



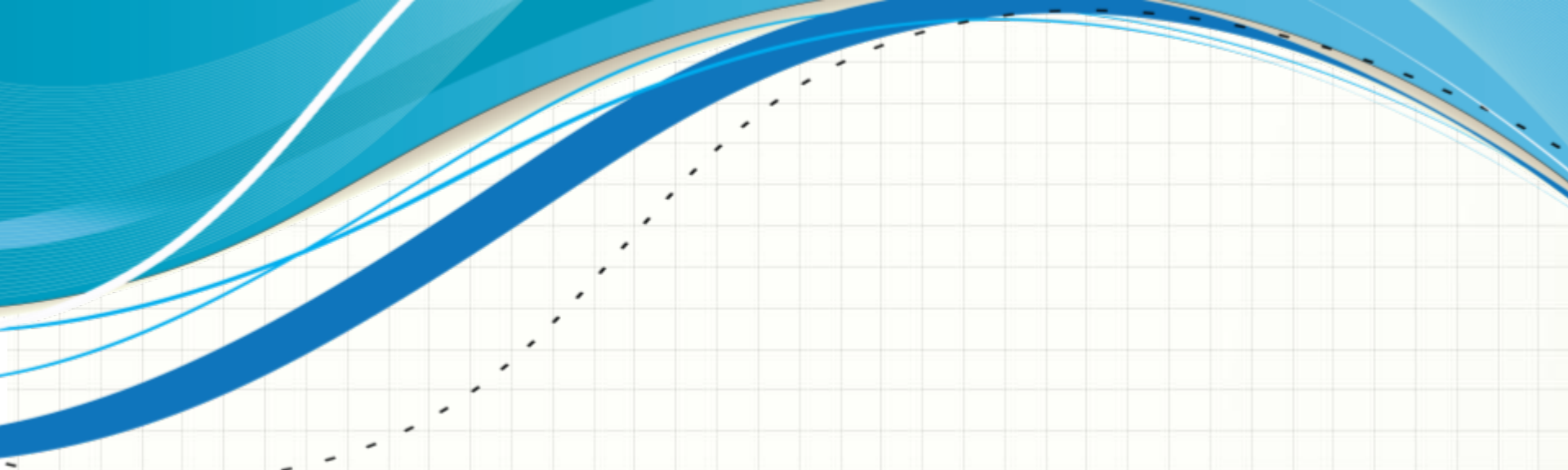
KRITIKUS INFRASTRUKTÚRÁK VÉDELME: KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁKRÓL ÁLTALÁBAN

Kovács László

Nemzeti Közszolgálati Egyetem

kovacs.laszlo@uni-nke.hu





Prof. Dr. Kovács László mk. ezredes
Nemzeti Közszolgálati Egyetem
Informatikai és Elektronikai Hadviselés Tanszék
egyetemi tanár
tudományos és nemzetközi dékánhelyettes

Posta: 1581 Budapest, Pf.: 15.

Telefon: +36-1-432-9000/29-015

E-mail: kovacs.laszlo@uni-nke.hu

Web: <http://kovacsx.hu>



INFORMÁCIÓS TÁRSADALOM

FÜGGŐSÉG

**INFORMÁCIÓS TECHNIKA ÉS
TECHNOLÓGIA**

Infrastruktúra

- **Általános feladatú infrastruktúra**
- **Információs rendeltetésű infrastruktúra**

Az általános feladatú infrastruktúra fogalma:

olyan állandóhelyű vagy mobil építmények, eszközök, rendszerek, hálózatok, az általuk nyújtott szolgáltatások, és működési feltételek összességét kell érteni, amelyek valamilyen társadalmi, gazdasági vagy akár katonai funkciók és rendszerek feladatorientált, zavartalan és hatékony működését teszik lehetővé

Az általános feladatú infrastruktúrák:

- közigazgatási;
- szállítási;
- ellátási;
- hírközlési;
- vezetési;
- védelmi (ország védelem, rendvédelem, katasztrófavédelem, polgári védelem);
- oktatási;
- egészségügyi;
- tájékoztatási.

Az információs infrastruktúra fogalma:

az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúra-rendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az infor-mációs társadalom komplex információs infrastruktúráját.”

Az információs infrastruktúrák:

- **funkcionális információs infrastruktúra:**

Rendeltetésük, hogy fizikailag lehetővé tegyék a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végezzenek. Az információs társadalom információs infrastruktúráin belül ezek az elsődlegesek. Biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását.

