HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2022

Nemzetközi Katonai Információbiztonsági Konferencia

tudományos szakmai
konferencia

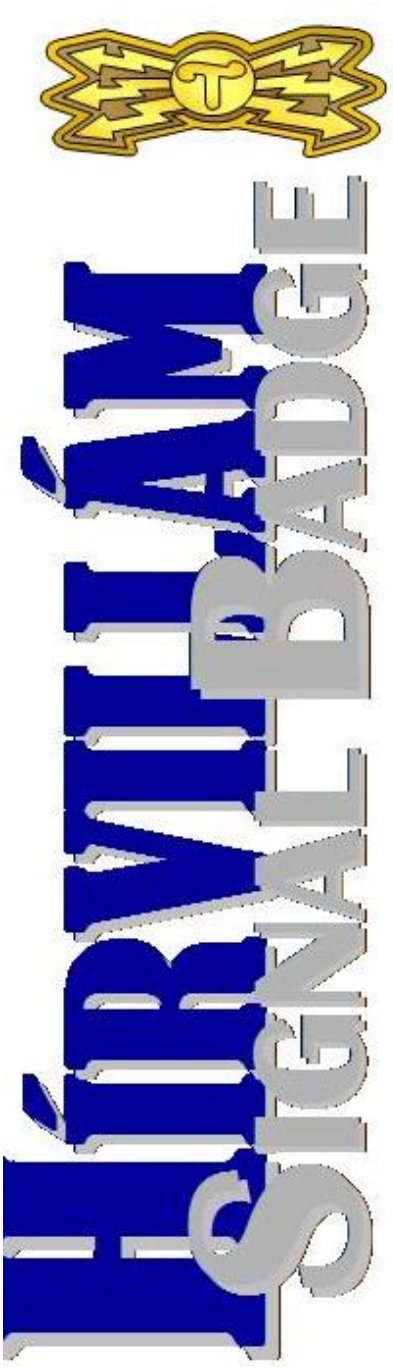
Konferencia kiadvány és korreferátum gyűjtemény

2022. április 27.

HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem, Híradó Tanszék tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement at the University of Public Service

Budapest, 2022



HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-407 mellék)

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Az NKE Hadtudományi és Honvédtisztképző Kar Híradó Tanszéke a Magyar Honvédség Parancsnoksága Infokommunikációs és Információvédelmi Csoportfőnökségével és a Hírközlési és Informatikai Tudományos Egyesület Információbiztonsági Szakosztályával együttműködve „Nemzetközi Katonai Információbiztonsági Konferencia" címmel szervezett tudományos konferenciát 2022. április 27-én a Magyar Honvédség Rekreációs Kiképzési és Konferencia Központban Balatonakarattyán.

A konferencia alapvető célja egy évente megrendezésre kerülő tudományos szakmai fórum biztosítása a kutatási eredmények bemutatása, ismeretterjesztés, valamint kapcsolatépítés céljából.

Jelen kiadványban a szerkesztőbizottság az egyes előadásokból készített korreferátumokat gyűjtötte össze, melyeket nagyon nagy örömmel bocsájt rendelkezésre a Kedves Olvasóknak.

Budapest, 2022. április 27.

Dr. habil. Kerti András
a Szerkesztőbizottság
elnöke

A konferencia programja

A HAZA SZOLGÁLATÁBAN

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Nemzetközi Katonai Információbiztonsági Konferencia
PROGRAM – 2022.04.27.

NAPIREND		
09:30-10:00	Regisztráció	
10:00-10:05	Nyitóbeszéd	Vasvári Géza ezredes
10:05-10:20	Kormányzati kiberstratégia	Prof. Dr. Rajnai Zoltán
10:20-10:35	Introduction of the basic conditions of classified electronic data processing during security incident's	Knapp Gábor alezredes
10:35-10:50	Elektronikai hadviselés az orosz-ukrán hadviselés tükrében	Szatmári Balázs százados
10:50-11:05	MH Kiberdoktrína	Karancsiné Kovács Rita őrnagy
11:05-11:30	Kávészünet	
11:30-11:45	Kibervédelmi gyakorlatok tapasztalatai. „Párhuzamosságok a való világgal."	Dr. Magyar Sándor ezredes
11:45-12:00	The impact of Internet of Things devices on modern warfare	Dr. Tóth András őrnagy
12:00-12:15	Az MH kiberműveleti és információvédelmi feladatai összefüggései	Pozderka Gábor ezredes
12:15-12:30	Az infokommunikációs infrastruktúrák biztonsági kérdései	Dr. Nyikes Zoltán őrnagy
12:30-12:45	Csoportfotó	
13:00-14:00	Ebéd	

Rajnai Zoltán: Kitekintés a hazai kiberbiztonság stratégiai feladataira

Korreferátum

A modern demokráciákban a digitális forradalom az élet minden területére kiterjed, ami jelentős függőséget generál. Manapság a társadalom tagjai kevésbé életképesek, ha nem használnak e-mail címeket, bankszámlákat és kártyákat, vagy valamilyen pozicionáló rendszert. A digitális infrastruktúrák szerepe és jelentősége vitathatatlan, az átlátható állami funkciók, a gazdasági jólét és a sikeres tudományos kutatás megkérdőjelezhetetlen összetevőivé váltak. Egyrészt a modern információs társadalom az információs és kommunikációs technológiákat tekinti a társadalmi evolúció motorjának. Másrészt a függőség kihívásai, a fejlődés dinamikája és a penetráció üteme komoly fenyegetésekkel járnak.

2013-ban Parlamentünk elfogadta a nemzeti kiberbiztonsági stratégiát, ami meghatározza a kiberbiztonság fő céljait és irányait. Ugyanebben az évben pedig közzétettük a kormányzati hálózatok információbiztonságáról szóló törvényt is. Ez a két kiberbiztonsági törvény fekteti le a magyar kiberbiztonsági megközelítés alapjait. Az információbiztonságról szóló törvénnyel létrejött a Nemzeti Kiberbiztonsági Koordinációs Tanács, amely a minisztériumok és az akadémiai szektor képviselőiből áll, azzal a céllal, hogy meghatározza a stratégiában meghatározott célokat. Ez a törvény azt is előirányozza, hogy a nemzeti kiberbiztonsági fórumon

keresztül bevonják a vállalkozások képviselőit a kiberbiztonsági kérdésekbe.

Magyarország kiberkoordinátorának feladatkörét is ezzel a jogszabállyal vezették be, azzal a céllal, hogy összehangolják a technikai és politikai szintet, valamint a kormányzati szándékokat. Magyarország kiberkoordinátorának egyik fő feladata a kormányzati és a magánszektor közötti partnerség és bizalom erősítése is. A Kormány feladata a koordináció, hídként való működés az érintett vállalatok között, az információk megosztása és az érintetteknek segítség nyújtása. Nemzeti Kiberbiztonsági Intézet több magyar céggel is kétoldalú megállapodást kötött a magyar távközlési szolgáltatókkal.

A GovCERT fontos szerepet játszik a kiberbiztonsági folyamatokban, közvetítőként a kutatók és a hálózatgazdák, hálózat tulajdonosok között. A kutatók a talált sebezhetőséggel kapcsolatosan felvehetik a kapcsolatot a GovCERT-tel, kormányzati szervként pedig a bizalmat erősíti mind a kutatás, mind a vállalati szolgálttások iránt. Legtöbbször a GovCERT rendelkezik a hálózatgazdákkal kapcsolatos ismeretekkel, és segíthet nyújthat a talált probléma megoldásában. Magyarországon elvárják, hogy a rendszer sebezhetőségét felfedő kutatók tájékoztassák a rendszerek tulajdonosait a problémákról. De ez számos kihívást jelent.

Fontosnak tartjuk, hogy bizalmat építsünk a sebezhetőségi bejelentésben részt vevő felek között, és mint kormányzati szerv döntő szerepet játszhat a bizalom kiépítésében, a felekkel való koordinációban és az információk megosztásában való

segítségnyújtásban. A bevált gyakorlatok és iránymutatások összegyűjtése és népszerűsítése támogatni fogja ezeket az erőfeszítéseket. Sok munka áll előttünk a sebezhetőségek összehangolt közzétételével kapcsolatos tudatosság növelése terén, de az információk és tapasztalatok nemzetközi szintű megosztása támogatni fogja erőfeszítéseinket.

Az ENISA "Helyes gyakorlat útmutató a biztonsági rések nyilvánosságra hozatalához" című kiadványa azt javasolja, hogy a beszállítók rendelkezzenek olyan szabályzattal, amelyet követniük kell a biztonsági rések felfedezésekor és bejelentésekor. Folyamatban van, hogy felhívjuk a figyelmet ezekre a bevált gyakorlatokra a magyar vállalatok körében.

Nagyon fontos, hogy beszéljünk a nemzetközi fórumokon szerzett tapasztalatokról és bevált gyakorlatokról, hogy közös iránymutatásokra jussunk, de figyelembe kell vennünk a különböző országok különböző helyzetét is, figyelembe kell vennünk a nemzeti sajátosságokat is.

A hálózat- és információs rendszerek biztonságról szóló uniós irányelv (NIS) jelentős előrelépést jelent a magánszektorral való együttműködés terén. Ez az uniós jogszabály a legkritikusabb ágazatok szervezetével is foglalkozik, és meghatározza az állami és magáncégek közötti együttműködés alapvető szintjét. Ez gyorsítja fel a szervezetek közötti bizalom kiépítését és együttműködését. Véleményünk szerint még mindig van mit tenni az állami és a magánszektor közötti együttműködés javítása érdekében.

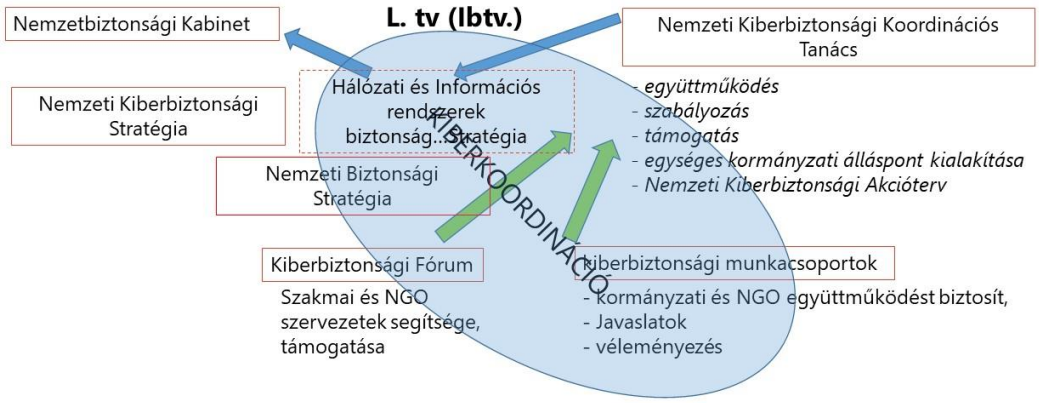
Kulcsszavak: kiberbiztonsági stratégia, digitális infrastruktúra, GovCERT, NIS irányelv

Kitekintés a hazai kiberbiztonság stratégiai feladataira

Az információbiztonság közös felelősségünk!

Prof. Dr. Rajnai Zoltán, Magyarország kiberkoordinátora

Szervezet, funkciók, hatásmechanizmus



Kiberbiztonsági munkacsoportok (elaprózott munkacsoportok)

Belbiztonsági MCS

E-közigazgatási MCS

Energiabiztonsági MCS

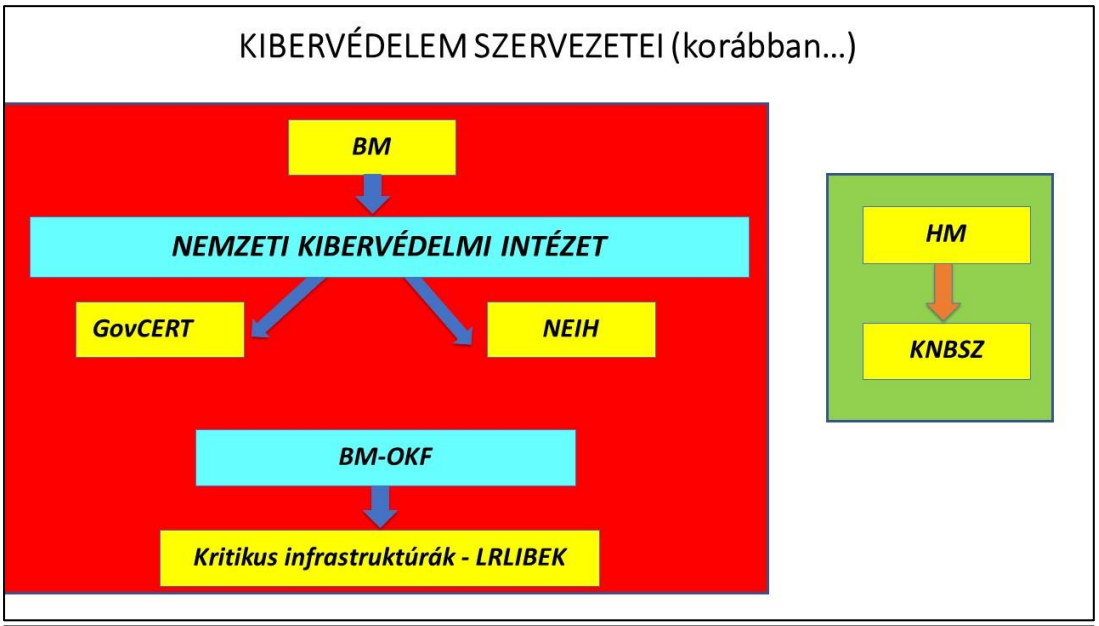
Gyermekvédelmi MCS

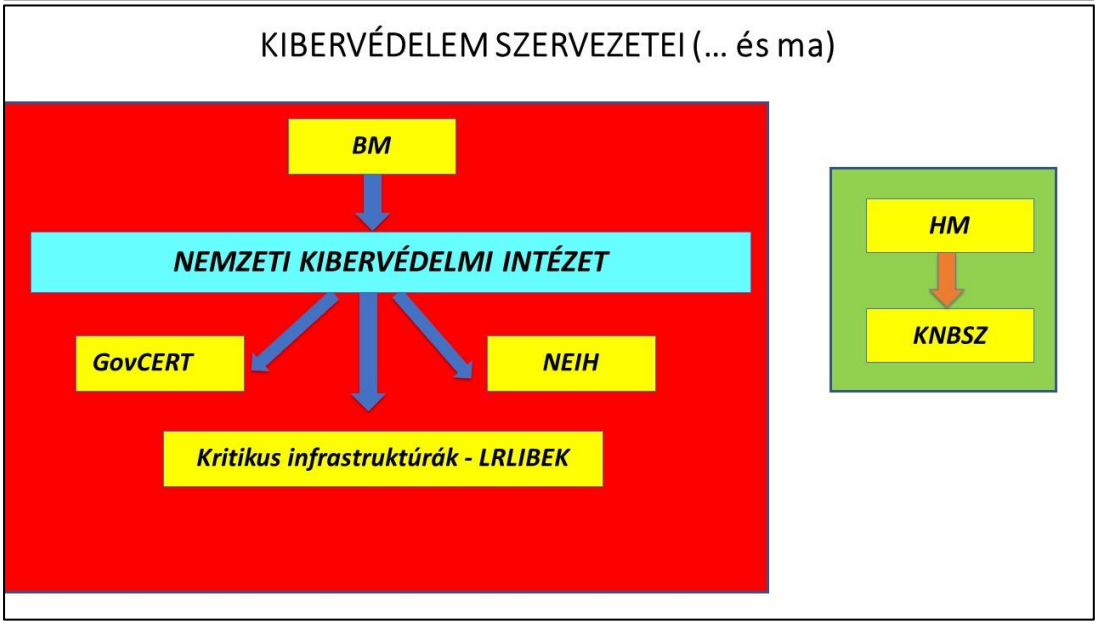
Egészségügyi MCS

Pénzügyi MCS

Stratégiai előzmények

- ***2013.: Magyarország Nemzeti Kiberbiztonsági Stratégiája és Ibtv***
- ***2018.: Hálózati és információs rendszerek bizt. stratégia***
- ***Intézkedési Terv 2020-2024***
- ***Kiberkoordináció átgondolása, átalakítása***
  - ***Nemzeti kiberbiztonsági Koordinációs Tanács***
    - Nemzeti Kibertér Munkacsoport
    - Nemzetközi és Európai Uniós Kibertér Munkacsoport
  - ***Nemzeti Kiberbiztonsági Fórum***


KIBERVÉDELEM SZERVEZETEI (korábban...)
BM
NEMZETI KIBERVÉDELMI INTÉZET
GovCERT
NEIH
BM-OKF
Kritikus infrastruktúrák - LRLIBEK
HM
KNBSZ


KIBERVÉDELEM SZERVEZETEI (... és ma)
BM
NEMZETI KIBERVÉDELMI INTÉZET
GovCERT
NEIH
Kritikus infrastruktúrák - LRLIBEK
HM
KNBSZ

Áttekintés: 259/2021. (V. 20.) Korm. Rendelet 26-29. §

Nemzeti Kiberbiztonsági Koordinációs Tanács

- a belügyminiszter,
- az emberi erőforrások minisztere,
- a honvédelmi miniszter,
- az igazságügyi miniszter
- a külgazdasági és külügyminiszter,
- az innovációs és technológiai miniszter,
- a pénzügyminiszter,
- az agrárminiszter,
- a miniszterelnök kabinetfőnöke
- az NBSz főigazgatója
- a kiberkoordinátor

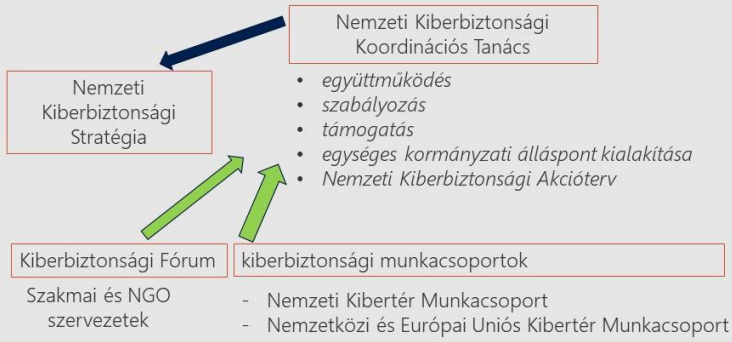
A Tanács munkáját segíti:

- az Állami Számvevőszék elnöke,
- a Magyar Nemzeti Bank elnöke,
- a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke,
- a Nemzeti Hírközlési és Informatikai Tanács elnöke,
- a Nemzeti Média- és Hírközlési Hatóság elnöke,
- a Magyar Energetikai és Közmű-szabályozási Hivatal elnöke vagy az általa delegált

Kiberbiztonsági Fórum

A Tanács által felkért egyetemi, kutatói, szakmai, gazdasági és más nem kormányzati szereplőkből álló Kiberbiztonsági Fórum vezetését a Tanács elnöke, a Fórum munkájának szakmai koordinálását a kiberkoordinátor látja el.

