NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

AZ OROSZ UKRÁN HÁBORÚ KIBERVONATKOZÁSAI

Kovács László
kovacs.laszlo@uni-nke.hu

Dr. Kovács László dandártábornok, DSc

Nemzeti Közszolgálati Egyetem

egyetemi tanár

kovacs.laszlo@uni-nke.hu

Az előadás csak nyílt források felhasználásával készült.

Az előadás minősítése: nyílt.

Az előadásban elhangzott állítások és következtetések az előadó sajátjai, azok nem szükségszerűen egyeznek meg és nem tükrözik a Magyar Honvédség és/vagy a Nemzeti Közszolgálati Egyetem hivatalos véleményét vagy álláspontját.

Tartalom

- Fogalmi maghatározások:
  - információs műveletek
  - hibrid műveletek
  - kiberműveletek
- A háború előtti kibertéri akciók
- A háború kezdete
- Célpontelemzés
- Következtetések

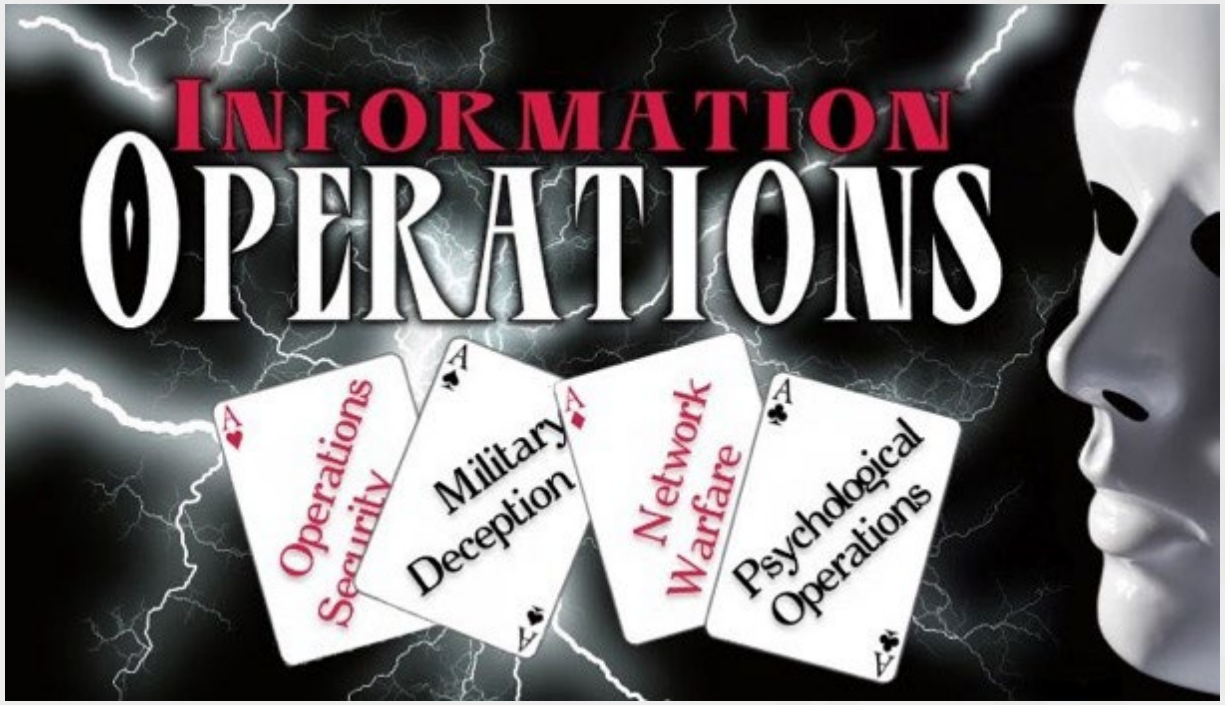
Fogalmi tisztázás

- információs műveletek
- hibrid műveletek
- kiberműveletek

Információs műveletek

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

Haig, 2018



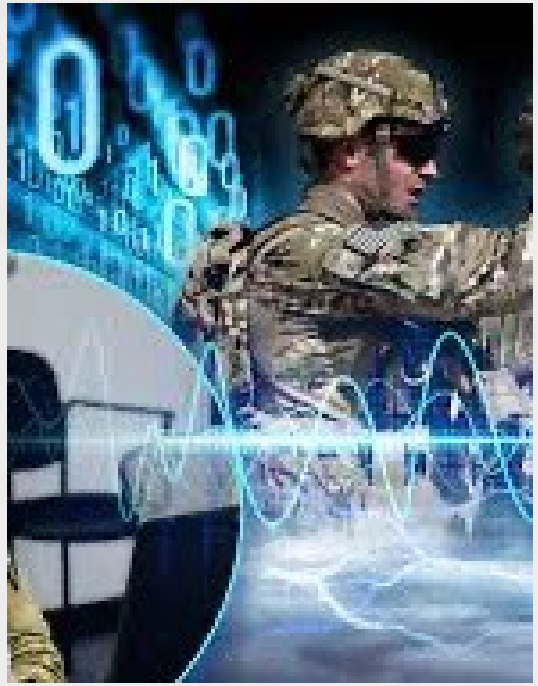
Kép forrása: https://www.linkedin.com/pulse/what-information-operations-daniel-clark/

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

Elektronikai hadviselés

„Azon tevékenységek összessége, amelyek az **elektromágneses spektrum** ellenség által történő felhasználásának meghatározására, felderítésére, csökkentésére vagy megakadályozására, illetve az elektromágneses energia és az irányított energia felhasználására, az elektromágneses spektrum saját célú felhasználására, valamint az ellenség vezetési és irányítási rendszerei támadásának támogatására, a saját csapatok védelmére irányulnak.”

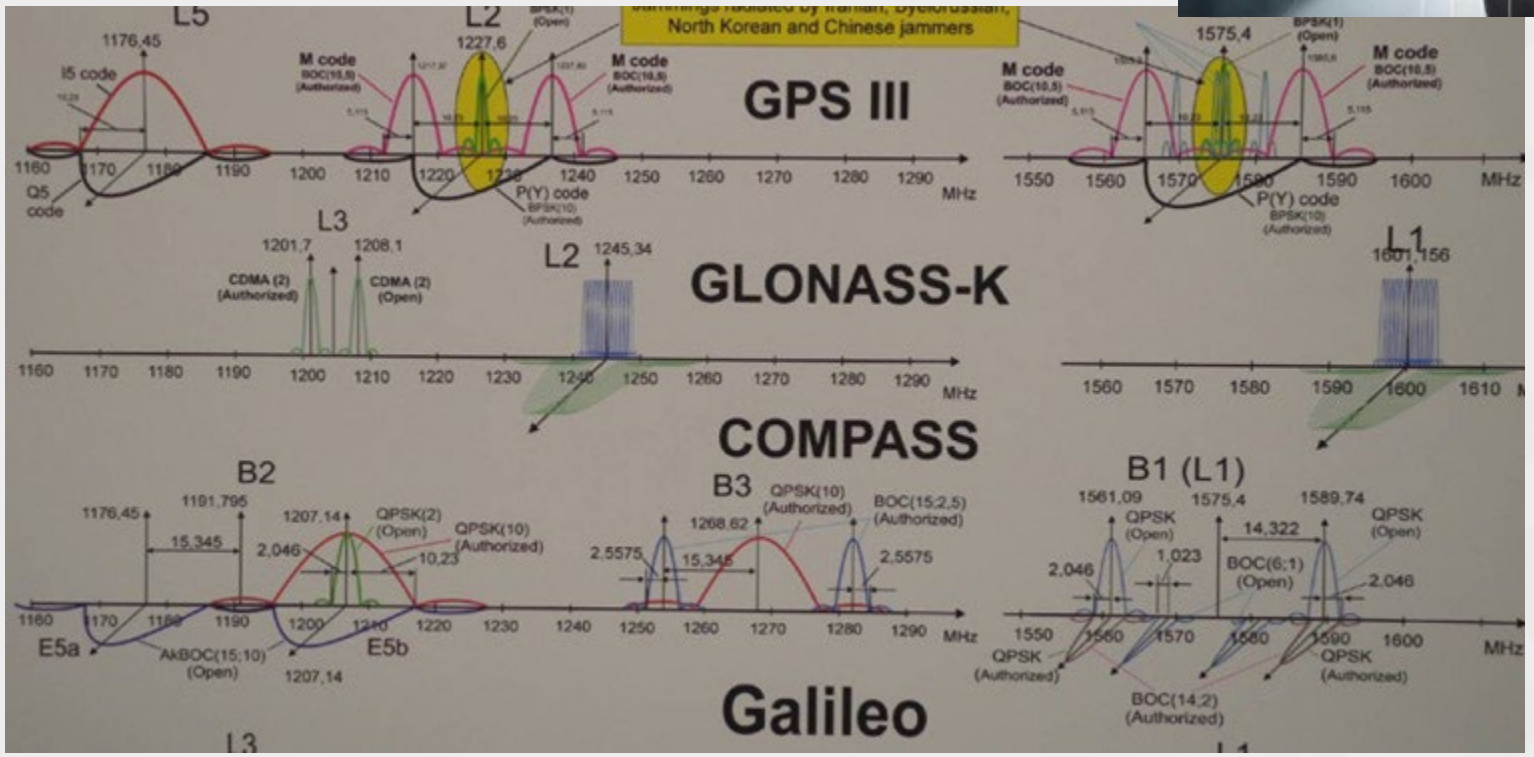


NEM NYILVÁNOS

Forrás: Magyar Honvédség Összhaderőnemi Doktrína, 2012.

Elektronikai hadviselés





Forrás: https://www.ainonline.com/aviation-news/blogs/ain-blog-gps-jammer-guy-touts-wares-dubai-air-show

Hibrid hadviselés (műveletek)

- A hibrid hadviselésnek nincs általánosan elfogadott meghatározása

- A NATO walesi csúcstalálkozója alapján:
„a hibrid fenyegetés széles körű nyílt és fedett katonai, félkatonai és nem katonai eszközök és eljárások alkalmazása egy szorosan integrált műveleti terv mentén.”



Forrás: Kiss Álmos Péter: A hibrid hadviselés természetrajza.
https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf

Hibrid műveletek

- kényszerítő és felforgató tevékenységek
- hagyományos és nem hagyományos módszerek együttese:
  - katonai, diplomáciai, gazdasági, technológia
  - social media, félretájékoztatás, befolyásolás
- állami vagy nem állami szereplők összehangolt akciói
- döntéshozatal befolyásolása
- a deklarált hadviselés szintjét el nem érő módon (és háborúban is!)