- **támogató információs infrastruktúra:**

Rendeltetésük, hogy létrehozzák, és folyamatosan biztosítsák az alapvető információs szolgáltatásokat végző funkcionális információs infrastruktúrák zavartalan működéséhez és fejlődéséhez szükséges szellemi és anyagi alapokat, valamint támogató háttereket

Kritikus és sebezhető infrastruktúrák:

ezek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe.

Az információs társadalomban a **kritikus infrastruktúrák nem egyeznek meg a kritikus információs infrastruktúrákkal!**

A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló zöld könyv szerint :

„kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak stb.)”.

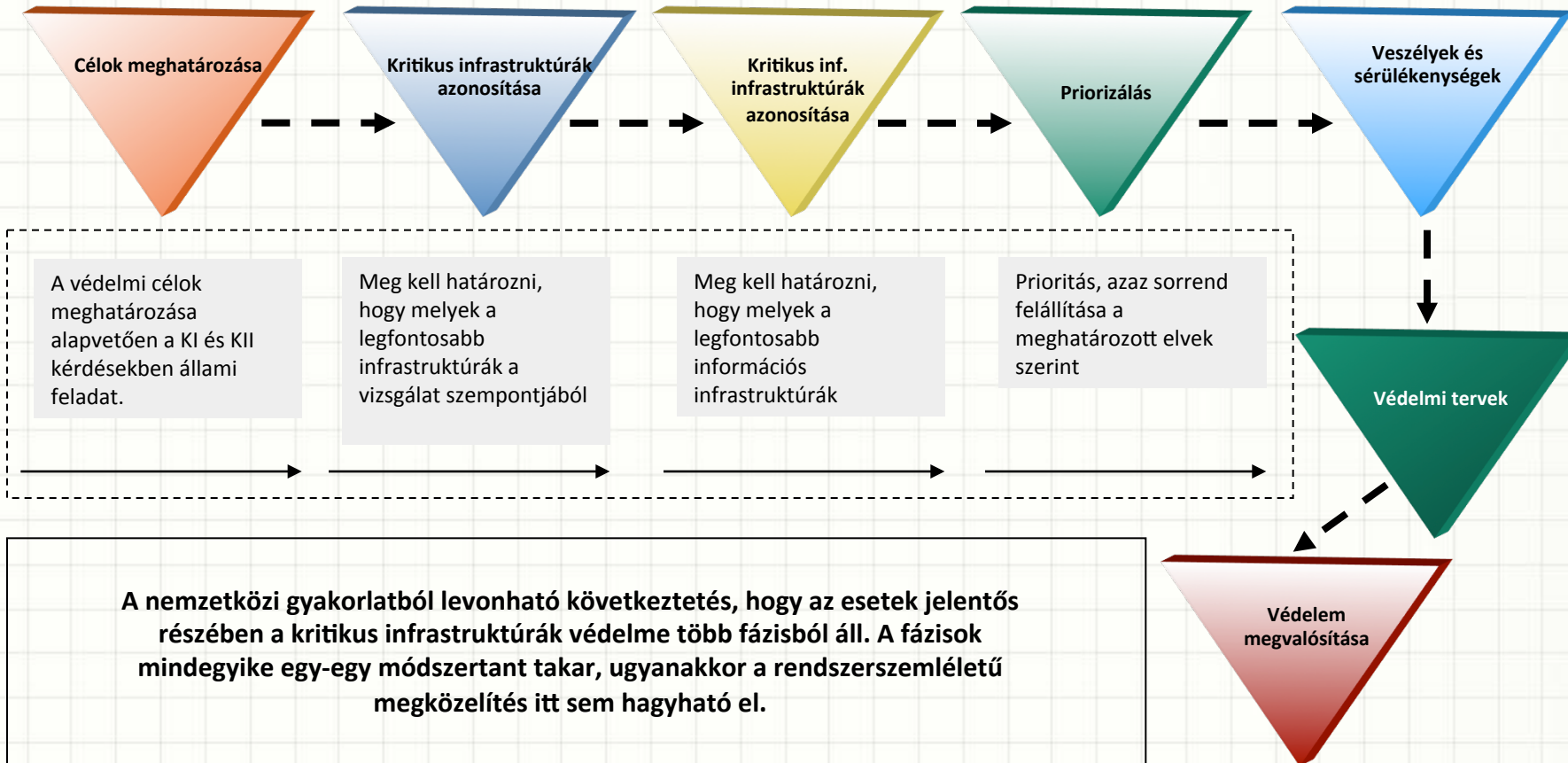
Kritikus információs infrastruktúrák közé a következők tartozhatnak:

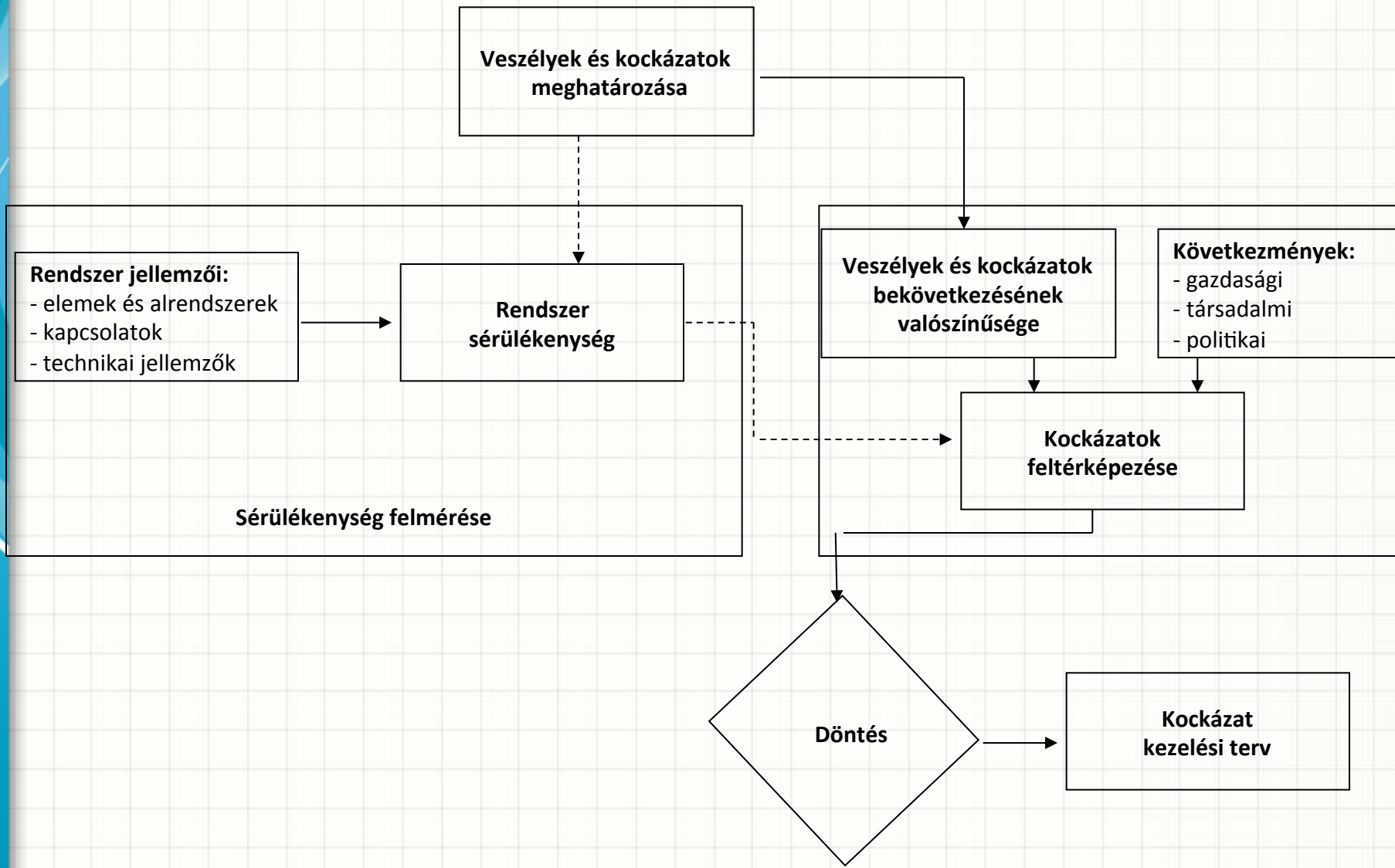
- er
- sz
- ko
- m
- kö
- há
- pé
- vé
- há
- eg
- ko

Mindezeknek
megfelelően
MAGYARORSZÁGON
is ezek a kritikus
információs
infrastruktúrák!

ító
bil,
ép-
;
ép-
tok.