Áttekintés



Intézkedési terv 2020-2022

Minisztériumi válaszok
NKI, HM, KKM, ITM

Olyan fórumot kell biztosítani, ahol lehetőség nyílik a **társadalmi párbeszédre és a széleskörű tájékoztatásra, az etikus hackerek szerepének**, illetve a társadalom és az etikus hackerek viszonyának tisztázására	Elsősorban szakmai fórumok és konferenciák révén valósul meg, melyeken rendszeresen részt vesznek. Például: "Robothadviselés Konf. (2020.05.14); "A Spektrum Stratégia Jövője (2020.11.010.); NKE Nemz. Információbiztonsági Konf. (2020.09-03); Digitális Jólét Fórumok – folyamatosan
Azonosítani kell, hogy mely területen **szükséges javítani a meglévő együttműködésen**	A javítandó együttműködési területek azonosítása és a folyamatos, napi szintű együttműködés biztosított. Az NBSZ NKI 2020-as továbbképzésén bemutatásra kerültek a honvédelmi ágazatot érintő kérdések.
Összehangolt megelőzési, feltárási, mérséklési és reagálási mechanizmusok létrehozása /**információ megosztás, kölcsönös segítségnyújtás**/	A HÁEIBEK (Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ) és a HÁEIBH (Honvédelmi Ágazati Elektronikus Információbiztonsági Hatóság) napi kapcsolatban van az NBSZ NKI-val, mint kiemelt együttműködő partnerrel. A szakmai kérdések egyeztetése, a jogszabályok változtatásával kapcsolatos javaslattétel gyors és folyamatos.

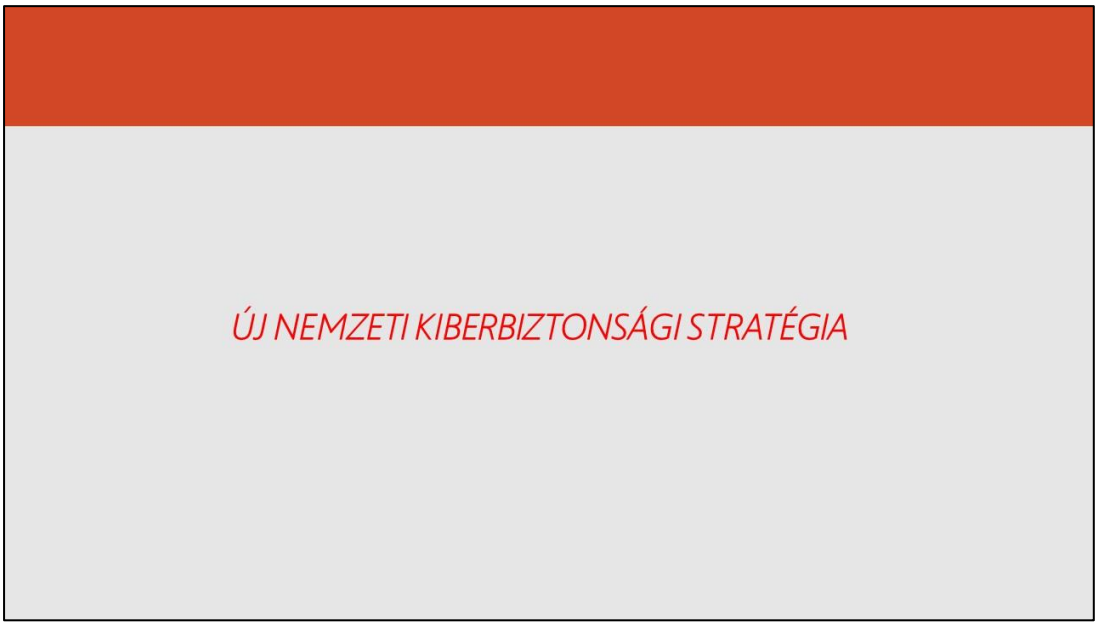
Meghatározott időközönként kiberbiztonsági gyakorlatot kell tartani a reagáló és védekezési képesség továbbfejlesztése érdekében	Rendszeres és aktív részvétel nemzeti kibervédelmi feladatok végrehajtásában. *JAVASLAT: MHP Kiber Akadémia és NKI közös gyakorlatok, KA részvétele az NKI gyakorlatokon*
Működjenek együtt aktívan és osszanak meg információkat az illetékes szervek a **kiber-bűncselekmények elleni hazai és nemzetközi szervezetekben, összefogásokban**	Az eseménykezelés közben szerzett információk társágazati megosztása folyamatos honvédelmi tevékenységet képez (pl. zsarolóvírusok, banki csalási kísérletek adatai, stb.), a bűncselekmények feltárásának elősegítése érdekében. Az ilyen információk az NBSZ NKI CSIRT felé kerülnek továbbításra
Fejleszteni kell a létfontosságú rendszerek, létesítmények és szolgáltatások információbiztonsági hatósági rendszerét az irányelvben megfogalmazott követelmények ágazatokon átívelő érvényesítése érdekében	A hatósági feladatok fejlesztése érdekében a honvédelmi célú létfontosságú infrastruktúra kijelölésével és ellenőrzésével kapcsolatosan folyamatos a kapcsolattartás a *BM OKF-el és az NBSZ NKI-vel*. Az ágazaton belüli és kívüli kijelöléssel kapcsolatban *több konzultáció is volt, az érdekeltek bevonásával.*

Kerüljenek kidolgozásra olyan ösztönzők, melyek segítségével a kis- és középvállalkozási szektorban az információbiztonsági politikával rendelkező szervezetek aránya növekszik. Ezen belül: „részletes felmérés a vállalkozások kibervédelmi képességeiről”	ITM, Modern Vállalkozások Programja (MVP, Magyar Kereskedelmi és Iparkamara):Az MVP már most is végez a KKV-kat érintően kiberbiztonsági tevékenységeket pl. biztosít (rész)tanácsadást és szervez a témában rendezvényeket. célzott IT biztonsági tanácsadás, audit, egyéb IT szolgáltatások bevezetése is. Az MVP-hez kapcsoltan pályázati támogatások is elérhetők, melyeken elszámolható költség a cégek számára az IT biztonsági célú (szoftver, szolgáltatás vagy tanácsadási) kiadás.
Külképviseletek kiberbiztonságának tesztelésére, ellenőrzésére az NBSZ NKI-vel közös akcióterv készítése és végrehajtása.	A nagyobb elektronikus adatforgalmat bonyolító külképviseleteken a regionális rendszergazda és az NKI egy szakértője ellenőrzést hajt végre, amelynek eredményéről tájékoztatja a KKM-et. 2020-ban a pandémia miatt távolról végezték el a feladatot. Az NKI-val közös megelőző munkát újraindítják egy-egy kiemelt kockázatú külképviselet informatikai rendszerének helyszíni ellenőrzésével, a vírushelyzet csillapodása után.

a tudatosítás korszerű eszközeinek felhasználásával felhívni a figyelmet az információbiztonsággal kapcsolatos közös felelősség és tudatos magatartás szükségességére	A BIZPOL munkatársai rendszeresen részt vesznek az EU, a NATO és az EBESZ keretei között szervezett kiberbiztonsági gyakorlatokon. A BIZPOL kibertér koordinátora nemezetközi szereplései során felhívja a figyelmet a köz-és magánszféra közös felelősségvállalásának fontosságára.
A nemzeti kiberteret fenyegető korai előrejelző képesség kialakítása, növelése. Olyan passzív kibervédekezési eszközök infrastruktúrában történő elhelyezése, amelyek a fenyegetések elleni védelmi funkciót töltenek be, illetve biztosítják a fenyegetésekre vonatkozó információk kellő időben történő rendelkezésre állását.	Megkezdődött a honvédelmi korai előrejelző rendszer jogalapjának előkészítése. Az eljárásrendek kidolgozása és frissítése (fenyegetések és tapasztalatok beépítése) a honvédelmi ágazatnál folyamatosan zajló feladat. A honvédelmi szervezetek részére kockázatelemzéssel, osztályba sorolással és beszerzésekkel összefüggő eljárásrendek ajánlásai kerültek biztosításra. A magas szintű biztonságtudatosságot a Heti Kibervédelmi Szemle kiadása, illetve a Kiberakadémia (MH Kiber Képzési Központ) munkája biztosítja.

Tanúsítási keretrendszer 5G hálózatokra

NESAS


ÚJ NEMZETI KIBERBIZTONSÁGI STRATÉGIA

Knapp Gábor: Introduction of the basic conditions of classified electronic data processing during security incident's

Correferatum

If we are not prepared for it in advance, security event management of classified electronic systems must be performed using adhoc methods. The security incident management, similar to criminal investigative activity stations, must be pre-defined and procedures have follow an agreed order. For this reason, the use of individual solutions is only appropriate in emergency or unexpected situations. The tasks of the classified electronic data event management can be traced back to Act L of 2013 on the information security of state and local government bodies. Tasks related to classified data management that should also be performed to ensure security, are not new, but have not been tested before.

In the defense sector, where classified data management is not only carried out in stationary, permanent locations, but also in temporary settlement areas, in combat vehicles and aircraft's.

In my presentation I represent the findings from different aspects of my previous research. I will show the personal study questions, the personnel, physical, administrative and INFOSEC requirements both from the data management and from the security event management organization side.

Interesting details can also come in front by presenting the tasks in view of duality, parallelism and if they are, in some cases additional organizational actors play a connecting role.

Looking to the future, I would like to highlight a few solutions and fancy areas that I consider to be challenging. I present the dangers inherent in the emerging and disruptive techniques, which the defense sector needs to prepare for and have to research in advance.

Keywords: classified data processing, incident handling, personnel security, physical security, document security, information security

„Introduction of the basic conditions of classified electronic data processing during security incident's”

International Military InfoSEC Conference
27. April 2022

LtCol Knapp Gábor
Cyberspace Operation Centre
subbranch head

KIBERTÉR MŰVELETI KÖZPONT

1

Content

KIBERTÉR MŰVELETI KÖZPONT

- Actualities
- Legislation background
- Overview of the incident handling steps
- Personal conditions
- Requested tasks
- Personnel security requirements
- Physical security requirements
- Administrative security requirements
- INFOSEC requirements
- Other conditions, interesting thoughts, challenges

2

Actualities

KIBERTÉR MŰVELETI KÖZPONT

- **Security incidents of classified systems**
- **Airgap is the perfect solution?**
- **Rumour or not?**

- **The attitude of the defence sector**

Legislation background

KIBERTÉR MŰVELETI KÖZPONT

- Act CLV of 2009 on security of classified data
  - 90/2010 Governmental Decree on the operation of National Security Authority, and the protection of classified data handling
  - 161/2010 Governmental Decree on the protection of electronic classified data, the authorisation of cryptographic activity and detailed rules of security authority

4

Legislation background continued

KIBERTÉR MŰVELETI KÖZPONT

- Act L of 2013 on the Identification, Designation and Protection of Vital Systems and Facilities and on the Information Security of State and Municipal Bodies
  - 271/2018 Governmental Decree on the computer system incident response centre's task and responsibility, and handling and technical investigation of security incidents, and the rules of conduct an vulnerability test
  - 41/2015 Ministry of Interior Decree on requirements of technology security, and secure devices, products, and classification of security class and level determined in the Act L of 2013 on the Identification, Designation and Protection of Vital Systems and Facilities and on the Information Security of State and Municipal Bodies

5

Legislation background continued

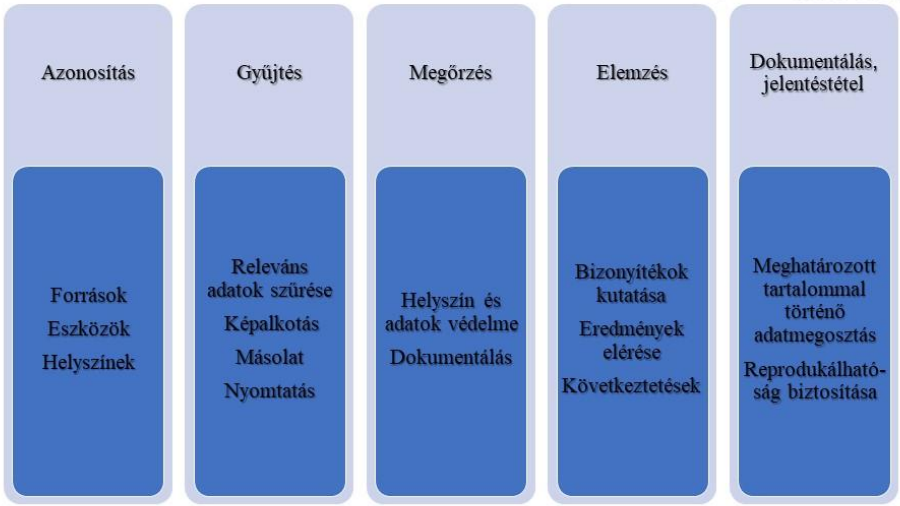
KIBERTÉR MŰVELETI KÖZPONT

- Act CXXV of 1995 on national security services
- Act CXII of 2011 on informational self-determination and freedom of information
- NATO C-M(2002)49 REV1 Security within the North Atlantic Treaty Organisation (NATO)

6

Overview of the incident handling steps

KIBERTÉR MŰVELETI KÖZPONT



Phases of the electronic forensics activity

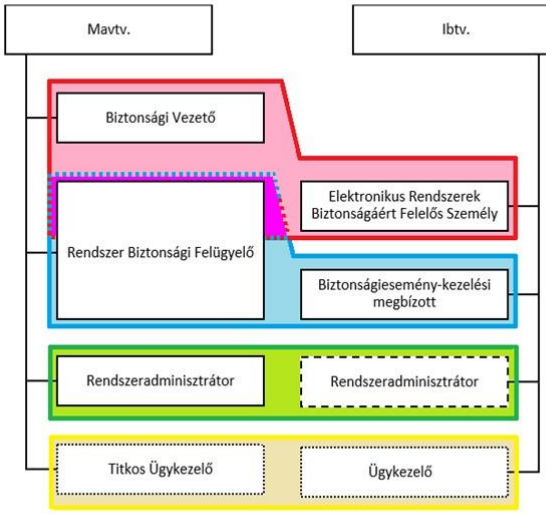
Source: Knapp Gábor - A minősített elektronikus adatkezelés feltételterndszerének vizsgálata az eseménykezelés során. KNBSZ Szakmai szemle, XIX. évfolyam 4. szám 2021. december, 122. oldal

7

Personell security

KIBERTÉR MŰVELETI KÖZPONT

- Who?
- What?
- Why?



