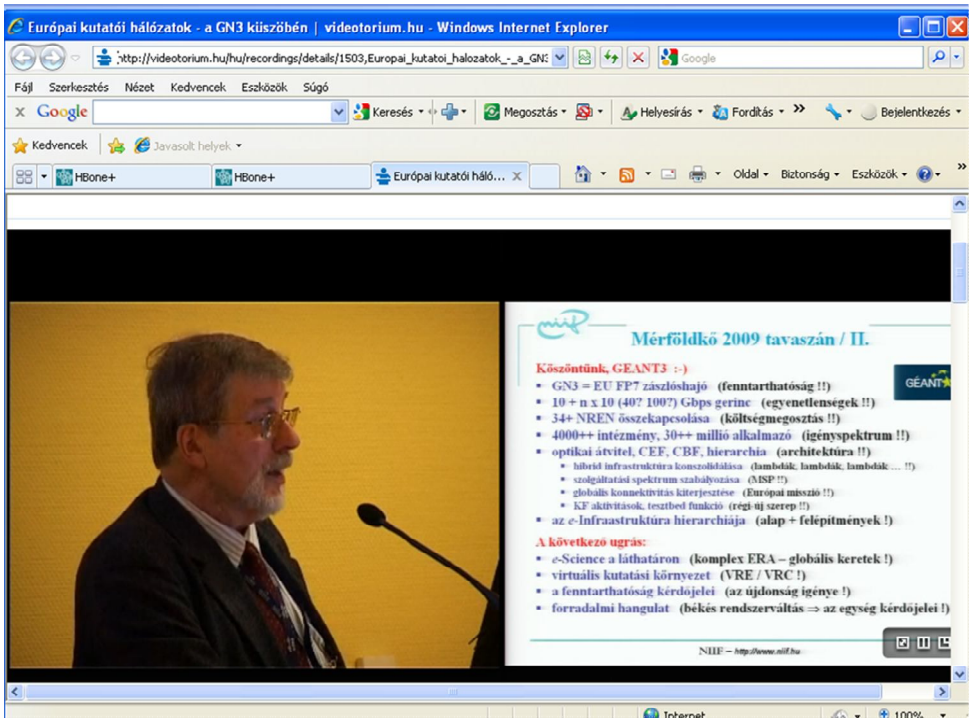
A HBONE+ egy országos gerinchálózat, amelynek feladata, hogy a HUNGARNET tagintézményeket egy nagyterületű, országos gerinchálózattal egymással összekapcsolja, továbbá biztosítsa számukra a nemzetközi kapcsolatot, a teljes Internet hozzáférést. A HBONE kialakítása, fejlesztése az NIIF Műszaki Tanácsa, illetve a HBONE hálózatot üzemeltető menedzserek által közösen kidolgozott és az NIIF vezető testületei által jóváhagyott terveknek megfelelően folyik.[4] [13]

A kutatói hálózatok nemcsak nemzeti, hanem nemzetközi szinten is kiépítésre kerültek.

Az európai kutató hálózat a GEANT3 ((Gigabit European Academic Networking Technológy) GN3).

Az európai kutató hálózatokról bővebben Bálint Lajos NIIF nemzetközi kapcsolatok igazgatóhelyettese Networkshop előadásából lehet ismereteket nyerni.[5]

3 http://www.hboneplus.hu/node/98 Dr. Nyitrai Zsolt infokommunikációs államtitkár átadta az NIIF Intézet új generációs hibrid hálózatát. 2010. december 9-étől elérhetővé válik Magyarországon az ún. hibrid hálózat.
4 https://nws.niif.hu/
5 http://videotorium.hu/hu/recordings/details/1503,Europai_kutatoi_halozatok_-_a_GN3_kuszoben



A TERENA *Trans-European Research and Education Networking Association* - Trans-Europai Kutató és Oktató Hálózati Egyesülés és az ERAB *European Research Area Board* – Európai Kutatási Terület Egyesület szintén a kutatói hálózatok közé tartoznak.

