A kritikus infrastruktúrákat célzó *hibrid kiberműveletek evolúciója*

Dr. Krasznay Csaba BME CrySyS Lab · egyetemi docens

Honnan indultunk? a fizikai hatás paradigmája

2010 | STUXNET

kiber → ipari folyamat → fizikai károkozás

→

2015–16 | UKRÁN ENERGIA

villamosenergia-rendszer elleni kibertámadások

→

2017 | NOTPETYA

az IT bénítása is leállíthat fizikai működést

KORAI FENYEGETÉSKÉP: KIBER → OT → FIZIKAI HATÁS

2022: kitör a háború de nem jön el a „cyber Armageddon”

WHISPERGATE / HERMETICWIPER

destruktív műveletek, kormányzati és vállalati IT

VIASAT / KA-SAT

katonai kommunikáció + civil spillover

INDUSTROYER2

célzott OT-támadás az energiaszektor ellen

A kiberműveletek nem váltották ki a kinetikus műveleteket.

Beépültek a háború teljes műveleti rendszerébe.

A háború 5. éve tart a kiberműveletek fejlődnek

ROMBOLÁS
wiper • OT

ZAVARÁS
DDoS • szolgáltatás

FELDERÍTÉS
hozzáférés • előpozicionálás

ADATLOPÁS
hírszerzés • célpontképzés

BEFOLYÁSOLÁS
leak • narratíva

A cél már nem feltétlenül az, hogy „lekapcsoljunk” valamit.

A hozzáférés, az információ és a társadalmi hatás önmagában is stratégiai érték.

2026: mit jelent a hibrid művelet? Definíciós kérdések

D — DIPLOMACY

politikai nyomás
kényszerítés

I — INFORMATION

FIMI • propaganda
cyber

M — MILITARY

kinetikus művelet
fenyegetés

E — ECONOMY

energia • kereskedelem
gazdasági kényszer

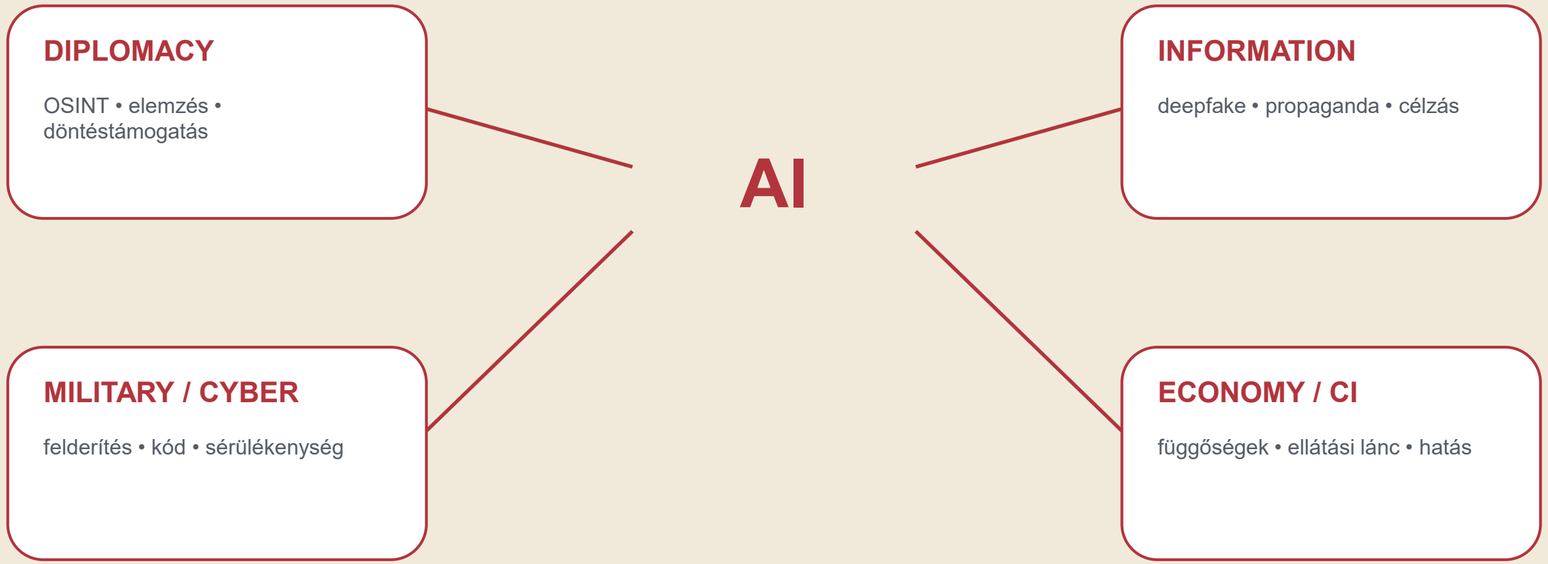
D + I + M + E

„coordinated harmful activities … through a variety and often a combination of means”

Council of the European Union, Hybrid threats / Council Conclusions, 2026

A „hybrid” nem egy támadástípus. Az eszközök összehangolásának módja.

Mesterséges intelligencia: a hibrid műveletek multiplikátora



AI × DIME → gyorsabb • olcsóbb • skálázhatóbb • személyre szabottabb művelet

CYBERSEC

A kritikus infrastruktúra és a célpont fogalma kitágult

OT
ipari vezérlés

IT
üzleti működés

FELHŐ
digitális szolgáltatás

TELEKOM
kapcsolat

ŰR
navigáció • kommunikáció

ELLÁTÁSI LÁNC
beszállítók

EMBER
emberek • döntések

A célpont nem egy PLC vagy szerver: egy kritikus SZOLGÁLTATÁS működőképessége.

Európa válasza: a védelemtől a rezilienciáig

NIS → NIS2

szélesebb ágazati kör
kockázatkezelés
ellátási lánc
incidenskezelés
vezetői felelősség

CER

kritikus szervezetek ellenálló képessége
all-hazards megközelítés
fizikai + szervezeti reziliencia

TÁGABB EU-ÖKOSZISZTÉMA

CRA • DORA
Cyber Solidarity
koordináció és termékbiztonság

A szabályozás fókusza is a szolgáltatás és az ökoszisztéma ellenálló képessége felé mozdult.

CYBERSEC

Kibervédelemtől ellenállóképességig



Nem tudunk minden támadást megakadályozni.

A kérdés az, hogy egy sikeres kibertámadásból lesz-e sikeres stratégiai művelet.

15 év evolúciója mi változott?

2010 körül

KIBER
↓
OT
↓
FIZIKAI KÁR

→

2026

KIBER + INFORMÁCIÓ + ŰR
+ PROXY + GAZDASÁG + KINETIKUS

↓
KRITIKUS SZOLGÁLTATÁS
↓
REZILIENCIA

A hibrid kiberművelet célpontja végső soron nem az informatikai rendszer, hanem a társadalom működőképessége.

Köszönöm a figyelmet!

Dr. Krasznay Csaba
krasznay.csaba@crysys.hu