HORVÁTH LÁSZLÓ

KIBERVÉDELMI KÉRDÉSEK A HONVÉDELEMBEN

A 21. századi hadviselés digitális dimenziói — Magyarország és a NATO szemszögéből

2026. április 16.

ELŐADÁS FELÉPÍTÉSE

01 **A kibertér mint hadszíntér**

A hagyományos hadviselés határain túl

02 **Globális fenyegetések 2025–2026**

Állami szereplők, APT-csoportok, hibrid hadviselés

03 **Magyarország kibervédelmi struktúrája**

MH szervezetrendszer, KNBSZ, NCC-HU

04 **NATO kibervédelem – Cyber Coalition 2025**

Kollektív védelem, 32 szövetséges

05 **Kritikus infrastruktúra védelme**

Energetika, kommunikáció, logisztika

06 **AI és technológiai fejlesztések**

Mesterséges intelligencia a kibervédelemben

07 **Jogi és doktrinális kérdések**

NIS2, Nemzeti Kiberbiztonsági Stratégia 2025

08 **Összefoglalás & Záró gondolatok**

Teendők, fejlesztési irányok

01 | A KIBERTÉR MINT HADSZÍNTÉR

SZÁRAZFÖLD

TENGER

LÉGTÉR

VILÁGŰR

KIBERTÉR

NATO: "A kibertér minden időben vitatott." -- NATO Stratégiai Koncepció 2022

Aszimmetria

Kis befektetéssel nagy pusztítás — állami és nem állami szereplők egyaránt képesek rá

Folyamatos versengés

A kibertérben nincs béke — az ütközetszint alatti műveletek állandóak

Plausible deniability

A támadások nehezen attribuálhatók, az agresszor identitása elrejthető

Kritikus infrastruktúra

Energia, víz, közlekedés, pénzügy — minden digitalizált rendszer célpont

02 | GLOBÁLIS KIBERFENYEGETÉSEK 2025–2026

OROSZORSZÁG

GRU Unit 54654, APT28, Sandworm

KÍNA

APT40, Volt Typhoon, kritikus infra

ÉSZAK-KOREA

Lazarus Group, zsarolóvírus

IRÁN

APT33, proxik, Közel-Kelet

HIBRID HADVISELÉS NAPJAINKBAN: Kibertámadások, dezinformáció, szabotázs és a migráció fegyverként való alkalmazása.

“Kiberhírszerzés”

Katonai titkokhoz, tervekhez való hozzáférés

Dezinformáció

Közvélemény manipulálása, szövetségi rendszerek bomlasztása

Infrastruktúra-támadás

Energia, víz, kommunikáció leállítása

Zsarolóvírus

Állami szervek, kórházak, védelmi cégek

03 | A HONVÉDELEM KIBERVÉDELMI SZERVEZETRENDSZERE

Honvédelmi Miniszter

Hatósági felügyelet

HVK Kiber- és Információs Műveleti Csoportfőnökség

Stratégia, kiber- és információs műveletek

MH Kiber- és Információs Műveleti Központ

Kiberképzés, hazai és nk. együttműk., nem kinetikus műveletek

KNBSZ Kibertér Műveleti Központ

Incidenskezelés, sérülékenységvizsgálat

Honvédelmi Kiberbiztonsági Hatóság

hatósági felügyelet, kiberbiztonsági tanúsítás

NEW Jelentős lépések 2025-2026

- Új Kiberbiztonsági Törvény
- Nemzeti Kiberbiztonsági Akcióterv
- Óbudai Egyetem–MH együttműködési megállapodás: AI-alapú kibervédelmi eszközök fejlesztése
- Honvéd Kibervédelmi Szaktechnikusi és AI Szaktechnikusi képzés indítása
- NCC-HU (Nemzeti Kiberbiztonsági Koordinációs Központ) NBSZ-hez rendelése

04 | NATO KIBERVÉDELEM — CYBER COALITION 2025

1 300+

Résztvevő kibervédő

29 NATO + 7 partner állam

32

NATO szövetséges

Kollektív kibervédelem

2025

NATO Hágai Csúcs

5% GDP védelmi cél

VCISC

Virtuális Kiberincidens Támogató Képesség

Villámgyors kollektív válasz

Cyber Coalition 2025

Nov. 28–dec. 4., Tallinn (CR14) — NATO egyetlen NATO Secret minősítésű kiberteszt-centruma. Első ízben gyakorolt a VCISC valós multi-exercise környezetben.

