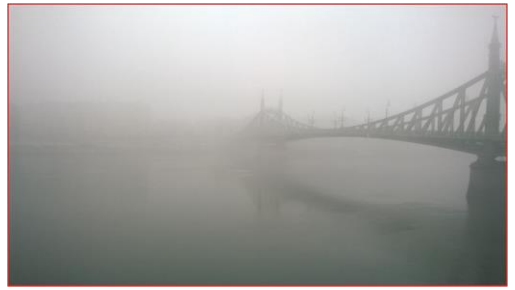
A kibertér keretrendszerének stratégiai szintű változásai, fontosabb hatások
(amelyek cselekvési irányokat mutatnak számunkra…)

Infokommunikáció 2023 Konferencia

Budapest, NKE, 2023. 11. 15.

Dr. Kassai Károly

Tartalom



- **Fenyegetések, EU, NATO stratégiai irányok**
  - Összetett, bonyolult biztonsági helyzet
- **Változást jelentő folyamatok**
  - Rengeteg nemzetközi változás

- **Honvédelmi gondolatok**
  - A honvédelmi folyamatok, eljárások naprakészsége

Stratégiai irányok

- **Fenyegetések**
  - Stratégiai versenykörnyezet, fokozódó stratégiai verseny, összetett biztonsági fenyegetések
  - A nyílt tenger, a légtér, a világűr és a kibertér egyre inkább vitatott, műveleti terület
  - NATO elrettentés és védelem: a nukleáris, a hagyományos és a rakétavédelmi képességek megfelelő összetételén alapul, amelyet űr- és kiberképességek egészítenek ki
  - a világűr és a kibertér biztonságos használatának és korlátlan hozzáférésének biztosítása
- **2022-es reagálások a biztonsági helyzet változásaira**
  - NATO Stratégiai Koncepció (2022): biztonsági és katonai cselekvési irányok kijelölése
  - EU Stratégiai Iránytű (2022): iránymutatás a következő 5 - 10 évre a stratégiák, szakpolitikák számára
- **Hibrid szemlélet – ellenállóképesség fejlesztés**
  - Összkormányzati szemlélet – a komplex megközelítés szükségessége!

EU fejlett kockázatok 2023

EU Gazdasági Biztonsági Stratégia (2023), fő kockázattípusok

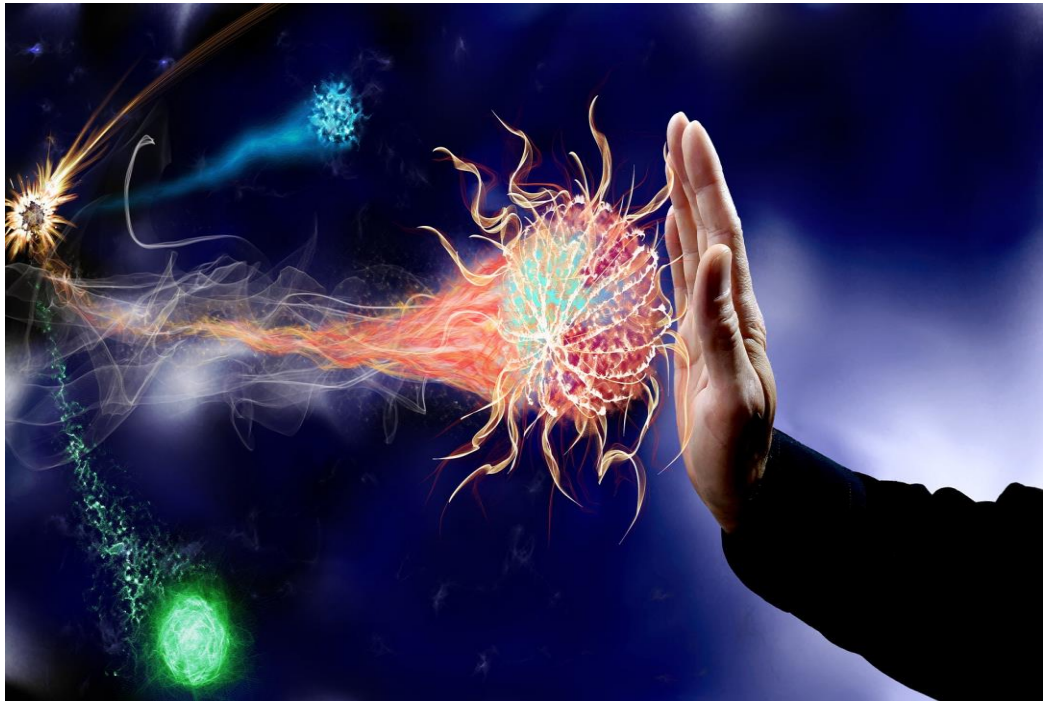
- Ellátási láncok ellenállóképessége, beleértve az energiabiztonságot
- Kritikus infrastruktúra fizikai és kiberbiztonságával kapcsolatos kockázatok
- Technológiai biztonsággal és a technológia kiszivárgásával kapcsolatos kockázatok
- Gazdasági függőségek és a gazdasági kényszerítés fegyverként való felhasználásának kockázata

