Magyarország kiberbiztonsága stratégiai szinten

Rajnai Zoltán
Magyarország kiberkoordinátora

Áttekintés:
259/2021. (V. 20.) Korm. Rendelet 26-29. §

- ***Nemzeti Kiberbiztonsági Koordinációs Tanács***

- **a belügyminiszter,**
- **a honvédelmi miniszter,**
- **az igazságügyi miniszter,**
- **a külgazdasági és külügyminiszter,**
- **a földművelésügyi miniszter,**
- **a technológiai és ipari miniszter,**
- **kulturális és innovációs miniszter,**
- **miniszterelnökséget vezető miniszter**
- **pénzügyminiszter,**
- **akadémiai szektor,**
- **a kiberkoordinátor**

Inter-miniszteriális szerepvállalás

Össztársadalmi funkciórendszer

KOORDINÁCIÓ

<u>A Tanács munkáját segíti:</u>

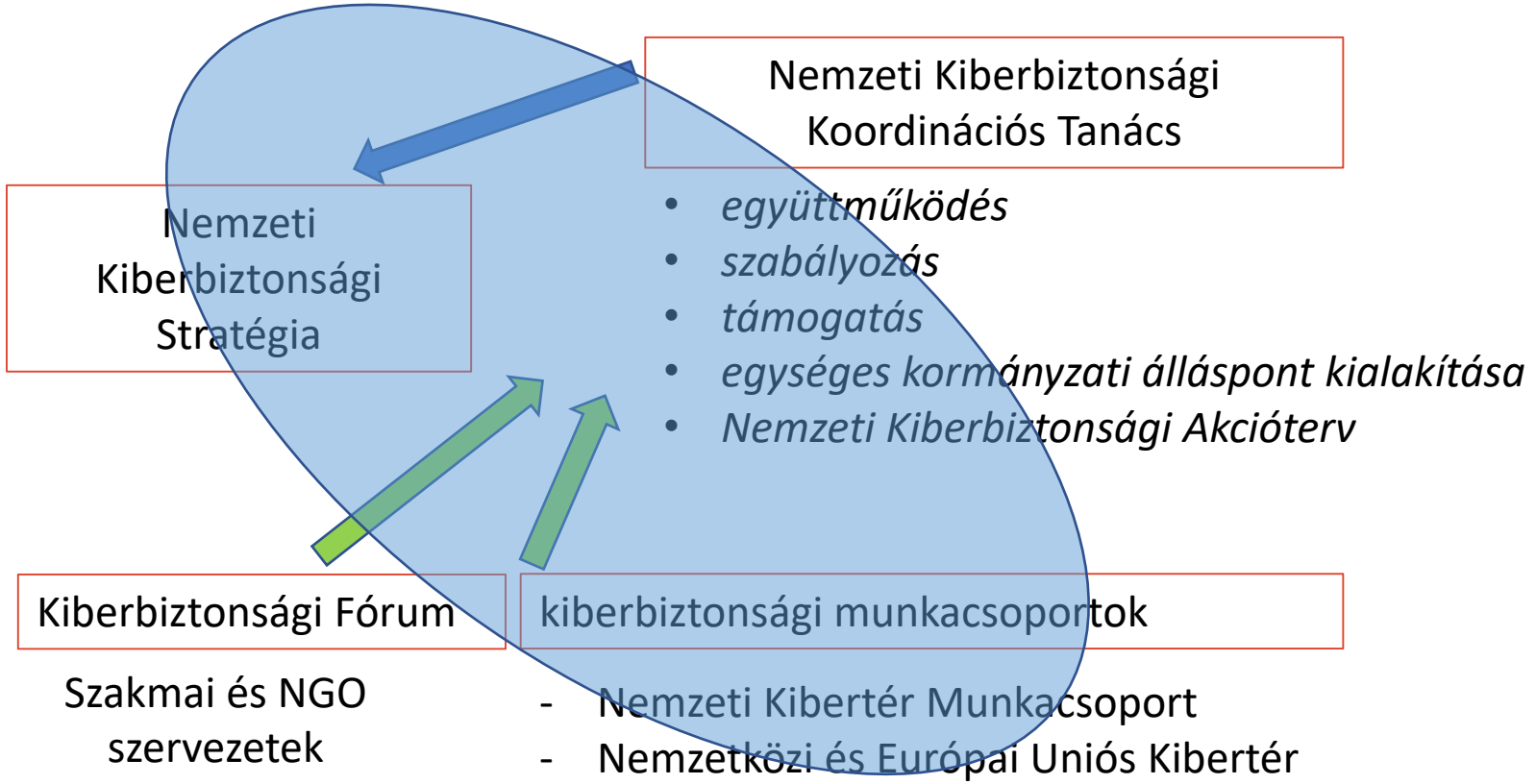
- az Állami Számvevőszék elnöke,
- a Magyar Nemzeti Bank elnöke,
- a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke,
- a Nemzeti Hírközlési és Informatikai Tanács elnöke,
- a Nemzeti Média- és Hírközlési Hatóság elnöke,
- a Magyar Energetikai és Közmű-szabályozási Hivatal elnöke vagy az általa delegált