A GRNET (Greek Research and Technology Network - Görög Kutatás és Technológia Hálózat) és a GEANT projektek a grides alkalmazások közé tartoznak. Ezeket a projekteket az EU FP7 keretprogram támogatja.

Mi indokolja a kutatói hálózatok fejlesztését?

Ha megvizsgáljuk a 21. század fejlődési trendjeit, akkor számos olyan ismérv fedhető fel, amelyek az on-line együttműködés szükségességének irányába hatnak.[6]

- kialakulóban van a digitális társadalom, új IT (információ technológia) alapú közösségek jönnek létre;
- globális kényszer igényli a termelékenység növekedését, a hozzáadott érték fokozását, az IT tudásmenedzsment magas szintjét, a jó minőségű adatok és informatikai hálózatok meglétét;
- nemzeti populáció egyre heterogénebb lesz;
- nemzeti oktatási rendszerek produktivitása kezd elmaradni a gazdaság igényeitől;
- kreativitás, innováció növekvő hatalma;
- feldolgozói programok portál alapúvá válása (webes alkalmazások);
- strukturálatlan adatfeldolgozási technológiák terjedése;
- maga a technológia már nem elégséges, hanem az a lényeg, hogy a technológia milyen szolgáltatásra képes;
- ICT (infó kommunikációs technológiák) uralma;

[6] Networkshop 2011 konferencia Kaposvár 2011.április 27-29. plenáris előadások, Prof. Dr. Kroó Norbert akadémikus, MTA alelnök, Tázló József műszaki igazgató CISCO Systems Magyarország Kft., Veres Zsolt vezérigazgató IBM Magyarország

- digitális tartalmak terjedése (multimédia, tudásbázisok, videotorium[7], repozitorium, videokonferencia);
- grafikus processzorok szükségességének növekedése;
- tudásgazdaságok lesznek csak életképesek;
- az internet a tárgyak hálózata lett;
- az IT elérkezett a harmadik fejlődési mérföldkőjéig, a szuperszámítógépekhez[8] és cloud[9] –hoz (felhő).

A fenti trendek jól mutatják, hogy a gazdaság, az oktatás olyan környezetbe kerül, amelyben az információ, az új kommunikációs eszközök és az új technológiák játsszák a fő szerepet. A globális kényszer generál egy összefüggést. A gazdaság, a társadalom működéséhez egyre több, jó minőségű, gyorsan megszerezhető információra van szükség, de ezen információkat egy globális, hatalmas információhalmazból kell kinyerni, ugyanakkor az információ elévülési időtartama is erősen lecsökken. Lehet, hogy egy megszerzett pénzügyi információ, pár óra múlva már értéktelenné válik. Az innováció, hatékonyság sok esetben megköveteli a csoportmunkát, nagy számításigényű feladatvégzést, a legkorszerűbb eszközök és technológiák alkalmazását. Viszont a ráfordítás – létrehozott érték viszony annál jobb, minél nagyobb mértékben használható a meglévő eszközpark és technológia. Ezekből generálódik az ellentmondás, ha valaki nem használ újabb és újabb eszközöket, technológiákat, az lemarad az innovációs küzdelemben, de ha beruház új eszközökre és technológiákra, akkor a nyeresége csökken, illetve nincs is forrása beruházásra. Ez a probléma fokozottan jelentkezik a költségvetési szerveknél. Az igény nő a korszerűsítés, az állampolgárok számára nyújtott szolgáltatások minőségének javítására, de nincsen pénz beruházásokra.

Ezen ellentmondás feloldására látszik járható útnak az IT fejlődés harmadik mérföldköveként megjelenő szuperszámítógépek rendszere és a cloud (felhő).

