



KIBERVÉDELMI FELADATOK A HONVÉDELEMBEN

Dr. Kovács László dandártábornok

kovacs.laszlo@uni-nke.hu



Prof. Dr. Kovács László dandártábornok

Magyar Honvédség

Kiberműveleti Parancsnokság

Parancsnokság

kovacs.laszlo4@hm.gov.hu



Prof. Dr. Kovács László dandártábornok

Nemzeti Közszolgálati Egyetem

Hadtudományi és Honvédtisztképző Kar

egyetemi tanár

kovacs.laszlo@uni-nke.hu

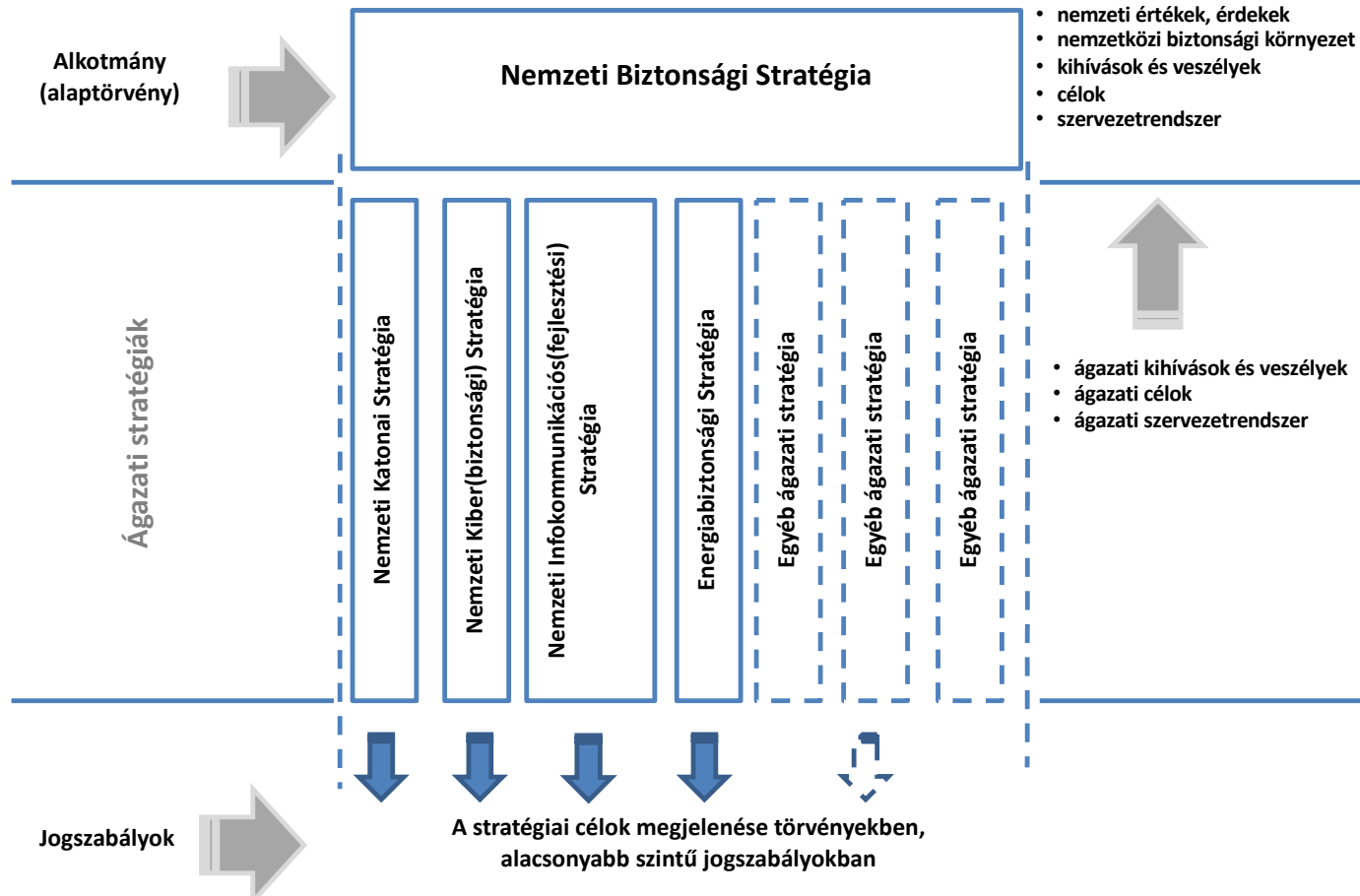


Tartalom

- Stratégiai – jogszabályi meghatározottság
- Kibervédelem – Kiberműveletek – Információs műveletek
- Hazai kibervédelem felépítése
- Katonai kibervédelem és kiberműveletek
- Háború: tapasztalatok
- Következtetések



Biztonsági dokumentumok rendszere





Új Nemzeti Biztonsági Stratégia (2020)

- 101. pont: „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, **alkalmazásukat fegyveres agresszióknak tekinti**, amelyre a fizikai térben megvalósuló válaszadás is lehetséges.”
- 135. pont: „**A haderőt úgy kell fejleszteni**, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a **kibertérben** egyaránt.”
- 159. pont: „A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a **haderő kinetikus műveleteinek kibertérbeli támogatására**, ki kell alakítani a kiberműveletekben alkalmazható **offenzív képességeket**.”



Új Nemzeti Katonai Stratégia (2021)

1. A 21. SZÁZAD MŰVELETI KÖRNYEZETE

Egy potenciális európai hadszíntéren vívott háború során szerepet kaphatnak, illetve célponttá is válhatnak Magyarország kommunikációs és közlekedési infrastruktúrái, valamint más létfontosságú rendszerlemei, emiatt az ország teljes területe, légtere és **kibertere** katonai műveletek színtere lehet. A modern konfliktusoknak a legtöbb esetben **kiberbiztonsági** összetevője is van. A **kibertérben végzett műveletek** szolgálhatnak a kinetikus műveletek előkészítésére, kísérésére vagy helyettesítésére, ugyanakkor önálló célok mentén is alkalmazhatók.

2. A MAGYAR HONVÉDSÉG SZEREPVÁLLALÁSÁT IGÉNYLŐ FENYEGETÉSEK ÉS KIHÍVÁSOK

Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes **kiberképességeket fegyvernek, alkalmazásukat pedig akár fegyveres támadásnak tekinti**, amelyre adott esetben katonai válaszadás is lehetséges.