Comparison of the requirements of „Mavtv." and „Ibtv." depending on level of their tasks and repsonibilites

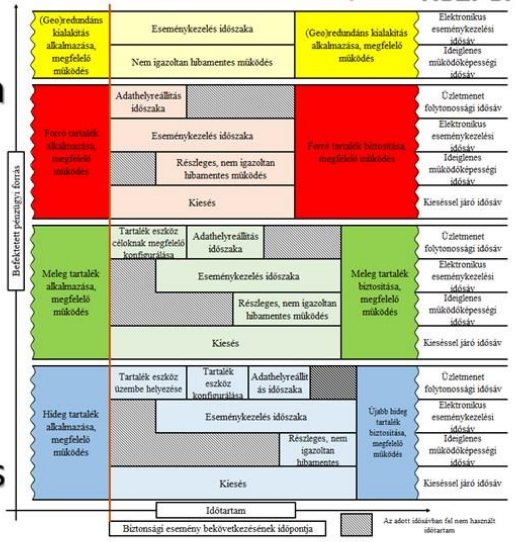
Forrás: Knapp Gábor - A minősített elektronikus adatkezelés feltételterndszerének vizsgálata az eseménykezelés során. KNBSZ Szakmai szemle, XIX. évfolyam 4. szám 2021. december, 125. oldal

8

Requested tasks

KIBERTÉR MŰVELETI KÖZPONT

- Before, during, an after
- On the data processing site and on the CSIRT location
- Comparison of possible solutions



Comparison of reserve allocation based on the time importance on depending on the financial source

Forrás: Knapp Gábor - A minősített elektronikus adatkezelés feltételrendszerének vizsgálata az eseménykezelés során. KNBSZ Szakmai szemle, XIX. évfolyam 4. szám 2021. december, 130. oldal

9

Personnel security requirements

KIBERTÉR MŰVELETI KÖZPONT

Data processing site

- Authorisation of data handling
- Confidentiality statement

CSIRT location

- Authorisation of data handling
- Attestation of Personnel Security Clearance

10

Physical security requirements

KIBERTÉR MŰVELETI KÖZPONT

Data processing site

- Authorisation of local data processing
- On demand additional temporary measures

CSIRT location

- Authorisation of local data processing
  - Different level +/-
- Mobile/Site abroad

11

Administrative security requirements

KIBERTÉR MŰVELETI KÖZPONT

Data processing site

- Registry
- Transfer
  - How
  - Who

CSIRT location

- Registry
- Transfer
  - How
  - Who

Data processing site 2

- Registry
- Transfer
  - How
  - Who

NADPFI

- Classification supervisory authority proceedings

12

INFOSEC requirements

KIBERTÉR MŰVELETI KÖZPONT

Data processing site	CSIRT location
• (Initial, Limited) Approval to Operate • Logging • Interconnection, conditions of connecting devices	• Approval to Operate • Capacity and suitability of storage • Add forensics software's to AFPL

13

Other conditions, interesting thoughts, challenges

KIBERTÉR MŰVELETI KÖZPONT

- Standalone vs. Network solution vs. „Cloud" solution
- Virtualisation technology
- Cryptography

14


THANK YOU FOR YOUR ATTENTION
KIBERTÉR MŰVELETI KÖZPONT
15

Szatmári Balázs: Elektronikai hadviselés az orosz-ukrán háború tükrében

Korreferátum

Az infokommunikációs technológia fejlődése és elterjedése a világban mind a polgári és mind a katonai életre nagy hatással van. Ennek egyik ékes példája az elektronikai hadviselés fejlődése is. A II. világháború és az elmúlt bő 60 év helyi háborúk tanulsága alapján kijelenthetjük, hogy az elektronikai hadviselés szerepe folyamatosan nő a konfliktusokban. Az elektronikai hadviselés jelentőségét az adja, hogy a haderők fejlesztése számos új eszköz megjelenésével jár, melyek jelentős része az elektromágneses spektrumban működik.

Az orosz haderő köztudottan kiemelkedő elektronikai hadviselési képességgel rendelkezik. Bizonyították már erejüket és képességüket a szíriai polgárháborúban és a kelet-ukrajnai hibrid háborúban is.

Az előadásom elején ismertetem az elektronikai hadviselés magyar doktrína szerinti definícióját, területeit és funkcióit. Bemutatom az orosz haderő elektronikai hadviselés doktrína szerint felépített alakulatait, képességeit és rendszeresített eszközeit.

A nyílt forrásból szerzett információkkal sok esetben lehetnek tévesek, így igyekeztem hiteles forrásból tájékozódni. Az egyik legjobb forrásnak az Európai Biztonsági és Együttműködési Szervezet speciális ukrajnai missziójának jelentései bizonyultak, mivel semleges félként csak tényeket igyekeztek közölni. A

jelentések pilóta nélküli repülőgépek által készített fényképeket is tartalmaznak, így magam is kiértékelhettem a képeket.

Kijelenthető, hogy az orosz fél 2018 óta számos elektronikai hadviselési eszközt telepített át Ukrajnába. Ennek ellenére a katonai szakértők egyhangzó véleménye szerint nem várt módon, kis hatékonysággal jelenik meg az elektronikai hadviselés a műveletekben. Számos hír jelent meg a médiában hátrahagyott nagy harcértékű orosz eszközökről, amely az orosz hadseregben szolgáló katonák alacsony szintű moráljára utal. Így jutott ukrán kézre a Krasukha-4S elektronikai hadviselési rendszer parancsnoki állomása. A vezetés-irányítási rendszer hiányosságaira utalnak azok a hírek, mely szerint számos civil felhasználásra szánt rádiókkal kommunikálnak a katonák egymás között.

2014. után az ukrán haderő jelentős támogatást kapott nyugati országoktól és NATO (North Atlanic Treaty Organization - Észak-atlanti Szerződés Szervezete) tagállamoktól. Ez a hozzájárulás nem kizárólag haditechnikai eszközökben merült ki, hanem kiképzésben is. A krími háború tapasztalatait felhasználva az ukrán hadsereg elektronikai hadviselési képessége jelenős fejlesztésen esett át. Az ellenséges vezeték nélküli kommunikáció felfedésére, lehallgatására, helyének meghatározására és zavarással való lefogására képes korszerű eszközök kerültek beszerzésre. Számos drónelhárító eszközt is vásárolt az ukrán hadsereg.

A fentiekben összefoglalt okoknak köszönhetően a háború menete nem várt módon alakult. Nagy valószínűséggel elhúzódó harcokra kell számítani, amelyben mindkét fél nagymértékben ki használja az

elektronikai hadviselés nyújtotta lehetőségeket. Biztos vagyok benne, hogy a konfliktus elemzése során rengeteg új tapasztalat keletkezik, melyeket fel kell használnunk a hazai képzésben, hogy a Magyar Honvédség elektronikai hadviselési képességét javítsuk.

Kulcsszavak: információs műveletek, elektronikai hadviselés, vezetés-irányítás, infokommunikációs technológia

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Elektronikai hadviselés az orosz-ukrán háború tükrében

Hadtudományi és Honvédtisztképző Kar
Elektronikai Hadviselés Tanszék
Szatmári Balázs szds. (szatmari.balazs.gabor@uni-nke.hu, 29217, +36309811851)

Elektronikai hadviselés

Az elektronikai hadviselés olyan katonai tevékenység, amely **elektromágneses környezetben**, az elektromágneses energia tudatos használatával biztosítja az **elektromágneses műveletek** részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését.

Elektronikai hadviselés funkciói

- **Elektronikai támogatási funkció** (Electronic Support Measures - ESM)
- **Elektronikai ellentevékenységi funkció** (Electronic Counter Measures - ECM)
- **Elektronikai védelmi funkció** (Electronic Protective Measures - EPM)

Elektronikai hadviselés alakulatok

Nyugati katonai körzet:

15 EHV dandár (Tula)

16 EHV dandár (Kursk)

Déli katonai körzet:

19 EHV dandár (Rassvet)

Központi katonai körzet:

18 EHV dandár (Nizhneudinsk)

Keleti Katonai körzet:

17 EHV dandár (Mateevka)

~9000 fő

OSCE SMM to Ukraine/EBESZ

OSCE SMM: Organization for Security and Co-operation in Europe Special Monitoring Mission

2018. július 28-ai jelentés:

Mini UAV felderített több elektronikai hadviselési rendszert Chornukhyne településhez közel:

Leer-3 RB-341V,

1L269 Krasukha-2

RB-109A Bylina

Repellent-1

OSCE Special Monitoring Mission to Ukraine

OSCE SMM to Ukraine/EBESZ

2020. március 10-ei jelentés:

Mini UAV felderített több elektronikai hadviselési rendszert Luhansk településhez közel:

RB-636Svet-KU,

RB-341V Leer-3

R-934B Sinitsa

OSCE Special Monitoring Mission to Ukraine

OSCE Special Monitoring Mission to Ukraine (48°31'41.2"N 39°21'24.2"E)

OSCE Special Monitoring Mission to Ukraine (2021. május 17.)

Vészleszállást kellett végrehajtani az operátornak az UAV-val GPS jel interferencia miatt Stepanivka közelében.

OSCE Special Monitoring Mission to Ukraine jelentése (2022. feb. 07.)

UAV operátorok **84 alkalommal** tapasztaltak interferenciát az irányító frekvencián és a GNSS (GPS) frekvenciákon.

4 alkalommal tüzet is nyitottak az eszközre

Schiebel CAMCOPTER® S-100

RB-636 Svet-KU

Légi sávban működő kisugárzók felfedése, lehallgatása, irányának és helyének meghatározása.

KTK gyártja

LLC Special Technology Center (St. Petersburg)

Kamaz alvázra telepítették

2012 óta gyártják

Ford Transitra épített verziója is létezik

Stacioner változat: Svet-VSG

RB-636 Svet-KU (Ford Transit)

25 MHz – 18 GHz

Mozgás közben is képes feladatot végrehajtani

Iránymérés pontossága:

30-100 MHz: 5°

1-3 GHz: 1-2°

GNSS-t használ a pozíciója meghatározására

Leer-3

Mobiltelefon (GSM- 900/1800) szolgáltatás lefogása, bázisállomások imitálása, üzenetek küldése (SMS)

Eszközök helyzetének megállapítása (DF, hálózatelemzés, metaadatok), digitális térképen való ábrázolása

Tüzérség számára céladatok szolgáltatása

Légifelderítés UAV alkalmazásbal

Krasukha eszközkomplexum:

- Krasukha-20
- Krasukha-4S
- 1990-es években kezdték el a fejlesztését

1L269 Krasukha-20

Pelena-1 (SZU.) zavaró rendszer modern verziója

BAZ-6910 alvázra telepítették

Zavarással való lefogása az AWACS (Airborne Warning and Control Sytem) pl.: Boeing E-3 Sentry, Northrop Grumann E-8 JSTAR rendszerekne

250 km-es max. hatótávolság

Moskva-1 komplexummal együtt alkalmazzák

Szárazföldi erők oltalma a radar vezérelt fegyverrendszerek és rakétákkal szemben, célok imitálása

Iskander harcászati ballisztikus rakéta csapatok oltalmát biztosítja

1RL257 Krasukha-4S

- Kamaz-6350 alvázra telepítik
- **Felderítő légijárművek (UAV, felderítő repülőgépek, elfogó vadászok) és LEO műholdak (Lacrosse) radarjainak zavarással való lefogása**
- Hatótávolság: 150-300 km
- A sorozatgyárátását 2011-ben kezdték meg(Bryansk Electromechanical Plant), 2013-ban szállították le az első eszközt
- Stratégia rakétaerők (RVSN)
- **2014-15 között: 18 rendszert szállított le gyártó cég**

1RL257 Krasukha-4S C2 konténer megszerzése (2022. marc. 22.)

Moskva-1 komplexum

1L267: vezetési pont
1L265: radar zavaróállomás
1L266: elektronikai támogató tevékenység modul

Passzív radar mód
400 km-es hatótávolság
45 perces telepítési idő
Stealth technológiával készült repülő eszközök detektálása

Több tíz van rendszerben az orosz hadseregen (KRET gyártja)

R-330Zh Zhitel

Automatikus zavaróállomás

Adó berendezések felfedése, irányának(helyének) meghatározása, jelelemzés

Satcom felhasználói terminájának zavarással való lefogása INMARSAT, IRIDIUM,

NAVSTAR GPS és GSM (900/1800)

RB-301B – Borisoglebsk-2

Automatikus zavaróállomás

Adó berendezések felfedése, irányának(helyének) meghatározása, jelelemzés

HF/VHF rádiók

R-330 MV CC

Orosz C2

- Kínai civil felhasználásra szánt rádiók:
  - BaoFeng UV-82HP
  - VHF-UHF (136-174 MHz, 400-520 MHz)
  - 1-7 W
  - Katonai titkosításra nem alkalmas

- ERA cryptophone (3G/4G)-> ukrán infrastruktúrát használja/használná ha nem rombolták volna le
- Azart-P1 (27-520 MHz, max. 4 km)

Ukrán C2

Nem annyira centralizált

Aselsan rádiók

L3Hariss rádiók

Ukrán EHV rendszer

2014 után kezdték el a fejlesztéseket

DF, kommunikációs zavarás, radar vezérelt prcecíziós fegyverek elleni tevékenység

- Bukovel-AD
- NOTA
- Mandat-B1E R330UM

Bukovel-AD

- Proximus ukrán cég fejlesztése
- Rendelkezik drónelhárító képességgel (Orlan-10)
- **3g, 4g felfedés, zavarás**
- **SMS üzenetek küldése felhasználóknak**
- **UAV detektálás 100 km távolságból**
- **Irányítófrekvencia és GNSS frekvencia zavarással való lefogása 16km távolságból**

NOTA

Mobil és telepíthető verzió
300-6200 MHz
450 W
C-UAV
GSM, UMTS, LTE, CDMA, Wi-fi, VHF
UAV felderítése 20 km
UAV ellentevékenység 20 km
GNSS (Glonass, BeiDou)

Mandat-B1E R330UM

Rádiókommunikáció zavaró állomás

Szélessávú és keskenysávú zavarásra is képes

Képes az ellenség helyének meghatározásra

Frekvencia ugratásos rádiók ellen is hatékony

400- 2500 MHz

Maximum hatótávolság 40 km

Rádió”amatőrök”

HF Russian Navy Digital Encrypted (FSK, CIS-36-50)

http://kiwisdr.com/public/

http://websdr.ewi.utwente.nl:8901/

HF DF TDoA US299$

8131 kHz USB HF stratégia bombázó forgalmazás

https://soundcloud.com/tomteej/russian-bomber-hf-voice-net-24th-feb-2022-81310khz

Orosz katonai doktrína

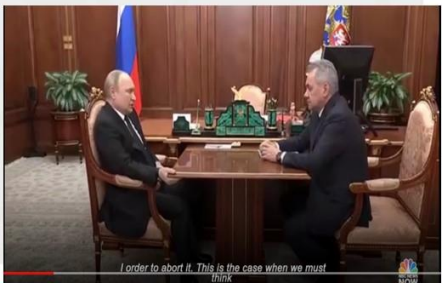
Centralizált vezetés

Senki nem hajt végre semmit, amíg arra parancsot nem kap

Túl sok kommunikáció

Ha nincs kommunikáció ->

Nincs feladatvégrehajtás



Következtetések, tapasztalat (vélt)

- Nagyobb aktivitást vártak a szakértő Oroszországtól az EHV területen
- Oroszország fejlett EHV eszközökkel rendelkezik, DE!
- A felderítési információk mindig az eszközök képességeire fókuszáltak és kihagyták az emberi tényezőt
- Nem rendelkeznek az orosz EHV operátorok megfelelő tapasztalattal (Elektron-2016)
- EHV szimulátor: Magnii-REB (2016-ban kapták)

Magyar Sándor: Kibervédelmi gyakorlatok tapasztalatai. „Párhuzamosságok a való világgal."

Korreferátum

Digitalizáció térnyerésének kezelése kiberbiztonsági szempontból egyre összetettebb feladat. Napjaink megnövekedett számú és komplexitású kibertámadásai egyre jobban indokolják a szükséges megelőző, detektáló és korrigáló területek fejlesztését, amihez a kibervédelmi gyakorlatok területe hatékonyan tud hozzájárulni.

A kibervédelmi gyakorlatok kérdésköre napjainkban egyre nagyobb hangsúlyt kap, mivel aktívan képes hozzájárulni a kibertérből érkező fenyegetések elleni felkészüléshez. A gyakorlatok célja a hiányosságok feltárása mellett a képességek fejlesztése, továbbá az együttműködés, az információmegosztás elősegítése. Az együttműködés nem csak a szakmai területek között (informatikai üzemeltető, fejlesztő, eseménykezelő, sérülékenységvizsgáló, malware elemző stb.) kerülhet előmozdításra, hanem szervezetek között, továbbá nemzetek között is.

A gyakorlatoknak számos típusa van, amelyek lehetnek table top, stratégiai, technikai és komplex. Mindegyik gyakorlatnak megvan a maga életciklusa, amelyben a gyakorlat végrehajtásának 1-2 napja a legrövidebb időszak. A felkészülés hónapjai és a tapasztalatfeldolgozás teszik ki a ciklusból a leghosszabb időtartamot. A tapasztalatfeldolgozásra, mint a legfontosabb területre különösen nagy figyelmet kell szentelni, annak nem szabad csak a bekért vélemények összegzésében lezáródni. A

tapasztalatfeldolgozás eredményeit mindenképpen be kell építeni a következő gyakorlatok tervezése esetén már a korai fázisoknál is.