Áttekintés: 2013-2022

- ***Kiberbiztonsági Fórum***

- ***A Tanács által felkért egyetemi, kutatói, szakmai, gazdasági és más nem kormányzati szereplőkből álló Kiberbiztonsági Fórum vezetését a Tanács elnöke, a Fórum munkájának szakmai koordinálását a kiberkoordinátor látja el.***

Áttekintés

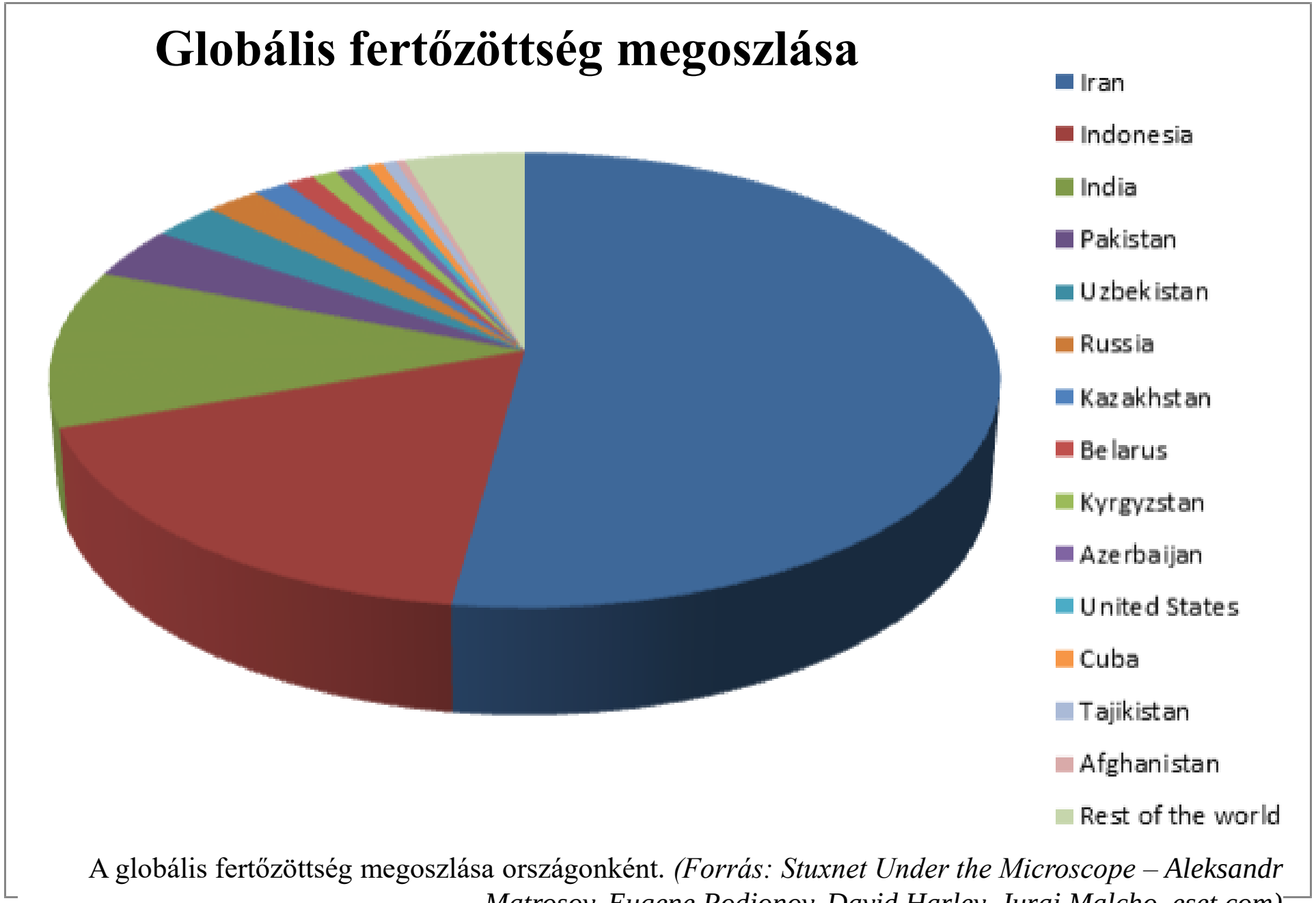

Nemzeti Kiberbiztonsági Koordinációs Tanács
Nemzeti Kiberbiztonsági Stratégia
• együttműködés
• szabályozás
• támogatás
• egységes kormányzati álláspont kialakítása
• Nemzeti Kiberbiztonsági Akcióterv
Kiberbiztonsági Fórum
kiberbiztonsági munkacsoportok
Szakmai és NGO szervezetek
- Nemzeti Kibertér Munkacsoport
- Nemzetközi és Európai Uniós Kibertér Munkacsoport