Új Nemzeti Katonai Stratégia (2021)

5.1. A MAGYAR HONVÉDSÉG

A **katonai kibertérműveleti erők** a **kibertérben** végrehajtott műveleteikkel, beleértve az **offenzív műveleteket is**, hozzájárulnak a szárazföldi erők és a légi erők kinetikus műveleteinek hatékonyságához. Békében aktívan közreműködnek a nemzeti kibervédelmi feladatokban, valamint felkészülnek a különleges jogrendi helyzetben történő feladatvégrehajtásra.

5.1.2. Harc- és harctámogató képességek

A kialakításra kerülő és folyamatosan fejlesztett **katonai kibertér műveleti képességek** biztosítani fogják a kibertérből érkező katonai jelentőségű fenyegetések és veszélyek azonosítását, hatékony kezelését, illetve az azokkal kapcsolatos válaszlépések és ellenintézkedések végrehajtását. Ezek a képességek támogatják a szárazföldi erők, a légi erők és a különleges műveleti erők kinetikus képességeit, valamint aktívan **hozzájárulnak Magyarország kiberbiztonságához.**



Új Honvédelmi törvény (2022.11.01)

2. Értelmező rendelkezések

3. § E törvény és a honvédelmi jogszabályok alkalmazásában

24. *műveleti terület*: a műveleti tervben meghatározott és kijelölt földrajzi terület és a felette levő légtér, továbbá a **kibertér**,



NATO 2016: A 4. műveleti tér (Domain of Operations)

“ Now, in Warsaw, we reaffirm NATO's defensive mandate, and **recognise cyberspace as a domain of operations** in which NATO must defend itself as effectively as it does in the air, on land, and at sea.





Új Honvédelmi törvény (2022.11.01.)

48. A katonai kibertér műveletekre vonatkozó különös szabályok

- kibervédelmi feladatokat;
- kibertéri támadások megszakítását;
- kiberműveleti fellépést.



Kiberbiztonság

“ „A kibertérben létező **kockázatok kezelésére** alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és **tervszerű alkalmazása**, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteget megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez.”



Kibertér műveletek

“ **Kibertér műveletek:** a kibertérben vagy azon keresztül olyan tevékenységek együttese, amelyek célja, hogy a **saját kibertéri és valós téri cselekvési szabadságát megőrizzék** és/vagy olyan hatásokat hozzanak létre, amelyek **hozzájárulnak a saját (műveleti) célok eléréséhez.**



A kiberműveletek felosztása (NATO)

KIBERMŰVELETEK

- IT infrastruktúra kialakítása;
- védelmi kiberműveletek;
- kibertéri felderítés;
- támadó kiberműveletek.



Információs műveletek

“ „Az információs környezetben
érvényesülő információs képességek
integrált, összehangolt és
koordinált alkalmazása ...”

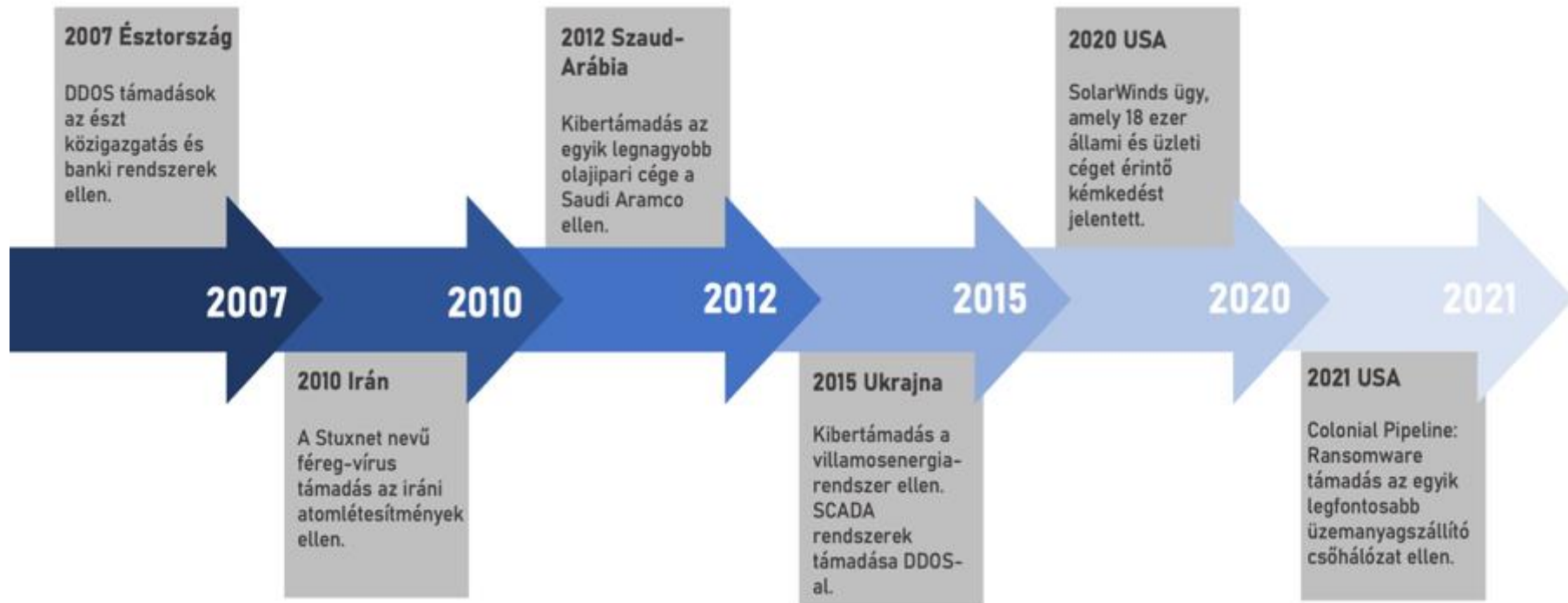


Az információs műveletek elemei

- **kiberműveletek**
(korábbi terminológiával számítógép-hálózati műveletek)
- elektronikai hadviselés
(Electronic Warfare, EW)
- lélektani műveletek
(Psychological Operations, PSYOPS)
- civil-katonai együttműködés
(Civil Military Co-Operation, CIMIC)
- katonai tájékoztatás
(Military Public Affairs, MPA)
- műveleti biztonság
(Operations Security, OPSEC)
- katonai megtévesztés
(Military Deception, MILDEC)
- megjelenés, viselkedés, arculat
(Present, Posture, Profile, PPP)
- kapcsolattartás