A gyakorlatok feladatvégrehajtása során számos párhuzamosság tapasztalható az éles feladatvégrehajtással, ahol például a megfelelő eljárásrendek betartása ugyanúgy fontos, mint a napi életben. Amennyiben nem áll rendelkezésre megfelelő erőforrás (eszköz, idő, szoftver, emberi erőforrás, képzettség stb.) a gyakorlat végrehajtása sem lesz sikeres.

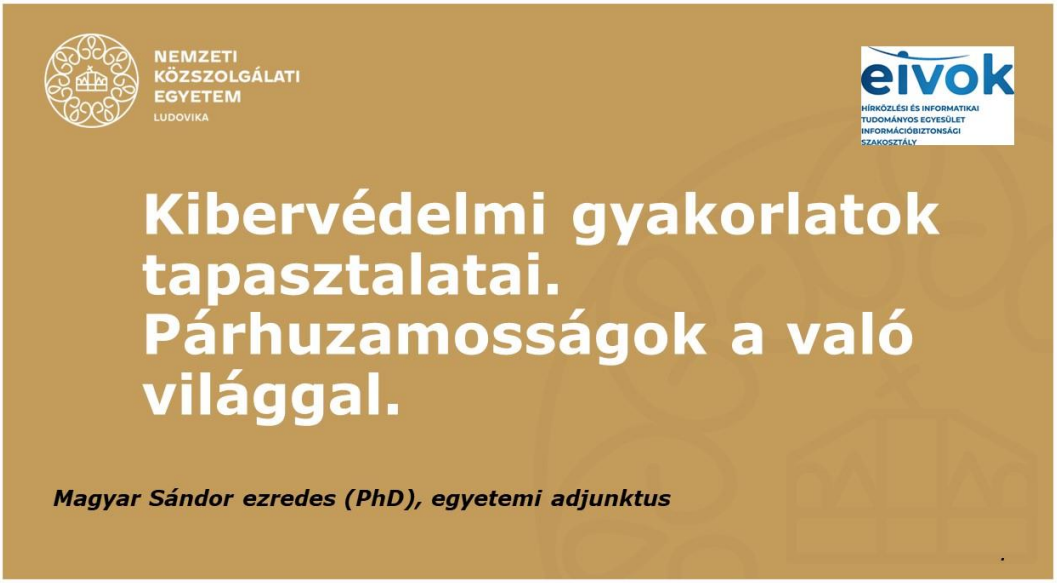
Legalább a kulcsszereplő szakemberek esetében minimum több napot/hetet érdemes a részletek mélyebb feldolgozásra ráfordítani (optimálisan egy külső helyszínre szervezve) minden szakterületen. Ez sok esetben kihívást jelenthet, mivel a senior szakembereket a vezetőik nem tudják a kért időszakokra elengedni, sok esetben a tényleges részvételüket is felülírhatja az élet. A senioritásnak a gyakorlatok szempontjából több fajtája lehet, amely takarhatja például azt, hogy már részt vett korábban kibervédelmi gyakorlatokon, vagy azt is, hogy a szakterületét mennyire „uralja”.

Az információs technológia folyamatos fejlődését követni kell. Az új technológiák, kiberbiztonsági szoftverek tesztelése is megtörténhet a gyakorlatokra felkészülés és végrehajtás során. A jövőben azonban a feltörekvő és felforgató technológiákkal is számolni kell.

A folyamatok területén is kölcsönösen használható (éles rendszereknél, cyber range-en) a jó gyakorlatok beépítése például a tevékenységi láncok, jelentési és munkafolyamatok kialakítása során.

Összegzésként elmondható, hogy ami az életben nem működik, akadozik, az a gyakorlat során is felmerül kihívásként, ezért ezek fejlesztése, valamint a hiányosságok feltárása miatt is egyre nagyobb jelentősége van a kibervédelmi gyakorlatok szervezésének, végrehajtásának.

Kulcsszavak: kibervédelmi gyakorlatok, sérülékenységvizsgálat, eseménykezelés, tapasztalatfeldolgozás



Kihívások

- Digitalizáció térnyerésének kezelése kiberbiztonsági szempontból egyre komplexebb.
- Kibertérből érkező fenyegetések azonosítása, kezelése.
- Kritikus infrastruktúrák ellen irányuló kibertér műveletek számának emelkedése.
- Katonai oldalon a hibrid hadviselés.
- Kibertér szereplőinek azonosítása.
- Kibervédelem, mint támogató szerepkör.

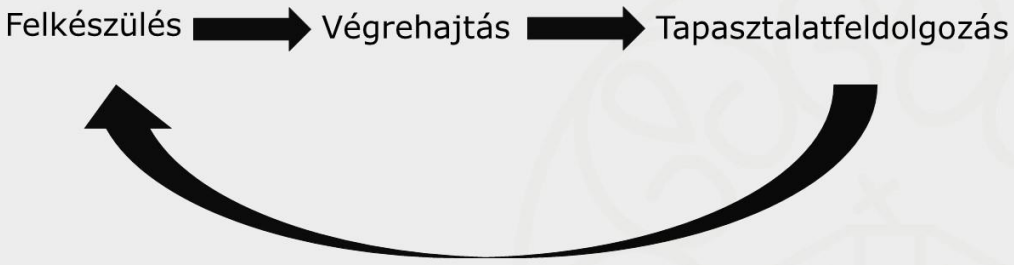
A kibervédelmi gyakorlatok célja

- Felkészülés a kibertérből érkező fenyegetésekre.
- Képességek fejlesztése.
- Hiányosságok feltárása.
- Együttműködés, információmegosztás elősegítése:
  - szakmai területek között;
  - szervezetek között;
  - nemzetek között.

A kibervédelmi gyakorlatok típusai

- Table top.
- Stratégiai.
- Technikai.
- Komplex.

A kibervédelmi gyakorlatok fázisai



Tapasztalatfeldolgozás

- A tapasztalatfeldolgozásnak nem szabad csak a bekért vélemények összegzésében lezáródni.
- Legalább a kulcsszereplők esetében minimum több napot/hetet érdemes a részletek mélyebb feldolgozásra fordítani (optimálisan egy külső helyszínre szervezve) minden szakterületen.

Emberek

- Humán erőforrás száma, képzettsége.
- Szenioritás, nélkülözhetetlenség. Hol vannak a határok?
- Felelősségi mátrix:
  - **R**esponsible;
  - **A**ccountable;
  - **C**onsulted;
  - **I**nformed.

Folyamatok

- Tevékenységi láncok.
- Jelentési folyamatok.
- Munkafolyamatok kialakítása.

Technológia

- Folyamatosan fejlődik, amelyet követni kell.
- Jövőben a feltörekvő és felforgató technológiákkal is számolni kell.
- Támogatja a hatékonyabb, gyorsabb munkavégzést.

Összegzés

- Ami az életben nem működik, akadozik, az a gyakorlat során is felmerül kihívásként.
- Nagy hangsúlyt kell fordítani a tapasztalatfeldolgozásra a gyakorlatok után.
- A megelőzés, észlelés, korrekció területei hatással vannak egymásra.

Felhasznált irodalom

- 1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján) A hálózati és információs rendszerek biztonságára vonatkozó Stratégia
- 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról
- 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról
- Kovács László: Kiberbiztonság és -stratégia. Dialóg Campus, Budapest, 2018.
- Marsi Tamás, Kiberbiztonsági Gyakorlatok, Beszámoló A Hunex 2019 Tapasztalatairól
- Szabó András, Technikai kiberbiztonsági gyakorlatok – nemzetközi kitekintés, Hadmérnök XIII. Évfolyam 1. szám

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Köszönöm szépen a figyelmet!

Tóth András: The impact of Internet of Things devices on modern warfare

Correferatum

Modern information and communication technologies have enabled the Internet of Things devices and systems to become more widespread. IoT devices are not only becoming more common in civilian life but also industrial environments, for example. The fundamental problem is that IoT devices are not always secure, one reason being that manufacturers are not obliged to guarantee the security of their devices. Accordingly, these devices can contain several vulnerabilities that attackers can easily exploit, potentially causing serious damage to a system.

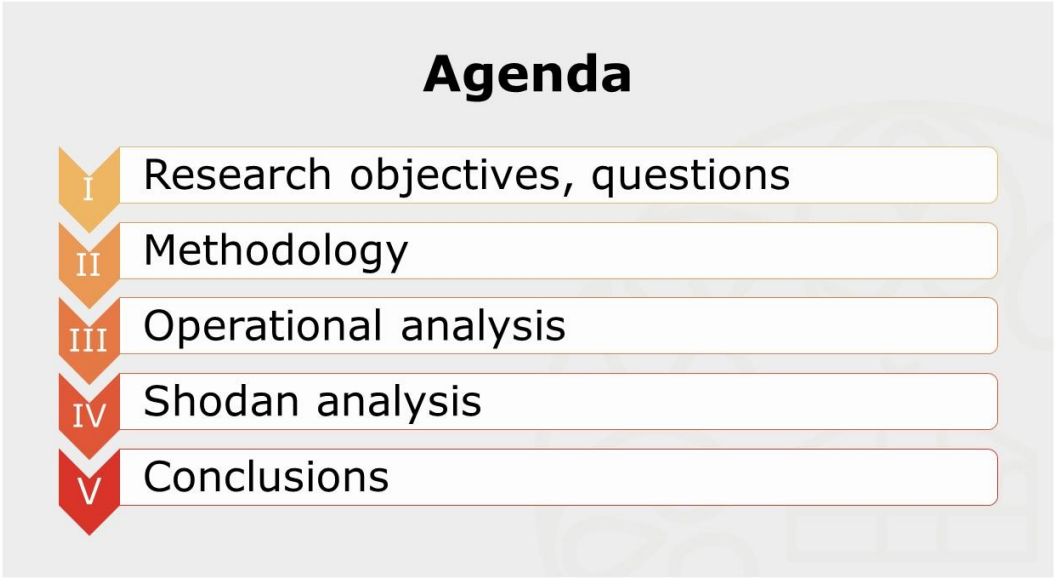
In the military environment, IoT devices have also appeared typically designed to resist the natural, weather, mechanical and other impacts they may be exposed to in military applications. However, even for these devices, it cannot be definitively stated that they are fully resistant to all cyber attacks.

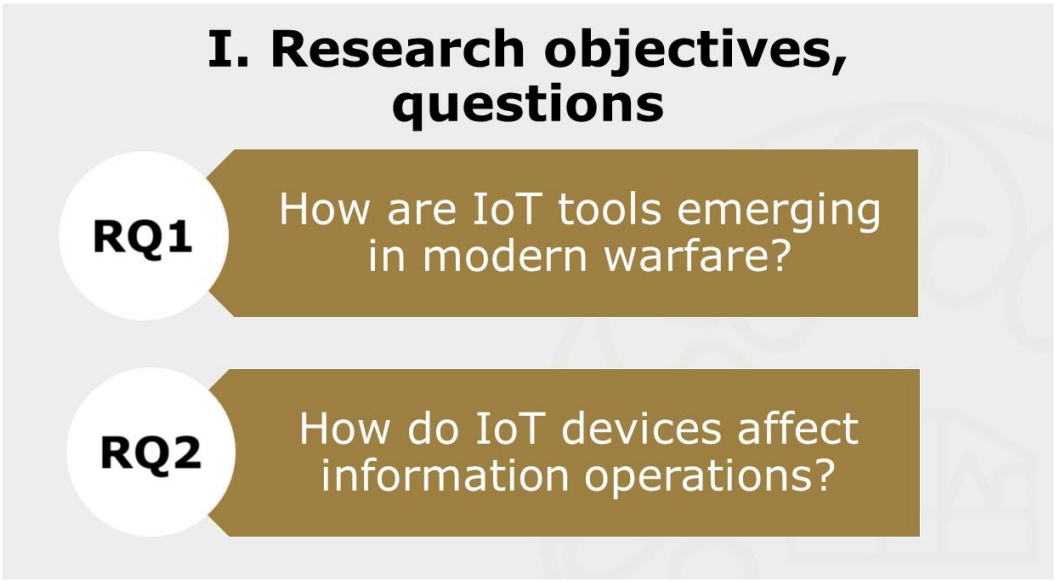
The Russian-Ukrainian conflict has drawn attention to a new use of smart devices in everyday life, which has not been observed in warfare until now. For example, civilians used social media platforms to share in real-time the movements and locations of enemy troops. This information greatly improved reconnaissance activities.

The author examined the impact of these IoT technologies and applications on modern warfare in the project was supported by the

János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-21-5-NKE-149 New National Excellence Program of the Ministry of Innovation and Technology.

Keywords: Internet of Things, modern warfare, IMINT, OSINT, intelligence, surveillance, target acquisition, and reconnaissance


Agenda
I Research objectives, questions
II Methodology
III Operational analysis
IV Shodan analysis
V Conclusions


I. Research objectives, questions
RQ1
How are IoT tools emerging in modern warfare?
RQ2
How do IoT devices affect information operations?

II. Methodology

- Analysis of relevant technical reports;
- Shodan.io;
- OSINT.

III/1. The Russian-Ukrainian operations

- Early 2022 - DDoS attacks (GRU - UK NCSC)
  - DanaBot, a malware-as-a-service platform
- 03 March: The hackers fighting on the Ukrainian side of opRussia and Anonymous have identified the entire critical infrastructure of Russia accessible from the internet and local networks and shared the targets. As a result, a large part of Russia's #IoT infrastructure has been hit.
- 05 March: Russia is suffering a continuous wave of DDoS attacks in the digital space, with experts uncovering an attack botnet network spanning 150 countries. Hungary was also affected (nearly 50 IP addresses - meaning that we also had zombified IoT and similar devices that were part of the attack network) (US CISA)

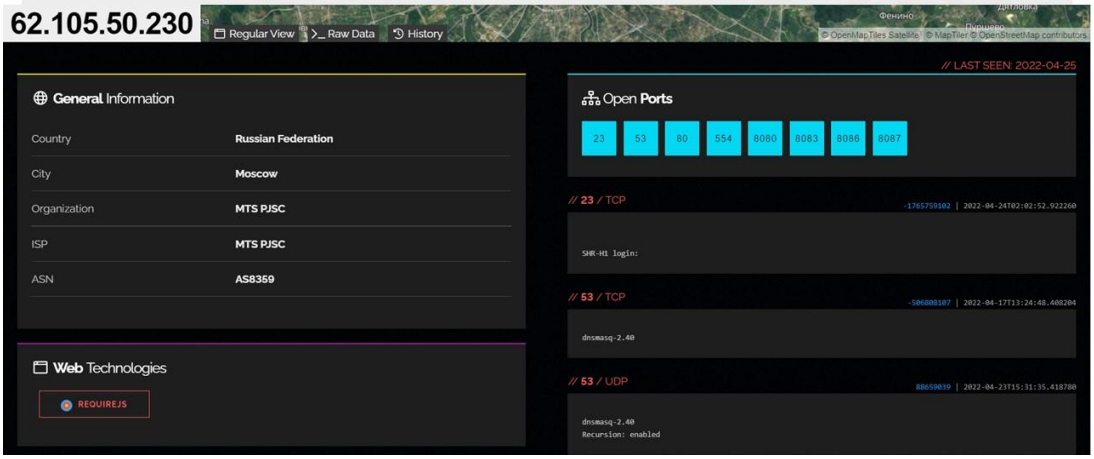
III/3. IoT devices available on Shodan in Hungary

Search	Results in Hungary
Most typical ports	54321, 161, 80, 1883, 8889
Most typical cities	Budapest, Pécs, Rajka, Szigethalom, Kecskemét
Most typical companies	Magyar Telekom, Vodafone Hungary, DIGI, Satelit Híradástechnikai Kft., Tarr Kft.
Most typical products	Xiaomi IoT, Mosquitto, nginx, InfluxDB
Most typical OS-s	MikroTik RouterOS 6.47.7, MikroTik RouterOS 7.1.3, Windows 10 IoT Enterprise 22581