Hibrid Fenyegetések Koordinátora

2025-ben új pozíció: Jean Charles Ellermann-Kingombe ASG, aki integrálja a NATO összes hibrid fenyegetéssel kapcsolatos tevékenységét.

Kollektív védelem — 5. cikk

A kibertámadás kellő súlyossága esetén az 5. cikk szerinti kollektív védelmi kötelezettség aktiválható — ez deterrens hatással bír.

05 | KRITIKUS INFRASTRUKTÚRA VÉDELME

Energetika

KRITIKUS

› Erőmű vezérlők (SCADA/ICS)

› Villamoshálózat

› Gáz/olajvezetékek

Kommunikáció

KRITIKUS

› Katonai rádióhálózat

› Titkosított csatornák

› Tengeralattjáró kábelek

Logisztika

MAGAS

› Utánpótlás-lánc

› Szállításirányítás

› Üzemanyag-ellátás

Egészségügy

MAGAS

› Katonai kórházak

› Betegnyilvántartás

› Telemedicina

Pénzügy

MAGAS

› Honvédelmi kifizetések

› Bankrendszer

› Ellátó szerződések

Navigáció/GPS

KRITIKUS

› GPS-zavar (spoofing)

› Drónnavigáció

› Precíziós fegyverek

06 | MESTERSÉGES INTELLIGENCIA A KIBERVÉDELEMBEN

AI A VÉDELEMBEN

✓ **Anomáliadetekció**

ML-alapú valós idejű hálózatfigyelés, ismeretlen fenyegetések azonosítása

✓ **Automatizált válasz**

SOAR platformok — másodperceken belüli incidensmegoldás

✓ **Prediktív analitika**

Támadási minták előrejelzése korábbi adatok alapján

✓ **Természetes nyelvfeldolgozás NLP**

OSINT elemzés, darkweb-monitorozás automatizáltan

✓ **MH–Óbudai Egy. kutatás**

Közös AI-alapú kibervédelmi eszközfejlesztés (2025)

AI A TÁMADÁSBAN

✗ **Deepfake hadviselés**

Parancsnoki hangok hamisítása, katonai dezinformáció

✗ **AI-vezérelt malware**

Önfejlesztő, adaptív kártékony kódok — nehezebben észlelhetők

✗ **Spearphishing 2.0**

Személyre szabott, AI-generált csali üzenetek

✗ **Automatizált APT**

Nagy sebességű, skálázható fejlett tartós fenyegetések

✗ **Kognitív hadviselés**

Social media manipuláció, katonai morál rombolása

07 | JOGI ÉS DOKTRINÁLIS KÉRDÉSEK

NIS2 irányelv (EU 2022/2555)

› Kiberbiztonság kötelező magas szintje EU-szerte

› Honvédelmi ipari vállalatok kötelezettségei

› Incidensjelentési határidők (24h/72h)

› SZTFH felügyeli a piaci szereplőket

Tallinn Manual & NATO Jog

› Mikor aktiválható az 5. cikk kibertámadásra?