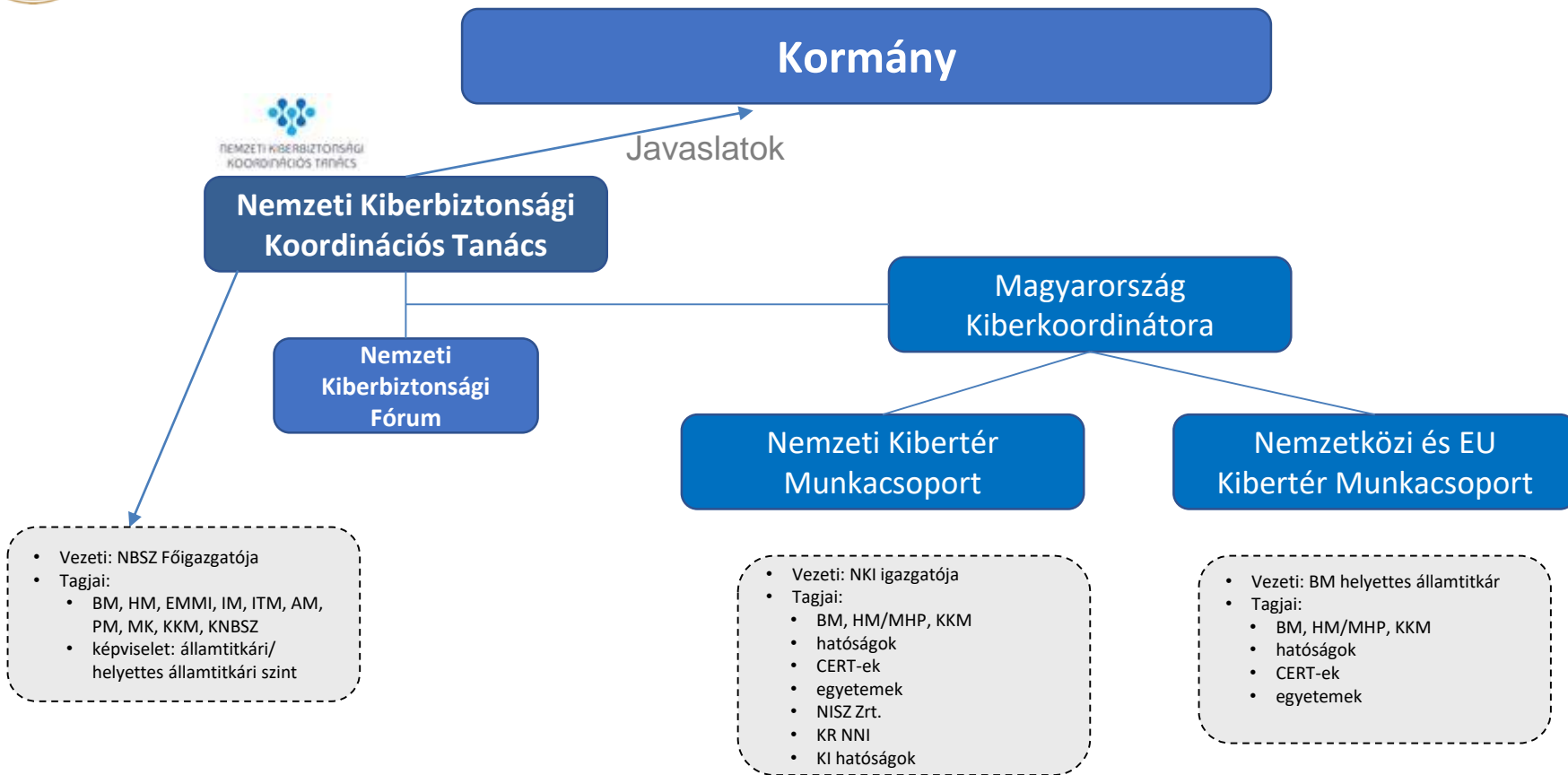


Kibertámadások



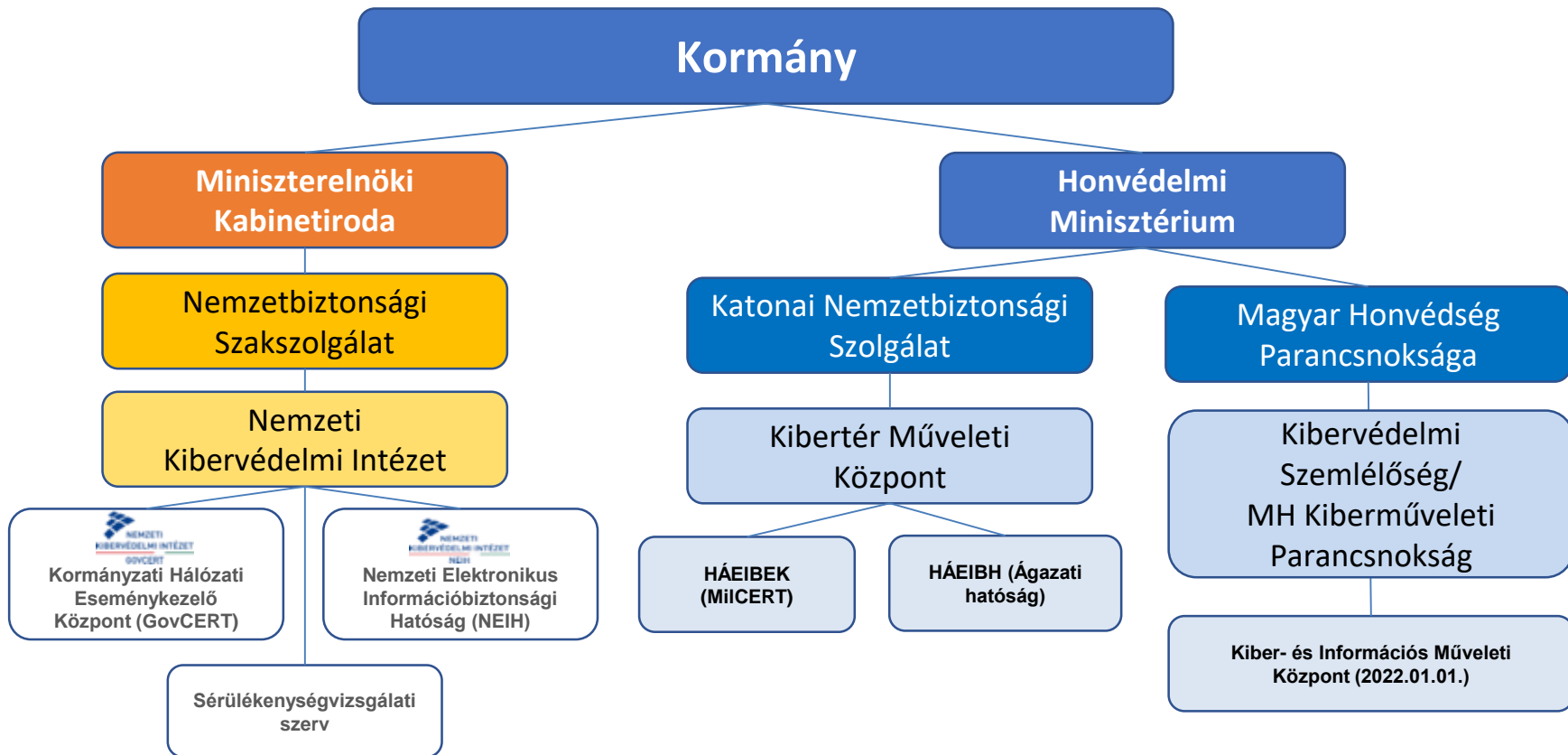


Magyarország: kibervédelmi szervezeti keretrendszer



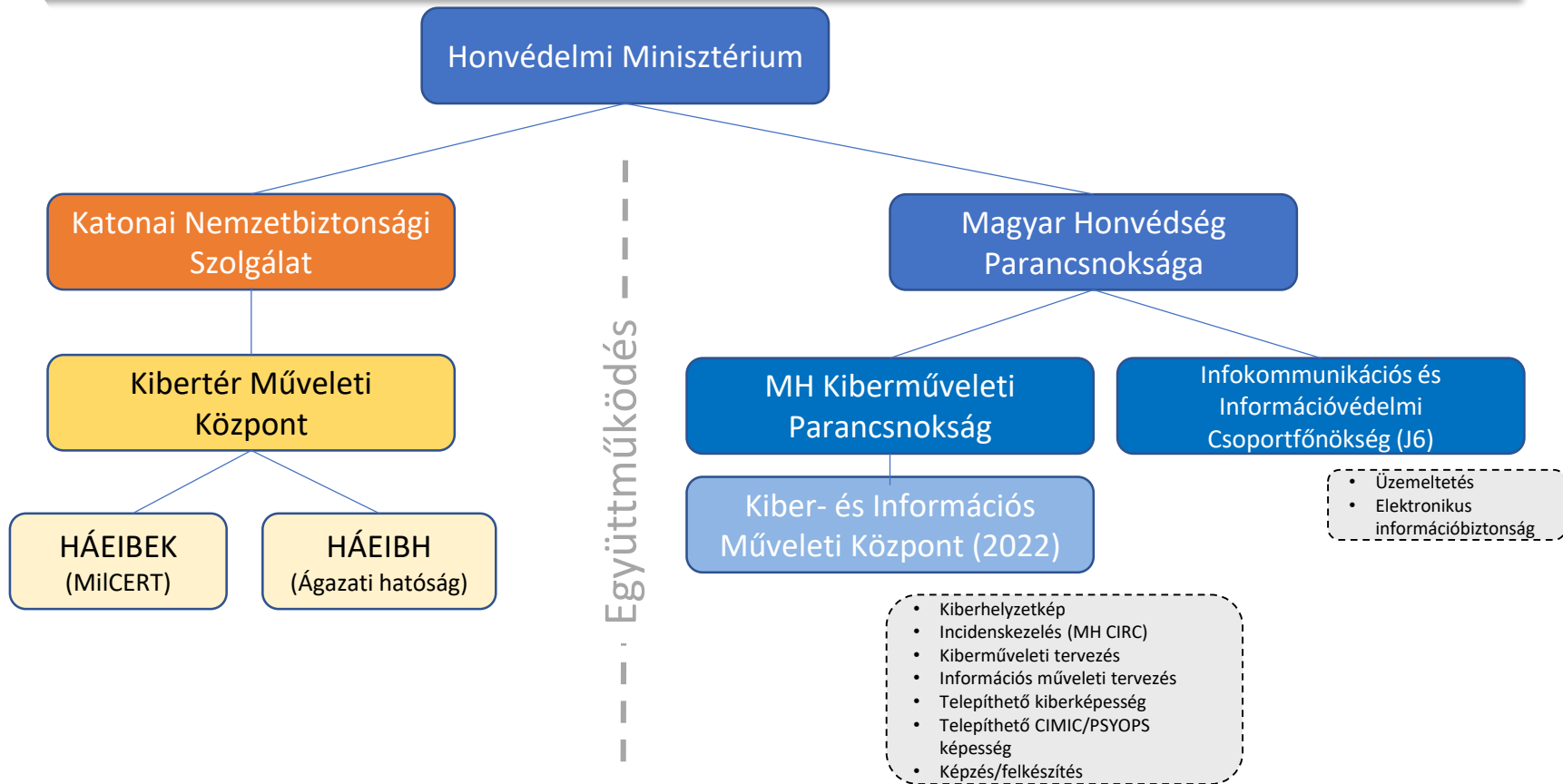


Magyarország: kibervédelmi szervezeti keretrendszer





Magyarország: honvédelmi ágazat kibervédelmi keretrendszer





MHP Kiberműveleti Parancsnokság

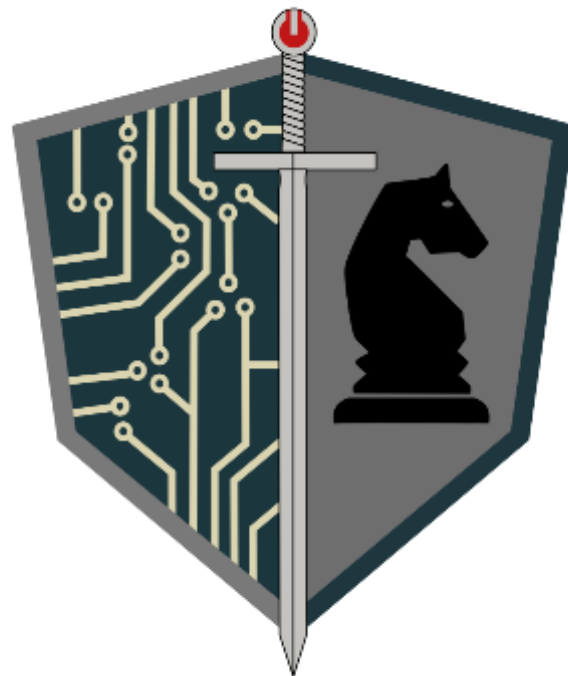
- Oktatási és képzési keretrendszer kialakítása:
 - „Kiberakadémia”
- Doktrínális háttér kialakítása:
 - MH Kiberműveleti Doktrína 2022
- Kiberműveleti képességek fejlesztése:
 - MH Kiber- és Információs Műveleti Központ
 - telepíthető képességek kialakítása
- Kiber- és információs műveletek tervezése, vezetése
- Kibervédelmi és kiberműveleti technikai fejlesztések folytatása





Magyar Honvédség

Kiber- és Információs Műveleti Központ





Magyar Honvédség

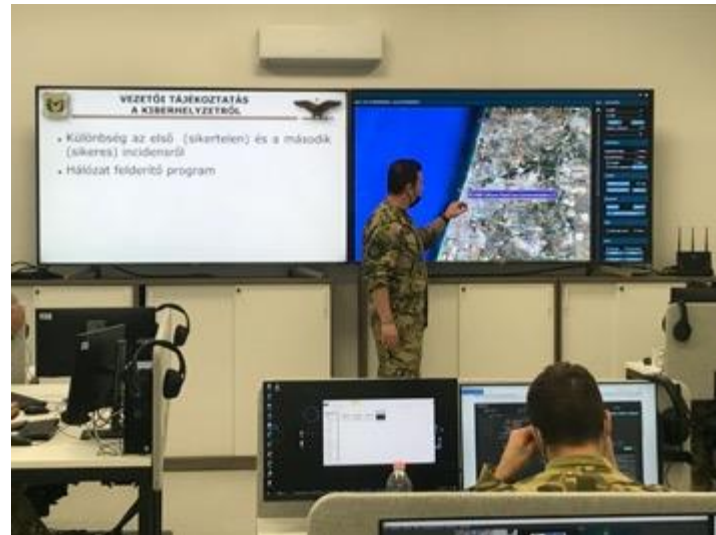
Kiber- és Információs Műveleti Központ





Magyar Honvédség

Kiber- és Információs Műveleti Központ





HÁBORÚ



Háború: tapasztalatok

Információs műveletek:

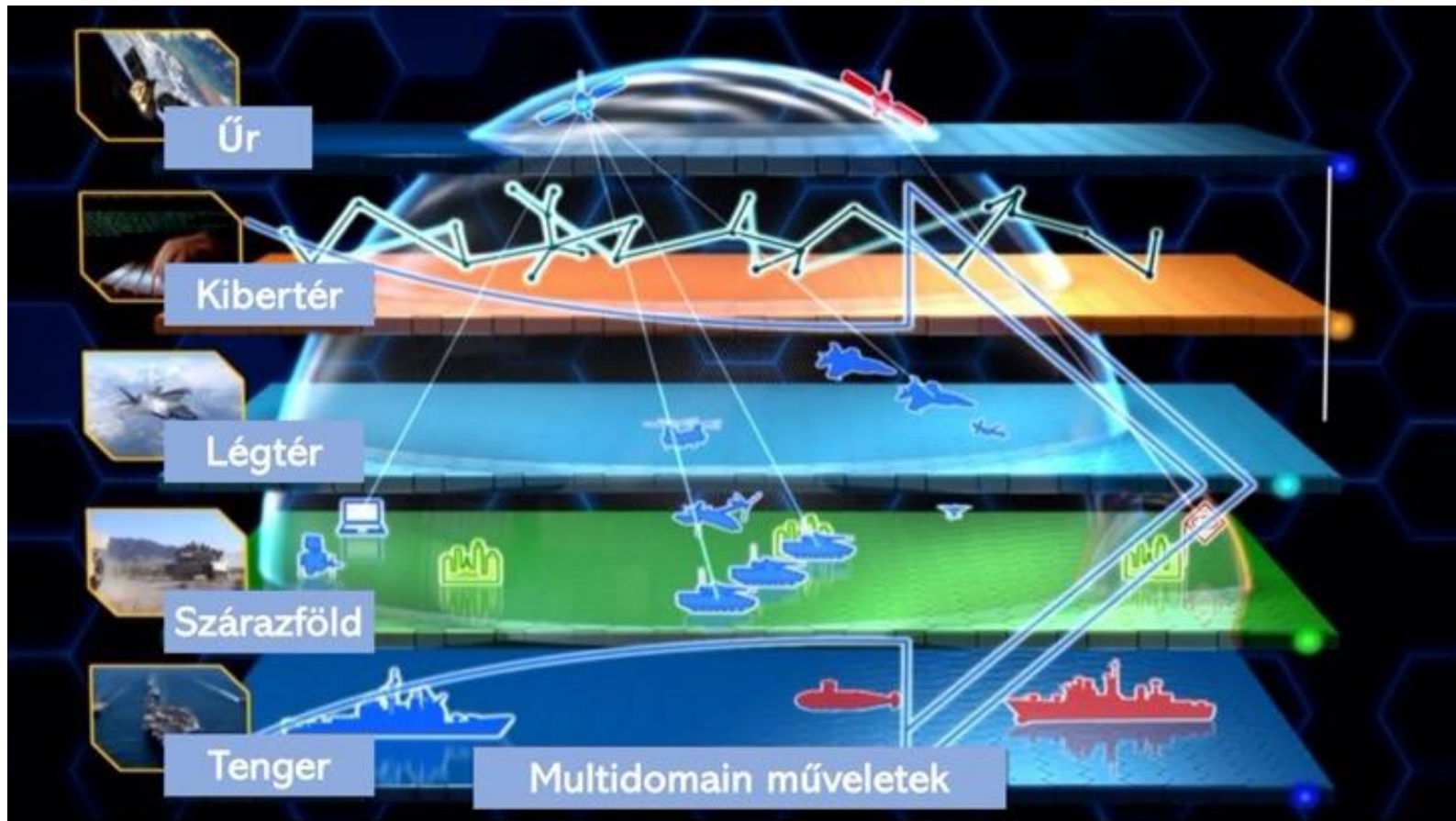
- STRATCOM szerepe: eltérő narratívák, eltérő befolyásolás
- média műveletek hangsúlya: TV, social media
- fake news kiszűrésének nehézségei
(elemzői kapacitás, szoftvertámogatás, gyakorlat és tapasztalat)