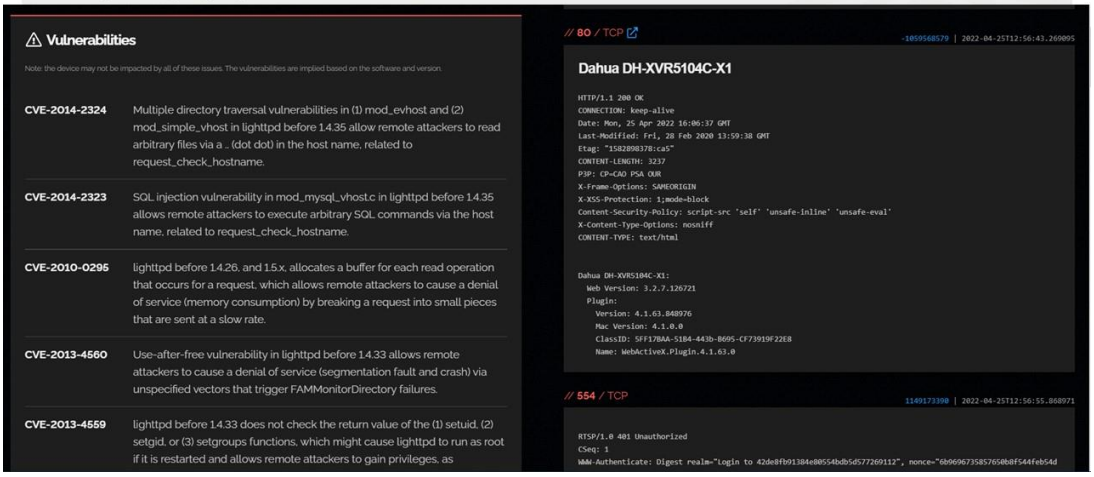
III/3. Industrial IoT devices on Shodan in Hungary

Industrial device	Featuring	Results in Hungary
Siemens S7	A proprietary protocol for Siemens devices that provides communication between PLC devices and the Siemens S7 product family	464
Modbus	Popular protocol in ICS can give easy access to the system without logging in	377
EtherNet/IP	An industrial Ethernet network solution, introduced in 2001, whose main application is in manufacturing automation	256
OMRON FINS	A factory network interface service that communicates over physical channels such as Ethernet, Controller Link or RS-232C	81
CODESYS	Programming interface for software automation tasks	36

III/4. IoT tools available on Shodan



III/4. IoT tools available on Shodan



IV. OSINT is the new RECCE?

Twitter – TikTok
Fake news – EIVOK Fórum: *TikTok hadviselés – Z generációs influencerek szerepe az orosz-ukrán háborúban*
Dr. Guld Ádám

április 8., péntek 15:32

Látta a biztonsági kamerán, hogy oroszok állomásoznak a háza mellett, megadta a koordinátákat az ukrán hadseregnek

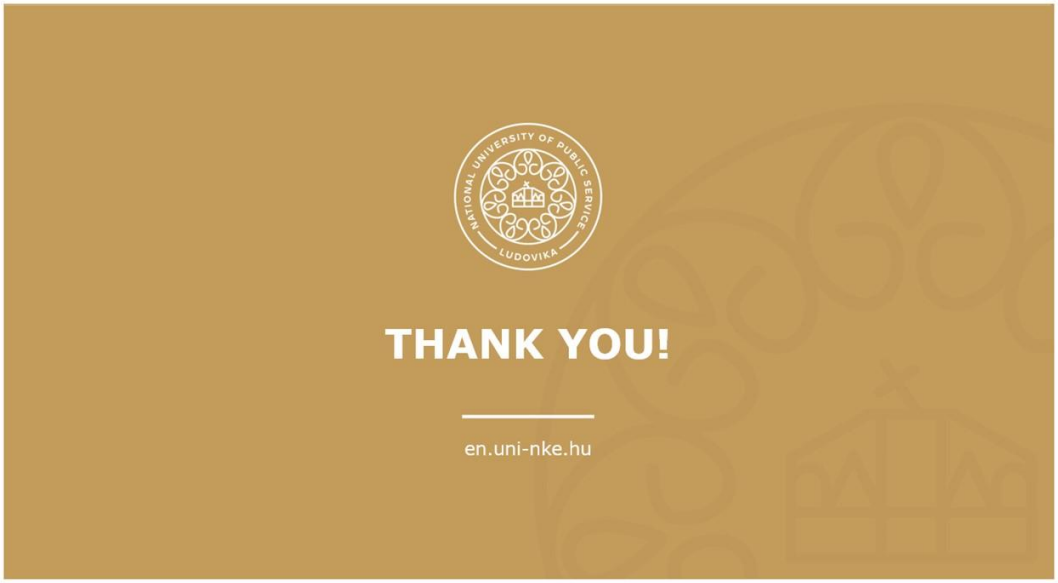
Egy odesszai üzletember beáldozta a házát, hogy segítsen kiiktatni egy orosz hadegységet.

Andrij Stavnitser Kijev melletti házának biztonsági kameráján vette észre, hogy az épület mellett orosz katonák telepítenek rakétákat, és rájött, hogy a házát valószínűleg búvóhelyként akarják használni.

Bei Plünderungen gestohlen: Ukrainer tracken Airpods und Smartphones in Belarus – das könnte einen Vorteil im Krieg bringen

Conclusions

- Improperly configured (I)IoT devices can present a serious attack potential, even in the hands of volunteer cyber warriors.
- mart devices and/or surveillance systems can provide useful information for battlefield reconnaissance.
- Cloud of Military Things/Katonai Egységes Felhőalapú Eszközrendszer


NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA
THANK YOU!
en.uni-nke.hu

Pozderka Gábor: Magyar Honvédség kiberműveleti képességeinek kialakítása és fejlesztése

Korreferátum

A NATO 2016-ban különálló műveleti területként azonosította a kiberteret, ezzel felgyorsítva és felerősítve a nemzeteknél korábban is megjelenő igényt, amely magába foglalta a kiber képességek hatékony kialakításának mihamarabbi megkezdését. Az informatikai rendszerek és alkalmazások dinamikus fejlődése még inkább előtérbe helyezte azok védelmi eljárásainak igényét, az egységes és összehangolt válaszreakciók kidolgozását a kibertérben. A kibervédelmi majd kiberműveleti képességeket sokan a kezdeti időszakban csak a technikai képességek kialakításához kötötték, azonban a képességfejlesztési folyamat során gyorsan nyilvánvalóvá vált, hogy sokkal komplexebb feladatrendszerről beszélünk, amely magába integrálja többek között a szükséges jogi háttér, oktatási-kiképzési folyamatok, információmegosztó képesség, nemzetközi együttműködés, szükséges technikai megoldások kialakítását is.

Kezdeti lépések

A nemzeti és nemzetközi környezetben kialakult irányokkal összhangban a Magyar Honvédség 2019-es szervezeti átalakításának részeként megalakításra került a Kibervédelmi Haderőnemi Szemlélőség (továbbiakban: KIBSZ) mint a kibervédelem és kiberműveletek stratégiai szintű vezetési eleme. A szervezet kezdeti lépésként végrehajtotta a meglévő képességek

felmérését, azok racionalizálását, melynek eredményeként már 2019-ben megalakításra került az MH Kiberakadémia, mint a Magyar Honvédség kiber oktatási központja. Itt az általános és vezetői kiberbiztonsági tudatosító tanfolyamokon kívül megtalálhatóak az üzemeltető állomány technikai felkészítéséhez szükséges oktatások és platformok is.

Fejlesztési irányok

A Magyar Honvédség kiberműveleti és információs műveleti képességeinek fejlesztése, képességfokozása érdekében 2022.01.01-én Szentendre helyőrségben megalakításra került a Magyar Honvédség Kiber- és Információs Műveleti Központ (továbbiakban KIMK), amely magába integrálta a Katonai Kibertér Műveleti Központ Előkészítő Osztály, a Kiberakadémia, a Civil-katonai Együttműködési és Lélektani Műveleti Központ és az Elektronikus Eseménykezelő Főközpont feladatrendszerét. A fenti elemek képességeinek integrálásával a KIMK képes a harcászati szintű feladatok ellátására, aktuális kiberhelyzetkép előállítására a szárazföld, légierő és különleges művelet műveleteinek hatékony támogatása érdekében. A kiber műveleti és nem-kinetikus műveleti képességek csak folyamatos és hatékony koordináció mellet fejtik ki kívánt hatásukat, az MHP KIBSZ ennek szellemében egységes vezetési rendszert dolgozott ki a feladatvégrehajtás érdekében.

A vezetés és szakmai irányítás biztosításának érdekében szükségessé vált a kiber- és információs műveleti képesség stratégiai és műveleti szinten történő újragondolása, a KIBSZ feladatrendszerének kiegészítése és a meglévő szervezeti elemek

felépítésének átalakítása. A kiegészített szervezeti elem a kibervédelmi és nem-kinetikus hatások, fejlesztések stratégiai és műveleti szintű koordinált biztosításával járul hozzá a Magyar Honvédség békeidős és különleges jogrendi céljainak eléréséhez, felgyorsítva a döntési folyamatokat és a szükséges válaszreakciókat, kiemelt figyelemmel a Hvt. -ben meghatározott feladatokra.

Kihívások és szakmai koordináció

A szakterület kialakítása során az alábbi pontokban szereplő kihívások kerültek azonosításra, mint a képességfejlesztés főbb irányai és befolyásoló tényezői:

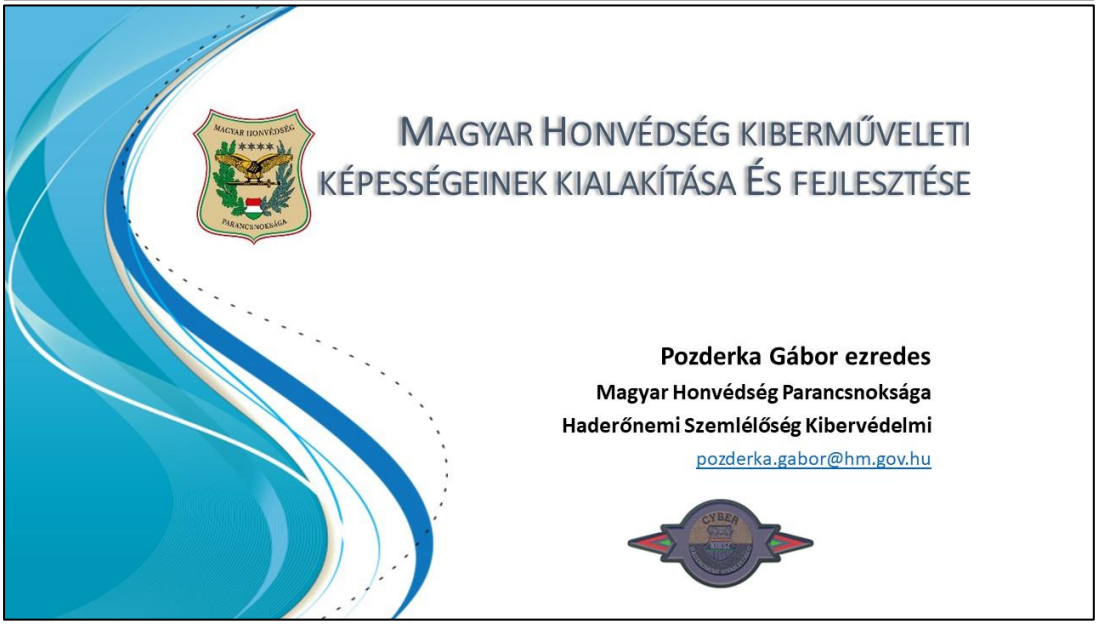
- Nemzeti műveleti feladatok támogatása;
- Nemzetközi vállalások teljesítése összhangban a nemzeti érdekekkel;
- Szükséges szakterületi képességek azonosítása, kiválasztott személyek felkészítése, a megszerzett képesség folyamatos szinten tartása;
- Speciális, a műveleti igényeket támogató hardver és szoftver komponensek beszerzése, azok rendszerbe illesztése.

A Magyar Honvédség felismerve a változó környezet hatásait és kihívásait, 2019-ben megalakította a Kibervédelmi Szemlélőséget, mint a kibervédelem és kiberműveletek stratégiai szintű vezetési elemét. A szervezet kezdeti lépésként végrehajtotta a meglévő képességek felmérését, azok racionalizálását és kialakította a jövőbeni koncepciót. A koncepció egyik fő elemeként 2022-ben megalakításra került a Kiber- és Információs Műveleti Központ, melynek képességfejlesztése jelenleg is folyamatban van. Az eredeti

koncepció kiegészült az Információs Műveleti elemek rendszerszintű integrációjával és műveleti vezetésbe történő beillesztésével.

Kulcsszavak: kiberműveleti képességek, információs műveleti képességek, kiberbiztonsági stratégia, stratégiai és műveleti koordináció


HADERŐNEMI SZEMLÉLŐSÉG
KIBERVÉDELEM


MAGYAR HONVÉDSÉG KIBERMŰVELETI KÉPESSÉGEINEK KIALAKÍTÁSA ÉS FEJLESZTÉSE
Pozderka Gábor ezredes
Magyar Honvédség Parancsnoksága
Haderőnemi Szemlélőség Kibervédelmi
pozderka.gabor@hm.gov.hu

Kibervédelem és kiberműveletek képességfejlesztése

- **Képesség kialakítás:**
- 2019 – KIBSZ és Kiberakadémia megalakulása
- 2020 – Műveleti Központ Előkészítő Osztály
- 2021 – K+F, KIMK szervezeti struktúra jóváhagyása
- 2022 – KIMK megalakulása és KIBSZ bővítése
  - Nem-kinetikus képességek integrálása
- **KIMK megalakításának célja:** A Magyar Honvédség információs műveleti képességeinek fejlesztése, képességfokozása, illetve egy információs műveleteket összehangoló és végrehajtó szervezet létrehozása.
- Folyamatban – Telepíthető kiber képesség (modulelem), nemzeti és nemzetközi vállalások

KIMK - Kiberakadémia

KIMK - Kiberakadémia

Kibervédelmi képző és oktató hely létrehozása:

- ügykezelők számára:
  - ✓ kiberbiztonsági tudatosítás (2 v 5 nap);
- szakbeosztásokat ellátók számára (Cyber Range):
  - ✓ elektronikus eseménykezelő;
  - ✓ IT Forensics;
  - ✓ ethical hacking;
  - ✓ Kiberműveleti (E-learning);
- parancsnokok számára:
  - ✓ kiberbiztonsági tudatosítás;
  - ✓ kiberműveletek alapjai;
  - ✓ kinetikus képességek kibertámogatása.
- gyakorlatokra történő felkészülés.

MH Kibervédelmi Szemlélőség feladatai

- **Stratégiai feladatok**:
  - az MH kibervédelmi és kiberműveleti képességei fejlesztéséhez szükséges stratégia irányok meghatározása
  - az MH információs műveleti képességei fejlesztéséhez szükséges stratégia irányok meghatározása
  - hosszútávú technikai fejlesztések megtervezése, azok vezetése, menedzselése
  - kiberműveleti humánerőforrás stratégiájának kidolgozása, bevezetése és fenntartása
  - a nemzeti és nemzetközi kibervédelmi és kiberműveleti MH szintű együttműködések felügyelete, vezetése (NATO, EU, bilaterális együttműködések)
- **Műveleti feladatok**:
  - tervezi, szervezi, **irányítja és vezeti** az MH kiberműveleteit, információs műveleteit (CIMIC, PSYOPS)
  - közreműködik az MH elektronikus információbiztonsági tevékenységében
  - irányítja és vezeti az MH Katonai Kiber- és Információs Műveleti központ szakmai tevékenységét
  - különleges jogrend bevezetése esetén kordinálja az MH kibervédelmi szakembereinek meghatározott helyszíneken történő biztosítását


Szakterület előtt álló kihívások
Valós nemzeti műveleti feladatok támogatása
CYBER DEFENSE PLEDGE
NATO OTAN
Nemzetközi vállalások teljesítése összhangban a nemzeti érdekekkel
Szükséges szakterületi képességek azonosítása, kiválasztott személyek felkészítése, a megszerzett képesség folyamatos szinten tartása
Speciális, a műveleti igényeket támogató HW és SW beszerzése és rendszerbe illesztése


KÖSZÖNÖM A FIGYELMET!
Pozderka Gábor ezredes
Magyar Honvédség Parancsnoksága
Haderőnemi Szemlélőség Kibervédelmi
pozderka.gabor@hm.gov.hu

Nyikes Zoltán: Az infokommunikációs infrastruktúrák biztonsági kérdései

Korreferátum

Napjainkban a digitális eszközök és az internet elterjedése miatt elengedhetetlen a legalább alapszintű informatikai ismeret mindenki számára. A munkahelyek és a szakmák döntő többségéhez szükséges valamilyen mértékben a digitális írástudás képessége. Ezért fontos a munkavállalók és a cégek számára, hogy az alkalmazottak magas szintű digitális ismeretekkel rendelkezzenek. Az egyén ugyanolyan felelős azért, hogy a részére biztosított javakat el tudja érni, mint maga a társadalmat irányító vezetés.

A COVID-19 világjárvány miatt világszerte a legtöbb munkavállaló kényszerült távmunkában dolgozni. Még a járvány elmúlása után is sokan azt jósolják, hogy a távmunka továbbra is elterjedt lesz több ágazatban. Ahogy a távmunka a munkavégzés új normájává alakul, a bűnözők is megpróbálják kihasználni az ebben rejlő sérülékenységeket. Ezért elengedhetetlen, hogy komoly figyelmet fordítsunk az otthoni információbiztonságra. A legtöbb kiberbiztonsági, otthoni munkavégzéssel kapcsolatos fenyegetettség könnyen megelőzhető a legjobb gyakorlatok alkalmazásával.