Ki végzi a stratégiai kiberbiztonság feladatait? (Visszatekintés)

Ki végzi a stratégiai kiberbiztonság feladatait? (Visszatekintés)

2010. november 16-án Irán leállította az urándúsítóit, miután a centrifugák több mint 20%-a megsemmisült a Stuxnet tevékenysége nyomán.

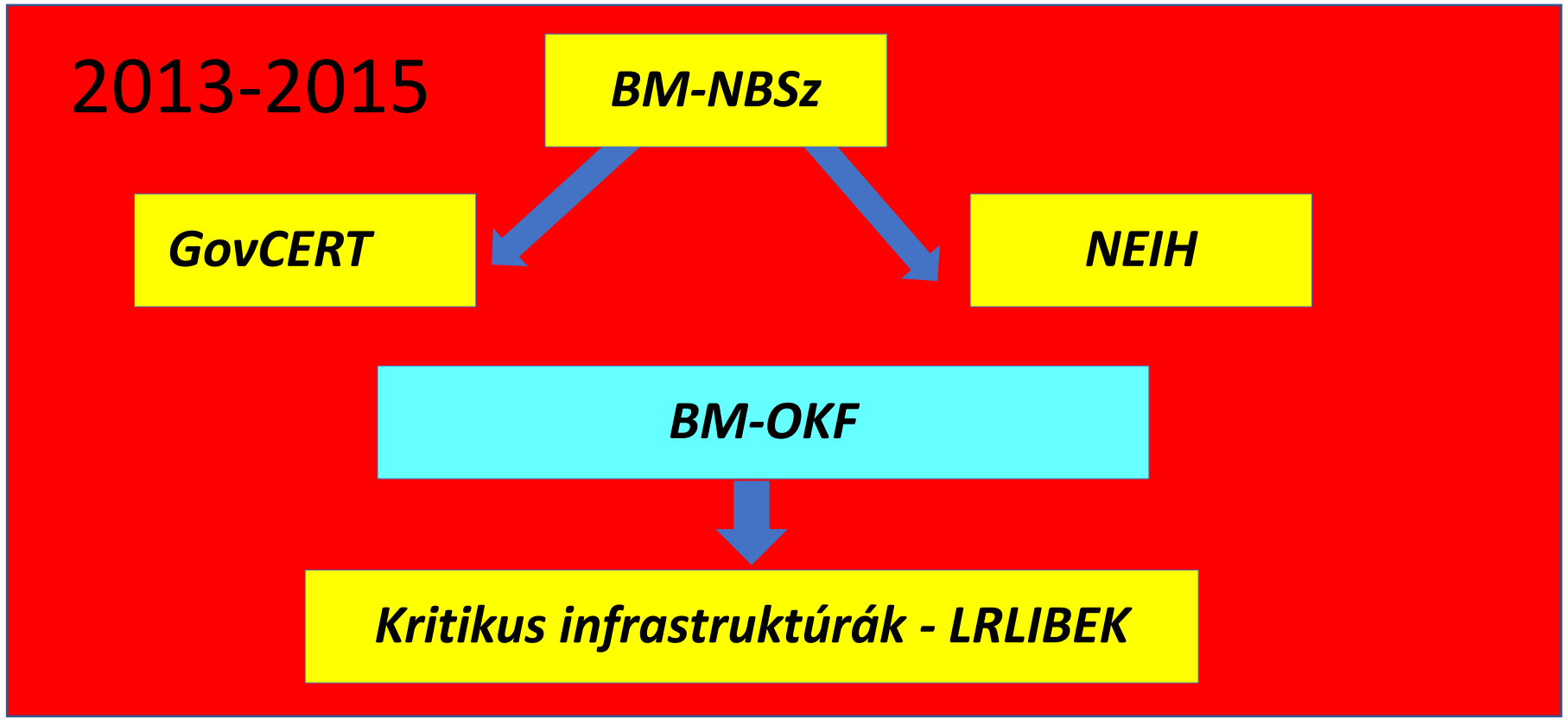
Szakértők szerint az amerikai és az izraeli kormány megrendelésére készült vírus, az iráni Natanz-i atomerőmű urándúsító centrifugáinak tönkretételével szakemberek szerint legalább egy-két évvel sikerült visszavetni az ország atomprogramját. Az amerikaiak és az izraeliek hivatalosan sosem ismerték el, hogy ők állnának a Stuxnet mögött, de független szakértők egybehangzó véleménye szerint ez többszörösen bizonyított tény.