ÚJ TECHNOLÓGIÁK ÉS MODELLEK (SZUPERSZÁMÍTÓGÉP, GRID, CLOUD / FELHŐ) A TUDOMÁNYOS KUTATÁS SZOLGÁLATÁBAN

„Az intézmények egyre gyorsuló ütemben növekvő adattárolási igényeinek a biztonságos kiszolgálásához megbízható, költséghatékony, nagy teljesítményű elosztott adattárolási infrastruktúrára van szükség. Ezt az adattárolási igényt a fejlesztés eredményeként egy - a közelmúltban világszerte újdonságként megjelent - "cloud computing" architektúra segítségével tudjuk majd a felhasználóink rendelkezésére bocsátani, pl. adatmentési és adatbányászati célokra. Nem tévesztjük szem elől, hogy a nemzetközi tapasztalatok szerint az európai kutatók meghatározó többsége (mintegy két-harmada) már 1 Tflops teljesítménynél nagyobb számítási erőforrásokhoz is hozzá tud férni, ami egyrészt jelentősen növeli Európa kutatási-fejlesztési potenciálját és versenyképességét, másrészt viszont kihívást is jelent a nemzeti - köztük a magyarországi - fejlesztések számára. A projekt eredményeként a Magyarországon elérhető kapacitás meg fogja haladni az 5 Tflops értéket, ami már biztosítani fogja a magyar kutatók versenyképességét. Mindezeken túl a szuper-számítástechnikai fejlesztések eredményeként Magyarország az európai szuperszámítógépeket és grideket integráló konzorciumoknak (PRACE, DEISA) is teljes jogú tagja lehet, így a hazai kutatók az

[7] http://videotorium.hu/hu/recordings/details/1503,Europai_kutatoi_halozatok_-_a_GN3_kuszoben
[8] Tázló József (műszaki igazgató CISCO Systems Magyarország Kft) előadása a Networkshop 2011 konferencia Kaposvár 2011.április 27-29. plenáris ülésén (első mérföldkő 1981 IBM PC –k megjelenése, második 1951 UNIVAC I kereskedelmi forgalomban megjelenő számítógépek)
[9] Később kifejtve

Európai Unió keretében elérhető kapacitásokhoz is az eddigieknél jóval egyszerűbben tudnak majd hozzáférni."[10]

A szuperszámítógépek óriási kapacitású, nagyon gyors számítógépek, amelyeknek a szolgáltatásai bérelhetők.

A cloud (felhő) olyan IT működési modell, amelyben a felhasználónak nincsen szüksége drága hardver eszközökre, alkalmazói szoftverekre, IT szakembergárdára, állandó fejlesztési beruházásokra, csak egy egyszerű monitorra, billentyűzetre és megbízható, nagy sávszélességű adatátviteli hálózatra.[11]

Mit takar ez a modell? Az összes hardver eszköz, alkalmazó program valahol a világban, jól védett, többszörös redundáns megbízhatósági szinten lévő szerverfarmokban nyer elhelyezést. A Microsoftnak konténer rendszere van, egy konténerben több száz szerver üzemel, amelyek meghibásodás esetén automatikusan átadják a processzeket a másik, működő szervernek, az alkalmazó ebből semmit nem vesz észre. Ha egy bizonyos százaléka meghibásodik a szervereknek, az egész konténert lecserélik egy új, teljes működő képességű konténerre.

Az IT szakembergárda is ezeken a szerverfarmokon található, a fejlesztés a szerverfarm üzemeltetőjének feladata, amely azt eredményezi, hogy mindig a legkorszerűbb eszközök és technológiák állnak a felhasználó számára.

A felhasználó egy bérleményen keresztül jut hozzá ezen szerverfarm szolgáltatásaihoz. Ha például az adott cégnek gépelési, számítási feladatai vannak, akkor szövegszerkesztői és táblázatkezelői szolgáltatásokat bérel, ha Microsoft környezetben van, akkor a felhőben lévő valamely szerverpark számítógépén fut a Word és az Excel is. A cég a monitorján és az adathálózatán keresztül a felhőben futtatja ezt a két szoftvert, az adatait is a felhőben tárolja, csak az eredményeket jeleníti meg a cég eszközein. [14]

Mit jelent ez az adott cég számára? Első sorban beruházási és működési költségmegtakarítást. A 2011. április 28.-án megtartott Microsoft Cloud konferencián bemutatott számvetések alapján a beruházáson 70% -t, a működtetésen 50% -t lehet megspórolni. Másod sorban ez a cég az innovációs versenyben állandóan az élen halad, hiszen szolgáltatásként mindig a legkorszerűbbet kapja.

