NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Kiberhadviselés az ukrán-orosz háborúban

Dr. Krasznay Csaba
intézetvezető
Kiberbiztonsági Kutatóintézet

Szun Ce és a kiberhadviselés

Szun-ce mondotta:

Minden csatában egyenes támadással vehetjük fel az érintkezést az ellenséggel, de cselvetéssel győzünk. Ezért aki ért hozzá, hogyan alkalmazzon cselvetést, az (képességeiben) határtalan, mint az ég és föld [a természet], és kimeríthetetlen, akár a folyók és folyamok.

Negyedik generációs hadviselés

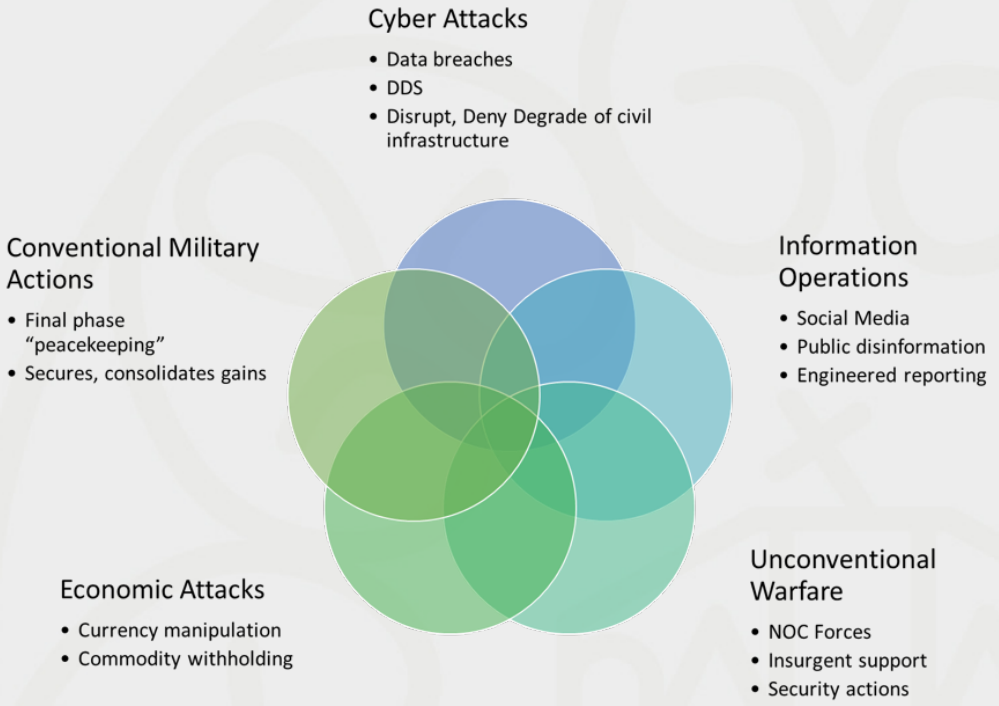
Forrás: Jobbágy Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai. – Fogalmi kitekintő

XX. századi háború a XXI. század információs terében

Harmadik generációs hadviselés: „A harci siker kivívása legfontosabb eszközének a gyors mozgások végrehajtását, az erők és eszközök meglepetésszerű alkalmazását, a mélységi hadműveletek végrehajtását, a bombázókkal felszerelt gépesített hadseregek alkalmazását, a totalitás elvének követését, a hátország háborúba történő bevonását és támadását tartották. A harc megvívásának legfontosabb célkitűzése részben az ellenség erejének megsemmisítése mellett harci kedvének megtörése, az erők és eszközök ellátásának, valamint az információcserének a megakadályozása volt.”

Hibrid hadviselés

- A hibrid fenyegetések felölelik a hadviselés teljes spektrumát, beleértve a hagyományos képességeket, az irreguláris harceljárásokat és alakulatokat, a válogatás nélküli erőszakot és kényszerítést alkalmazó terrorista akciókat, valamint a bűnügyi zavargásokat. Hibrid háborúkat az állami és a legkülönfélébb nem állami szereplők egyaránt folytathatnak. Ezeket a szerteágazó tevékenységeket egymástól elszigetelt egységek, vagy akár ugyanazon alakulatok is végrehajthatják, de ezek általános műveleti és harcászati irányítása és koordinálása a fő harctéren történik annak érdekében, hogy szinergikus hatásokat érjenek el a konfliktusok pszichológiai és fizikai dimenzióiban egyaránt. Ezen hatások a háború valamennyi szintjén elérhetők. *Frank G. Hoffmann: Conflict in the 21st Century: The Rise of Hybrid Wars*