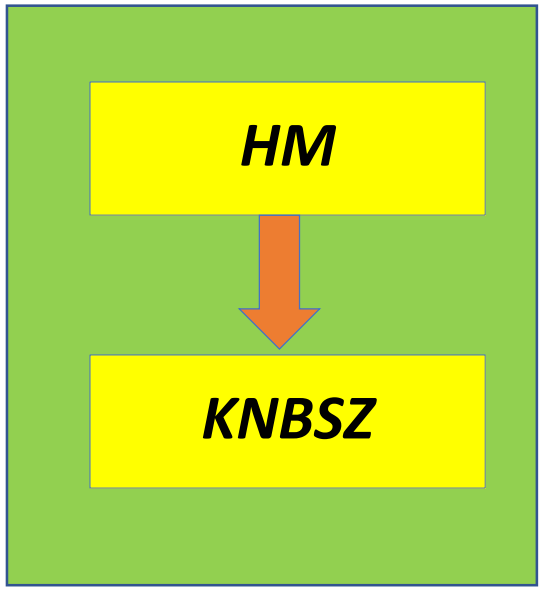


A globális fertőzöttség megoszlása országonként. *(Forrás: Stuxnet Under the Microscope – Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho, eset.com)*

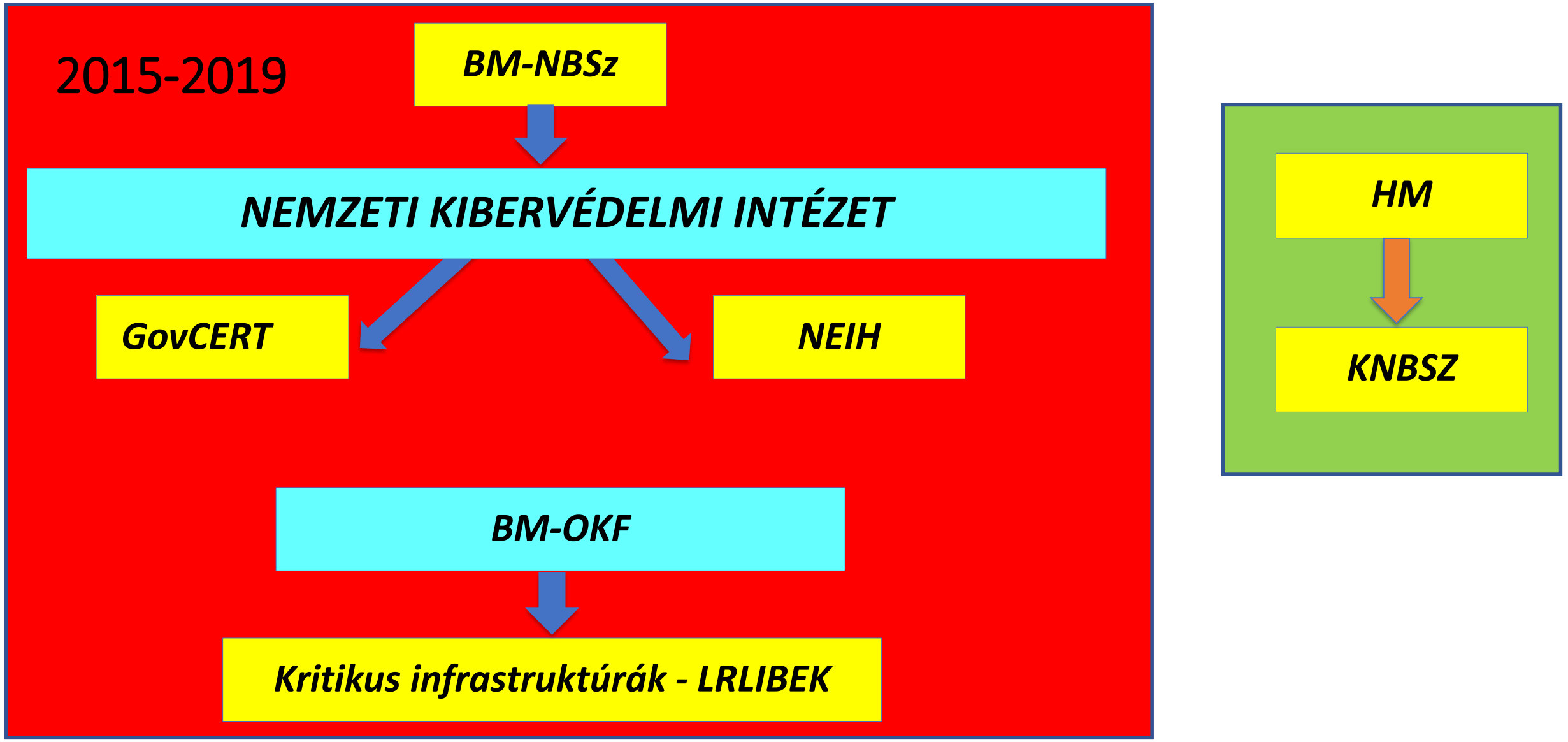
Ki végzi a stratégiai kiberbiztonság feladatait? (Visszatekintés)