Azok a felhasználók, akik korábban nem használták nagy mértékben az internetet, azokra rengeteg olyan veszély leselkedett, amelyek biztonságtudatosítással elkerülhetőek. A veszélyek számos formájának voltak kitéve. A nagy számú digitális károkozó mellett,

a rosszindulatú célzott támadások, az adat- és személyiséglopás is megjelent. Emellett több bűncselekménytípus is hatalmas növekedést mutatott. Ilyenek voltak a pedofilok által kelkövetett bűncselekmények, például a Cyber-Grooming. Az elkövetett Cyberbullying esetek is jelentős emelkedést mutattak. Számos olyan megtévesztésen alapuló bűncselekmény történ, amely a kialakult helyzetet kihasználva a kiberbűnözői csoportok aljas módon vették célba az áldozataikat. Rengeteg megtévesztésre alapuló kampány zajlott, amely a felhasználók adatainak megszerzésére irányult. A felhasználók nagyon nagy száma nem volt felkészülve a támadásokra.

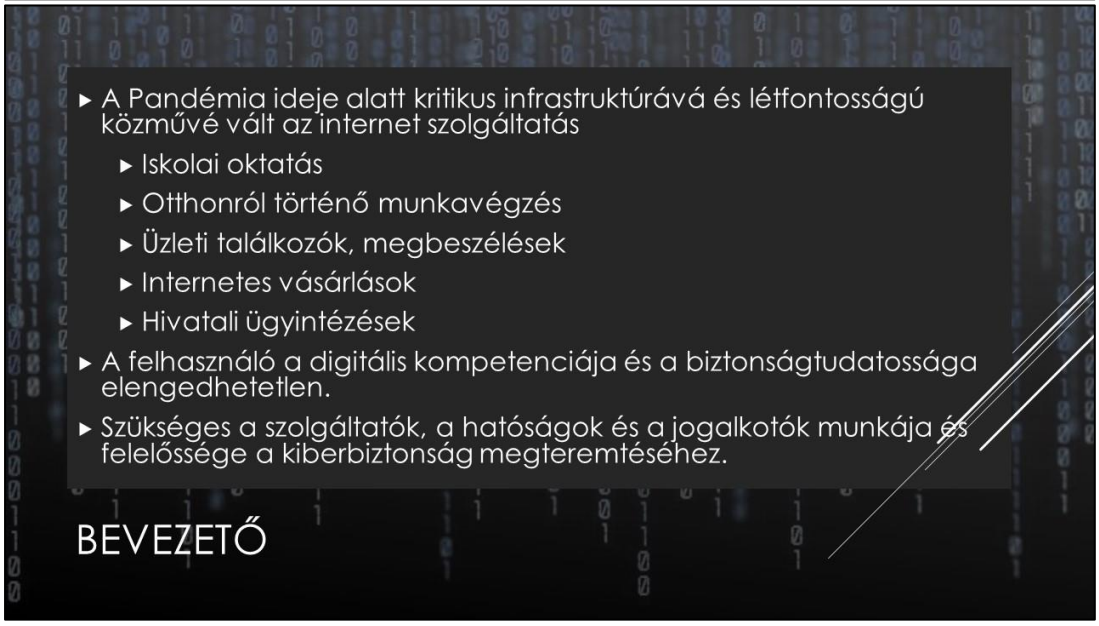
Könnyű a védtelen, átlag felhasználóra hárítani a felelősséget. Tőlük nem várható el, hogy profi szintű informatikai és információvédelmi ismeretekkel rendelkezzenek. A biztonságos kibertér kialakításának két irányát tudjuk beazonosítani. Egyik a határok védelme, a másik az országok kiber-belbiztonságának a megteremtése. Az egyik megoldás az lehetne, hogy az állam a hatóságokon keresztül kötelezze a szolgáltatókat arra, hogy ezeket az extra díjért igénybe vehető szolgáltatásokat az alapcsomag részeként, extra díj megfizetése nélkül biztosítsák a felhasználók számára. Azt gondoljuk, hogy ez a kritikus infrastruktúra is megérdemelné, azt, hogy olyan szigorú jogszabályi környezet vonatkozzon ezen szolgáltatókra is, mint más kritikus infrastruktúrák esetében teljes mértékben megszokott.

A Pandémia megmutatta, hogy az internet olyan szintű közművé emelkedett, mint az elektromos hálózat, vagy a vízhálózat. Minden

felhasználónak alapvető kötelessége, hogy legalább azokat az alapvető biztonsági szabályokat betartsa a kibertérben is, amit betart a fizikai térben. Addig, ameddig a szolgáltatók a kiberbiztonságban üzletet látnak és van is lehetőségük azt kiaknázni, addig nem várható el, hogy a szolgáltatásaik alapvető része legyen annak biztosítása. Ezért kell a jogszabályokkal kikényszeríteni a felhasználók kiberbiztonságának a biztosítását.

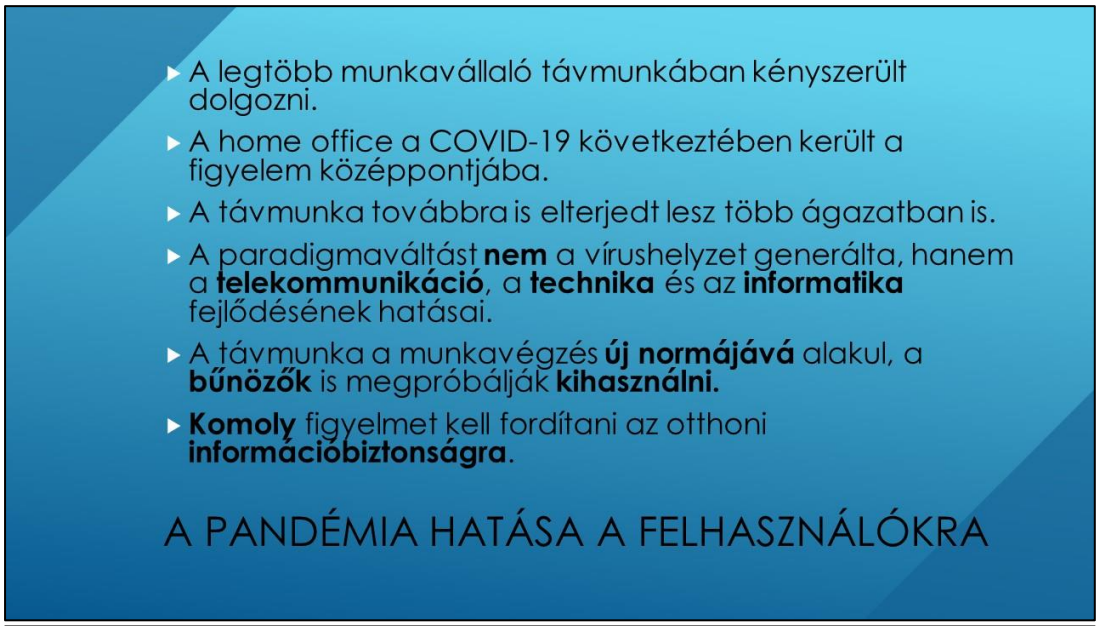
Kulcsszavak: Pandémia, infokommunikációs infrastruktúrák, távmunka, kiberbiztonság, biztonságtudatosság.

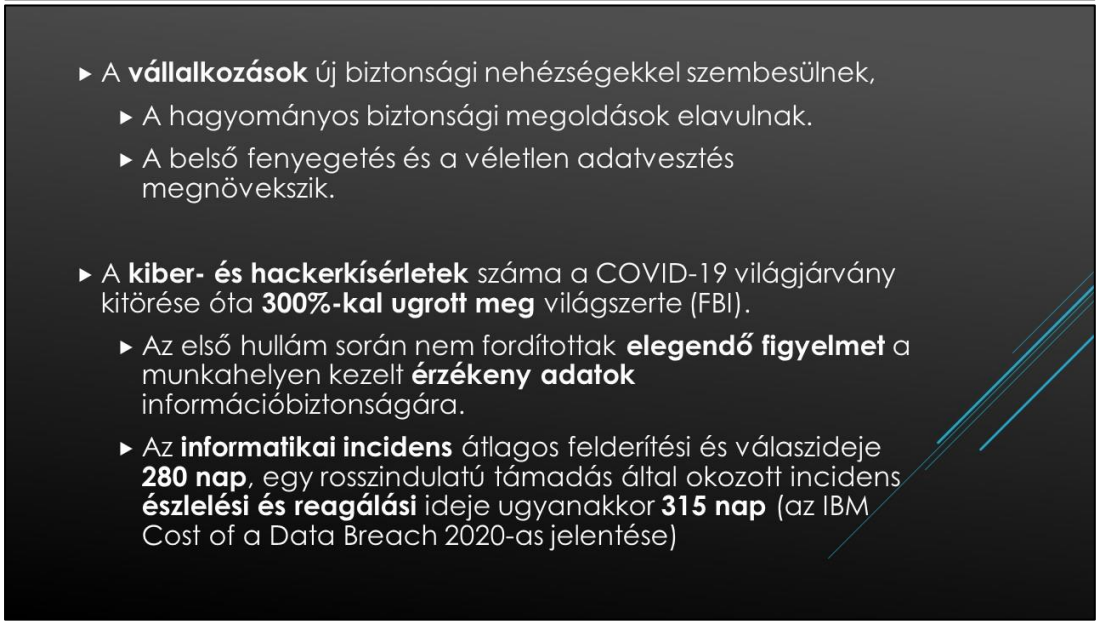

NEKIK 2022
Balatonakarattya, 2022. 04. 27.
AZ INFOKOMMUNIKÁCIÓS INFRASTRUKTÚRÁK BIZTONSÁGI KÉRDÉSEI
Dr. Nyikes Zoltán őrnagy, docens
MH Kiber- és Információs Műveleti Központ
Milton Friedman Egyetem

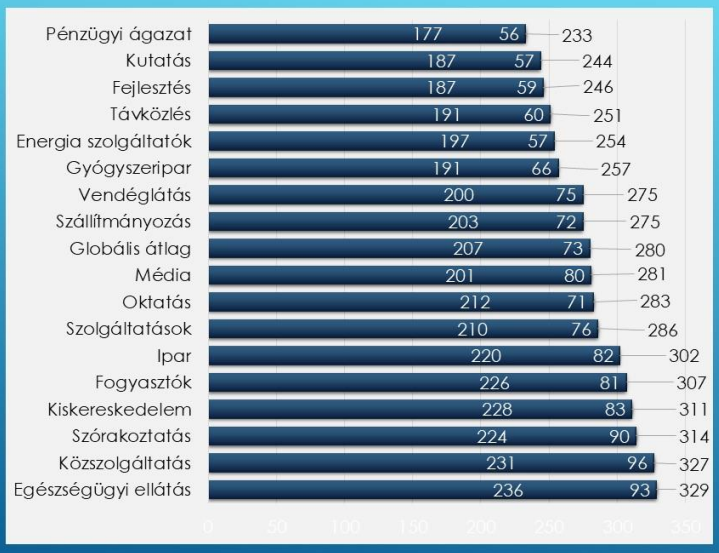

A Pandémia ideje alatt kritikus infrastruktúrává és létfontosságú közművé vált az internet szolgáltatás
Iskolai oktatás
Otthonról történő munkavégzés
Üzleti találkozók, megbeszélések
Internetes vásárlások
Hivatali ügyintézések
A felhasználó a digitális kompetenciája és a biztonságtudatossága elengedhetetlen.
Szükséges a szolgáltatók, a hatóságok és a jogalkotók munkája és felelőssége a kiberbiztonság megteremtéséhez.
BEVEZETŐ

- Az informatika és az internet robbanásszerű **fejlődése** társadalmi **változásokat** hozott magával.
- Az **informatika** oktatása és a **digitális kompetencia** fejlesztése már egész kora **gyermekkortól** kezdődően **biztosított**.
- **Élethosszig** tartó tanulás biztosítja azt a tudást, amivel **piacképes** lehetőséget tud teremteni.
- Az ipar digitalizációját **Ipar 4.0**-nak nevezik. **Elengedhetetlen** a rendszerek **„leggyengébb láncszemének”**, az ember **tudásának** és **tudatosságának** az elvárt szintre történő **emelése**.

A BIZTONSÁGTUDATOSSÁG ÉS A DIGITÁLIS KOMPETENCIA KAPCSOLATA


A legtöbb munkavállaló távmunkában kényszerült dolgozni.
A home office a COVID-19 következtében került a figyelem középpontjába.
A távmunka továbbra is elterjedt lesz több ágazatban is.
A paradigmaváltást nem a vírushelyzet generálta, hanem a telekommunikáció, a technika és az informatika fejlődésének hatásai.
A távmunka a munkavégzés új normájává alakul, a bűnözők is megpróbálják kihasználni.
Komoly figyelmet kell fordítani az otthoni információbiztonságra.
A PANDÉMIA HATÁSA A FELHASZNÁLÓKRA


A vállalkozások új biztonsági nehézségekkel szembesülnek,
A hagyományos biztonsági megoldások elavulnak.
A belső fenyegetés és a véletlen adatvesztés megnövekszik.
A kiber- és hackerkísérletek száma a COVID-19 világjárvány kitörése óta 300%-kal ugrott meg világszerte (FBI).
Az első hullám során nem fordítottak elegendő figyelmet a munkahelyen kezelt érzékeny adatok információbiztonságára.
Az informatikai incidens átlagos felderítési és válaszideje 280 nap, egy rosszindulatú támadás által okozott incidens észlelési és reagálási ideje ugyanakkor 315 nap (az IBM Cost of a Data Breach 2020-as jelentése)

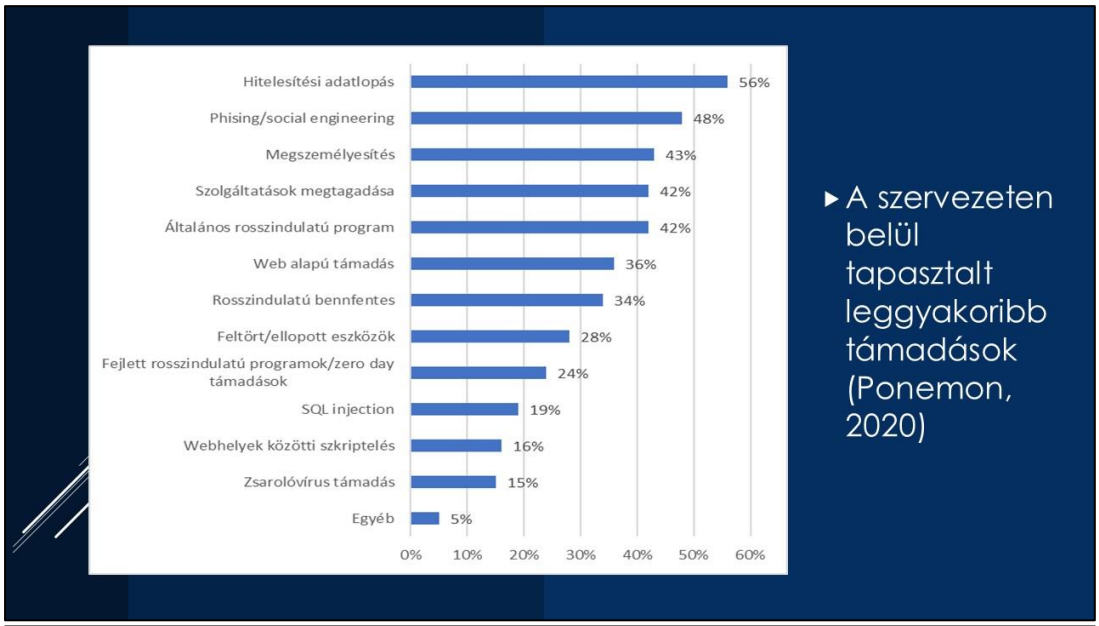


- A rosszindulatú támadások azonosításának és hatástalanításának átlagos ideje a különböző iparágakban (IBM, 2020)

A **kiberbűnözés** 2021 végére évi **6 milliárd** dollárba kerülhet a világnak, szemben a 2015-ös **3 milliárd** dollárral.

Ez a történelem **legnagyobb** gazdasági **vagyonátcsoportosítása** és **jövedelmezőbb**, mint az összes **illegális kábítószer** globális kereskedelme.

A COVID-19 járvány idején csak **egy hónap alatt 667%-kal növekedett** az adathalász csalások száma (ENISA)



- Az IT rendszerek védelmének **biztosítása** és a felhasználók **biztonságtudatosítása szükséges**.
- A gyerekek és felnőttek sok esetben **most használtak először** különböző **kollaboratív** alkalmazást, vagy akár **e-mail-t**, **csoportmunkát** segítő alkalmazást és **felhő** szolgáltatást.