KRITIKUS INFRASTRUKTÚRÁK VÉDELME





| Infrastruktúra | A kritikusságot meghatározó kritériumok | | |
|------------------------------------|---|---------------------|--------------------------------|
| | Nemzetvédelem | Gazdasági biztonság | Közegészségügy és közbiztonság |
| I. Energia | X | X | |
| II. Infokommunikációs technológiák | X | X | |
| III. Közlekedés | X | X | |
| IV. Víz | | | X |
| V. Élelmiszer | | | X |
| VI. Egészségügy | | | X |
| VII. Pénzügy | | X | |
| VIII. Ipar | | X | |
| IX. Jogrend – Kormányzat | X | | X |
| X. Közbiztonság – Védelem | X | | X |

Nemzeti szintű besorolás lehetséges szempontjai:

| besorolás: | alacsony | közepes | magas |
|------------|------------|---------|--------------------------|
| Hatókör: | kistérségi | megyei | nemzeti magasabb vagy |

Népességre gyakorolt hatás szempontjai:

| besorolás | alacsony | közepes | magas |
|--|-----------|------------|-------------|
| az érintett lakosság száma | <10.000fő | <100.000fő | >100.000 fő |
| a lehetséges áldozatok száma | <10 fő | <100 fő | >100 fő |
| a lehetséges megbetegedések, súlyos sérülések száma | <100 fő | <1.000 fő | >1.000 fő |
| az esetleges kitelepítésben érintett lakosság száma | <1.000 fő | <10.000 fő | >10.000 fő |

Jogszabályi háttér – Magyarország:

- **2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről;**
- **A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény;**
- **Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.);**
- **A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény;**
- **A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról;**
- **Digitális Megújulás Cselekvési Terv 2010-2014., Nemzeti Fejlesztési Minisztérium, Budapest, 2010;**
- **38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról.**

Jogszabályi háttér – Magyarország:

- **2080/2008. (VI.30.) Korm. határozat A Kritikus Infrastruktúra Védelem Nemzeti Programról;**
- **1249/2010. (XI. 19.) kormányhatározat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról;**
- **2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről**
- **65/2013. (III. 8.) Korm. Rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról**



- **Kibervédelmi stratégia:**

1139/2013. (III. 21.) Korm. határozat Magyarország
Nemzeti Kiberbiztonsági Stratégiájáról



Tartalomjegyzék

| | | |
|--|---|-------------|
| 82/2013. (III. 21.) Korm. rendelet | Az UNESCO által 2005. október 19-én elfogadott, a sportbeli dopping elleni nemzetközi egyezmény melléklete módosításának kihirdetéséről | 4769 |
| 83/2013. (III. 21.) Korm. rendelet | A Rendszerváltás Történetét Kutató Intézet és Archívum létrehozásáról | 4783 |
| 84/2013. (III. 21.) Korm. rendelet | Egyes szakképzési tárgyú kormányrendeletek módosításáról | 4784 |
| 85/2013. (III. 21.) Korm. rendelet | A közfoglalkoztatással összefüggő egyes kormányrendeletek módosításáról | 6171 |
| 86/2013. (III. 21.) Korm. rendelet | Az egyes talajvédelmi szakhatósági eljárásokat szabályozó kormányrendeletek módosításáról | 6172 |
| 1/2013. (III. 21.) HM rendelet | A Magyar Honvédség egyes beosztásaihoz kapcsolódó munkaköri követelményekről szóló 20/2002. (IV. 10.) HM rendelet módosításáról | 6174 |
| 11/2013. (III. 21.) NGM rendelet | A gáz csatlakozóvezetékekre, a felhasználói berendezésekre, a telephelyi vezetékekre vonatkozó műszaki biztonsági előírásokról és az ezekkel összefüggő hatósági feladatokról | 6220 |
| 18/2013. (III. 21.) VM rendelet | Egyes agrártárgyú miniszteri rendeletek módosításáról | 6324 |
| 19/2013. (III. 21.) VM rendelet | A földmérési és térképészeti tevékenység végzéséhez szükséges szakképzettségről | 6333 |
| 20/2013. (III. 21.) VM rendelet | Az arborétumok jegyzékéről szóló 19/2011. (III. 16.) VM rendelet módosításáról | 6335 |
| 151/2013. (III. 21.) KE határozat | Dandártábornok szolgálati viszonyának megszüntetéséről | 6336 |
| 1137/2013. (III. 21.) Korm. határozat | A 2015-ben megrendezésre kerülő Milánói Világkiállítás Magyarországi részvételéhez szükséges működési és finanszírozási feltételek megteremtéséről | 6336 |
| 1138/2013. (III. 21.) Korm. határozat | Az afganisztáni Nemzetközi Biztonsági Közreműködő Erők (ISAF) műveleteiben történő további magyar katonai szerepvállalásról szóló 2186/2008. (XII. 29.) Korm. határozat módosításáról | 6337 |
| 1139/2013. (III. 21.) Korm. határozat | Magyarország Nemzeti Kiberbiztonsági Stratégiájáról | 6338 |
| 1140/2013. (III. 21.) Korm. határozat | A Huawei Technologies Hungary Kft. magyarországi nagybefektetővel való stratégiai megállapodás megkötéséről | 6342 |
| 1141/2013. (III. 21.) Korm. határozat | A közfoglalkoztatással összefüggő, egyes döntést igénylő kérdésekről szóló 1044/2013. (II. 5.) Korm. határozat módosításáról | 6342 |