Puskás Tivadar Közalapítvány (2010-2013)

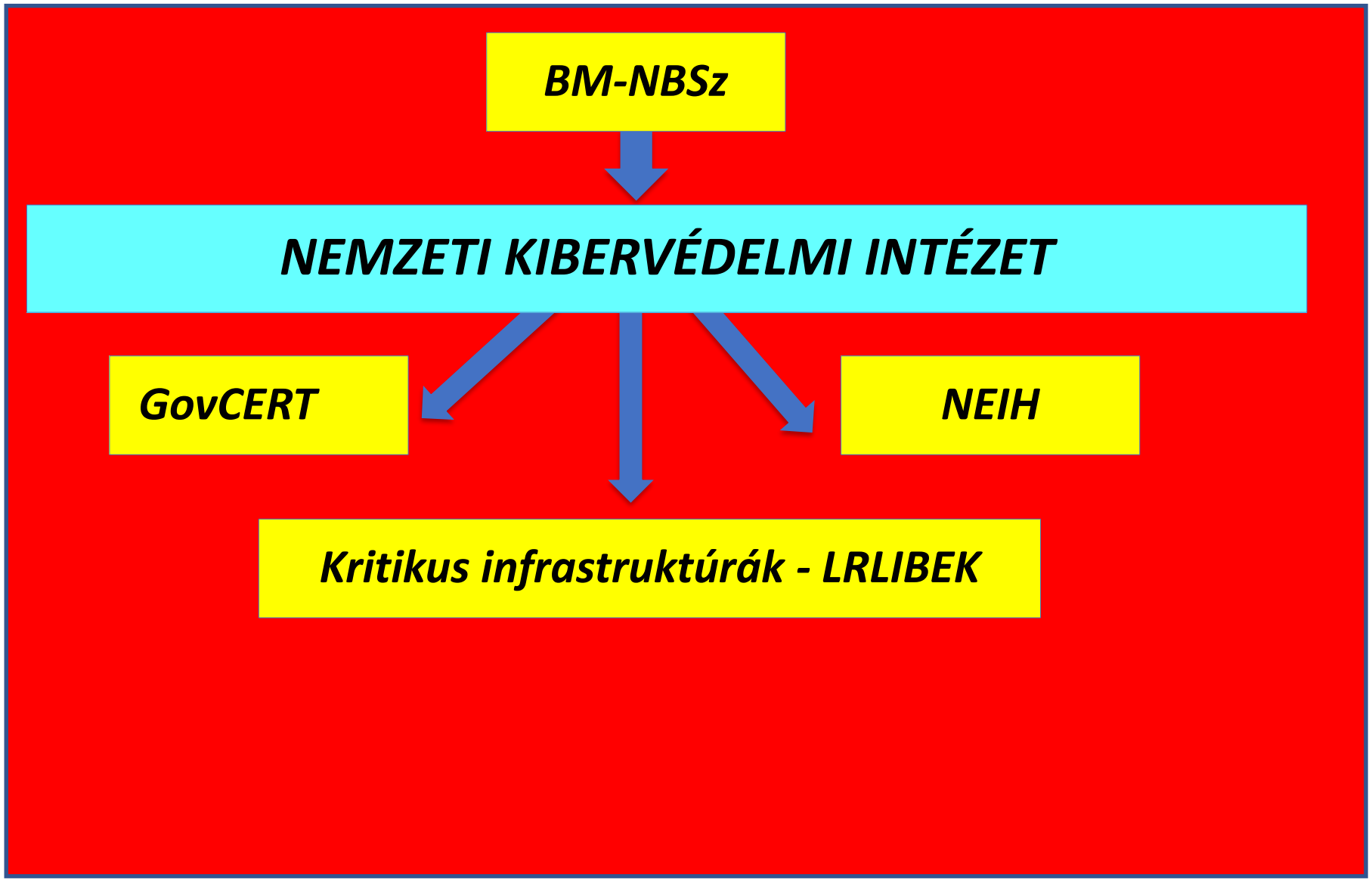


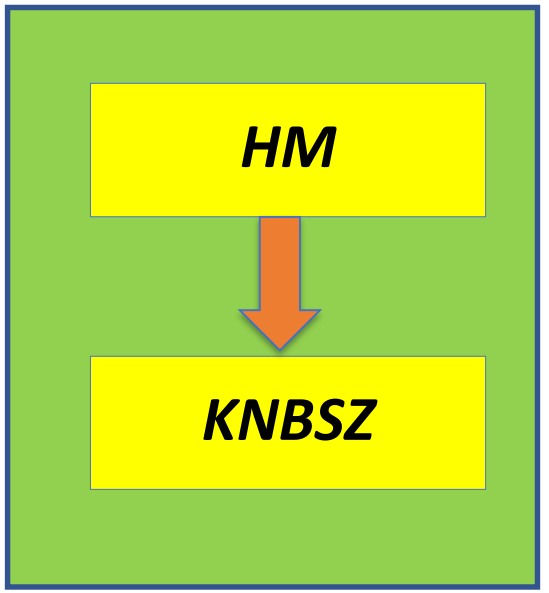


KIBERVÉDELEM SZERVEZETEI



KIBERVÉDELEM SZERVEZETEI (2019-2022)





KIBERVÉDELEM SZERVEZETEI (2022-)

Kiberbiztonsági stratégia 2013-2022

2013.: Magyarország Nemzeti Kiberbiztonsági Stratégiája

- ***először határozta meg*** a globális kibertér részeként a magyar kibertér gazdasági és társadalmi életben betöltött meghatározó szerepét.
- A stratégia mentén, a kibertérből érkező fenyegetések és az ezzel járó kockázatok tudatában ***megkezdődött a magyar jogi szabályozás előkészítése*** kormányzati, piaci és társadalmi szereplők összefogásával.
- ***2013. évi L. törvény*** megteremtette azt a jogszabályi környezetet, amely elsősorban az állami, közigazgatási elektronikus információs rendszerek tekintetében ***elősegítette a kiberbiztonság területén működő állami szervezetek kialakítását és megszilárdítását***.

2018: Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiája

Az új stratégia célja, hogy **a *Nemzeti Kiberbiztonsági Stratégiában* megfogalmazott értékeket megtartva, annak eredményeire építve, de az *új kihívásokra, fenyegetésekre reagálva***, az új lehetőségek és célok azonosításával kell erősíteni a hálózati és információs rendszerek védelmét annak érdekében, hogy az ***minden tekintetben megfeleljen a modern kor kihívásainak***.