Kiberműveletek:

- masszív DDoS támadások, de fókusz a fizikai dimenziókon
- célzott kibertámadások (pl. wiper)
- állami támogatású csoportok mellett a hazafias hacker csoportok aktivitása
- nemzetközi hacker csoportok megjelenése és aktivitása mindkét oldal felé
- Magyarország nem kiemelt célpont, de a támadások nem kerülnek el



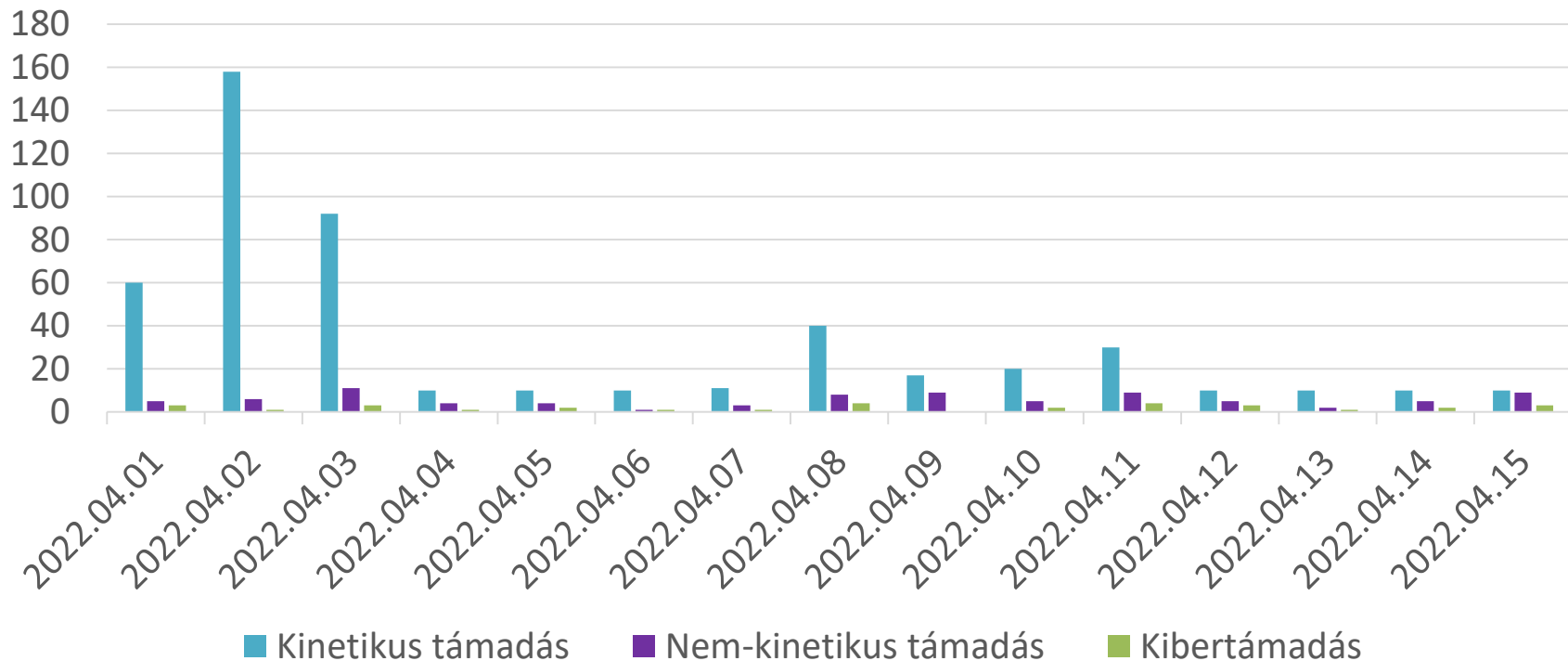
Megváltozott a hadviselés