- **Információbiztonsági törvény:**

2013. évi L. törvény

Az állami és önkormányzati szervek elektronikus
információbiztonságáról

**233/2013. (VI. 30.) Korm. Rendelet az elektronikus információs
rendszerek kormányzati eseménykezelő központjának, ágazati
eseménykezelő központjainak, valamint a létfontosságú
rendszerek és létesítmények eseménykezelő központja feladat-
és hatásköréről**

Elektronikus információs rendszer

1. § (2) E törvény alkalmazásában elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese

Forrás: Muha Lajos

Elektronikus információs rendszer

- a) számítástechnikai rendszerek és hálózatok;
- b) helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;
- c) rádiós vagy műholdas navigáció;
- d) automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek, stb.);
- e) a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

Jogszabályi háttér – EU:

2005. Zöld Könyv a kritikus infrastruktúra védelemről

2009. Kritikus Információs Infrastruktúra Védelme (COM(2009)149)

2010. Digitális Menetrend (Európa 2020 Stratégia része)

2010. Közlemény az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítésére és modernizálására vonatkozóan.

2011. Közlemény a kritikus informatikai infrastruktúrák védelméről: „Eredmények és következő lépések: a globális kiberbiztonság felé” (COM(2011) 163)



Jogszabályi háttér – EU:

Eredmények és következő lépések: a globális kiberbiztonság felé:

- CERT-ek létrehozása 2012-ig a fennmaradó tagállamokban és EU-intézményekben;
- 2012-ig európai készenléti terv elkészítése kiberbiztonsági incidensek esetére a hasonló tárgyú nemzeti készenléti tervek alapján;
- kiberbiztonsági gyakorlatok rendszeres szervezése nemzeti (ezt eddig csak 12 tagállam tette meg) és páneurópai szinten, mint például a 2010. évi „Cyber Europe” gyakorlat;
- globálisan elfogadott alapelvek érvényre juttatása az internet stabilitása és ellenálló képessége érdekében;
- stratégiai partnerségek létrehozása a kulcsfontosságú nem uniós országokkal (különösen az USA-val), valamint a nemzetközi fórumokon, például a G8-ak keretében folytatott eszmecsere előmozdítása;
- a globális hatást gyakorló, feljövőben levő technológiákra, mint például a számítási felhőkre vonatkozó szabályozási stratégiák kidolgozása.

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek

KRITIKUS INFRASTRUKTÚRA FIGYELMEZTETŐ INFORMÁCIÓS RENDSZER (CRITICAL INFRASTRUCTURE WARNING INFORMATION NETWORK — CIWIN)

- **Az EU rendszere (EPCIP - „Zöld Könyv”);**
- **A CIWIN egyfajta fórum, amelyen a kritikus infrastruktúra védelemmel kapcsolatos ötleteket és legjobb gyakorlatot cserélik ki egymással a kritikus infrastruktúra tulajdonosok és üzemeltetők;**
- **A CIWIN egy gyorsriasztási rendszer (Rapid Aware System — RAS), amely összeköti a tagállamokat a Bizottsággal**

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek

Európai Hálózati és Informatikai Biztonság Ügynökség (European Network and Information Security Agency — ENISA)

- 2004 márciusában jött létre;
- Célja: megteremteni és növelni, valamint koordinálni a közös európai biztonsági lépéseket a hálózat és az inf. bizt. területén;
- További feladata, hogy egy együttműködési keretet hozzon létre a hálózati és az informatikai biztonság fejlesztésére;
- Együttműködik az Európai Bizottsággal, a tagállamokkal, és a piaci élet szereplőivel, hogy meghatározza azokat a hálózati és informatikai biztonsági követelményeket, amelyek az EU hatáskörébe tartoznak vagy a jövőben, oda tartozhatnak;
- Könyvtárat hozott létre *Ki kicsoda a hálózati és informatikai biztonság területén* (Who is Who Directory on Network and Information Security);
- Hírlevél a CERT-ek tevékenységeiről (Inventory of CERT Activities in Europe).