Hibrid elemek az orosz-ukrán háborúban

Hagyományos hadviselés

- Oroszország "békefenntartásra hivatkozva indította a műveletet.
- A hadművelet során először speciális egységekkel és belügyi alakulatok beküldésével próbálkoztak az eredmények fenntartása érdekében

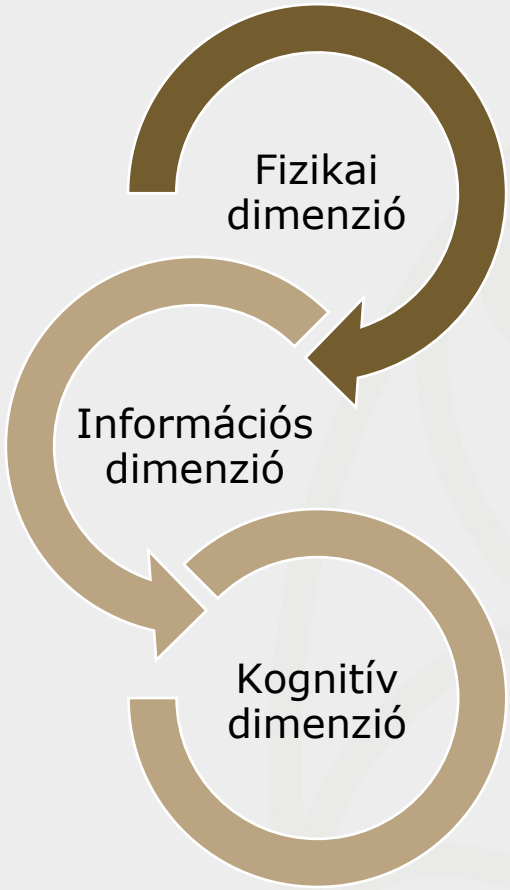
Gazdasági támadások

- A legerősebb pénzügyi szankciók bevezetése Oroszországgal szemben.
- Fejlett technológiától való elrekesztés
- Vezetők vagyonának befagyasztása

Nem konvencionális hadviselés

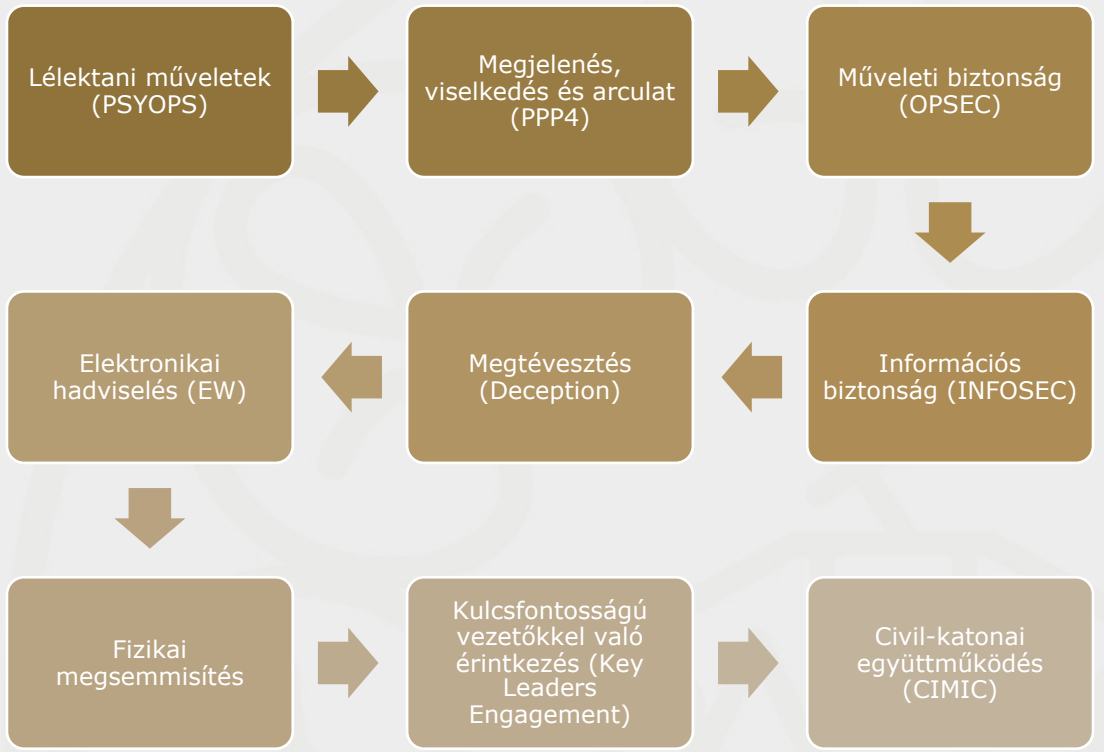
- Beszivárgó orosz műveleti támogatók Kijevben
- A nem-reguláris ukrán felkelők várható támogatása
- Nagyvárosi tisztogató műveletek idegen zsoldosok bevonásával