EU Tanácsi javaslatok kockázatelemzésre (2023)

- Fejlett félvezető technológiák
- Mesterséges intelligencia technológiák
- Kvantum technológiák
- Biotechnológiák
- Fejlett kommunikációs, navigációs és digitális technológiák
- Fejlett szenzor technológiák
- Űr és hajtómű technológiák
- Energia technológiák
- korszerű anyagok, előállítási és újra-hasznosítási technológiák

ENISA Threat Landscape 2023

- Zsarolóvírus
- Káros kód
- Pszichológiai megtévesztés
- Adatfenyegetés
- Rendelkezésre állás veszélyeztetése (Denial of Service)
- Rendelkezésre állás veszélyeztetése (Internet threats)
- Információs manipulálás, befolyásolás
- Támogatói lánc fenyegetések



EU kritikus szolgáltatások (2022)

- Energia
  - Villamos energia
  - Távfűtés vagy távhűtés
  - Kőolaj
  - Földgáz
  - Hidrogén
- Közlekedés
  - Légi
  - Vasúti
  - Vizi
  - Közúti
  - Tömegközlekedés
- Banki szolgáltatások

- Pénzügyi piaci infrastruktúra
- Egészségügy
- Ivóvíz
- Szennyvíz
- Digitális infrastruktúra
- Közigazgatás
- Világűr
- Élelmiszer-előállítás, -feldolgozás és -forgalmazás

NATO: a nemzeti ellenálló képességre vonatkozó követelmények

- Kormányzat, kritikus kormányzati szolgáltatások folytonossága
- Ellenállóképes energiaellátás
- Az ellenőrizhetetlen tömegmozgások hatékony kezelése
- Ellenállóképes élelmiszer- és vízkészletek
- A tömeges áldozatok és egészségügyi válságok kezelésére való képesség
- Ellenállóképes civil kommunikációs rendszerek
- Ellenállóképes közlekedési rendszerek

Új követelmények >> új megoldások

- **EU kritikus infrastruktúra szolgáltatók, hálózatbiztonsági irányelv (2022)**
  - Az új irányelvek alapján >> 2024-től változó/új NKBS, Lrtv. és Ibtv. valamint a végrehajtási rendeletek, új „Nemzeti Ellenálló Képesség Stratégia”
- **EU Kiber Szolidaritási Rendelet (2023?)**
  - Új funkciók, folyamatok: Cyber Shield (SOC-ok hálózata), Cybersecurity Emergency Mechanism (felkészülés, EU tartalék, kölcsönös segítségnyújtás), Cybersecurity Incident Review Mechanism (ENISA műszaki felülvizsgálat)
- **EU Kiberbiztonsági Jogszabály (CSA) módosítás (2023?)**
  - NIS2 irányelv által bevezetett irányított biztonsági szolgáltatás (MSS) kerüljön tanúsítási kötelezettség alá>> új tanúsítási kérdések
- **EU digitális elemeket tartalmazó termékek kiberbiztonsági követelményei (2023?)**
  - Igazolt termékek igénye, gyártók bejelentési kötelezettsége >> növekedő CSIRT folyamatok, feladatok