Alapvető nemzeti érdek a megfelelő ***kibervédekezési, elhárítási és reagálási*** képességek koncentrált rendelkezésre állásának biztosítása. ***"A cél a meglévő bázison a kiber-védekező, elhárító és reagáló képességek passzív és aktív eszközeinek széleskörű kialakítása és alkalmazása."***

INTÉZKEDÉSI TERV 2020-2022

Digitális környezet iránti bizalom erősítése

- Biztonságtudatosság növelése
- Bűnüldözés - kiber-bűnüldözés fejlesztése
- A szakmai irányító intézményrendszer fejlesztése

Digitális infrastruktúra védelem

- Informatikai fejlesztések minőség-menedzsmentje
- Kormányzati elektronikus szolgáltatások biztonságának növelése
- Nemzetközi együttműködés erősítése
- Alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme
- Kiber- védekező elhárító és reagáló képességek fejlesztése

A gazdasági szereplők támogatása

- Kutatóközpontokkal való együttműködés, valamint a kutatás és fejlesztés szerepének erősítése
- Hazai digitális innováció támogatása
- Versenyképes hazai tudásbázis létrehozása

IoT kihívások

Még okosabb bögre segít, hogy ne hűljön ki a forró ital

Itt az ideje, hogy a függöny is okos legyen

Már tolmácsolásra is bevethető az okosszemüveg

Ha akarjuk, ha nem, behálózza életünket az IoT

5G-technológia: mikorra várható az áttörés?

IoT kihívások

digitalizációra és okos gazdákra van szükség

Ha akarjuk, ha nem, behálózza életünket az IoT

Telemedicina

Szoftverhiba vezetett az önvezető Uber halálos balesetéhez

Újabb lépést tesz a teljes önvezetés felé a Tesla

Okoskukák és szenzorok: IoT a hulladék-gazdálkodásban

Fenyegetések:

- megzavarják az információs és kommunikációs rendszerek
- kormányzati gerinchálózatok rendeltetésszerű működését
- veszélyeztetik a nemzetállamok információs vagyonát és a kritikus infrastruktúra elemeit
- nagyszabású kibertámadások egyre gyakoribbak
- nő a kiberfenyegetések komplexitása és volumene
- különféle csoportok, szervezetek is egyre intenzívebb módon használják fel a kiberteret ideológiák terjesztésére

kiberbűnözés fő célja:

- a károkozás,
- a pénzügyi és
- a személyes adatok tömeges megszerzése, illetve
- a gazdasági, pénzügyi, politikai befolyásolás.

Az adatlopáson túl elterjedt az elektronikus szolgáltatások ***károkozási célú megbénítása***, illetve kéretlen levelek és kártékony kódok terjesztése, robothálózatok…

1.kérdés:

Melyik kibertámadási forma a leghatékonyabb (sérülékenység szempontjából)?

Lehetséges válaszok:

1. Zsarolóvírus
2. Kéretlen üzenetekben banki adatok „halászata”
3. E-mail üzenetekben vírus- és kémprogram terjesztés

Jelentős fenyegetés a hacktivizmus, amely gyakran ideológiai motivációjú támadásokat takar

növekvő veszélyt jelentenek a kiberkémkedési célú kifinomult, rejtett támadások, melyek mögött feltételezhetően állami „szponzoráció”, támogatás áll.

A fő veszélyt a rendkívül szofisztikált támadások jelentik, amelynek keretében a támadók hosszú időn át elrejtve tudják végezni a károkozó tevékenységüket (információszivárogtatás, rombolás, kémkedés, stb.)

HELYZETÉRTÉKELÉS

EU-ban vállalkozás 98%-a használ számítógépeket és közülük csak 32% formális IB politikával.
Nagyvállalatok esetében ~ 72%, KKV-k esetében > ~31%

Mo-on nagyvállalatok esetében 53 %, KKV-k esetében ~ 9%
(Forrás: EUSTAT)

Hazai építőipari szektorban átlagosan 3%, az IT szektorban is csak ~36% van IB szabályzat

EU átlagban ~20%-a gondoskodik védelemről az adatok megsemmisülésével vagy sérülésével járó biztonsági esemény bekövetkezte esetére, Mo-on: ~10%

2. Kérdés

Milyen arányban nőtt Magyarországon az **Információs rendszer felhasználásával elkövetett csalás?**

Lehetséges válaszok:

1.megduplázódott
2.megtízszereződött
3.15-20 szorosára

2015-2019

Kizárólag információs rendszereket érintő cselekmények	3554	2398	2819	4187	5098
Információs rendszer felhasználásával elkövetett csalás	250	1398	2176	3409	4467

Új elem a stratégiában
Védelempolitika: elhárító- és reagáló-képesség

Képesség más államok informatikai hírszerző és egyéb hibrid tevékenységének megelőzése, felderítése, elhárítása terén a hazai polgári és katonai nemzetbiztonsági szervek rendszerében

hálózatalapú védelmi képesség fejlesztése

megelőző védelmet szolgáló specifikus elhárító- és reagálóképesség megteremtése, szabályozási és szervezeti keretek

kibervédelmi képesség kialakítása:

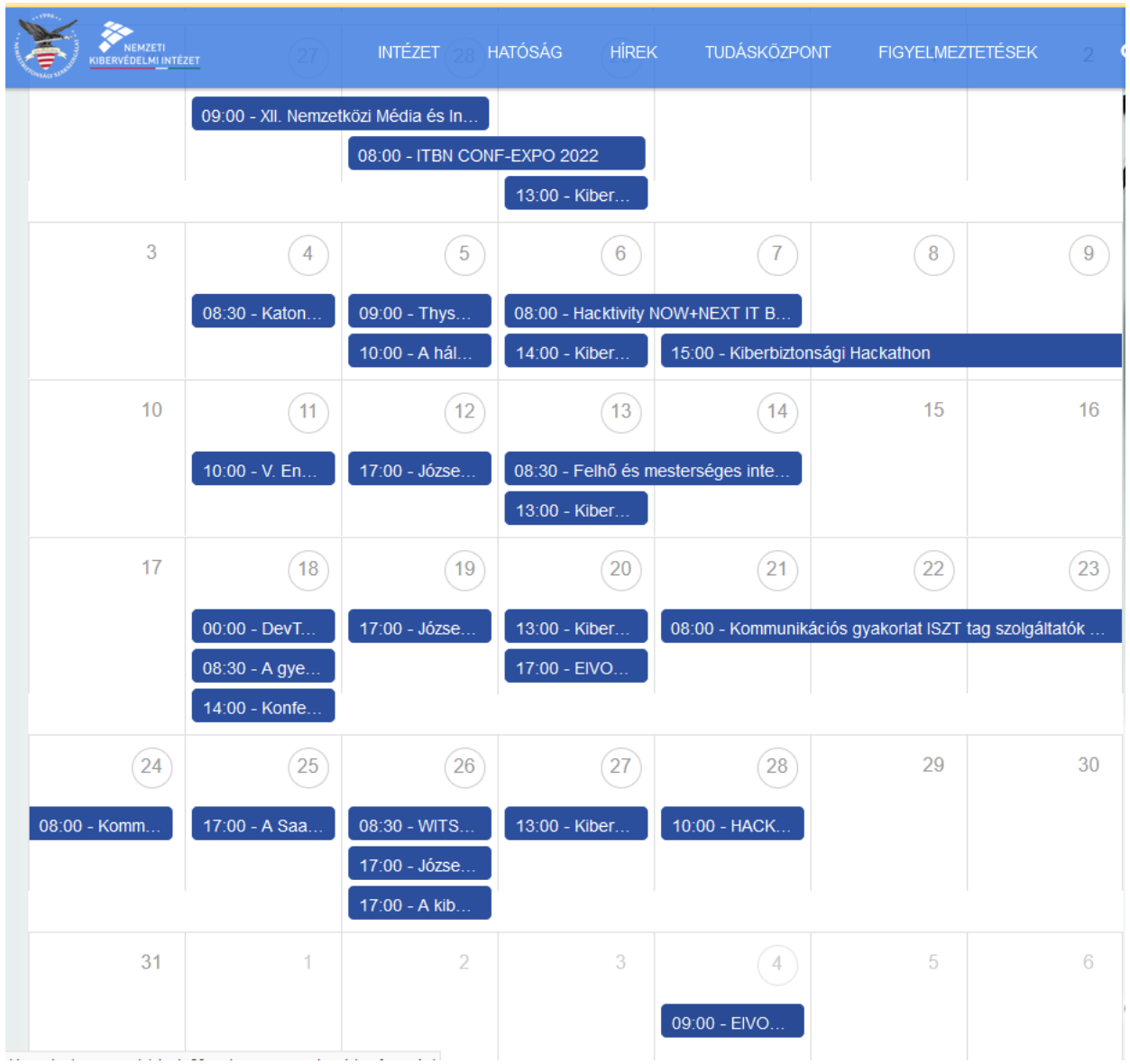
- Azonosítás
- Védekezés
- Észlelés
- Válaszadás
- Helyreállítás területein

ECSM

- **30 esemény**
- **Podcast-ok**

“Think Before U Click !”
“Gondolkodj, mielőtt kattintasz!”

ZSAROLÓVÍRUSOK ÉS ADATHALÁSZAT



Gondolkodj, mielőtt kattintasz!

Köszönöm a figyelmet!