Információs környezet

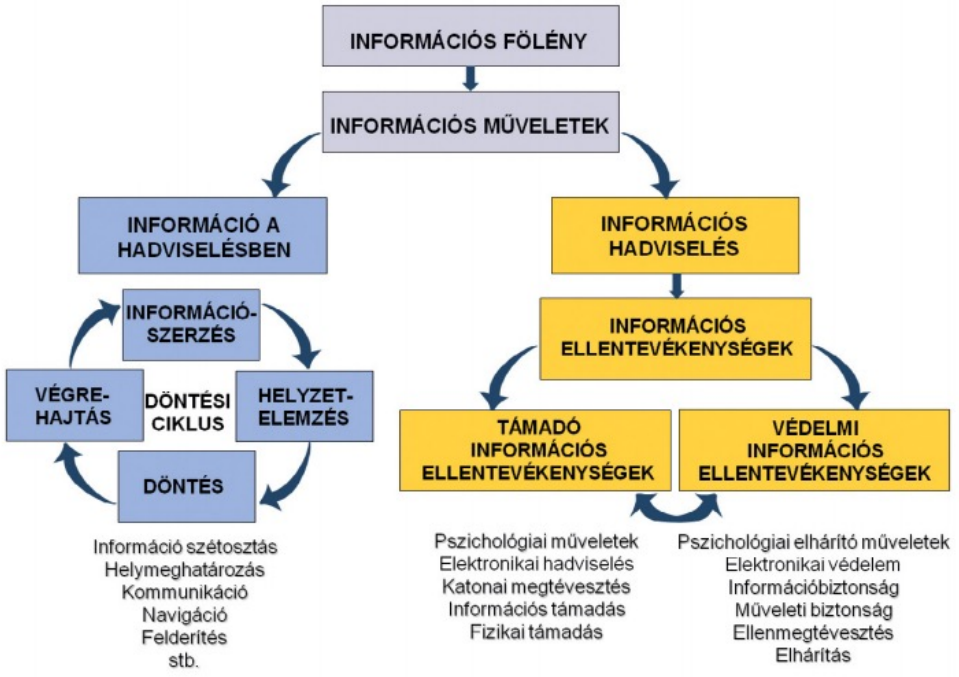


Információs műveletek (INFOOPS)

- Az információs műveletek az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.