Új követelmények >> új megoldások 2

- **EU Űr Stratégia a biztonságért és védelemért (2023?)**
  - Az űr infrastruktúrák kiemelt fontossága>> az új követelményeket át kell vezetni a kritikus infrastruktúra, NIS2 szabályokan (még nem készültek a nemezti végrehajtási elemek!)
- **EU Kibervédelmi Politika**
  - Együttes fellépés, uniós védelmi ökoszisztéma >> Szoros katonai – polgári együttműködés
- **NATO Összhaderőnemi Doktrína (AJP 01) (2022. 12.)**
  - Multidomain műveletek megjelenítése >> át kell vezetni a funkcionális doktrínákon az MDO gondolkodást >> ennek meg kell jelennie a magyar műveletnél is
- **NATO Kiber Műveleti Doktrína (AJP 3.20) (2020)**
  - Új Statégiai Koncepció/Új doktrinális elemek >> át kell vezetni a változásokat, értékelni kell a tapasztalatokat, a magyar kibertér műveleti kérdéseket célszerű felülvizsgálni…
- **Milyen változások szükségesek a Hvt-ben, Nbtv-ben, szervezeti keretrendszerben a kibertér műveletek sikere érdekében???** (Farkas Ádám, 2023 10. 27 konferencia)

A kiberműveletek rejtelmei…

Elektronikus információbiztonság(védelem) – kiberbiztonság

- Folyamatok, feladatok, felelősök (szereplők)

Kibervédelem (DCO) – benne támadás megszakítás

- Folyamatok-feladatok-felelősök (cél, jóváhagyó, határidő)

Offenzív kiberművelet (OCO)

- Folyamatok-feladatok-felelősök (cél, jóváhagyó, határidő)

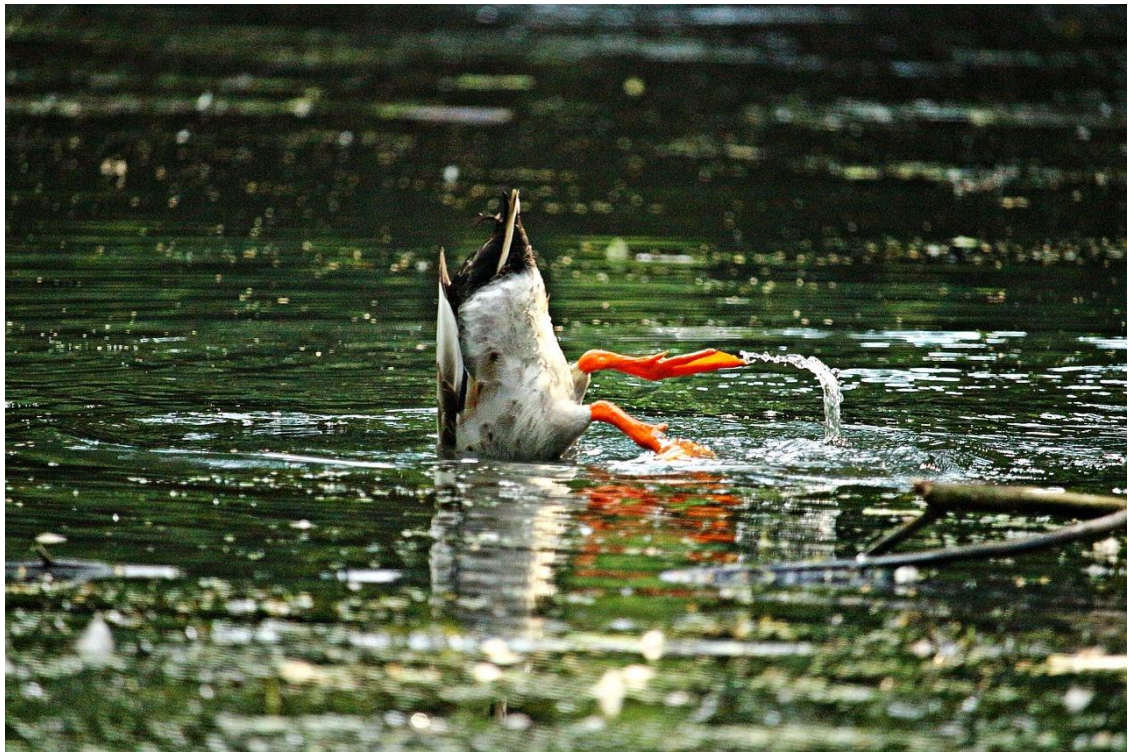
- Biztonsági követelmények, audit (…)
- Oktatás és tudatosítás
- Sérülékenységvizsgálatok
- Eseménykezelés
- Műszaki elemzés (…)
- Kiber hírszerzés (CTI)