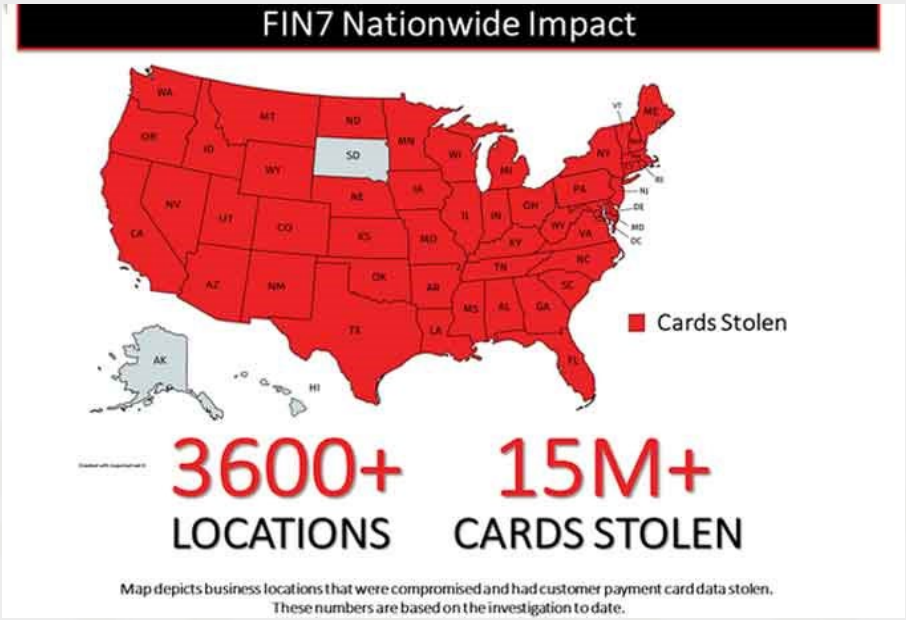




Forrás: Kiss Álmos Péter: A hibrid hadviselés természetrajza.
https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf

Hibrid hadviselés (műveletek)







Kibertér

> A kibertér **globálisan összekapcsolt**, decentralizált, egyre növekvő **elektronikus információs rendszerek**, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő **társadalmi és gazdasági folyamatok együttesét jelenti**.

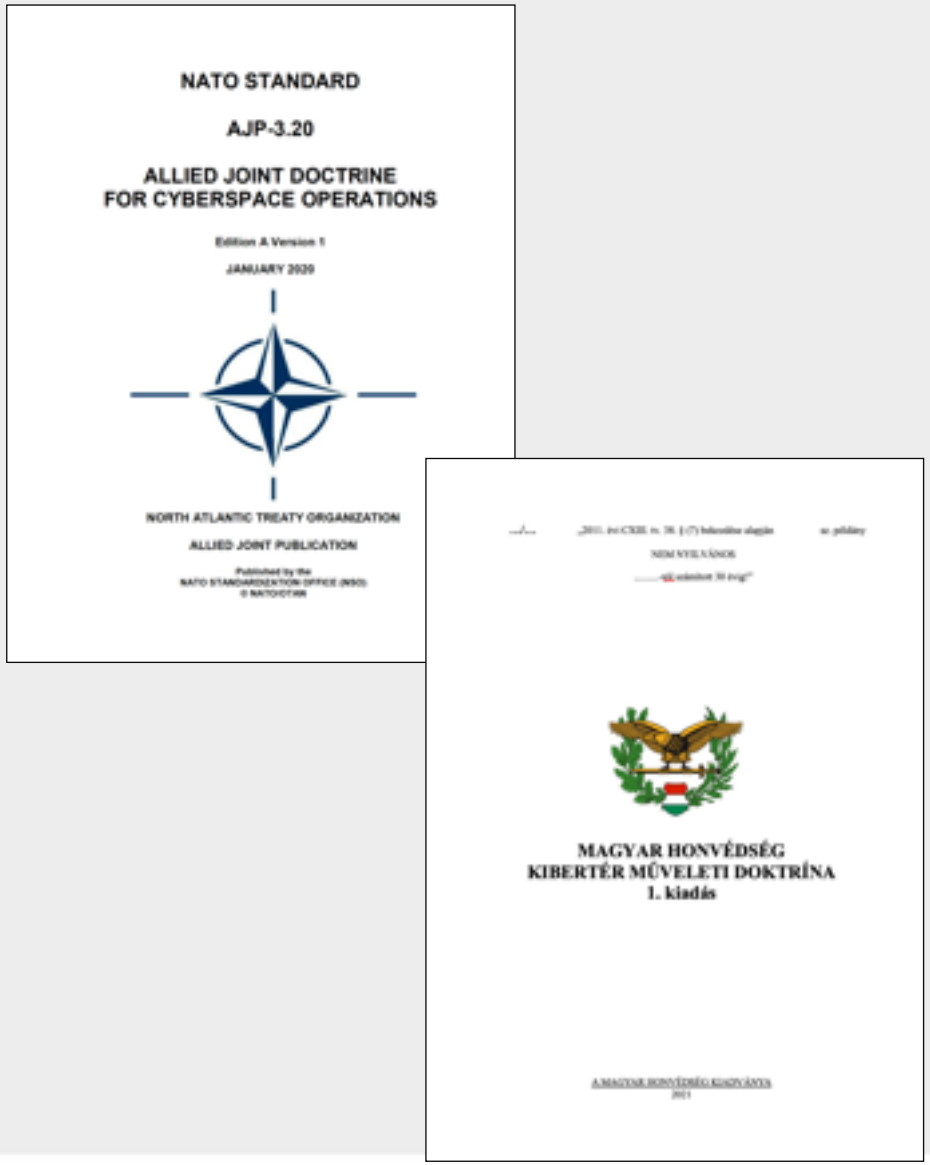
Forrás: 1139/2013. (III. 21.) Korm. határozat

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.

Forrás: NATO AJP-3.20 Kibertér műveletek doktrína (2020)

Kibertér műveletek



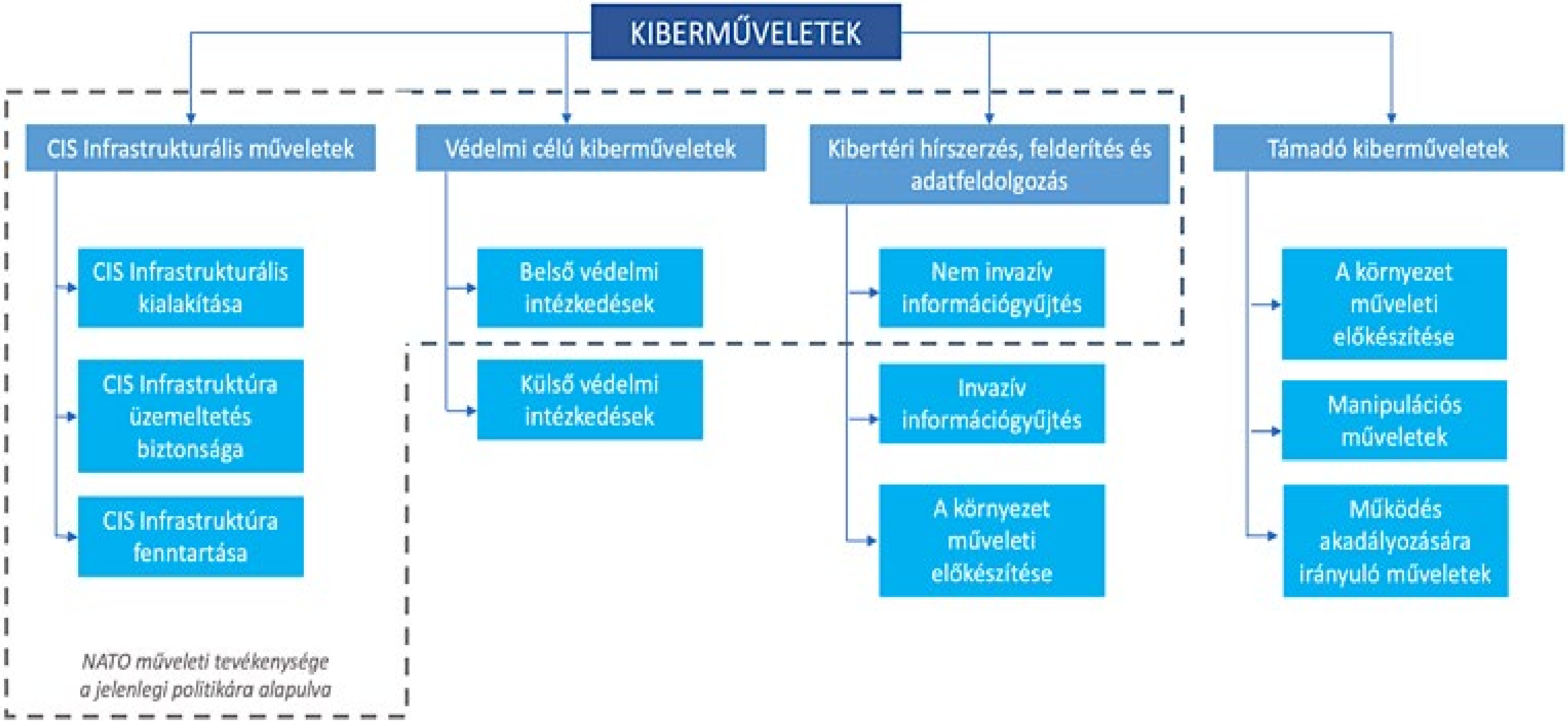
NATO doktrína:

- AJP 3.20: Cyberspace Operations Doctrine (2020)

Hazai doktrína:

- MH Kibertér Műveleti Doktrína (2022)

A kiberműveletek felosztása (NATO)