Természetesen a felhőmodell kérdéseket is felvet. Egyik ilyen kérdés az informatikai biztonság, a másik a kiszolgáltatottság. A részletek elemzése nélkül is jól látható, hogy az adott cég teljes mértékben a felhő működtetőjétől függ, hiszen nála vannak az adatai, az adatokat feldolgozó eszközök is, nem a saját irodájában, ha kell vaslemez szekrényben jól elzárva. Másik ilyen kockázati tényező az adatkapcsolat, adatátviteli hálózat megbízhatósága. Ha megszakad az adatkapcsolat, az említett cég működésképtelenné válik.

A felhőt üzemeltetők az informatikai biztonság magas szintjének megteremtésére garanciákat adnak, a jogi környezetet is folyamatosan alakítják át, hogy az is garantálja a megbízhatóságot.

A világfejlődési trendeket figyelve, nem lesz más választása sem a cégeknek, sem a költségvetési szerveknek, mint a felhőbe való bekapcsolódás. Olyan rohamos a technikai fejlődés, olyan gyorsan jönnek ki a piacra az új, modern eszközök, hogy azokat nem lesz képes a cégek, a költségvetési szervek mindegyike megvenni, mivel az új eszköz megjelenési ideje töredéke a meglévő eszköz amortizációs idejének. De aki nem alkalmazza az újat, az lemarad a versenyben. Ezért nem lesz más alternatíva, mint a felhő alkalmazása.

A rendvédelmi szervek is előbb – utóbb rákényszerülnek a felhő használatára. Már most jelentkezik az a gond náluk, hogy a tíz éves számítógéppark egyre kevésbé tud helytállni az elvárásoknak, de fejlesztésre nincsen forrásuk.

[10] http://www.hboneplus.hu/node/25

[11] http://videotorium.hu/hu/recordings/details/2738,Szekelyi_Szabolcs_-_NIIF_Cloud_NorduGrid

A felsőoktatási intézmények és a közgyűjteményi intézmények számára a HBONE+ projekt teremti meg a felhő használatának lehetőségeit. A digitális tartalmak használata nélkül már nem képzelhető el egy korszerű oktatás, egy jól működő könyvtár, viszont a digitális tartalmak létrehozása, alkalmazása gyors, modern számítógépeket igényel, tárolásuk pedig óriási tárkapacitást. Ilyen fokú beruházásra kevés intézmény képes, ezeket a szolgáltatásokat a HBONE+ -tól kell igényelniük. Komolyabb, a K+F+I –t szolgáló kutatásokra sem lesz képes egy-egy egyetem, csak közösségek, amelyek nem nélkülözhetik a szuperszámítógépeket. A közös on-line munkát, a szuperszámítógépeket szintén a HBONE+ tudja adni a kutatóknak.

A felhasználó, például egy egyetem, egy önkormányzat nagyon kevés IT beruházással képes a legkorszerűbb, leggyorsabb, leg megbízhatóbb információrendszert működtetni. Természetes, ezen működtetés pénzbe kerül, de mennél többen használják a felhőt, annál kevesebb lesz a bérleti díj. Jelenleg egy általános szolgáltatás havi 100 euró alatt vehető igénybe.

Felhasználói attitűd váltás is kell a felhő használatához. Sokan még bizalmatlanok, mivel az infrastruktúrára, az adatok tárolására nincsen rálátásuk. A cloud –nak vannak szolgáltatási szintjei, nincs szükség a teljes kiszolgáltatottságra. Elsőként csak az alkalmazói szoftvereket lehet bérelni, majd az infrastruktúrát is, ha a tapasztalatok kedvezőek, az adatbázisok is kihelyezhetők a felhőbe.

A kutatói hálózatok infrastruktúráját is alapvetően a szuperszámítógépek és a grid (nagy sebességű adatátviteli hálózat) alkotják.