- Műveleti koncepció/terv dokumentumok (jóváhagyó, cél, határidő, felelősök, feladatok)
- Katonai műveletbe történő integrálás (önálló művelet vagy támogató feladat)
- Együttműködők …

Összefoglalás

- *(A mesterséges intelligencia tovább bonyolítja a helyzetet… ☺)*
- Egyre súlyosabb hatású fenyegetések >> az EU, NATO válaszoknak tükrözni kell a reagálást, mint elrettentés, ellenálló képesség és együttműködés
  - Alkalmazási, együttműködési és hozzájárulási kötelezettségeink vannak
  - Az uniós, szövetséges és nemzeti biztonsági szolgáltatások ezer szálon függenek az elektronikus szolgáltatásoktól >> nem csak a biztonság, a függőség is stratégiai kérdés!
- A szabályozási felületek fejlődnek, növekednek a kapcsolódási pontok (és szereplők, eljárások, feladatok)
  - Követni kell a szabályozási lépéseket >> nemzeti és katonai eljárok kompatibilitása!
  - Kommunikálni kell, hogy mi a nemzeti álláspont a kibertérben történő események megközelítéséről
- Az EU és a NATO katonai feladatokban markánsan azonosíthatók a kibertér műveleti igények
  - A fejlődésből nem lehet kimaradni >> a szakmai feladatokat, külső kapcsolódási pontokat folyamatosan fejleszteni kell

Köszönöm a megtisztelő figyelmet!



Biztonságos Kiberteret! ☺

Források

1) A biztonság és a védelem területére vonatkozó stratégiai iránytű; Brüsszel, 2022. március 21. 7371/22
2) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
3) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről
4) COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States, Strasbourg, 3.10.2023 C(2023) 6689 final
5) ENISA Threat Landscape 2023

Források 2

6) Farkas Ádám: Az állami kiber képességek szervezésének és szabályozásának aktuális kérdései, Katonai Kibertér 2023 KOnferenccia, Budapest, 2023. 10. 25.
7) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL European Union Space Strategy for Security and Defence; Brussels, 10.3.2023 JOIN(2023) 9 final
8) KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK ÉS A TANÁCSNAK AZ EURÓPAI GAZDASÁGI BIZTONSÁGI STRATÉGIÁRÓL, Brüsszel, 2023.6.20. JOIN(2023) 20 final
9) KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Az EU kibervédelmi politikája, Brüsszel, 2022.11.10. JOIN(2022) 49 final
10) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents COM/2023/209 final

Források 3

11) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
12) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
13) NATO AJP 01 (2022)
14) NATO AJP 3.20 (2020)
15) NATO Stratégiai Koncepció 2022