A valóság: 2022. április

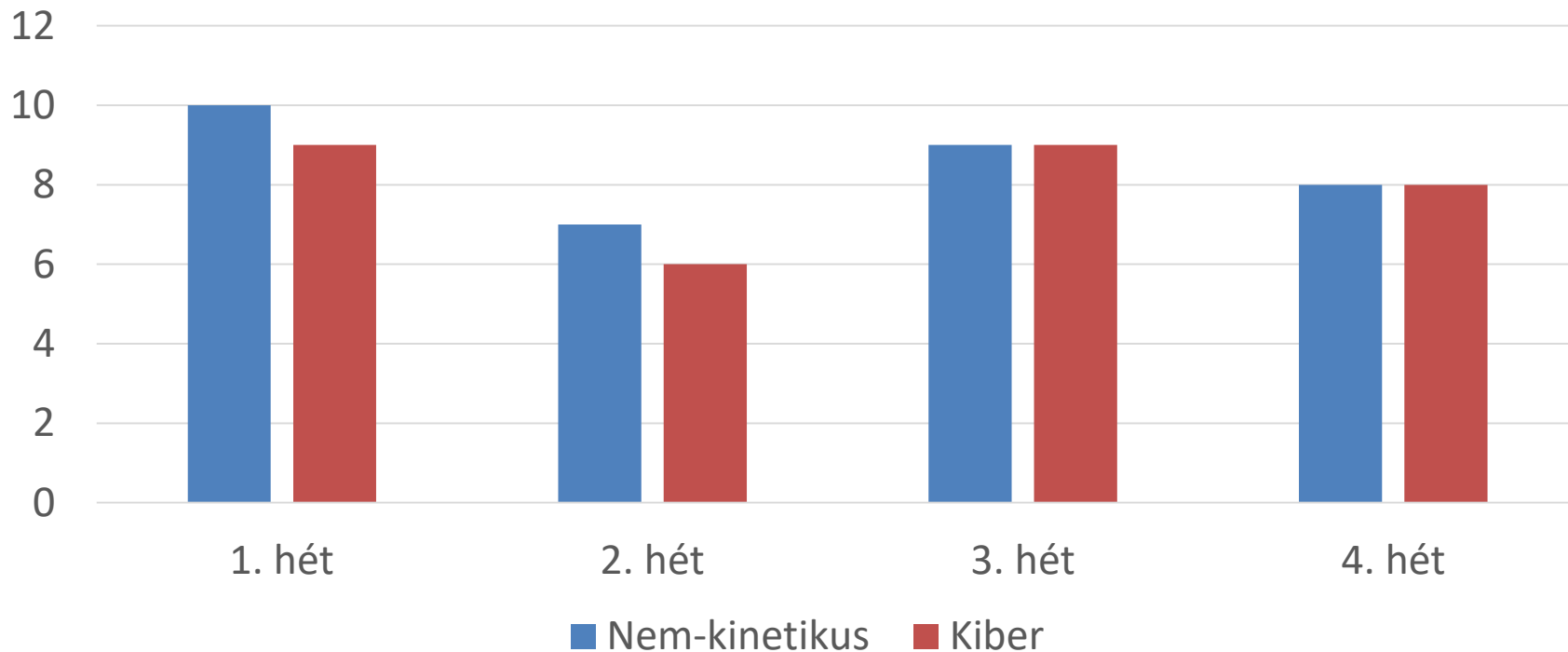
Támadások





A valóság: 2022. augusztus

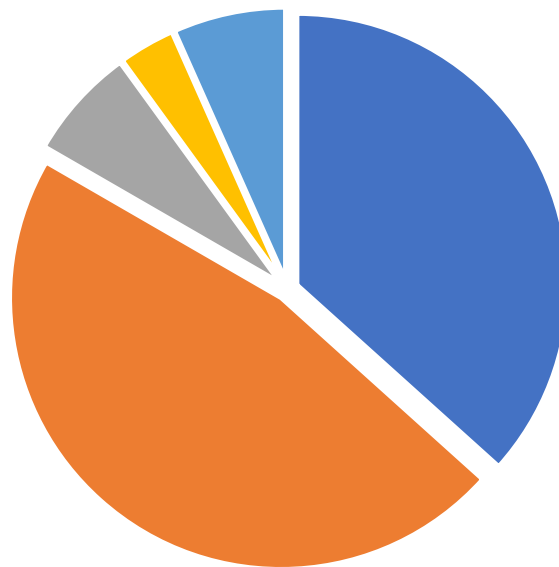
Nem-kinetikus és kibertámadások (augusztus)





A valóság: 2022. február

Célpont országok

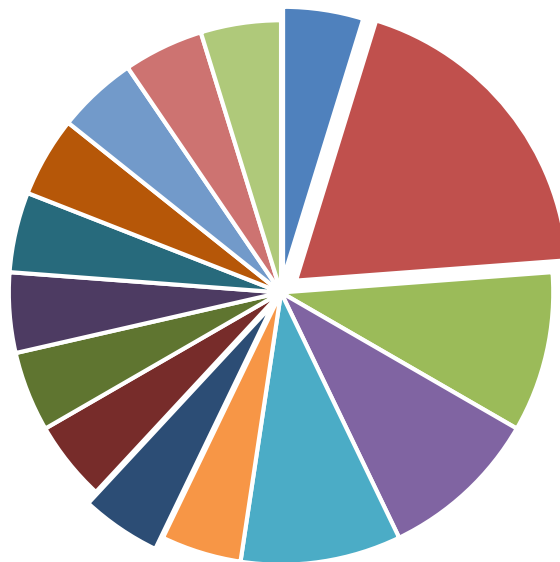


■ Ukrajna ■ Oroszország ■ EU ■ USA ■ BLR



A valóság: 2022. augusztus

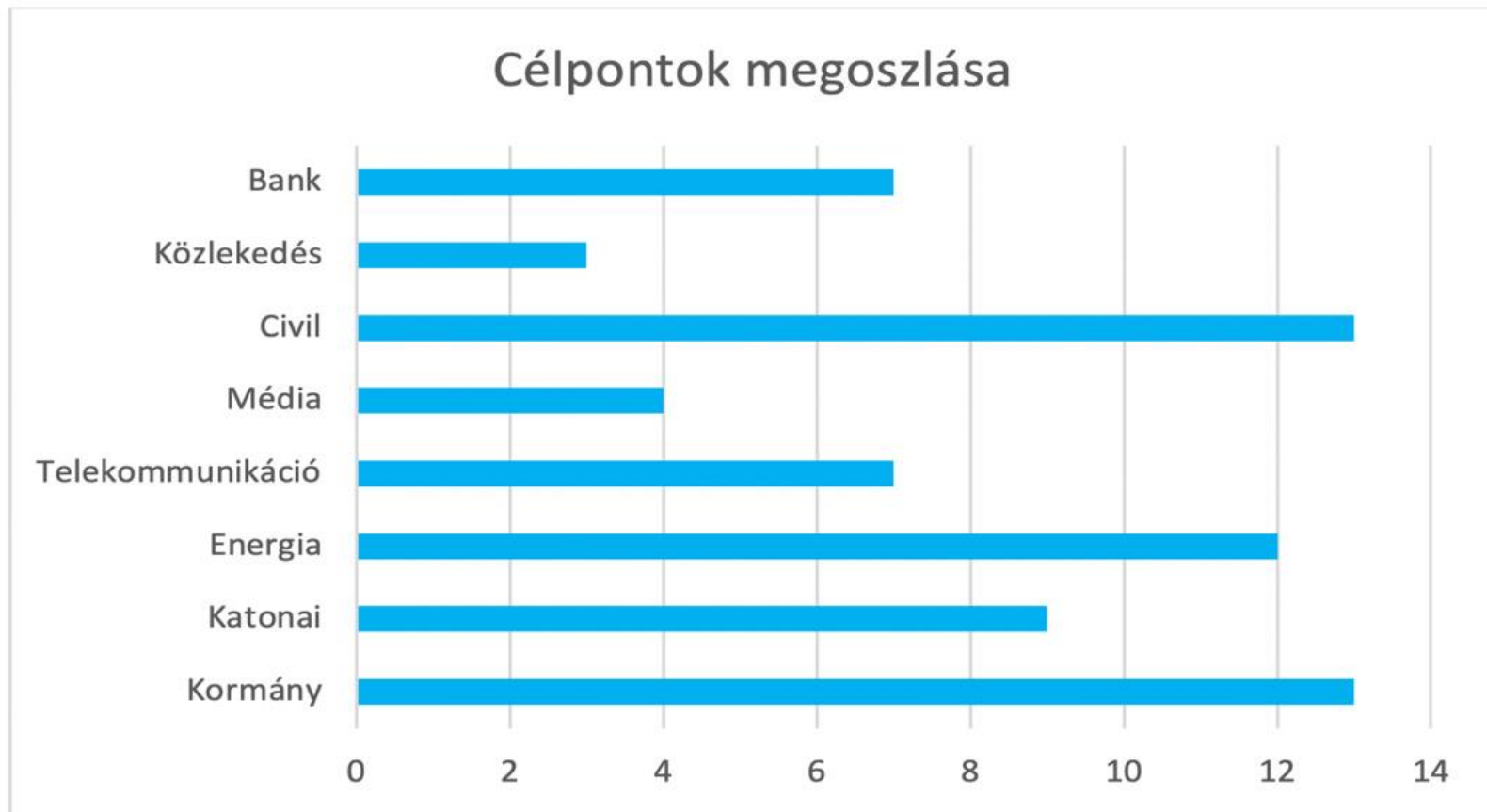
Országok (augusztus)



- RUS UKR TWN USA CHN ISR ALB FIN
AZE EET NATO AFG GRC FRA HUN



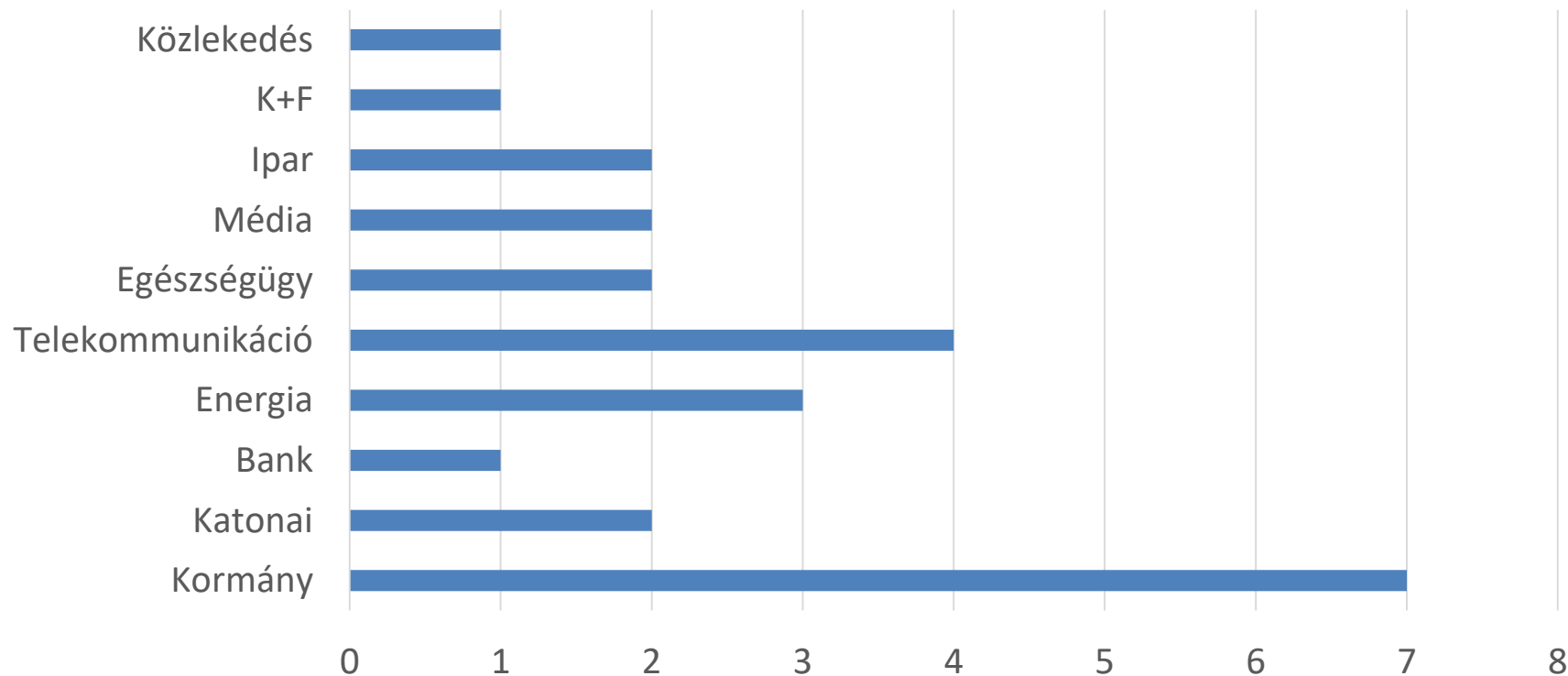
A valóság: 2022. február





A valóság: 2022. augusztus

Célpontok (augusztus)





ÖSSZEFOGLALÁS

- A nemzeti kibervédelem közös ügy!
- A Magyar Honvédség kibervédelmi feladata kettős:
 1. katonai kibernűveletek
 2. nemzeti kibernűveletek
- Az állami és magánszektor együttműködése elengedhetetlen
- Szabályozás és védelem csak együttesen hatékony
- A kibervédelemmel párhuzamosan a fizikai védelem is elengedhetetlen
- Oktatás, képzés, felkészítés, tudatosság hármasa
- Nemzetközi együttműködés fontossága



KÖSZÖNÖM A FIGYELMET!

Dr. Kovács László dandártábornok

Magyar Honvédség

Kiberműveleti Parancsnokság

parancsnok

kovacs.laszlo4@hm.gov.hu