Információs fölény



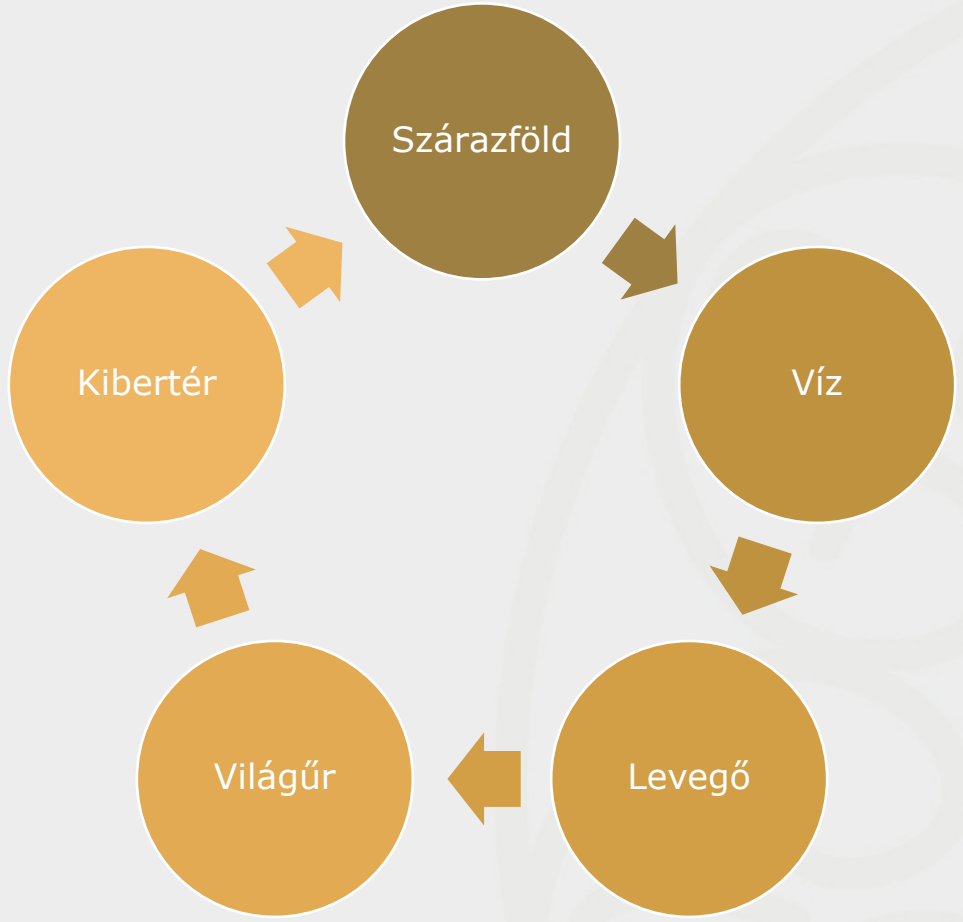
15. ábra

Az USA légierejének az 1998-as doktrína szerinti információs műveletek koncepciója

Forrás: AFDD 2-5 (1998), 3. alapján a szerző szerkesztése

Forrás: Haig Zsolt: Információs műveletek a kibertérben

Az ötödik műveleti tér



Kiberfölény

a különböző elektronikai és informatikai adatgyűjtő eszközökkel, szenzorokkal, valamint kommunikációs eszközökkel az információ biztosítása a másik fél képességeiről, a saját lehetőségekről és a környezetről

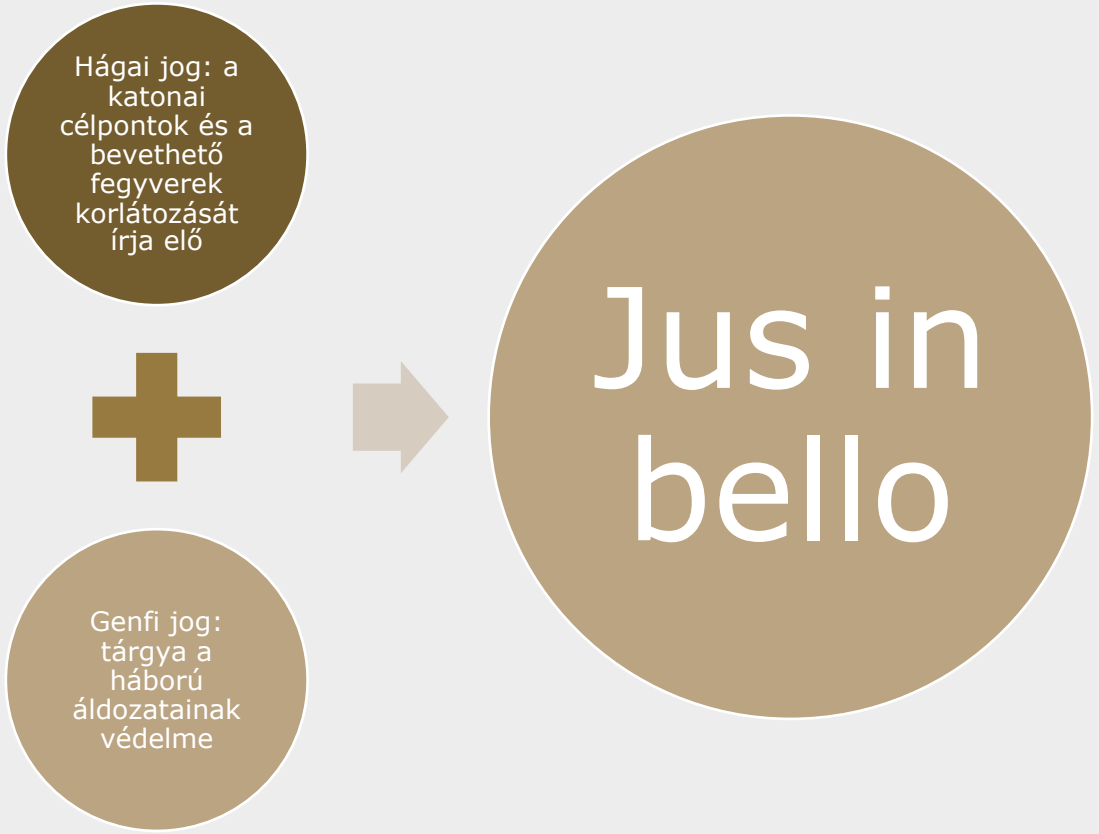
a másik fél hálózatos infokommunikációs rendszerei működésének akadályozása, az információ feldolgozásának, továbbításának korlátozása és megnehezítése, valamint a döntéshozók és a személyi állomány infokommunikációs hálózatokon keresztüli befolyásolása;