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek

International Watch and Warning Network (IWWN)

Tagja a 14 legfejlettebb gazdasággal rendelkező állam (pl. USA, Japán, Német-ország, Hollandia, stb.), valamint Magyarország. A szervezet célja, hogy minden tagországból közös fórumot biztosítson a nemzetgazdaságot érintő kockázatok kezelésben a jogszabályalkotóknak (Policy Makers), a kormányzati CERT szervezeteknek (governmental CERTs), valamint a büntetőszervezeteknek (Law Enforcement).

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek

TF-CSIRT

A TF-CSIRT az Európában működő CERT szervezetek közös szervezete, aminek célja a CERT szervezetek közötti információcsere hatékony biztosítása, valamint a globális fenyegetésekkel szembeni közös fellépés elősegítése.

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek

Forum of Incident Response Teams (FIRST)

A FIRST a CERT szervezetek világszervezete, aminek célja a CERT szervezetek együttműködésének elősegítése globális szinten, valamint a globális fenyegetésekkel szembeni közös fellépés erősítése.

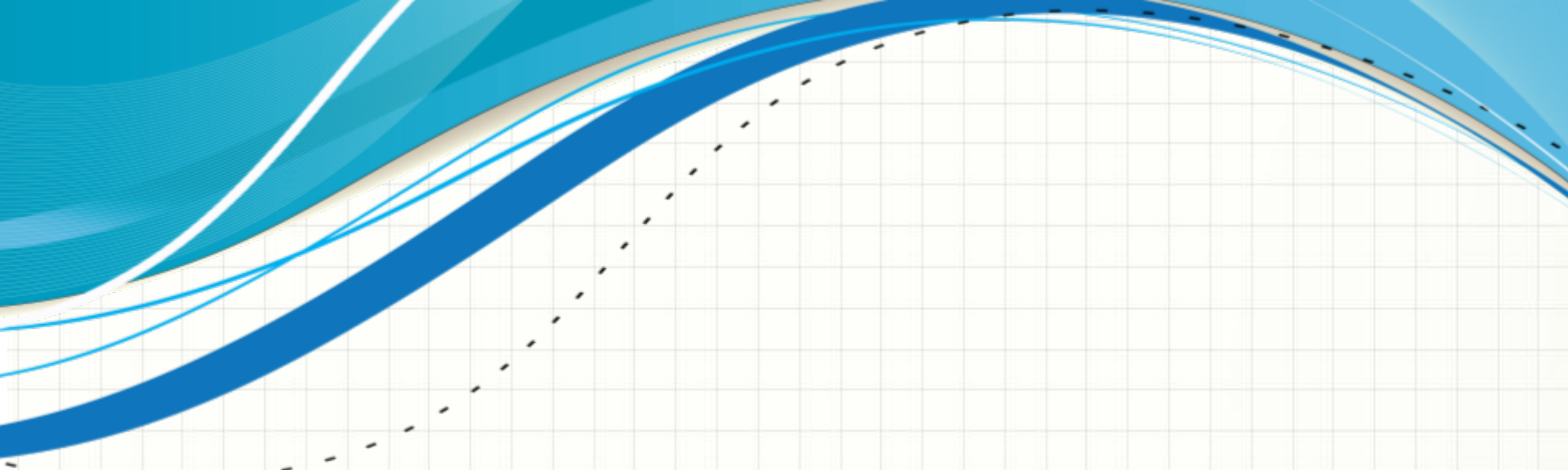
A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek

European Governmental CERTs (EGC)

Az EGC szervezet a vezető európai uniós államok kormányzati CERT szervezeteinek szoros együttműködését tűzte ki célul, és jelenleg hét tagja van (pl. Németország, Franciaország, Finnország, Hollandia).



KÖSZÖNÖM A FIGYELMET!



Prof. Dr. Kovács László
Nemzeti Közszolgálati Egyetem
Informatikai és Elektronikai Hadviselés Tanszék
egyetemi tanár

Posta: 1581 Budapest, Pf.: 15.

Telefon: +36-1-432-9000

E-mail: kovacs.laszlo@uni-nke.hu