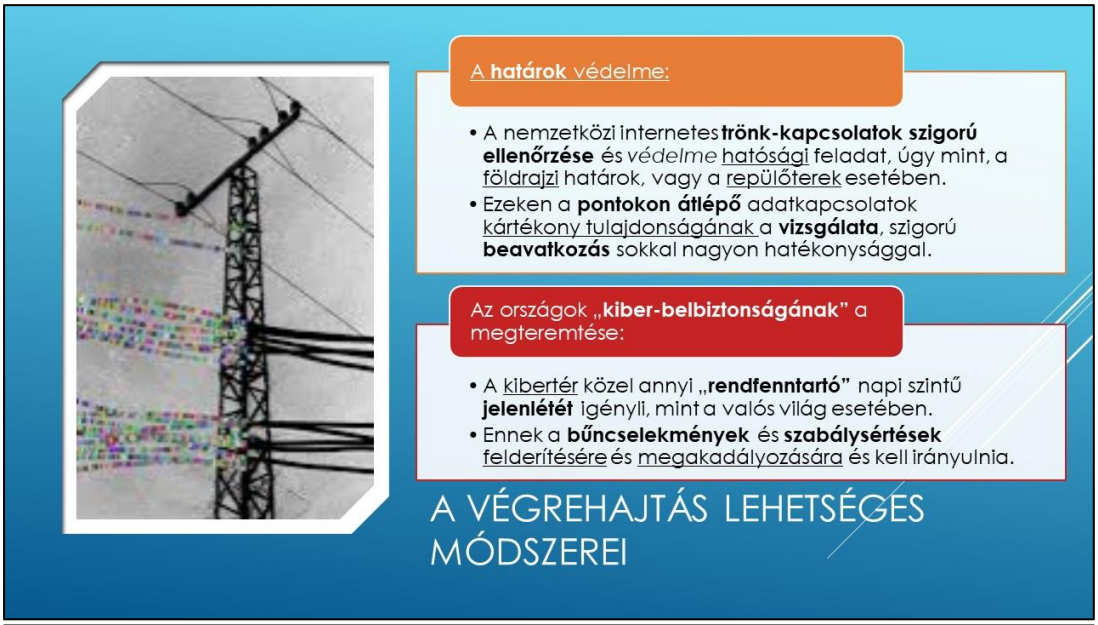
A DIGITÁLIS KOMPETENCIA ÉS A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉNEK SZÜKSÉGESSÉGE

- Digitális károkozók,
- Rosszindulatú célzott támadások,
- Adat- és személyiséglopások,
- Pedofilok által elkövetett bűncselekmények,
  - Cyber-Grooming,
  - Cyberbullying,
- Megtévesztésen alapuló bűncselekmények,
- Megtévesztésre alapuló kampányok.

A FELHASZNÁLÓKRA VESZÉLYES TEVÉKENYSÉGEK

A HATÓSÁGOK ÉS AZ INFOKOMMUNIKÁCIÓS SZOLGÁLTATÓK FELELŐSSÉGE

- **Könnyű** a védtelen, átlag felhasználóra hárítani a **felelősséget**.
- Tőlük **nem várható el**, hogy profi szintű **informatikai** és **információvédelmi** ismeretekkel rendelkezzenek.
- Nagyon ritkán hallani olyan híreket, hogy a hatóságok **felszámoltak** volna valamilyen **kiberbűnözői csoportot.**



AZ INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁS, MINT KRITIKUS INFRASTRUKTÚRA

- Az **ivóvíz** hálózatból kifogástalan és garantált minőségű ivóvizet kapunk.
- A vízszolgáltatók **szigorú jogszabályi** és **szabványi** előírásoknak megfelelni, melyeket az **állam** a **hatóságai** révén írt elő és kér számon.
- Az **ICT szolgáltató** cégek csak azt biztosítják, hogy **legyen internet** kapcsolatunk.
- Az, hogy szolgáltatás mennyire **biztonságos**, az a szolgáltatót **nem érdekli**.

Az ICT szolgáltatókat is **kötelezni** kellene a **szigorú** jogszabályi és szabványi előríások **betartására** az állam a hatóságain keresztül. Abban az **felhasználók** sokkal kevesebb **kiberbűncselekmény** áldozataivá válnának.

Megoldás:

Az állam a hatóságokon keresztül **kötelezze** a szolgáltatókat arra, hogy a cégek részére jelenleg **extra díjért** igénybe vehető szolgáltatásokat az **alapcsomag** részekén biztosítsák **MINDEN** felhasználó számára.

- Az egész társadalom **használja** a kiberteret.
- Az internet **közművé** emelkedett, mint az elektromos hálózat, vagy a vízhálózat.
- A felhasználónak **kötelessége** az alapvető **biztonsági** szabályokat betartása a kibertérben is.
- **Nem várható el** a felhasználótól, hogy professzionális szinten **értsen** az informatikai eszközéhez és professzionális kiberbiztonsági **szakértő** legyen.
- A **kormányzatnak** kell a **hatoságain** keresztül önmagának biztosítania és **kikényszeríteni** az **ICT** szolgáltatóktól a **biztonságot**.
- Ameddig a **szolgáltatók** a kiberbiztonságban **üzletet látnak** és van is lehetőségük azt kiaknázni, addig **nem várható** el, hogy a szolgáltatásaik alapvető része legyen annak biztosítása.
- Ezért **kell** a **jogszabályokkal** kikényszeríteni a felhasználók **kiberbiztonságának** a biztosítását.

ÖSSZEGZÉS


KÖSZÖNÖM A FIGYELMET!
Dr. Nyikes Zoltán őrnagy, docens
nyikes.zoltan@hm.gov.hu

Fekete Károly: Quantum Information Security, Quantum Communication and Quantum Cybersecurity in Military Technology

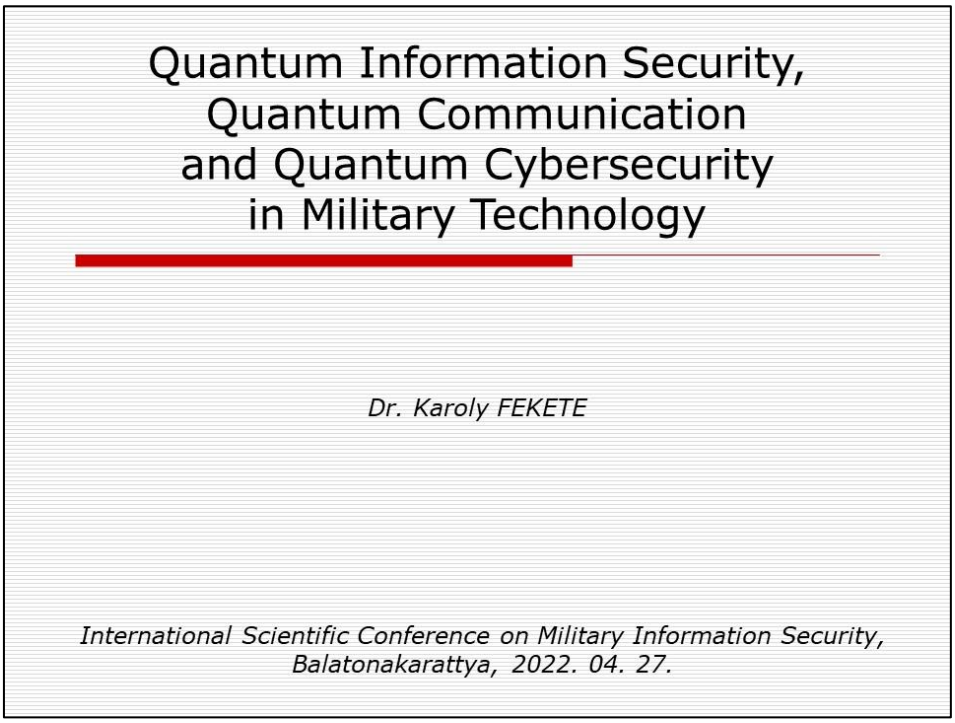
Correferatum

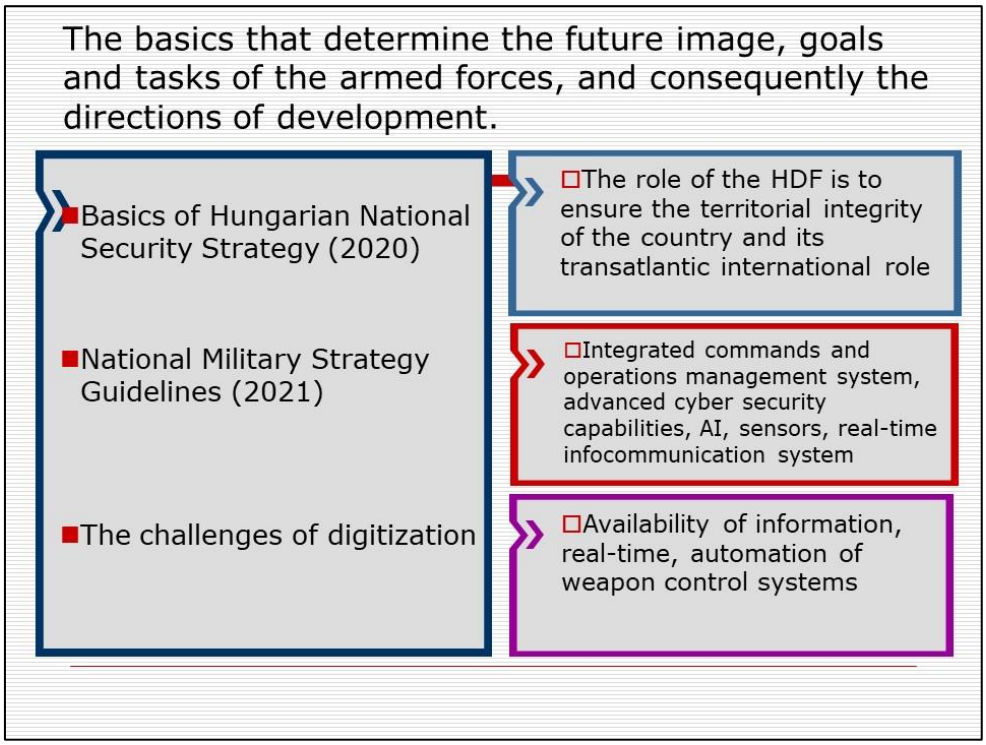
The basics that determine the future image, goals and tasks of the Hungarian Defence Forces, and consequently the directions of development are Hungarian National Security Strategy (2020), National Military Strategy Guidelines (2021) and the challenges of digitization. From point of view of the future developments the main role of the HDF is to ensure the territorial integrity of the country and its transatlantic international role, create Integrated commands and operations management system, advanced cyber security capabilities, AI, sensors and real-time infocommunication system.

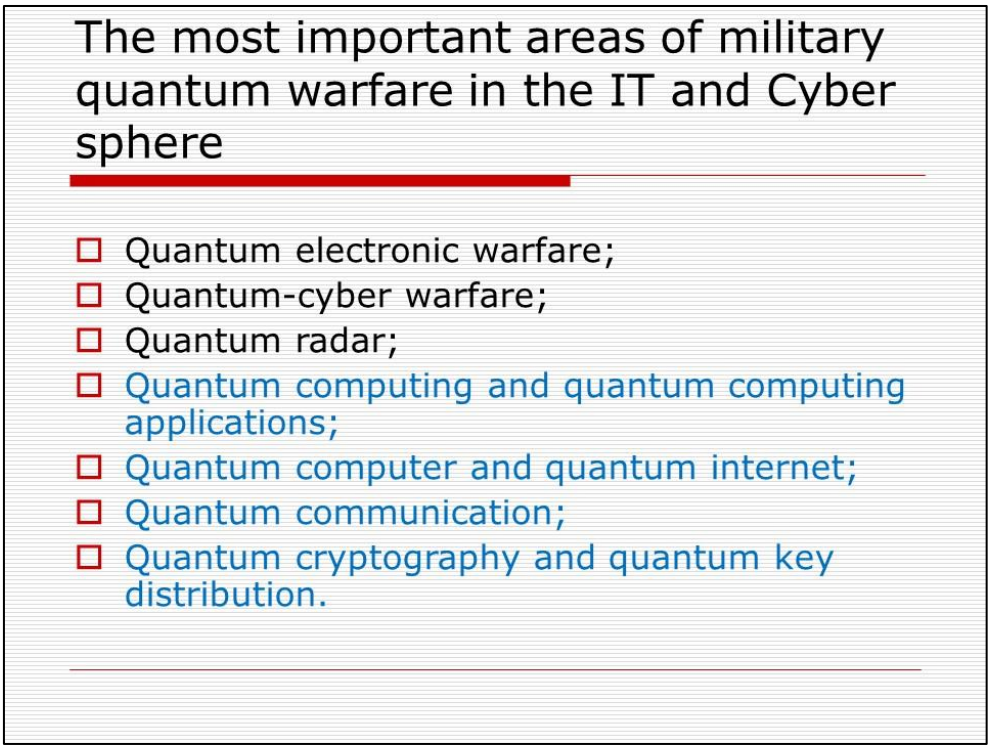
The such point of gravity within the security and defence quantum technologies as quantum computing and quantum computing applications, quantum computer and quantum internet, quantum communication, quantum cryptography and quantum key distribution can seriously influence military concepts and doctrines.

The quantum cybersecurity, quantum computing capabilities and quantum communication network for military applications might be characterized by special quantum defence capabilities, quantum attack capabilities, quantum computing capabilities, quantum clock synchronisation for the cooperation of C4ISR systems and such quantum information security applications as quantum key distribution, identification and authorization, quantum digital signature and position-based quantum cryptography.

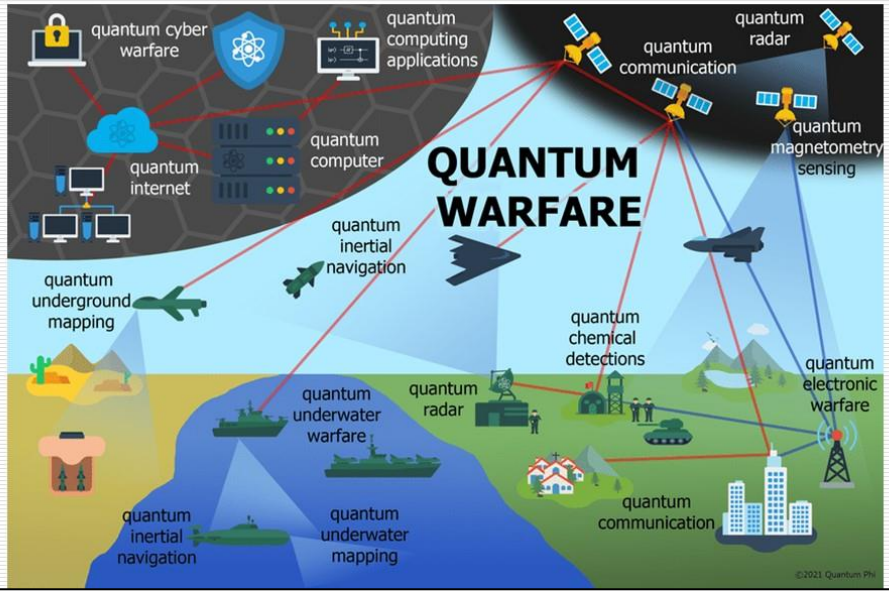
Keywords: Quantum Communication, Quantum Information Security, Quantum Cybersecurity, Quantum Cryptography




The basics that determine the future image, goals and tasks of the armed forces, and consequently the directions of development.
Basics of Hungarian National Security Strategy (2020)
National Military Strategy Guidelines (2021)
The challenges of digitization
The role of the HDF is to ensure the territorial integrity of the country and its transatlantic international role
Integrated commands and operations management system, advanced cyber security capabilities, AI, sensors, real-time infocommunication system
Availability of information, real-time, automation of weapon control systems


The most important areas of military quantum warfare in the IT and Cyber sphere
Quantum electronic warfare;
Quantum-cyber warfare;
Quantum radar;
Quantum computing and quantum computing applications;
Quantum computer and quantum internet;
Quantum communication;
Quantum cryptography and quantum key distribution.