a saját hálózatos információs képességek, valamint a saját döntéshozók és a személyi állomány védelme a másik fél hálózaton keresztül megvalósított különböző logikai és fizikai (elektronikai) támadásaival, valamint befolyásolási kísérleteivel szemben.

Kibertéri műveletek a.k.a kiberhadviselés

- A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.

Léteznek „kiberháborúk”?



Egy kibertámadás olyan kiberművelet, legyen az akár támadó, akár védelmi jellegű, mely alapján személyek sérülése vagy halála, illetve objektumok megrongálódása vagy megsemmisülése megalapozottan várható.

Tallinni Kézikönyv 92. szabály

Kiberfegyverek

- Tallinni Kézikönyv 103. szabály
  - A kiberhadviselés eszközei a kiberfegyverek és a hozzájuk kapcsolódó kiberrendszerek.
  - A kiberhadviselés módjai azok a kibertaktikák, technikák és eljárások, melyeket az ellenségek bevetnek.
  - Kiberfegyver az, melyet arra használnak, terveztek vagy terveznek használni, hogy személyek sérülését vagy halálát, illetve objektumok sérülését vagy megsemmisülését okozzák.
- Nem (feltétlenül) kiberfegyver:
  - Egy DDoS, amit pl. Észtország 2007-es támadása esetén használtak
  - Az a kártékony kód, mely nem teljesíti a fenti feltételeket
  - Az a szofisztikált 0-day, melyet kémkedésre használnak
  - Az a megoldás, melyet elsősorban védelemre használnak, pl. egy „weaponized honeypot”.