› Arányossági elv — válasz mértéke

› Attribúciós probléma a jogalkalmazásban

› Lex specialis vs általános hadijog

Nemzeti Kiberbiztonsági Stratégia 2025

› Magyar Közlöny 2025/35. szám

› Honvédelmi ágazati kibervédelmi rendszer

› Nemzeti Kiberbiztonsági Munkacsoport

› Digitális szuverenitás erősítése

Haderőfejlesztés

› Kibervédelmi képesség fejlesztése kiemelt cél

› Modern vezetési rendszer kialakítása

› Honvédelmi kiberbiztonsági incidenskezelő

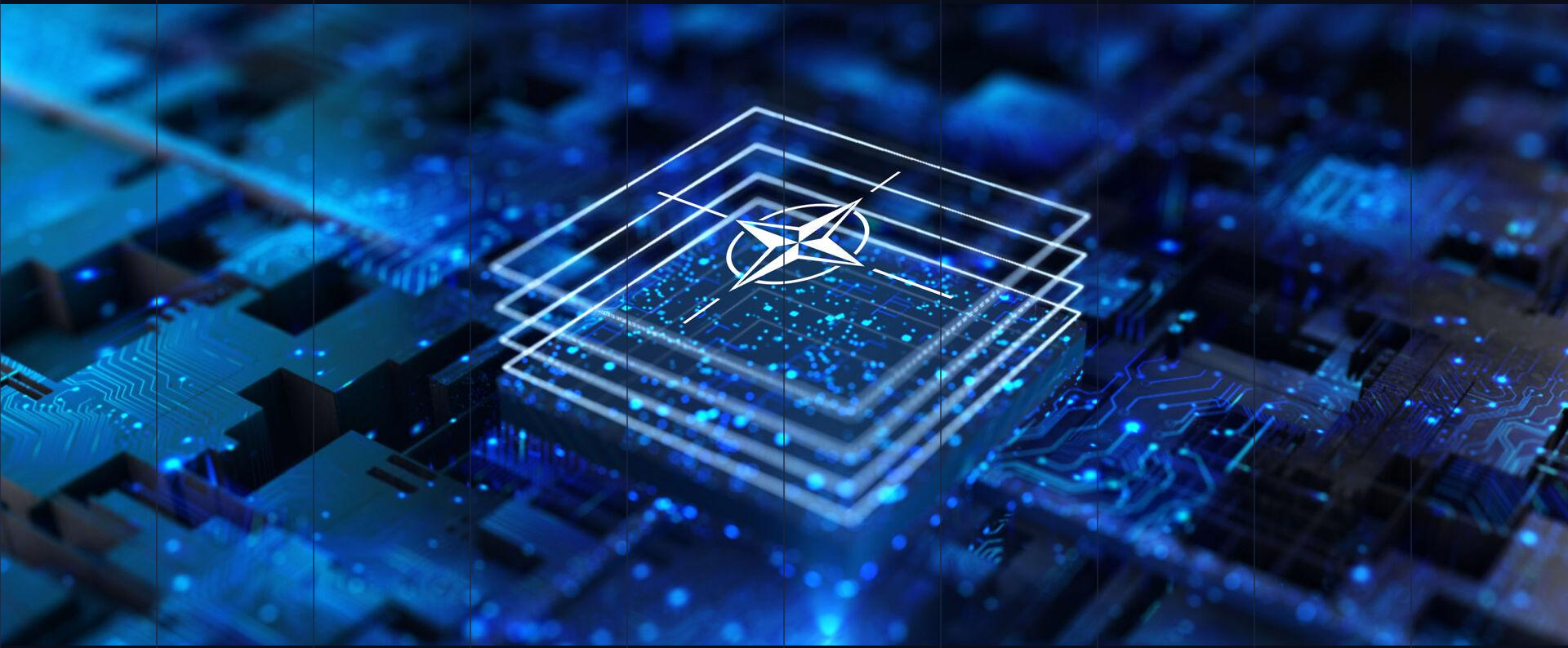
› NATO-képességfelajánlások teljesítése

08 | ÖSSZEFOGLALÁS ÉS ZÁRÓ GONDOLATOK

1. A kibertér ötödik hadszíntérként kiemelkedő prioritást élvez — a NATO stratégiai koncepcióban is rögzített.
2. Magyarország folyamatosan fejleszti kibervédelmi struktúráját — HVK KIMCSF, MH KIMK, KNBSZ, NCC-HU.
3. A hibrid hadviselés (orosz/kínai) ötvözi a kibertámadásokat, dezinformációt és fizikai szabotázst — holisztikus védelmet kíván.
4. Az AI kétélű fegyver: védekezés és támadás terén egyaránt alkalmazzák — folyamatos képességfejlesztés szükséges.

Záró gondolatok:

Kibervédelmi szakember-utánpótlás erősítése • NIS2 teljeskörű implementáció • NATO Cyber Coalition aktív részvétel • AI-alapú eszközök integrálása • Kritikus infra SOC-ok kiépítése • Szoros civil- és katonai együttműködés



KÖSZÖNÖM A FIGYELMET!