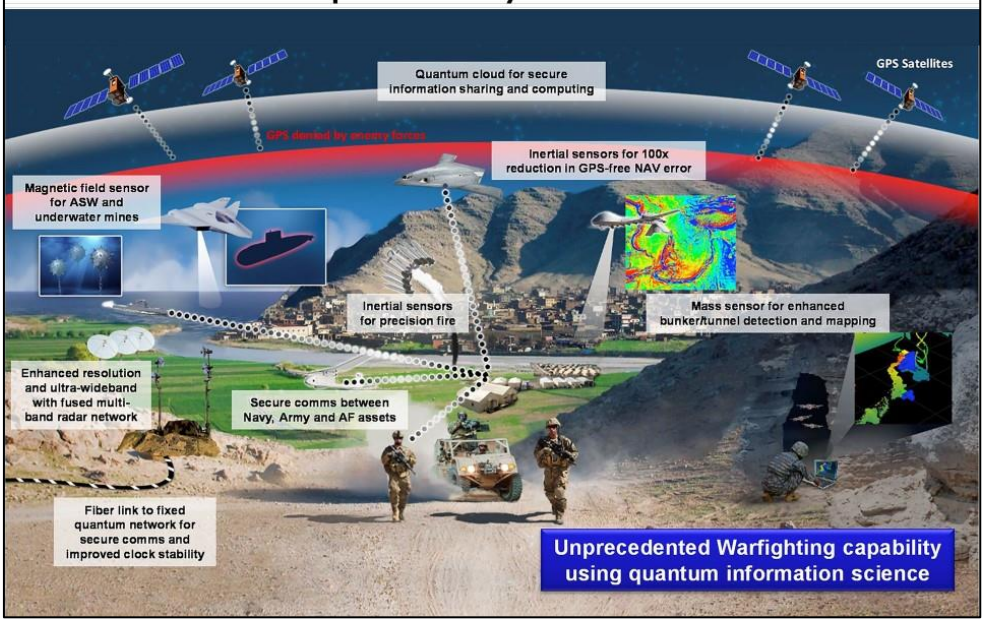
The most important areas of military quantum warfare



The main military areas of battle for data supremacy

- Sensor datas for extreme precision fire;
- Mass sensor for ASW, detection and terrain mapping;
- Enhanced resolution and ultra-widwband with fused (Multi-band) radar network;
- Secure comunications between military assets;
- GPS satellite communications and GPS denied by enemy forces;
- Quantum cloud between satellites for secure information sharing and computing;
- Quantum fiber links and fixed quantum network for secure communications.

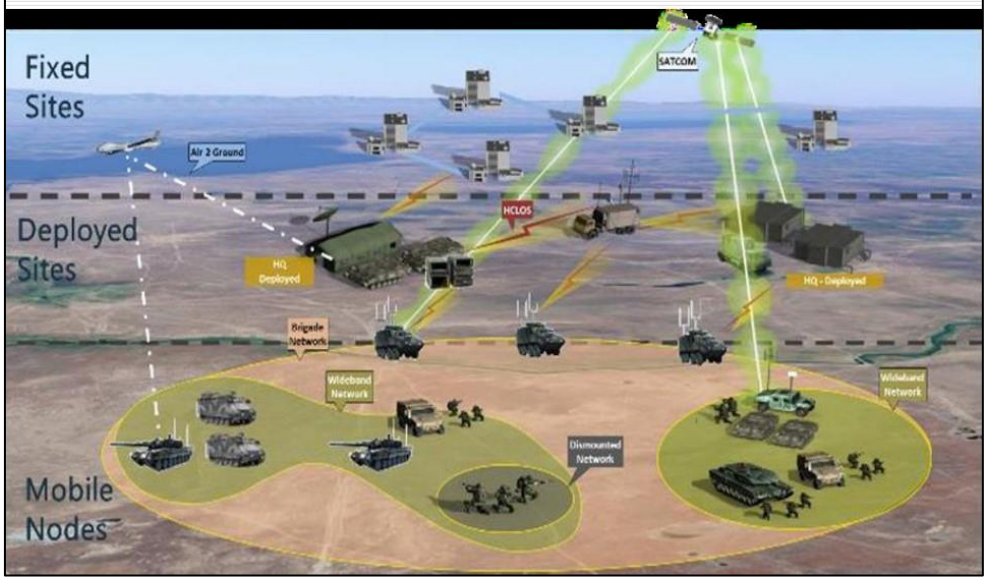
The main military areas of battle for data supremacy



Recent issues in Quantum Cybersecurity, Quantum Computing Capabilities and Quantum Communication Network

- Quantum Advantage in cyber warfare;
- Quantum Defence Capabilities (the post-quantum cryptography implementation, infrastructure for implementing quantum crypto-agility, new quantum-resilient algorithms);
- Quantum Attack Capabilities (Shor's algorithm based cryptoanalysis of PKE [RSA, DH, ECC], MAC, AES-GCM);
- Quantum Computing Capabilities (by increasing the number of qubits, put to the hybrid cloud, small embedded QCS, optimisation logistics, war planning, system validation, machine learining process, automatic cyber ops.);
- Quantum Communication Network (quantum clock synchronisation for the cooperation of C4ISR systems, quantum internet);
- Quantum InfoSec Apps. (quantum key distribution, identification and authorization, quantum digital signature, position-based quantum cryptography [by milsatcom]).

Satcom supported multi -level Hungarian military infocommunication system (one version)



References I:

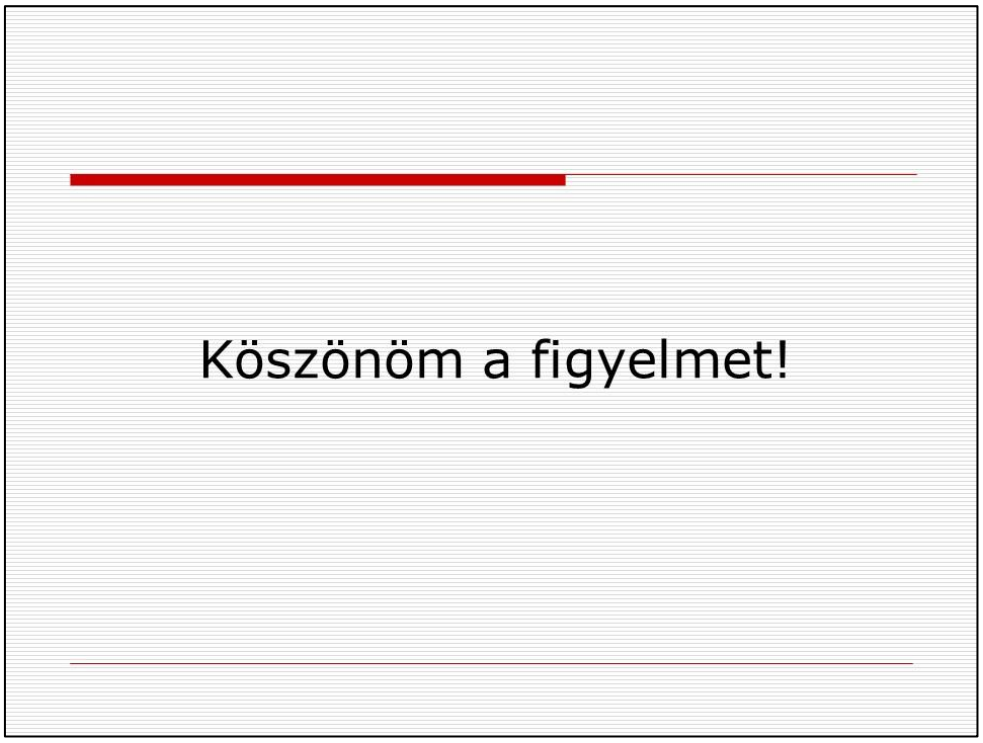
- Niels M. P. Neumann, Maran P. P. van Heesch, and Patrick de Graaf: Quantum Communication for Military Applications. In: (2020). arXiv: 2011.04989 [quant-ph];
- M.A. Nielsen and I.L. Chuang: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, 2010. ISBN: 9781139495486.;
- Juan Yin et al.: Satellite-based entanglement distribution over 1200 kilometers". In: Science 356.6343 (June 2017), pp. 1140{1144. doi: 10.1126/science.aan3211.;
- Isaac L. Chuang: Quantum Algorithm for Distributed Clock Synchronization". In: Physical Review Letters 85.9 (Aug. 2000), pp. 2006{2009. doi: 10.1103/physrevlett.85.2006.;
- Marco Lucamarini et al: Implementation Security of Quantum Cryptography. ETSI White Paper No. 27. July 2018.;

References II:

- Katie Kline, Marco Salvo, and Donyae Johnson: How Articial Intelligence and Quantum Computing are Evolving Cyber Warfare. Cyber Intelligence Initiative, The Institute of World Politics., Mar. 2019. url: https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/;
- Rajesh Uppal: Military decision support require ecient optimization algorithms. International Defense Security & Technology. Oct. 2019. url: https : / / idstch . com / technology / ict /military- decision-support- require- efficient- optimization- algorithms/;
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról;
- 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról;

References III:

- 1606/2021. (VIII.18.) Korm. határozata Magyarország Űrstratégiája elfogadásáról;
- Dr. Tóth András: Hálózatba kapcsolat harctéri eszközök (IoBT), ÚJ TÍPUSÚ KIHÍVÁSOK A BIZTONSÁGBAN, Budapest, 2022., Hírvillám, SIGNAL BADGE Professional Journal of the Signal Departement at the University of Public Service, pp.:229-235, HU ISSN 2061-9499 ;
- Marco Lucamarini et al: Implementation Security of Quantum Cryptography. ETSI White Paper No. 27. July 2018.;
- Farkas Tibor: A védelmi tevékenységeket támogató MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlesztési lehetőségeinek vizsgálata a honvédelmi és haderőfejlesztési program (Zrínyi 2026) tükrében – Hazai/nemzetközi szakirodalmi összefoglaló; Hadtudományi Szemle 12. (2019), 4. 5-16.;
- Quantum security technologies. NCSC (white paper). Mar. 2020. url: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.


Köszönöm a figyelmet!

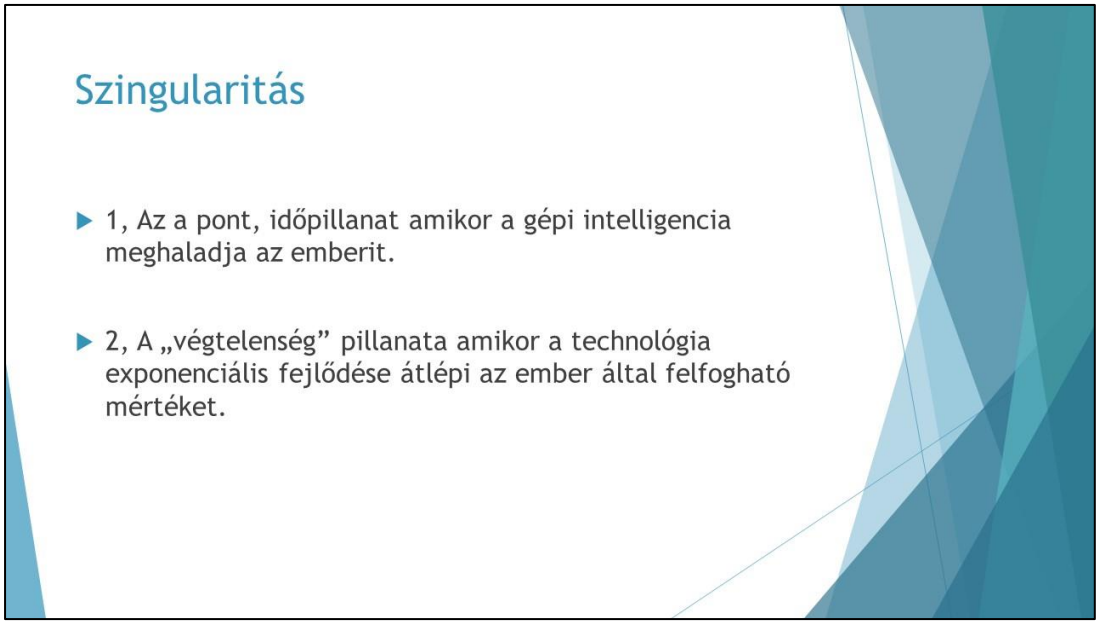
Szűcs Attila: Intelligens rendszerek – szingularitás

Korreferátum

A technológia szingularitást úgy szokás definiálni, mint azt a pontot, időpillanatot amikor a gépi intelligencia meghaladja az emberit. Vagy mint a „végtelenség” pillanatát amikor a technológia exponenciális fejlődése átlépi az ember által felfogható mértéket.
Ezt a jövőkutatók, hitech. szakemberek a közeljövőre várják, a gépi tanulás sebességének növekedésére, a Mesterséges Intelligencia önfejlesztő képességének létrehozására, valamint az agykutatás eredményeinek neurális hálózatokkal történő leképezésére alapozva.
Azonban, ha megnézzük a definíciókat, akkor azt kell látnunk, hogy legalábbis a második megfogalmazásban szeplő kritériumokat már most kimerítette a technológiai fejlődés.
A BigData, a hálózat kommunikáció sebessége, a lehetséges számítási kapacitások már ma is követhetetlené teszik a folyamatokat az ember számára.
A MI alkalmazások természetesen még mesze nem érik el a „skynet” szintjét, de egyes feladatok ellátásában már az öntanuló rendszerek jobbak az embernél. Az ilyen rendszerek összekapcsolása akár az általános problémamegoldás lehetőségét is elhozhatja kimerítve a szingularitás első megfogalmazását.

Kulcsszavak: Mesterséges Intelligencia, Szingularitás, BigData.


NKE HHK Híradó Tanszék
Intelligens rendszerek
Szingularitás
Előadó:
Szűcs Attila alezredes


Szingularitás
1, Az a pont, időpillanat amikor a gépi intelligencia meghaladja az emberit.
2, A „végtelenség” pillanata amikor a technológia exponenciális fejlődése átlépi az ember által felfogható mértéket.

Mikor? Mire alapozva?

- Raymond Kurzweil amerikai kutató (karakter felismerés, beszéd analízis) szerint 2045-re elérjük.
- A Morre törvény kiterjesztésére alapozva a növekvő számítástechnikai kapacitás alapján.
- Az agykutatás eredményeinek neurális hálózatok fejlesztésében történő felhasználásával. Ahol a Morre törvény szintén érvényes a diagnosztikai eszközök fejlődése és az eredmények kiértékelése terén.
- A gépi tanulás kiterjesztésével. Amikor már nem csupán egy meghatározott folyamatban kívánjuk tökéletesíteni a gépi döntéshozatalt hanem az általános problémamegoldás felé törekszünk.

Hol tartunk most?

- Az a véleményem, hogy a második megfogalmazás szerint már most túlhaladtuk azt a pontot amikor egy ember még képes lehet követni a technológia fejlődését, így az intelligens rendszerekét.
- Már évtizedekkel ezelőtt megfigyelhető volt, hogy a kutatásokat, fejlesztéseket nem a magányos zsenik végzik mint ahogyan az még a huszadik század második feléig is gyakorta történt. Ma már annak is külön tudománya van, hogy hogyan épüljön fel egy kutatócsoport. Milyen feladatokra milyen képzettséggel, tapasztalttal rendelkező munkatárs kell, hiszen senki sem érthet mindenhez.

- Az adatbázisok BigData amiket a MI elérni képes messze meghaladja azt amit egy ember átláthat.
- A IOT eszközök alkalmazásával ez az olló csak tágul az egyidejűleg elérhető információk szűrését, tematizálását, feldolgozását szintén informatikai rendszerek végzik.
- Az adatáramlás mértéke és a feldolgozás sebessége már szintén rég túl van azon, ami még „emberi léptéknek” nevezhető.

Akkor itt van a „Skynet”?

- A szingularitás 1. megfogalmazás szerinti értelmezésében még nem.
- Egy komplex, az emberi intelligenciát általános döntéshozatali képességben meghaladó MI még ismereteink szerint nem létezik.
- Véleményem szerint azonban már itt is határra érkeztünk. A különböző rendszerek összekapcsolásával már összetettebb feladatra is képesek az ilyen rendszerek. Ez a fejlődés pedig elhozhatja, hogy nem egy központi MI lesz hanem egy hálózat.
- Az, hogy ezt a hálózatot ki ellenőrzi, -ha ez egyáltalán lehetséges- jelenti a hatalmat a jövőben.

Köszönöm a figyelmet.

Kérdések?

Felhasznált irodalom

- Tilesch - Atamlech 2021. Dr. Tilesch György és Dr. H-Atamlech, Omar 2021. Mesterség és Intelligencia. Budapest: Libri,
- Wang - Lanz 2020. Wang, Yunwen and Lanz, Paulina 2020 :Why Is Artificial Intelligence Blamed More? Analysis of Faulting Artificial Intelligence for Self-Driving Car Accidents in Experimental Settings, *Inernational Journal of Human-Computer Interaction* 36.18.
- Dr. Seres György: A barlangrajzoktól a mesterséges intelligenciáig http://www.mmo.njszt.hu/Kiadvanyok/2021/MMO2021_Proceedings.pdf (Letöltés ideje 2021.08.25.)
- Gáspár Merse Előd: Mi az a technológiai szingularitás, és mikor jön már el? https://qubit.hu/2018/01/03/mi-az-a-technologiai-szingularitas-es-mikor-jon-mar-el (Letöltés: 2022.04.06.)
- Szűcs Attila 2022. Biztonsági kihívásiok a mesterséges intelligencia katonai alkalmazásában. *Signal badge* (Új típusú kihivások a biztonságban szakmai konferencia): 225-228
- Raymond Kurzweil: The Law of Accelerating Returns https://web.archive.org/web/20100619033859/http://www.kurzweilai.net/articles/art0134.html?printable=1# (Letöltés ideje: 2022.04.06.)

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és/vagy idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás*

nélkül - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Megjelent az NKE HHK Híradó Tanszék gondozásában

www.comconf.hu
www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-407 mellék)