Trojan.Killdisk: az orosz wiper

"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

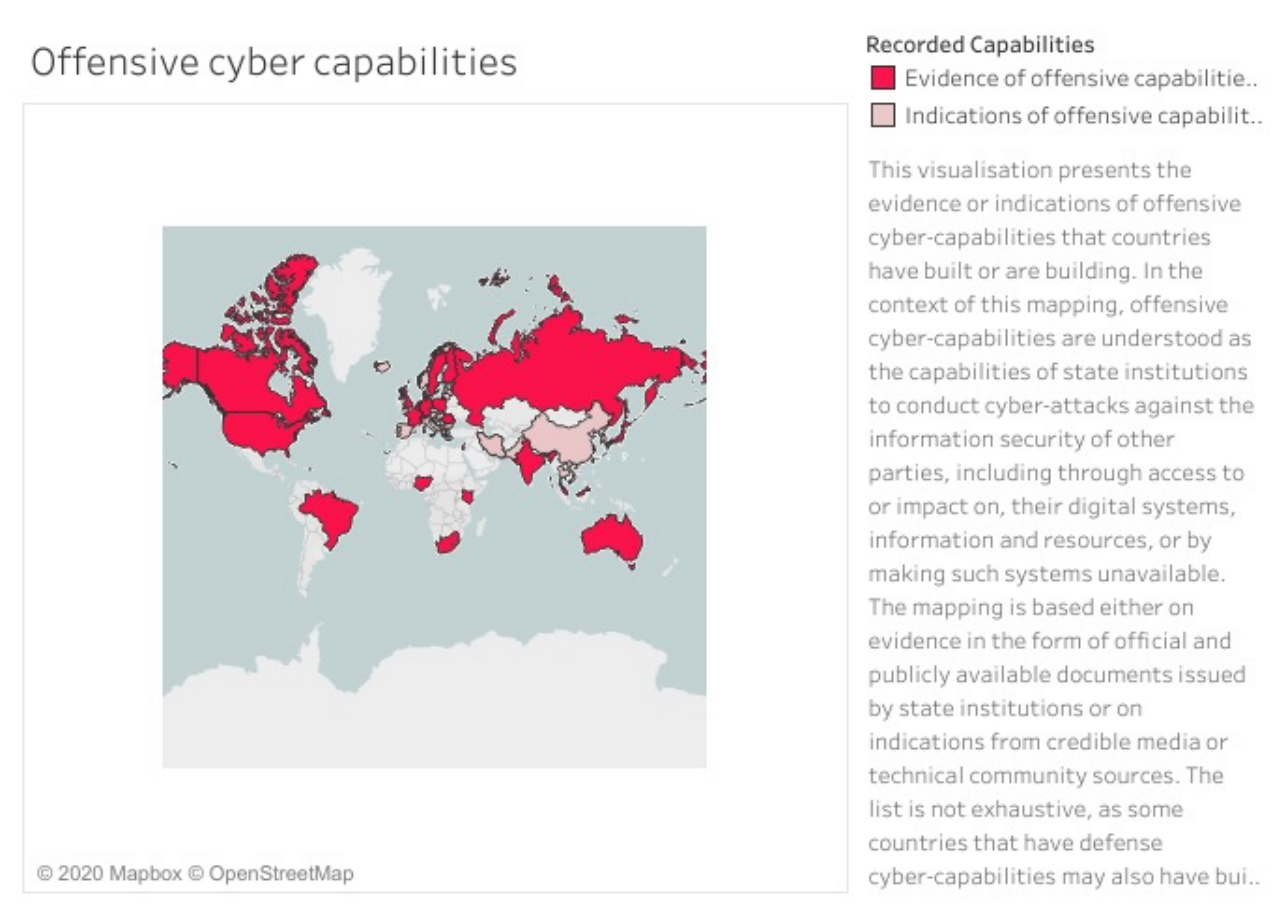
So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

Kiberképességek



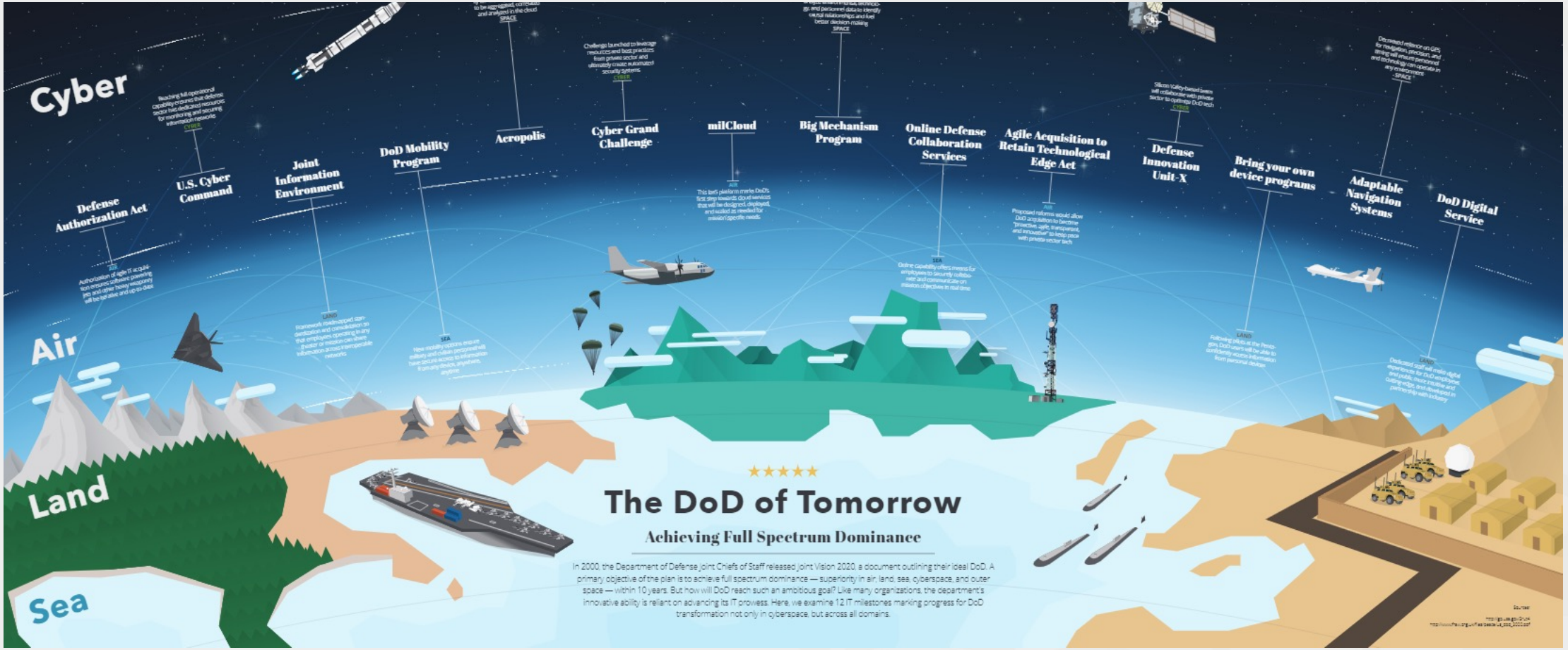
Forrás: https://dig.watch/processes/un-gge