A szuperszámítógépek óriási teljesítményre képesek, első sorban a számításigényes feladatokat támogatják. Az űrkutatásban, az élettudományokban, fizikai, kémiai kutatásokban használják őket számítás intenzív modellezésre, szimulációra, adatelemzésre, bio informatikai feladatokra, orvosi képfeldolgozásra, tudományos munkafolyamat gráfok feldolgozására, elosztott számolási infrastruktúrát igénylő tevékenységekre, meteorológiai modellezésekre. Általánosságban egy szuperszámítógép ára 250 millió forint, 1024 processzor magot tartalmaz, vízhűtésű, nagy az áramfelvétele, 24 TB a memóriája, 50 PFlops számítási kapacitása van. Egy ilyen szuperszámítógép például a BlueGene/Q gép.

Magyarországi viszonylatban a felsőoktatási intézményeknek a NIIF Intézet biztosít négy szuperszámítógépet és a grid kialakítását lehetővé tevő HBONE+ nagysebességű adathálózatot. A négy szuperszámítógép a szegedi, pécsi, debreceni egyetemen és az NIIF Intézetnél került telepítésre. Ezen szuperszámítógépek főbb adatai: 50 teraflops teljesítmény, 1536 core 3,33 GHz, 6 TB memória, 500 TB háttértár, Linux operációs rendszer, vízhűtés, vizualizációs szerver erős grafikus kártyával a képi megjelenítéshez. Sajnos, a rohamos technikai fejlődés következtében ezen szuperszámítógépek elavulása 3-4 év alatt megtörténik, az 50 teraflops teljesítmény is jövőre kevés lesz, mivel a számítási kapacitás évente duplázódik.[12]

Vannak olyan feladatok, amelyekre egy szuperszámítógép nem elegendő, ezért kialakítják a grideket[13], amelyekbe több szuperszámítógépet kapcsolnak össze. Például ilyen a HPC projekt, amelyben bulgár, magyar, román és szerb szuperszámítógépek kerültek összekapcsolásra. Magyar részről a projektben az MTA SZTAKI, Óbudai Egyetem és a NIIF Intézet vesz részt. Az Óbudai Egyetem fejleszti az alkalmazói programokat, a DeepAlinger –t és a DiseaseGene –t.[14]

A hibrid technológia teszi lehetővé a gridek létrehozását, azaz IP kapcsolatok mellett pont – pont kapcsolatok is kiépíthetők, dedikált kapcsolatok hozhatók létre az adott kutatásban résztvevő szuperszámítógépek között. A kapcsolat létrehozása az úgynevezett „köztes réteg” (ARC-AREX, gLite) kialakításával és használatával valósítható meg. A köztes réteg

[12] Stefán Péter: Networkshop 2011. Kaposvár előadása
[13] http://videotorium.hu/hu/recordings/details/2738,Szekelyi_Szabolcs_-_NIIF_Cloud_NorduGrid
[14] Röczei Gábor NIIF Intézet: Délkelet-Európai Grid Projekt, Networkshop 2011. Kaposvár előadása

elkészítése bonyolult programozói feladat. Köztes réteg elfedésére portál megoldásokat használnak, ezzel az eszközzel a felhasználók könnyebben hozzáférnek a távoli grides erőforrásokhoz. Az MTA SZTAKI is fejleszt ilyen portálalkalmazást, a gUSE –t.

A desktop grid az önkéntes felajánlásból összeállított grideket foglalja magában. Azok az intézmények, amelyek rendelkeznek szabad kapacitással, ezt felajánlják mások részére a számításigényes feladataik ellátásához. A grid használatának megkönnyítésére kutatások folynak a desktop gridek párosítására a web2 –vel.[15]

Befejezésül elmondható az, hogy az új közszolgálati egyetem széles kutatási lehetőségekhez jut összetétele, felépülése alapján, a kutatás infrastrukturális háttere biztosított lesz a számára.

A karok, de főként az egyetem tudományszervező szakemberei előtt állnak azok a feladatok, amelyek során ki kell alakítani a kutatási koncepciót, meg kell találni azokat a közös hon- rendvédelmi és közigazgatási problémákat, amelyek mentén kialakíthatók a konkrét kutatási programok, létrehozhatók a kutatói hálózatok, klaszterek.

A ZMNE kutatási kapacitásai, eddigi tudományos eredményei, a KKV –kal kialakított jó kapcsolatrendszere és eredményes tudományos együttműködése, jól felkészült, jelentős tapasztalatokkal rendelkezői kutatói megfelelő kiinduló alapot teremtenek az új egyetem kutatási tevékenységének megszervezéséhez.

Mivel a biztonság megteremtésének legfőbb tudományos műhelye is az új egyetem lesz, alapul véve a biztonság globális és egyetemes ismérveit, nem lehet megfeledkezni a nemzetközi, főleg az európai kutatási programokba és kutatási hálózatokba való bekapcsolódásról sem.

Az új egyetem könnyen válhat az EU biztonság megteremtésének vezető tudományos bölcsőjévé. Hiszen, a kiépített biztonsági állapot csak akkor marad tartós, ha az megvédésre kerül. A megvédése állandó harcot, jól szervezett, célirányos tudományos kutatómunkát igényel. Európában kevés olyan intézmény van, ahol központosított stratégia, egységes elméleti alapvetések, közös tudományos és oktatási stratégia mentén lehet egy tudományos felsőoktatási intézményben gondozni a biztonság megteremtésének tudományát, elméletét, gyakorlati iránymutatását. Ezt a lehetőséget kell kihasználnia az új egyetemnek.

Felhasznált irodalom

[1] KÖSZEGVÁRI Tibor: A hadtudomány mai problémái, területei és új fogalma (Hadtudomány (Magyar Hadtudományi Társaság, Budapest XVII. Évfolyam 2007/1 szám) 13. oldal.

[2] Dr. Hadnagy Imre József: A biztonság korszerű értelmezése, http://www.vedelem.hu/letoltes/tanulmany/tan135.pdf

[3] Finszter Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében, http://be.atw.hu/letoltes/Krimjegyzet.doc

[4] Dr. Balla Lajos: Adalékok a titkos információgyűjtés…, http://www.debreceniitelotabla.hu/doc/bunteto/TitkosAdatgyujtes.pdf

[5] Berek Lajos: A tudományos kutatás alapjai és módszertana, www.bereklajos.hu

[6] Kovács László: Hadmérnök, 2007. november 27. Különszám Kritikus információs infrastruktúrák Magyarországon

[15] Marosi Attila Csaba: Desktop Grid a Web 2.0 szolgálatában, Networkshop 2011. szekció előadás

[7] Varga Péter János Budapesti Műszaki Főiskola: A kritikus információs infrastruktúrák értelmezése Hadmérnök, III. Évfolyam 2. szám - 2008. június http://hadmernok.hu/archivum/2008/2/2008_2_varga.pdf

[8] Bukovics István: A katasztrófavédelem helye, szerepe a XXI. század elején http://www.vedelem.hu/letoltes/tanulmany/tan117.pdf

[9] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, (PhD) értekezés ZMNE

[10] Sik Zoltán Nándor, ENO Advisory Kft: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában, http://docs.google.com/viewe

[11] Précsényi Zoltán, Solymosi József: Kritikus infrastruktúrák azonosítása, körkép az EU-ban és az USA-ban tapasztalható nehézségekről, http://www.foodlawment.hu/downloads/kritikus_infrastrukturak_azonositasa_usa_eu.pdf

[12] Networkshop 2008-2011 konferenciák előadás anyagai https://nws.niif.hu/nws2011/ http://videotorium.hu/hu/

[13] HBONE+ architektúra, tenderek, eszköztenderek, hálózati eszközök: Jákó András jako.hujako.andras@eik.bme.hu

[14] MPLS alapú IP hálózat képességei: Gaál Géza PKI-FI Műszaki termékfejlesztési ágazat