A HÁBORÚ

Ukrajna

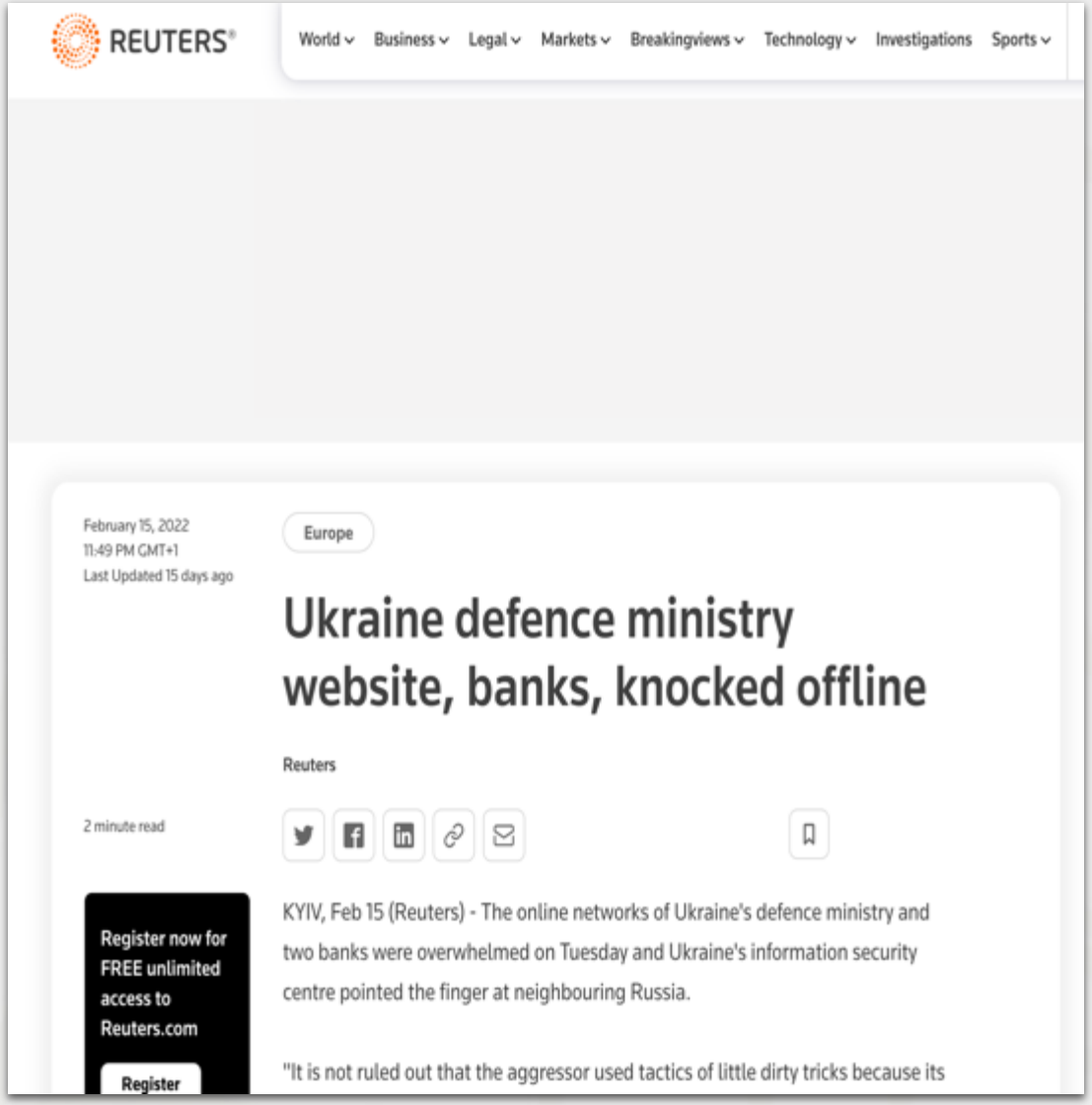
- **2015. december 23.**
  - a PJSC Kyivoblenergo (KOE) rendszereiben komoly üzemzavar keletkezett
  - behatlás a cég számítógépeibe és SCADA rendszereibe
  - a támadók 7 db 110 kV-os, valamint 23 db 35 kV-os alállomást kapcsoltak le
  - több, mint 3 órás áramszünet
  - 225 ezer fogyasztó nem jutott áramhoz
  - megoldás: kézi vezérlés



Forrás: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Ukrajna

- **2022. február 15.:**
  - túlterheléses támadások (masszív DDOS)
  - védelmi minisztérium ellen
  - kormányzat ellen
  - bankok ellen
  - a háború előszele (?)



Microsoft | Microsoft Security Solutions Products Partners Resources

January 15, 2022

Destructive malware targeting Ukrainian organizations

Microsoft Threat Intelligence Center (MSTIC)

Microsoft Digital Security Unit (DSU)

Microsoft 365 Defender Threat Intelligence Team

Detection and Response Team (DART)


```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

```
.3DM .3DS .7Z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2
.CGM .CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH
.DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM
.HTML .HWP .IBD .INC .INI .ISO .JAR .JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6
.LDF .LOG .MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .ODP .ODS .ODT .OGG
.ONETOC2 .OST .OTG .OTP .OTS .OTT .P12 .PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5
.PHP6 .PHP7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS .PPSM .PPSX .PPT
.PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK
.SLN .SNT .SQ3 .SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC .SXD .SXI
.SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM
.VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML
.XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW .YML .ZIP
```

A háború: 2022. február 24.



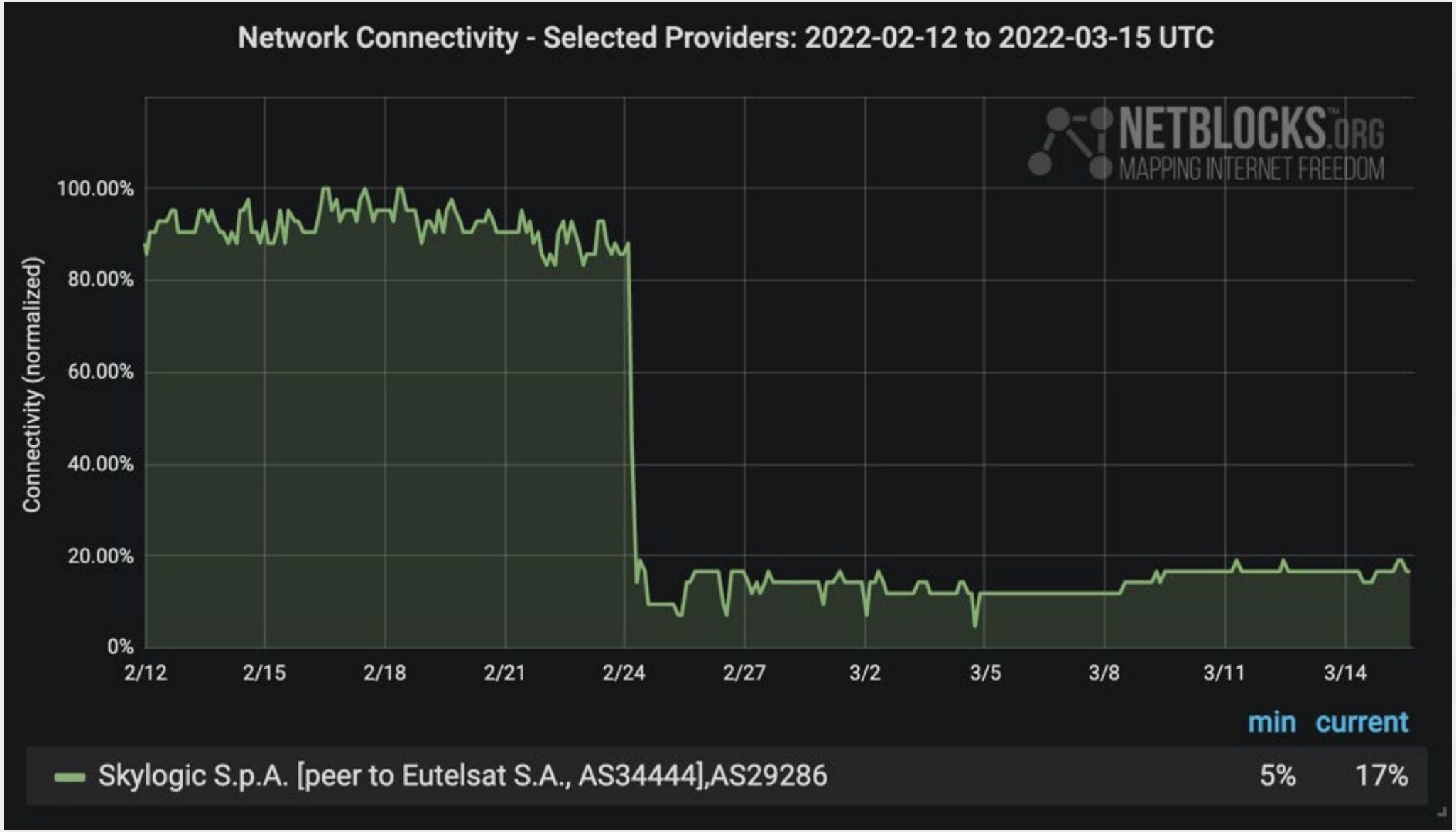
forrás: https://apnews.com/article/russia-ukraine-war-crimes-tracker-b39137c3a96eef06f4ba1793fd694542

Kibertámadások: Viasat – 2022.02.24.

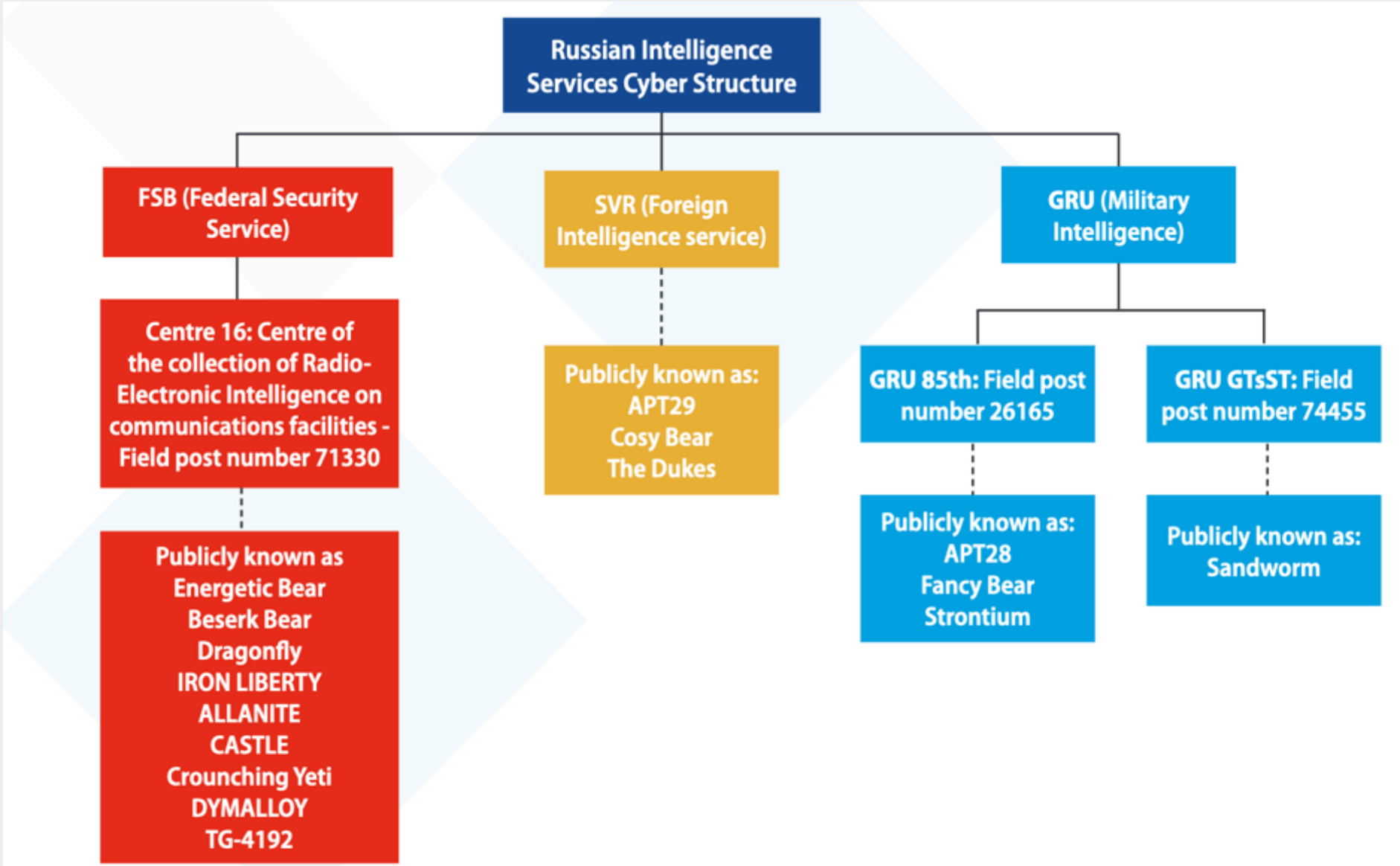


https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

Kibertámadások: Viasat – 2022.02.24.



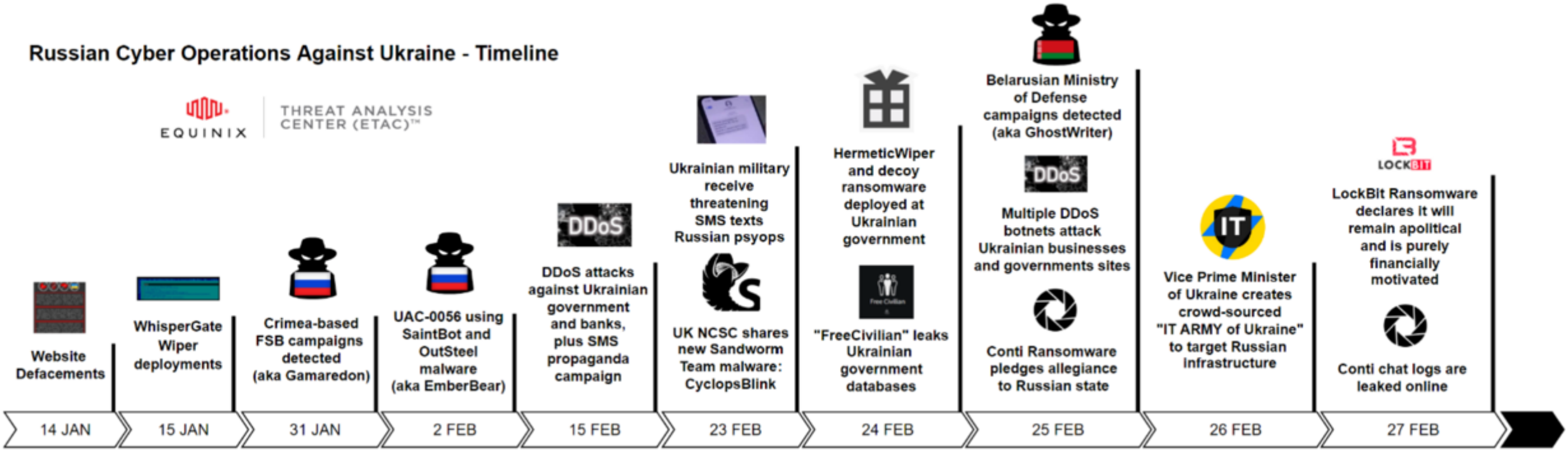
https://twitter.com/netblocks/status/1498365220107997191



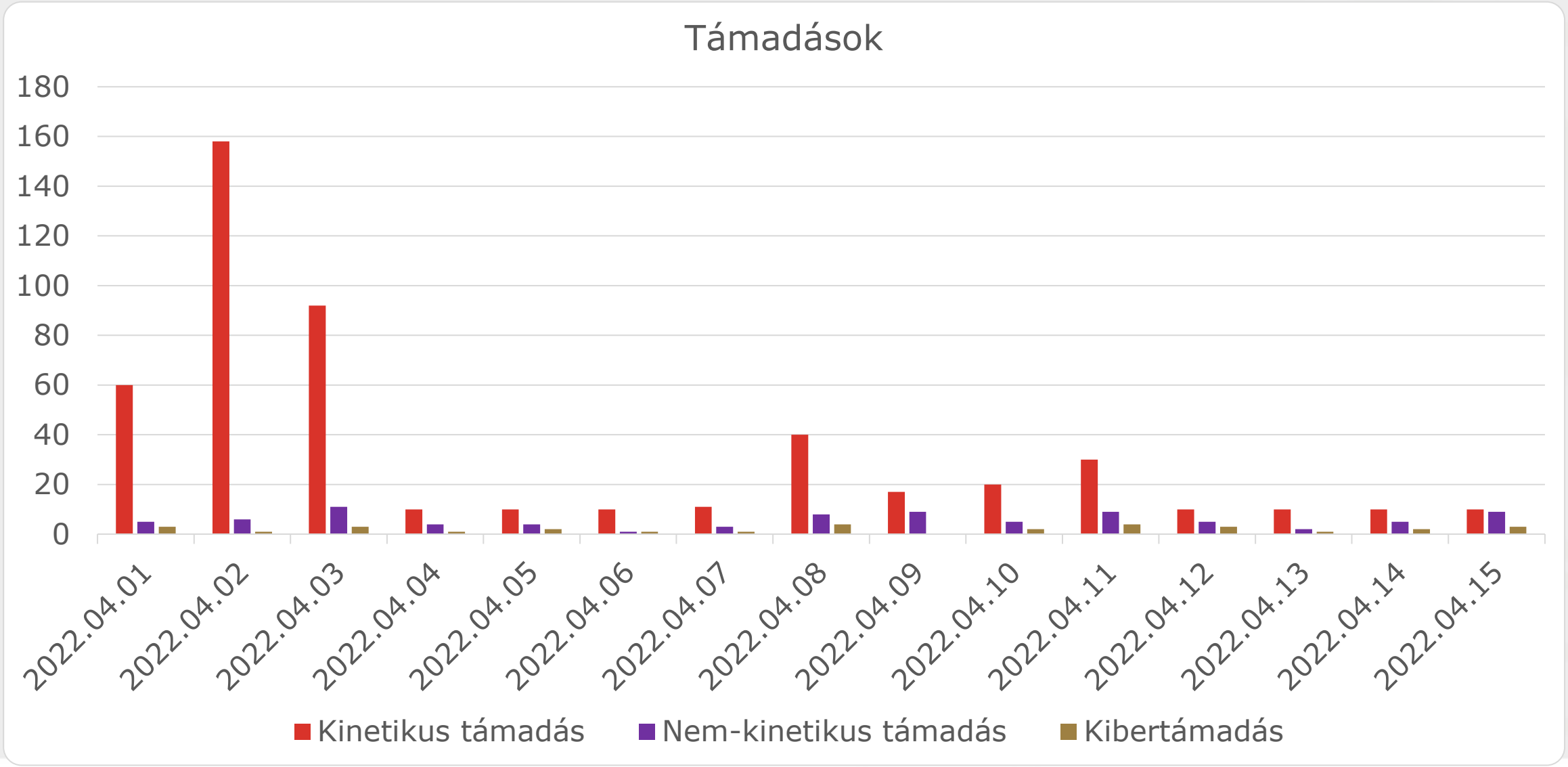
https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

Russian Cyber Operations Against Ukraine - Timeline

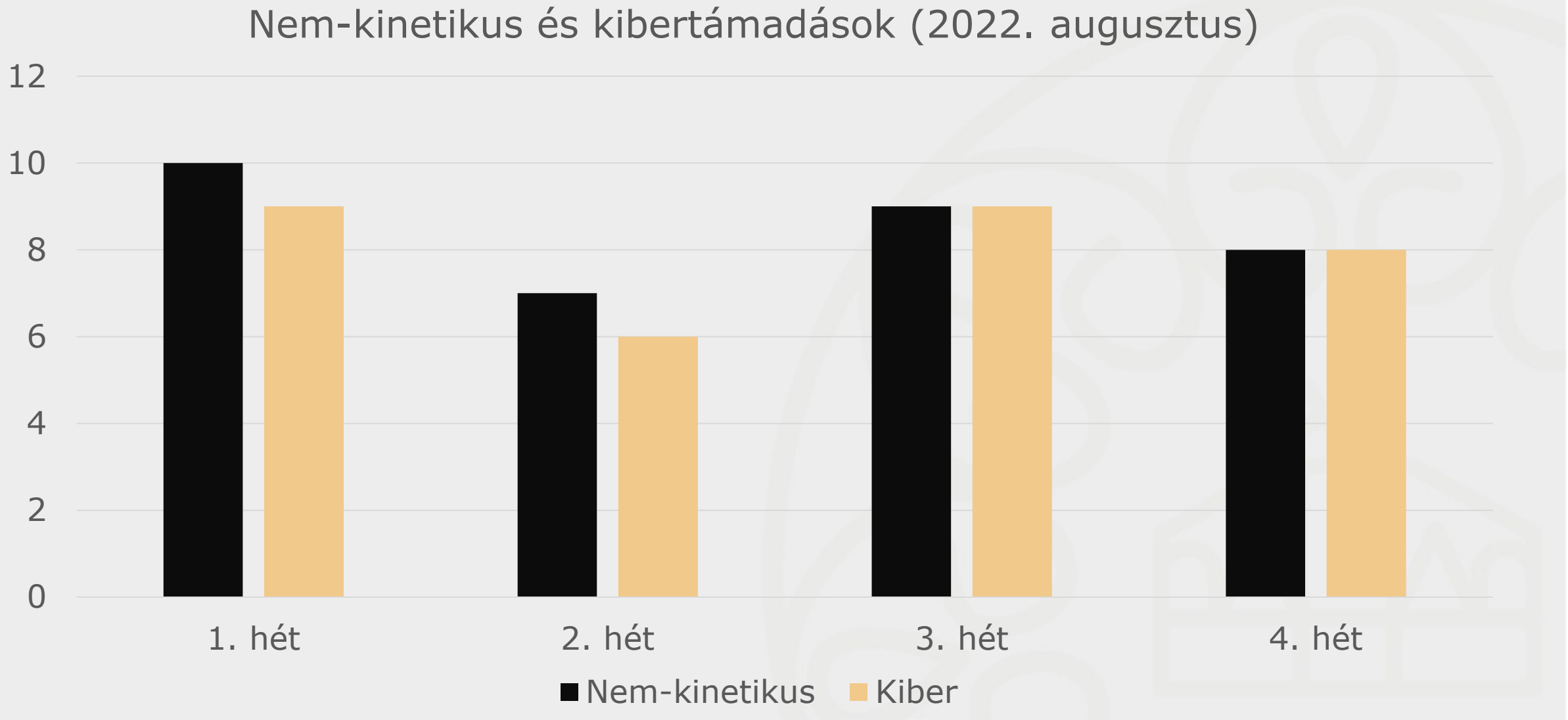
EQUINIX | THREAT ANALYSIS CENTER (ETAC)™



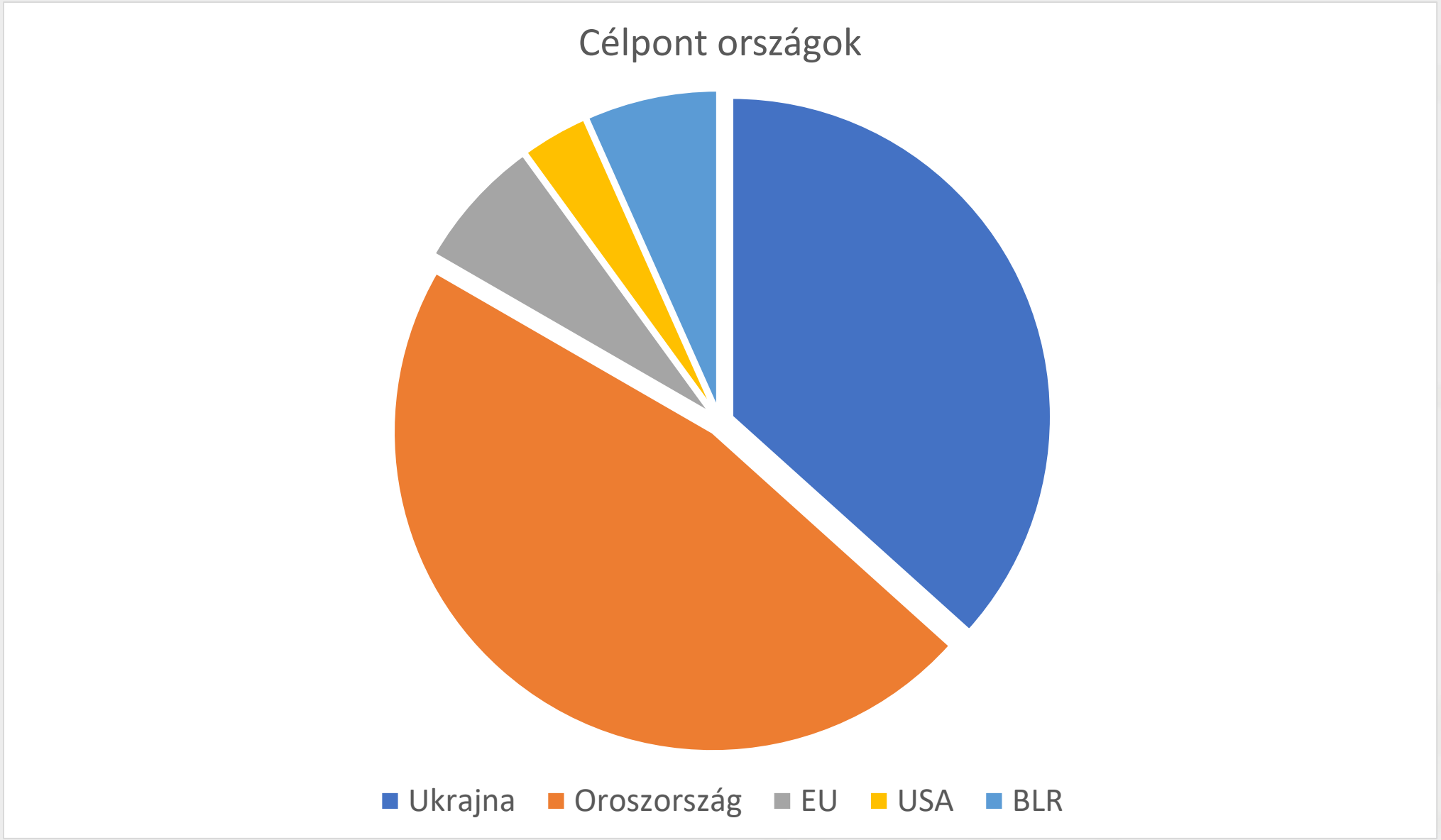
A háború: 2022. április



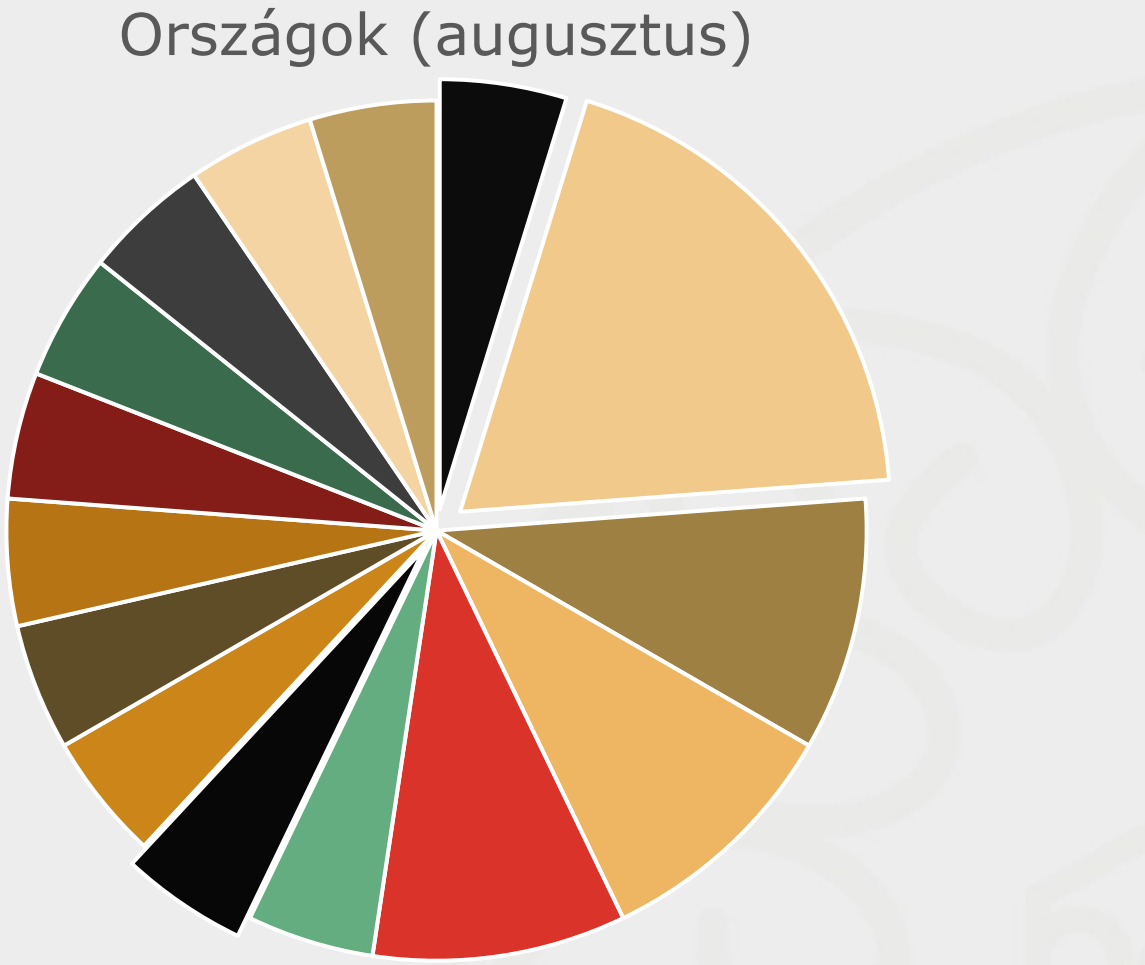
A háború: 2022. augusztus



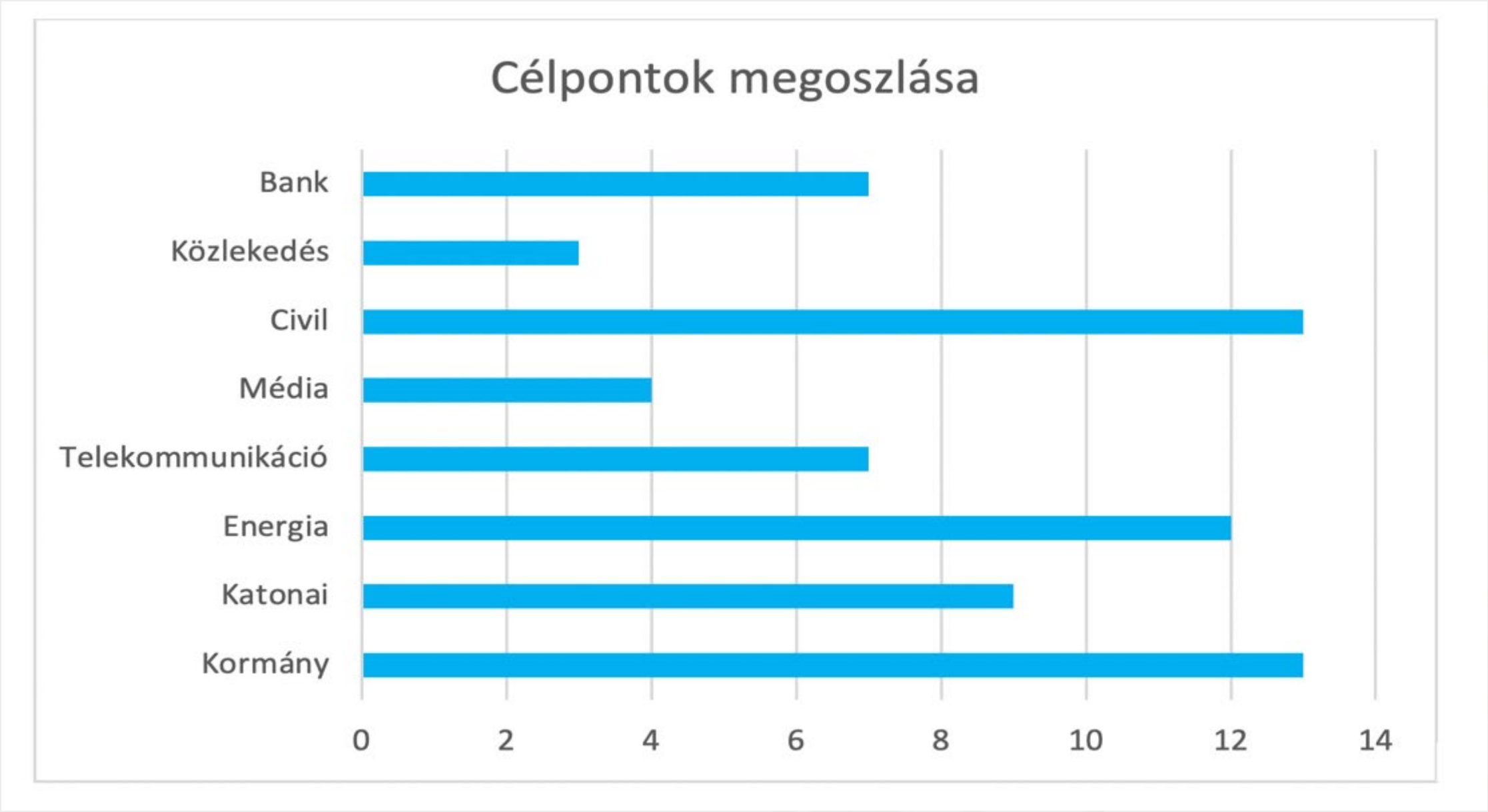
A háború: 2022. február



A háború: 2022. augusztus



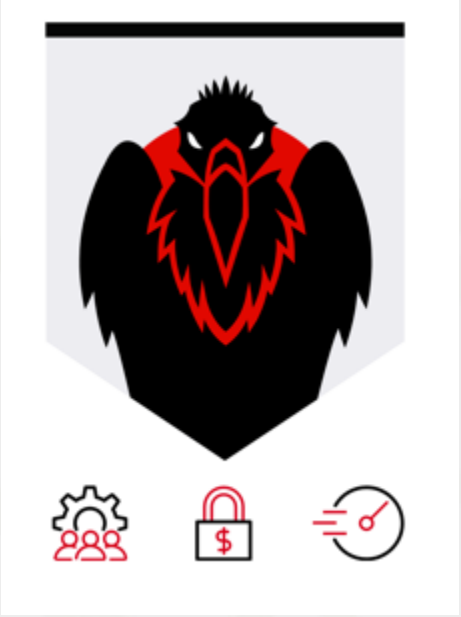
A háború: 2022. február



Bankszektor támadói:

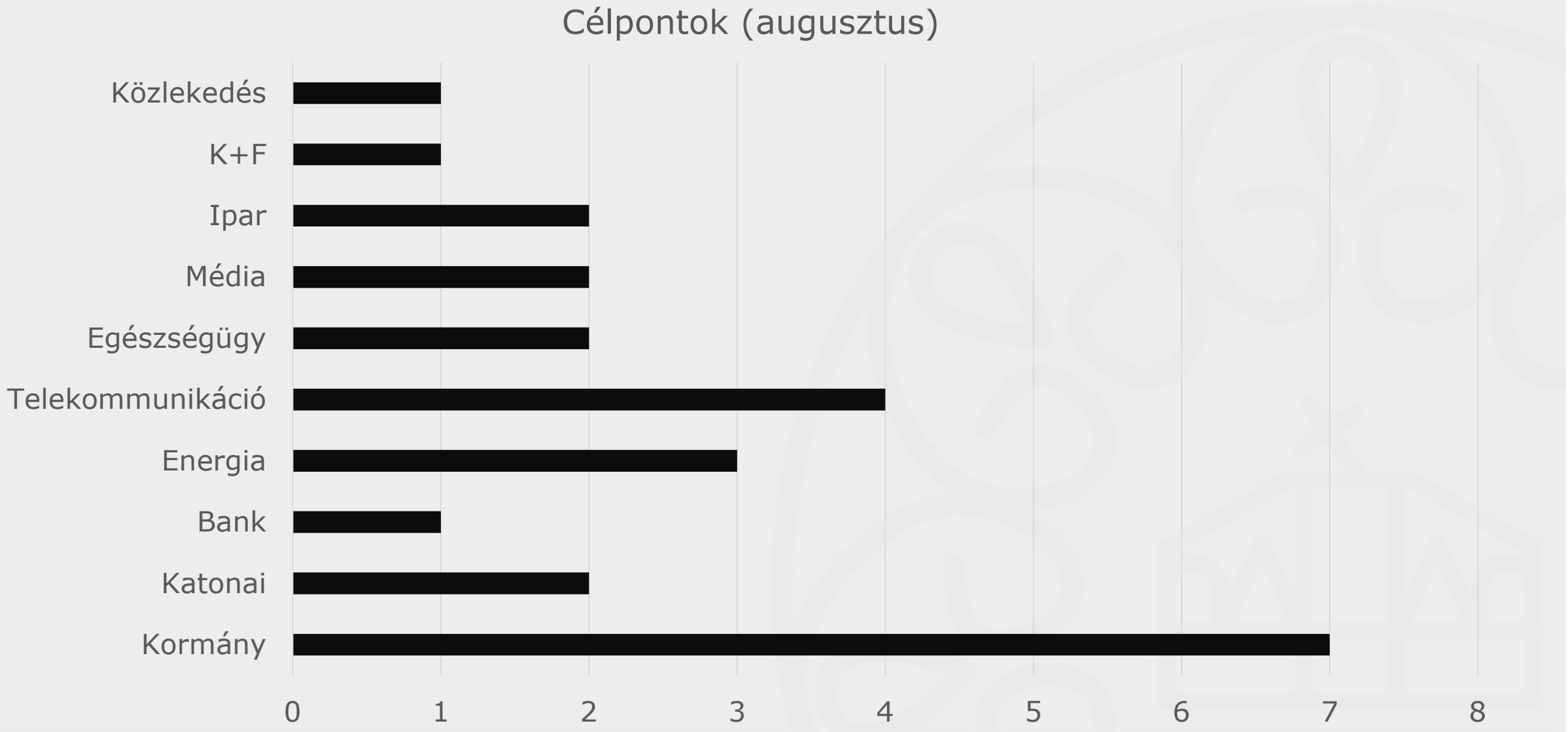
- FIN12 (RUS):
  - nagy értékű célok
  - nagyon gyors ransomware támadások

- UNC 1151 (BLR):
  - Ghostwriter információs műveletek kampány állami támogatással
  - social media információszerzés és befolyásolás

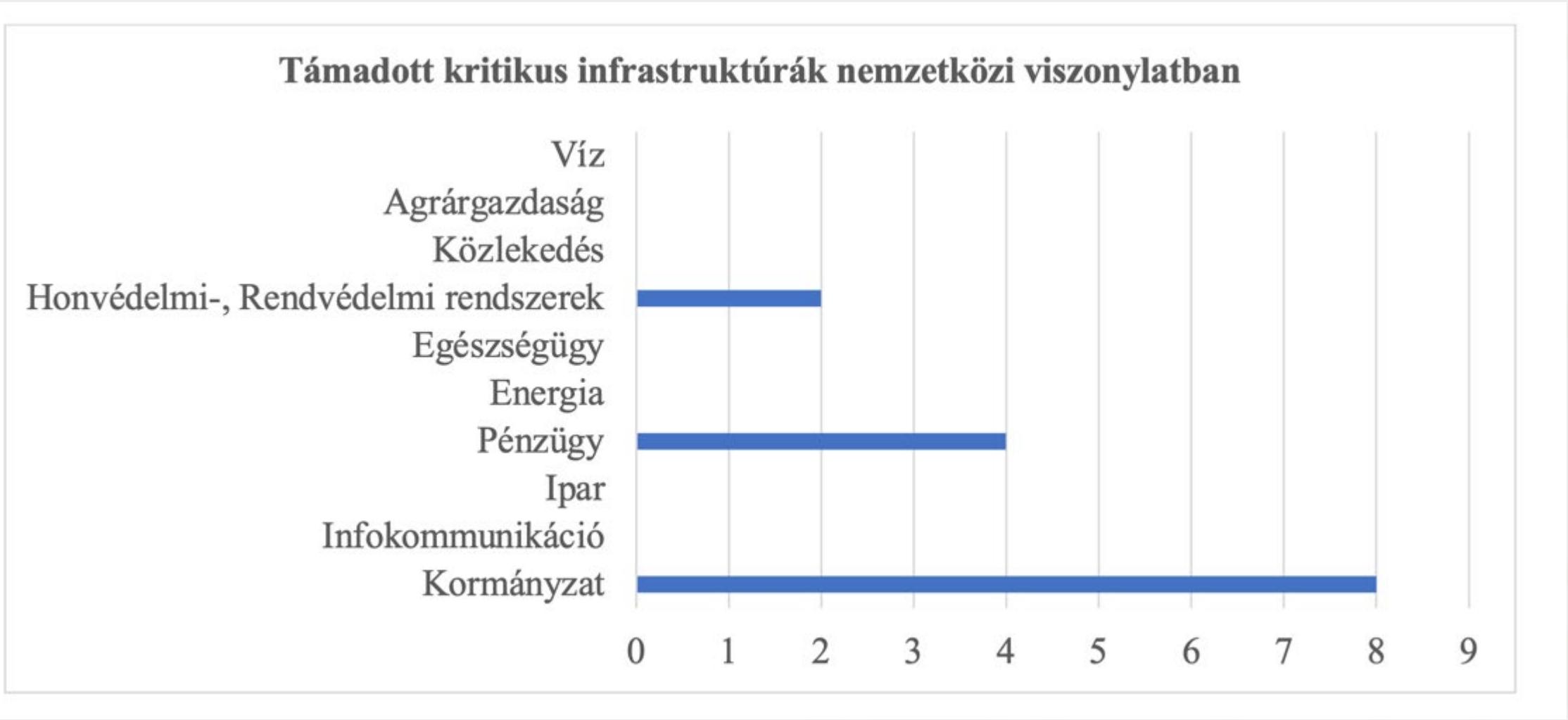




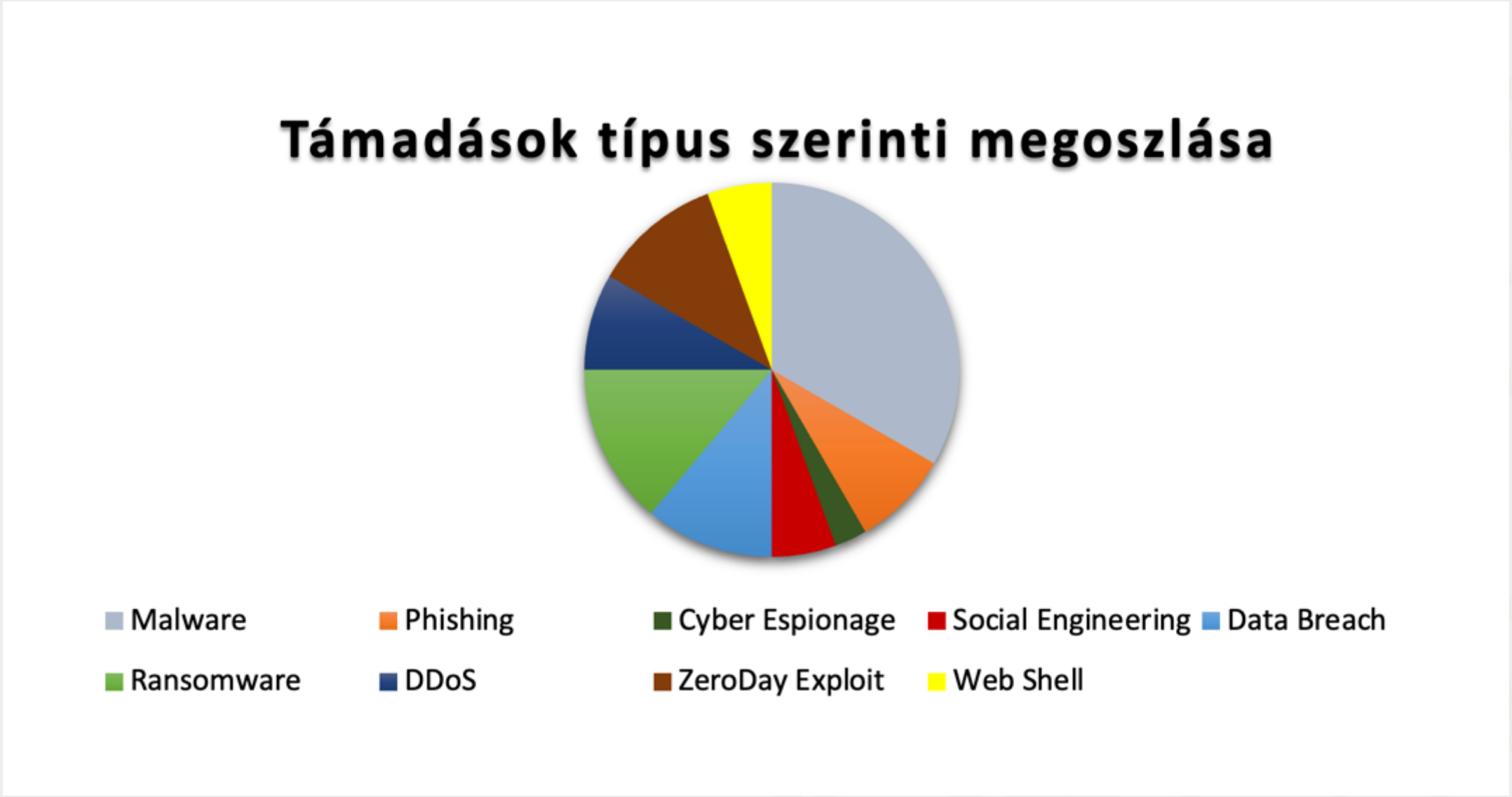
A háború: 2022. augusztus



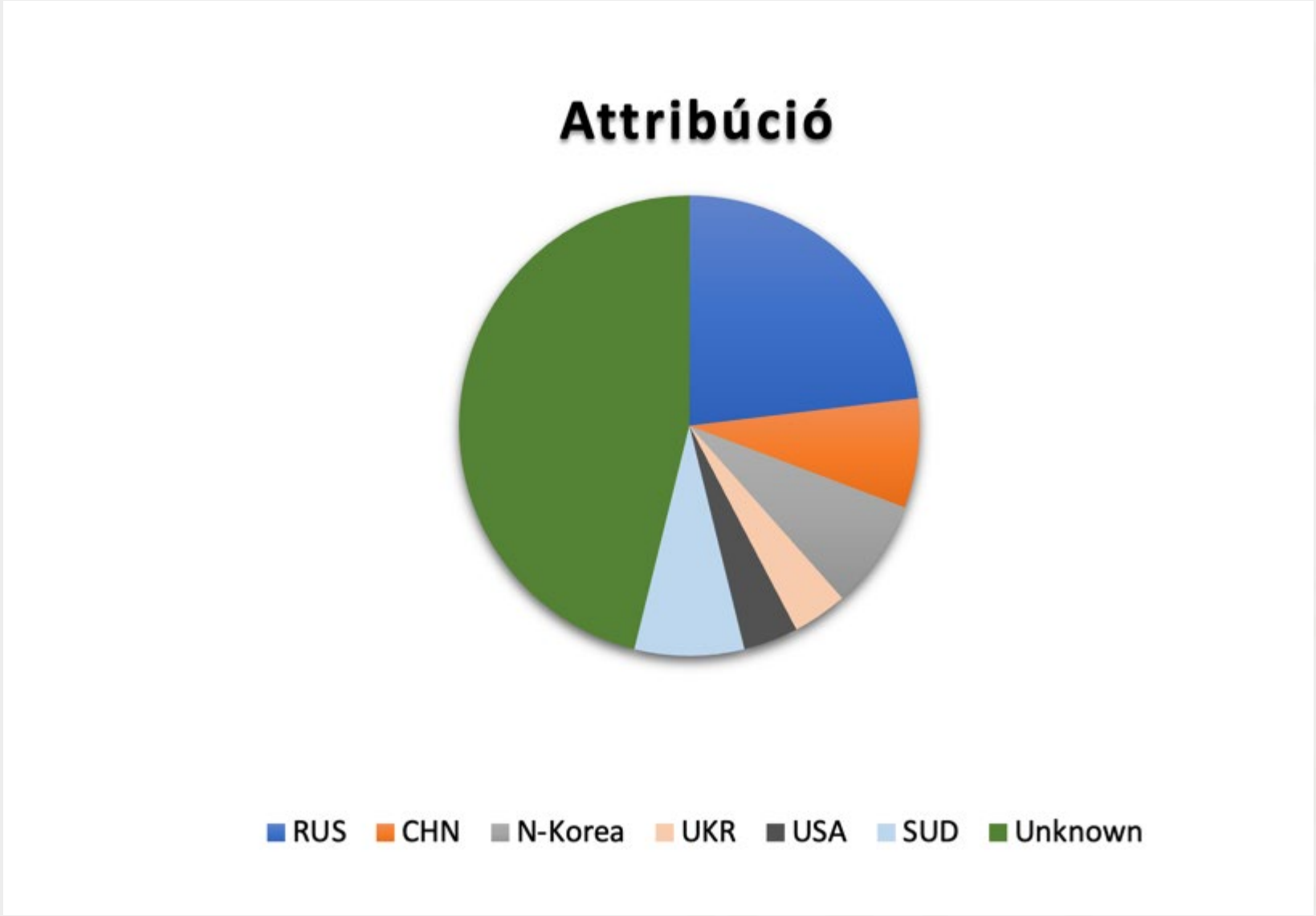
2023. június: a súlyos kibertámadások megoszlása



2023. június


Támadások típus szerinti megoszlása
Malware
Phishing
Cyber Espionage
Social Engineering
Data Breach
Ransomware
DDoS
ZeroDay Exploit
Web Shell

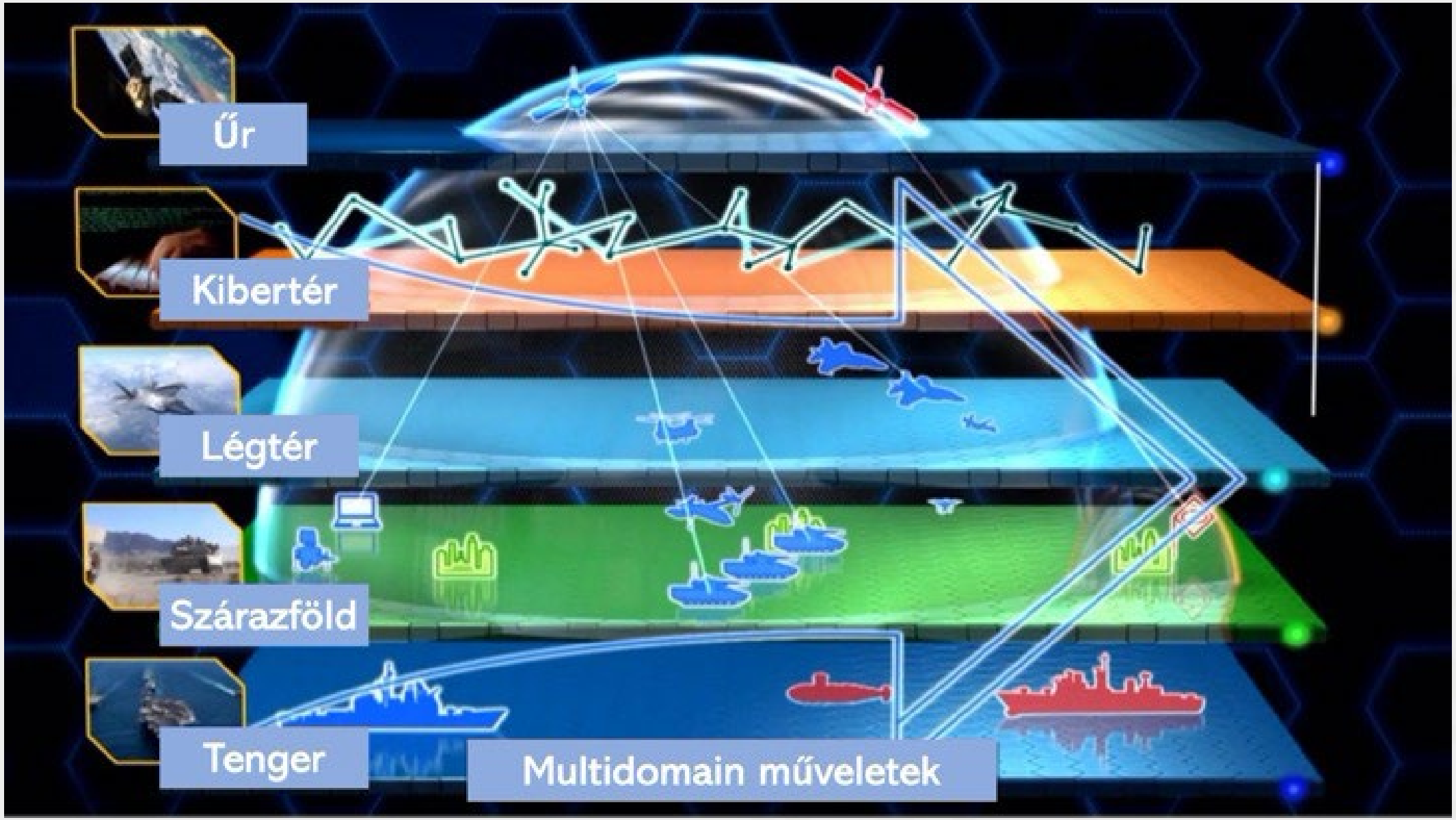
2023. június



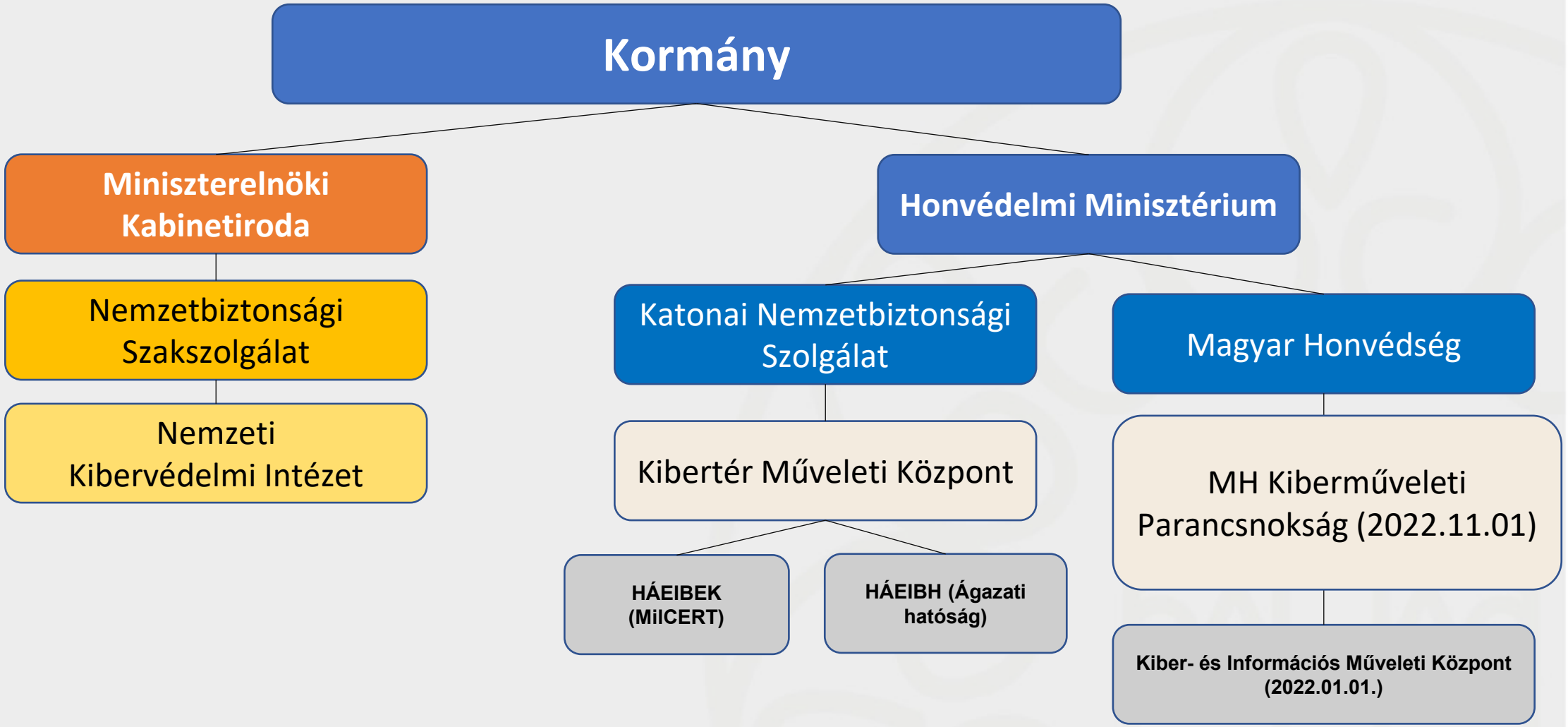
A JÖVŐ

A lehetséges jövő, amely azonban pontosan megjósolhatatlan...

Katonai műveleti terek

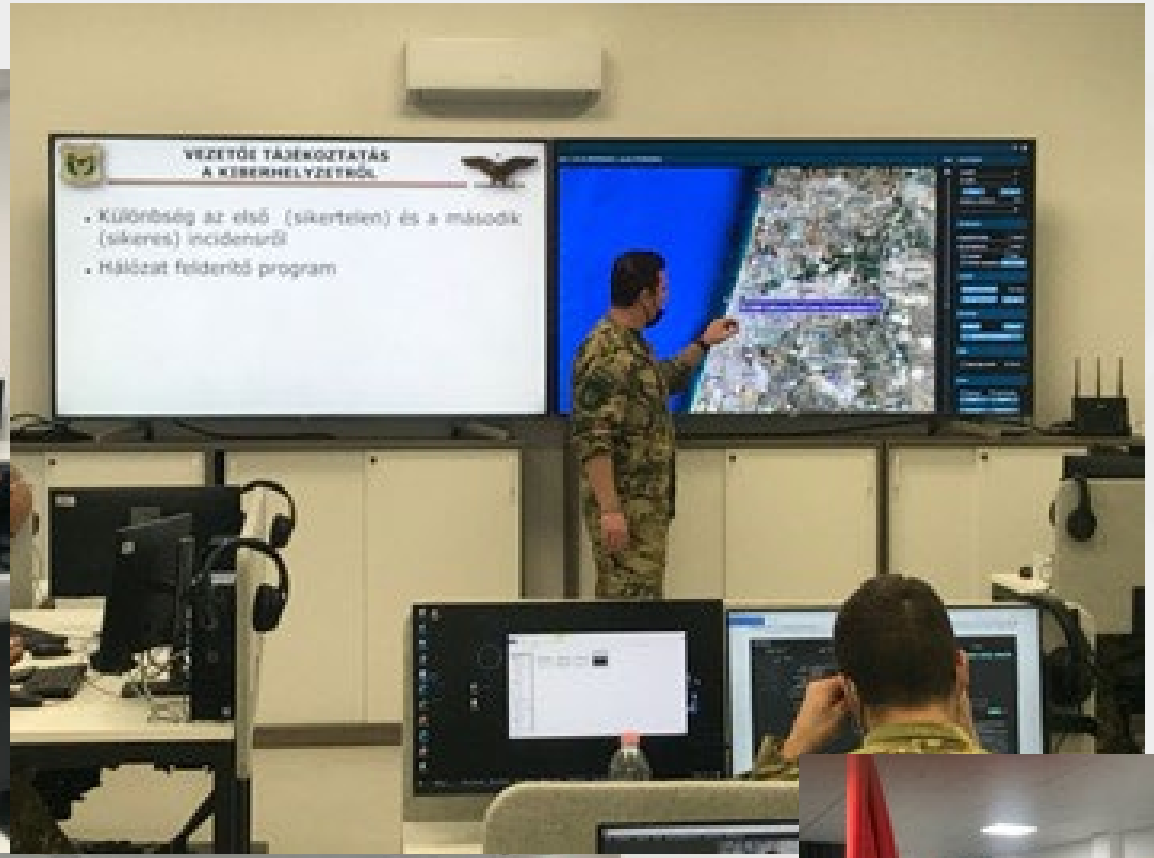


Magyarország: kibervédelmi szervezeti keretrendszer



MH Kiber- és Információs Műveleti Központ









Magyar Honvédség Kiberakadémia











Következtetések

Információs műveletek szerepe felértékelődik:

- STRATCOM szerepe: háborús narratíva vs. orosz narratíva
- média műveletek (különleges katonai műveletek vs. háború)
- social media szerepe
- fake news kiszűrésének nehézségei (elemzői kapacitás, szoftvertámogatás, gyakorlat és tapasztalat)

Kiberműveletek:

- masszív DDoS támadások, de nem átütők, ezért fókusz a fizikai dimenziókon van
- célzott nagyon gyors kibertámadások (pl. wiper), felderítés hatékonysága (!)
- állami támogatású csoportok mellett a hazafias hacker csoportok aktivizálódása (RUS támadja a Swift-et!)
- nemzetközi hacker csoportok megjelenése és aktivizálódása mindkét oldal részéről, nem egyértelmű előny
- Magyarország nem kiemelt célpont, de...



Kovács László (2018): A kibertér védelme.
Dialóg Campus Kiadó, Budapest.
http://kovacsx.hu



Kovács László (2018): Kiberbiztonság és -stratégia.
Dialóg Campus Kiadó, Budapest
http://kovacsx.hu



Kovács László:
Hadviselés a 21. században: kiberműveletek
Budapest, Ludovika Egyetemi Kiadó (2023)

https://webshop.ludovika.hu/termek/konyvek/hadtudomany/hadviseles-a-21-szazadban-kibermuveletek/



Krasznay Csaba (Szerk.):
Taktikák és stratégiák a kiberhadviselésben
Budapest, Ludovika Egyetemi Kiadó (2023)

https://webshop.ludovika.hu/termek/konyvek/hadtudomany/taktikak-es-strategiak-a-kiberhadviselesben/

KÖSZÖNÖM A FIGYELMET!

Dr. Kovács László dandártábornok, DSc

Nemzeti Közszolgálati Egyetem

egyetemi tanár

kovacs.laszlo@uni-nke.hu