Kiberképességek a két oldalon

GROUP	SUPPORTS	TYPE	COMMS	LOC	Legit
Anonymous Associated					
Anonymous	Ukraine	DDoS/Hack	Twitter	Global	Likely
BlackHawks	Ukraine	DDoS/Hack	Twitter	Georgia	Likely
Anon Liberland & PWN-BAR	Ukraine	DDoS/Hack	UNK	UNK	Likely
LiteMods	Ukraine	Psyops/DDoS	Twitter	UNK	Likely
SHDWSec	Ukraine	Hackivism	Twitter	Global	Likely
RootUser	Ukraine	Radio	Twitter	Ukraine	Likely
N3UR0515	Ukraine	DDoS	Twitter	UNK	UNK
PuckArks	Ukraine	Pysops	Twitter	UNK	Likely
GrenXPaRTa_9haan	Ukraine	Databreach	Twitter	Indonesia	Likely
YourAnonNews	Ukraine	Psyops	Twitter	UNK	Likely
DeepNetAnon	Ukraine	Radio/hack	Twitter	UNK	Yes
Anonymous Younes	Ukraine	DDoS/Hack	Twitter	UNK	Yes
0xAnonLeet	Ukraine	DDoS/hack	Twitter	UNK	Yes
AnonGh0st NEW	Ukraine	DDoS/Hack	Twitter	UNK	Likely
Anonymous Romania NEW	Ukraine	DDoS/Hack	Twitter	Romania	Likely
Nation-State					
GhostWriter UNC1151	Russia	Hack	UNK	Belarus	Yes
SandWorm	Russia	Hack	UNK	Russia	Yes
Gamaredon	Russia	Hack	UNK	Russia	Yes
IT Army of Ukraine	Ukraine	DDoS	Twitter	Ukraine	Yes
IT Army of Ukraine Pysops	Ukraine	Pysops	Twitter	Ukraine	Likely
Internet Forces of Ukraine	Ukraine	Social media	UNK	Ukraine	Yes
Pro-Ukraine Groups					
GhostSec	Ukraine	Hack	Telegram	UNK	Likely
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK	UNK
RaidForums Admin	Ukraine	Sanction	Site	UNK	UNK
GNG	Ukraine	DDoS	Twitter	Georgia	Likely
NB65	Ukraine	Hack	Twitter	UNK	Likely
RaidForums2	Ukraine	DDoS	Twitter	UNK	Likely
ContiLeaks	Ukraine	Databreach	Twitter	UNK	Yes
GhostClan	Ukraine	DDoS/Hack	Telegram	UNK	Likely
1LevelCrew	Ukraine	DDoS	Twitter	UNK	Likely
Hydra UG	Ukraine	Radio	Twitter	UNK	Likely
SecJuice	Ukraine	OSINT/Psyop	Twitter	UNK	Likely
v0g3lSec	Ukraine	Hack	Twitter	UNK	Likely

GROUP	SUPPORTS	TYPE	COMMS	LOC	Legit
NB65-Finland	Ukraine	DDoS	Twitter	UNK	UNK
Monarch Turkish Hacktivists	Ukraine	Defacement	UNK	Turkey	Yes
Shadow_Xor	Ukraine	UNK	Twitter	UNK	UNK
The connections	Ukraine	UNK	Twitter	UNK	UNK
TrickLeaks (new trickbots)	Ukraine	Databreach	Twitter	UNK	Yes
Spot (ATW)	Ukraine	Databreach	Twitter	Europe	Yes
Blue Hornet (ATW)	Ukraine	Databreach	Twitter	Europe	Yes
M3meryK1tten	Ukraine	Hack/support	Twitter	UNK	Likely
SecDet NEW	Ukraine	Hack	Twitter	US	Yes
Crystal_MSF NEW	Ukraine	Hack/DDoS	Twitter	UNK	Yes
Rabbit Two NEW	Ukraine	Hack/DDoS	Twitter	UNK	Yes
Pro-Russia Groups					
RedBanditsRU	Russia	Hack	Twitter	Russia	Yes
Free Civilian	Russia	Databreach	Site	UNK	Likely
CoomingProject	Russia	Databreach	Site	UNK	UNK
Stormous Ransomware	Russia	Ransomware	Telegram	UNK	Yes
Digital Cobra Gang	Russia	Dox/DDoS	Twitter	Russia	Likely
Xaknet	Russia	Hack	Site	Russia	Yes
Killnet	Russia	Hack/DDoS	Telegram	Russia	Likely
Hidden Cobra (Rumour)	Russia	UNK	UNK	UNK	UNK
RaHDit	Russia	Hack	UNk	Russia	UNK
Devilix-EU	Russia	UNK	Twitter	Russia	UNK
DragOn	Russia	Hijack	Twitter	Russia	Yes
404 Cyber Defense	Russia	DDoS	Twitter	UNK	Likely
Unknown Support					
NetSec	UNK	Databreach	Twitter	UNK	Yes
Conti ransomware gang	UNK	Ransomware	Site	Russia	Yes
ECO	UNK	DDoS/Hack	Twitter	UNK	Likely
KEY					
Legit indicators:	UNK = not confirmed if they have done claims				
	Likely = Provided evidence but unclear if true				
	Yes = security professionals vet -Attacks confirmed				
NEW = Added to this list does not mean the group is newly active.					
Any Tips/changes = https://twitter.com/Cyberknow20					

Teljes spektrumú fölény



Kiberműveletek az orosz-ukrán háborúban

- Az információs tér uralása
- Polgári és kormányzati IT rendszerek támadása
- Kritikus (információs) infrastruktúra támadása
- Katonai kiberműveletek

Niccolo Machiavelli: A fejedelem

- Hanem a rómaiak előrelátva a nyavalyákat, tüsténT orvoslást kerestek rájuk, s hogy elkerüljék a hosszadalmas háborút, nem hagyták a bajokat elhatalmasodni; tudták, hogy a háború elkerülhetetlen, s később csak ellenfeleik javát fogja szolgálni. Ezért hadjáratot indítottak Görögországban Fülöp és Antiochus ellen, hogy ne legyen dolguk velük Itáliában: ekkor még elkerülhették volna az összeütközést egyikkel is, másikkal is, de nem akarták. S bár nekik sohasem tetszett, amit bölcseink szájából hallunk unos-untalan, hogy éljünk az idő jótéteményével, mégis vitézek és előrelátók voltak; mert az idő sürget, s egyképpen hozhat magával jót is, mint rosszat; és rosszat, mint jót.
- Ha valaki most azt mondaná, Lajos király azért engedte át Sándornak Romagnát, a spanyolnak a Királyságot, hogy megmenekedjék a háborútól, a fenti indokkal felelem: soha nem szabad a háború helyett a zűrzavart választanod. Az előbbit úgysem a kerülheted el, az utóbbi pedig károdra fog kiütni.

Összefoglalás

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu