HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2024

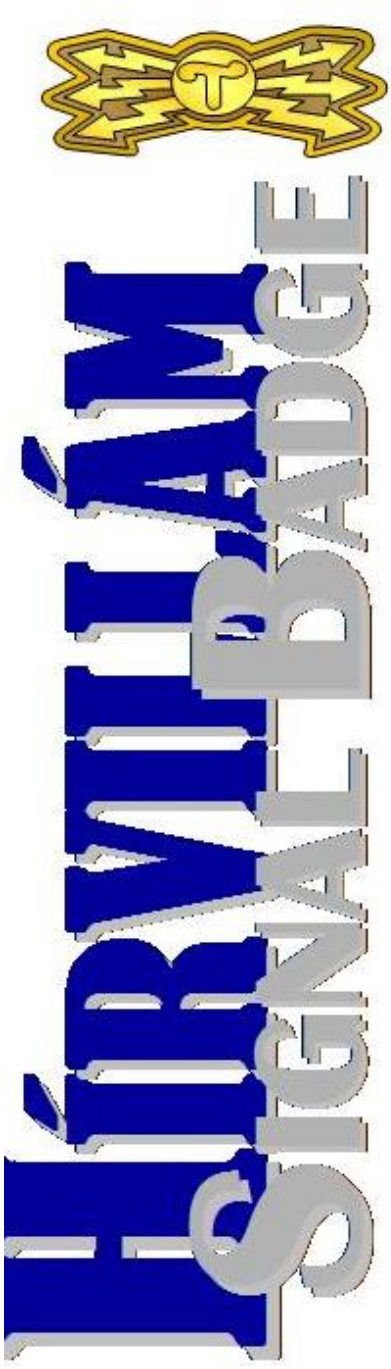
Proceedings of the International Scientific Conference on Military Information Security

09th May 2024

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, 2024



HU ISSN 2061-9499

University of Public Service
Signal Department
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15

Table of contents

Greetings

Welcome Dear Colleague, Dear Reader!

On May 9th, 2024, the Signal Department of the Faculty of Military Sciences and Officer Training at Ludovika University of Public Service, in cooperation with the Donát Bánki Faculty of Mechanical and Safety Engineering at Óbuda University, organized a scientific conference titled "International Scientific Conference on Military Information Security" at the Óbuda University campus in Budapest.

The primary aim of the conference is to establish an annual scientific and professional platform that facilitates the presentation and discussion of cutting-edge research findings, promotes the dissemination of knowledge, and encourages meaningful networking opportunities for scholars, researchers, and professionals within the field.

Fourteen researchers presented their research results, which were published in this professional journal with the authors' contributions. The reviews cover areas that have a fundamental impact on information security in today's military environment.

In this publication, the Editorial Board has collected the abstracts of the presentations, which it is very pleasing to make available to the Dear Readers.

Budapest, 09th May 2024

Dr. habil Tóth András
Editor in Chief

Conference Program

International Scientific Conference on Military Information Security

Conference Programme

09th May 2024

08:30-08:55	Registration	
08:55-09:00	Opening remarks	Prof. Dr. Rajnai Zoltán
Plenary I. Chair: Dr. Farkas Tibor		
09:00-09:15	*Current threats in cyberspace*	Dr. Kucsera Erika
09:15-09:30	*Az MI kiberbiztonsággal kapcsolatos fontosabb kérdéseinek vizsgálata*	Dr. Páll-Orosz Piroska Dr. Kassai Károly
09:30-09:45	*The role of security operation centres in the age of artificial intelligence*	Dr. Magyar Sándor
09:45-10:00	*The potential use of crowdsourcing in times of conflict*	Dr. Dobák Imre
10:00-10:15	*The impact of advanced ICT solutions on command and control systems, from an information security perspective*	Dr. Tóth András
10:15-11:00	Coffee break	

Plenary II. Chair: Dr. Magyar Sándor		
11:00-11:15	*Some vulnerabilities of global positioning systems*	Knapp Gábor
11:15-11:30	*Challenges of C2 in multidomain environment*	Fazekas Ferenc
11:30-11:45	*Opportunities and challenges in analysing the actions of cyber threat actors*	Szulcsányi Viktor
11:45-12:00	*The place and role of the cyber security trainings in the Hungarian Defence Forces*	Busa Attila József
12:00-12:15	*Egy publikus felhőszolgáltatás biztonsági kontrolljai egy pénzintézetnél*	Oláh István
12:15-13:00	Lunch	
	Plenary III. Chair: Dr. Tóth András	
13:00-13:15	*The need to develop information security awareness*	Stranszki Péter
13:15-13:30	*The Role and Impact of the Network Equipment Security Assurance Scheme (NESAS) in the 5G Era*	Haya Altaleb (Jordan)
13:30-13:45	*ICT and telecom Supply Chain, evolving threat Landscapes, countermeasures, and Solutions*	Lourdes Salvador Ruiz Cecilia (Ecuador)
13:45-14:00	*Mobile Communication Evolution and the development of 5G in China*	Yue Wu (China)
14:00-14:10	Closing remarks	

Erika Kucsera: Current threats in cyberspace

Correferatum

Nowadays, a variety of factors are shaping the current threats in cyberspace and with them the strategies and methods of protection. The rapid changes and the methods and technologies adopted in our times are constantly challenging the defence side, making it particularly important to be up-to-date and flexible in responding to new security challenges.

Many factors influence the focus and methods of cyber defence activities. An example of the impact of technological advances is the explosive growth and application of artificial intelligence for defence and offensive purposes, which poses a number of new challenges to the cyber sector.

The current motivation and methods of the attacking side are different, they can be financially, ideological, politically motivated, and the defensive side must be prepared for this.

Attacker groups are quick to copy and adopt new techniques used by other groups, and there is also a growing industry focus on the marketing of attacker services. A new trend is the development of interconnected Crime-as-a-Service marketplaces, which now offer a complete attack planning and execution service, combining several sub-services of disruptive activities and selling them as a complete package.

The Russian-Ukrainian war and conflicts influence the type and orientation of operations and activities in cyberspace and provide a range of cyber offensive and defensive experiences, the threat analysis processing of which will facilitate professional development in the defence domains. The Russo-Ukrainian war has emphasised the wide range of information manipulation that forces cyberspace actors to complement and restructure their defensive policies. The modes of attack encountered during the war so far have been DDOS, website content modification, information operations, disinformation campaigns, malicious code distribution, aimed at damaging the reputation of the government, disrupting communication and information sharing, information gathering, reducing the responsiveness of the armed forces and confusing the supporting countries.

The impact of the international regulatory environment is highlighted by the ongoing NIS2 harmonisation process, the transposition and application of which will be a challenge for the cyber actors, imposing a significant workload on them. The proliferation and detailed regulation of artificial intelligence is expected to create new regulatory and procedural challenges for the executive branches.

Advances in technology, changes on the offensive side, and changes in the regulatory environment challenge defence professionals and

encourage them to continuously update their knowledge in order to maintain a high level of effectiveness.

GENERAL BACKGROUND

- INTERNATIONAL PERSPECTIVES
- NATIONAL PERSPECTIVES
- BUSINESS-TYPE APPROACH

GROUPS

- GROUPS
- TECHNICS
- CHANGES IN TRENDS

RISKS RELATED TO MODERNISATION

- SYSTEM KNOWLEDGE
- SUPPLY CHAIN
- TECHNOLOGIES
- VALIDITY ISSUES
- USE OF NEW TECHNOLOGIES IN OPERATION, MONITORING

CYBERSPACE EXPERIENCES OF THE RUSSIAN-UKRAINIAN WAR

- MANIPULATION WEBSITE CONTENT
- DDOS
- INFORMATION OPERATIONS
- DISINFORMATION CAMPAIGNS
- PHISHING CAMPAIGNS, MALICIOUS CODE DISTRIBUTION

OTHER IMPACTS

- NIS2 IMPACTS
- RETHINKING, REVIEWING
- WORKLOAD VS SAFETY SITUATION IMPROVEMENT

Bibliography

271/2018. (XII. 20.) Korm. Rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól;

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;

A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. Törvény;

6/2020. (IV. 16.) HM rendelet a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok meghatározásáról;

AC/35-D/2005-REV3 Management Directive on CIS Security;

ENISA threats landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, 2023.11.11.


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
KÖSZÖNÖM A FIGYELMET!
uni-nke.hu

Kassai Károly[1]: A mesterséges intelligencia kiberbiztonsággal kapcsolatos fontosabb kérdéseinek vizsgálata (Hogyan lehet a megfoghatatlant megközelíteni és a biztonságáról beszélni?)

Korreferátum

Bevezetés

A mesterséges intelligencia (továbbiakban: MI) tanulmányozása elképzelhető több szinten, különböző szempontokra koncentrálva, eltérő mélységben vagy egy témakörre célozva, mint például az információbiztonság.

Az MI rendszerek megjelenése a honvédelem területén nemzeti stratégiai, stratégiai és (had)műveleti, valamint harcászati (technikai) szinten is elképzelhető. A cikk egy szélesebb területű kutatás részeként[2] azt vizsgálja, hogy a honvédelmi, katonai nemzetbiztonsági területeken milyen módon lehet és kell az alkalmazott (üzemeltetett vagy igénybe vett) *MI rendszerek szolgáltatásait biztonságossá tenni*. A biztonság ebben az esetben a meglévő jogszabályok, NATO és EU követelmények szerinti

[1] ORCID: 0009-9398-6158

[2] A KNBSZ mesterséges intelligencia (MI) hatásainak specifikus vizsgálata (2024-2025) kutatási terv; Az elektronikus információs rendszerek, szolgáltatások szervezeti szintű, kiberbiztonsági szempontú felkészítési feladatainak körvonalazása az MI hatások hatékony kezelése érdekében című kutatási program.

információbiztonsági (elektronikus információvédelmi vagy kiberbiztonsági), [3] valamint katonai követelményeknek való megfelelést jelenti, figyelembe véve az MI rendszerek fejlődésben lévő állapotát és ebből következően a folyamatosan változó helyzetet.

Egyszerűsítéssel élve a szakmai kérdés a következő: kell-e közeljövőben Magyarországon MI Informatikai Biztonsági Szabályzatot írni, vagy milyen más formában kell a biztonsági elemeket meghatározni és ezeket a kérdéseket hogyan kell kezelni a honvédelmi és katonai nemzetbiztonsági szervezeteknél?

A vizsgálati szempontok tisztázása

A megfelelően tisztázott vizsgálati cél és környezeti lehatárolás nélkül nincs értelme komoly vizsgálatról beszélni. Az MI-t övező számtalan megközelítés, a definíciós eltérések megvilágítása már önmagában túlmutat egy cikk horizontján. Hazánk EU tagsága támpont a megindításhoz, így a lehatároláshoz az EU „MI rendszer” megközelítés alkalmazása adja a megoldást. A felhasználáshoz szükséges adatok, az esetlegesen szükséges adatátvitel, a feldolgozó algoritmusok munkája, a szükséges be- és kimeneti interfészek és az ezt biztosító technikai környezet komplexitása jelenti a „rendszert”.

[3] A cikk nem vállalja a terminológiai kérdések megoldását, így az említett fogalmak lehető legtágabb értelmezésének elvét követi.

Az MI rendszer biztonság kérdésének megközelítésében további segítséget jelent az EU Kiberbiztonsági Ügynökség szelektálása, ahol az *„MI kiberbiztonság”* mellett további kategóriaként szerepel az *MI kiberbiztonságot támogató szerepe* (pl. védelmi rendszerekbe történő beépülés), illetve az *MI kártékony (ellenséges) használata*, mely esetek vizsgálatát a cikk nem vizsgál (ENISA, 2020, p. 7).

Az MI információs rendszer szerinti megközelítés Csáki véleménye szerint a *technológia* (szoftver), *adatok* (történeti, valós – klb. formátumok), *folyamatok* (fejlesztés, üzemeltetés), *ember* (szerepkörök szerint) részekre bontható (Csáki, 2023, p. 37).

Szervezeti szempontból elkülönített esetként kezelendő, illetve más-más felügyeleti és védelmi eljárásokat igényel a *saját üzemeltetésű MI rendszer*, vagy *más szereplő által üzemeltetett MI rendszer szolgáltatásának igénybe vétele*. Az MI rendszerek más elektronikus információs rendszerekhez hasonlóan „nem a semmiből születnek”, így másik lehatárolási szempontként az *életciklus szemlélet* nyújthat segítséget.

Fontos annak megértése is, hogy a napi életben, illetve a honvédelmi és katonai nemzetbiztonsági területen az MI rendszer nem csak egy szolgáltatási forrás, inkább a *sokféle MI rendszer szolgáltatás igénybevételét feltételező megközelítés a helyes megoldás*.

A fenti kiindulási pontok megalapozzák a következtetést, hogy az MI rendszerek megközelítésekor is alkalmazhatók az eddigi szempontok, *a súlypontot a specifikus jellemzők azonosítása képezi*.

Katonai alkalmazások

A világon az MI katonai alkalmazására rengeteg példa hozható. Egy védelemipari forrás példaként említi a *katonai rendszereket* (platformokat), a *stratégiai döntéshozatalt*, az *adatfeldolgozást és kutatást*, a *harci szimulációt*, a *célfelismerést*, a *veszélyfigyelést*, a *drónrajokat*, a *kiberbiztonságot*, a *közlekedést*, és a *sérültek ellátását és evakuálását* (SDI, 2024). A területek és szolgáltatások között átfedések lehetségesek, de a legfontosabb megoldások bemutatása rámutat arra a specialitásra is, hogy *az MI rendszerek és szolgáltatások stratégiai, hadműveleti és harcászati (technikai)* szinten is azonosíthatók, egyes megoldások *több szinten is alkalmazhatók*.

Felismerhető, hogy egyes katonai alkalmazások valamilyen *önállóan működő modell szolgáltatásain alapulnak* (pl. az elemző és szimulációs megoldások), ugyanakkor léteznek *független hardver eszközbe beépített megoldások* is (pl. a különböző szárazföldi, légi vagy vízi platformok). A katonai MI rendszer sokszínű alkalmazásának érzékeltetésére jó példa a NATO Kibervédelmi Kiválósági Központ[4] 2021-es tanulmánya, ahol a szerzők NATO

[4] NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

tagállamokra szűkített kutatása négy területre bontva több tucat MI rendszer szolgáltatást tartalmazó haditechnikai fejlesztést[5] említ (Maggie Gray - Amy Ertan, 2021, pp. 24-29).

Stratégiai szintű adatfeldolgozási képességre példa a NATO fejlesztés, ami megtöri a minősített adat MI rendszer által történő kezelésére vonatkozó félelmet (NATO, 2023). Ez a NATO szintű képesség független a szövetségesek nemzeti képességeitől, ugyanakkor példa arra, hogy *magas biztonsági követelményeket igénylő technikai környezetben is kialakíthatók MI rendszer üzemeltetési feltételek*.

A nemzeti megoldások kapcsán egy másik, amerikai példa mutatja, hogy a minősített adatkezelés körében a nemzetbiztonsági területen sem sem szabad lemondani az MI rendszer szolgáltatásairól (Edwards, 2024).

Mindkét példa aláhúzza, hogy az adatokért, adatkezelésért felelős szervezet hatáskörébe tartozik annak kimondása, hogy a betartandó normák, követelmények keretén belül *milyen MI rendszer szolgáltatása tekinthető szövetségi vagy nemzeti szempontból elfogadható kockázatú megoldásnak*.[6]

[5] Az említett adat mellett nyilvánvalóan több nyilvánosan nem megismerhető fejlesztés létezhet, illetve a jelentős számú fejlett technológiát képviselő országban is rengeteg haderőfejlesztést támogató, MI rendszerfejlesztést tartalmazó program képzelhető el.

[6] Az MI rendszerekkel kapcsolatos stratégiai dilemma nem egyedi. Hasonló kérdéseket kell megoldani a felhőszolgáltatások igénybevételekor, a federációs alapon kialakított kommunikációs hálózatok esetében, illetve a szövetségi (vagy nemzetközi) rejtjelző szolgáltatások biztonsági irányelveinek megfontolásakor.

Kockázat alapú megközelítés

A 2024. májusban véglegesített EU MI rendelet az MI rendszerek kockázatainak kézben tartása érdekében hármas megközelítést alkalmaz, mint *tiltott*, *magas kockázatú* és *alacsony kockázatú* megoldás. A megengedett, de magas kockázatú rendszerek esetében *kiegészítő biztonsági rendszabályok alkalmazása szükséges* (ezen belül kiemelt szempont az emberi felügyelet biztosítása), míg az alacsonyabb kockázat esetében elégséges az átláthatóság biztosítására vonatkozó követelmények teljesítése. A rendelet a tagállamok számára *felügyelő hatóság kijelölését határozza meg*, valamint *a szolgáltatók nyilvántartását*, *a termékek tesztelését és tanúsítását*, *nemzeti és EU adatbázis kialakítását*, valamint az MI rendszerek esetében tapasztalt *incidensek bejelentési kötelezettségét* (EU, 2024, 66, 76, 138. p. 9-10.§, 26.§, 59-60,§ és 73.§).

A rendelet kapcsán a magyar jogszabályokra kifejtett hatások még nem ismertek. A direkt követelmények (pl. felelős hatóság kijelölése) végrehajtása önálló jogszabályban, vagy meglévő szabály módosításával is elképzelhető. A kapcsolódó nemzeti szintű eljárások kialakítása többféle módon is megoldható, tehát szakmai szempontból a jelenlegi ismeretek alapján lehet érvelni egy MI rendszer törvény (vagy korm. rendelet) mellett, illetve másik a meglévő jogszabályok módosítása is járható útnak tekinthető, a jogszabály alkotó szándékai szerint.

A rendelet a védelem, a nemzetbiztonság és kutatás körébe tartozó *MI rendszerekre nem vonatkozik*, így jelenleg nyitott kérdés, hogy a magyar jogszabályi környezet ezt a kérdést hogyan fogja kezelni.

Rendszer szintű sajátosságként kell elkönyvelni, hogy a védelmi szférára vonatkozó mentesség csak abban az esetben érvényes, ha az MI rendszer *alkalmazása a rendeltetés szerinti*. Más területű felhasználás esetén (pl. katasztrófavédelem, polgári célú felhasználás) *a katonai MI rendszernek teljesítenie kell az összes általános követelményt*.

Az általános követelmények mellett érdemes a katonai sajátosságokra is figyelmet fordítani. Az Európai Parlament a halált okozó autonóm fegyverrendszerekkel kapcsolatban szorgalmazza egy olyan (nemzetközi) közös álláspont kialakítását, *amely garantálja a fegyverrendszerek kritikus funkciói feletti érdemi emberi ellenőrzést*, a telepítést is beleértve. Fontos a kritikus funkciók – például *a célpont kiválasztása és megtámadása* – terén emberi irányítást nélkülöző, halált okozó autonóm fegyverrendszerek fejlesztésének és előállításának megelőzése (EU, 2018, 2 és 4. p.).

Ezzel összecseng katonai platformra utaló 2024 május elsején történő amerikai sajtónyilvános kísérlet, ahol egy módosított F-16-os, MI vezérelt vadászrepülő vívott vizuális környezeten belüli légiharcot ember által vezetett technika ellen, amit a pilótafülkében

a légierő felügyeletéért felelő államtitkár közvetlenül szemlélhetett. A leszállás utáni interjú fontos része volt, hogy az államtitkár kifejezte, *a hasonló megoldásoknál mindig az emberi döntésnek kell a háttérben állnia* (Copp, 2024).

Az autonóm fegyverrendszerekre vonatkozó korlátozás egyértelműen azonosítható az amerikai Védelmi Minisztérium 2023 elején frissített szakirányú direktívájában. E szerint az autonóm és félig-autonóm fegyver rendszereknél *a parancsnokok, kezelők számára biztosítani kell, hogy megfelelő szintű döntéseik lehessenek az alkalmazáskor* (use of force) (US, 2023a, 1. 2. a. pont).

Az autonóm fegyverekkel kapcsolatos álláspont érzékelhetően szilárd. Ugyanakkor az is kijelenthető, hogy *a technológiai fejlődés akár rövid időn belül is produkálhat olyan eseteket, melyek határesetnek értékelhetők*, így kiemelten fontos az *új termékek, szolgáltatások kockázatainak menedzselése, illetve a funkcionális és biztonsági tesztek, megfelelőségi vizsgálatok valós eredményeket tükröző végrehajtása*.

Az eddigiek számtalan példát mutattak az MI rendszerekkel kapcsolatos fenyegetésekre, kockázatokra, melyeket szükséges mértékű védelmi rendszabályokkal, eljárásokkal lehet és kell ellensúlyozni. Ez a felvetés *megvilágítja a kockázatelemzés (és menedzsment) fontosságát* az ellensúlyozást igénylő szempontok

azonosítása érdekében, illetve az ehhez illesztett *biztosági kontrollok szükségességét*.

Az Európai Bizottság stratégiai szintű megfontolásként 2023-ban ajánlást adott ki a tagállamok felé *a legmagasabb kockázatúnak tekinthető kritikus technológiai területek áttekintésére*, mint MI technológiák, fejlett félvezető technológiák, kvantum és biotechnológia, *melyek sürgős kockázatcsökkentési eljárásokat kívánnak* (EU, 2023, p. 3).

Az elektronikus információs rendszerek üzemeltetésének és biztonsági felügyeletének logikáját követve az is leszögezhető, hogy az általánosan használt „biztonságos MI rendszer" vagy a „biztonságos elektronikus információs rendszer" elméleti fogalom.[7] Emiatt szükség van az adott MI rendszer paramétereinek ismeretére, ami lehetővé teszi a valósnak tekinthető *fenyegetések feltárását*,[8] majd a *védelmi rendszabályok meghatározását*.

A biztonsági követelmények jelenlegi bizonytalansága

[7] A biztonságosnak tekintett „rendszer" paramétereinek hiányában egy olyan elméleti modell megalkotására lenne szükség, ami az összes fenyegetés fennállása mellett az összes sérülékenység kiküszöböléséhez biztosít védelmi megoldásokat. Ez utal a gyakran hangoztatott „biztonságos rendszer nem létezik" vagy „száz százalékos biztonság nem létezik" közismert szlogenekre, de rámutat arra is, hogy minél részletesebben ismert az adott rendszer felépítése, működése, annál sikeresebben tárhatók fel a gyenge pontok és alakíthatók ki hatékony védelmi mechanizmusok, eljárások.

[8] Jó példa erre, hogy létező fenyegetés a meteorit becsapódás, de az adott védendő objektum (épület, kritikus infrastruktúra, elektronikus információs rendszer stb.) valóban igényli-e az ilyen esetek kezelését?

A fontosabb elektronikus információbiztosági szabványok, ajánlások jelenleg még MI rendszer specifikus vizsgálati szempontokat nem tartalmaznak. Az ISO/MSZ 27001 strukturált megközelítést biztosít az elektronikus információbiztonsági felügyeleti rend kialakításához, vonatkozó fejezete általános kockázatelemzési keretet biztosít, MI rendszer kitételeket nem alkalmaz (MSZ, 2023).

A kockázatmenedzsmentre vonatkozó MSZ ISO 31000: 2018 szabvány használható keretet biztosít kockázatok felmérésére és elemzésére a felhasználó szervezetek számára, így csak *az MI rendszerrel kapcsolatos specifikus információk meghatározására van szükség* (MSZ, 2018, 6.4.2 – 6.4.4. p.).

Előremutató külföldi példa az Amerikai Egyesült Államokban kiadott – nem kötelező érvényű MI Kockázatkezelési Keretrendszer, ami segítséget nyújthat az adott MI rendszerrel kapcsolatos, biztonsági vetületű kérdések felszínre hozatalában, a meglévő szabványok, ajánlások alkalmazásában, egyben segítséget nyújt a különböző megítélési szempontok azonosításához. Érthetően megvilágítja az életciklus állomások eltérő kockázatait a kockázatviselés (risk tolerance) és a kockázatok *priorizálásának központilag nem meghatározható*, helyi (szervezeti) szerepét és segít az MI szereplők azonosításában. Az MI rendszerek (és azok kockázataik) megítélése a *megbízhatóság* (trustworthiness) egymással is hatásban lévő elemein keresztül történik, ahol fontos

szerepe van a *biztonságnak* és az *ellenálló képességnek* (security and resilience).

Az MI rendszerek biztonságának alapja a szakmailag közismert *bizalmasság, sértetlenség és rendelkezésre állás* (confidentiality, integrity, and availability) hármasa, tehát új, lényegi elem látható a keretrendszerben. A dokumentum rámutat, hogy az AI rendszerek esetében követni kell a szövetségi Kiberbiztonsági Keretrendszer [9] a Kockázatmenedzsment Keretrendszer,[10] és az Adatvédelmi Keretrendszer[11] irányelveit.

Az MI kockázatmenedzsment központját (Core) négy funkció képezi, mint *irányítás, azonosítás, mérés és menedzselés* (govern, map, measure, manage), melyek kategóriák és alkategóriák további bontásával kialakítható *a szervezetnél szükséges eljárásrend és eszközrendszer*. Ezekre az eszközökre támaszkodva látható, hogy érdemes *használati profilokat* (use-case profile) kialakítani, pl. ideiglenes, jelenlegi, cél, bérelt, saját vagy szektorokon átívelő profilok azzal a magyarázattal együtt, hogy a keretrendszer a kellő rugalmasság biztosítása érdekében nem tartalmaz központi mintákat, *azt mindenkinek saját igénye szerint célszerű kialakítani* (US, 2020, pp. 6-7, 10, 12-13, 15, 17, 20, 33-34).

[9] NIST Cybersecurity Framework
[10] NIST Risk Management Framework
[11] NIST Privacy Framework

Magyar szabályozási területen az elektronikus információbiztonságra vonatkozó törvény (Parlament, 2013), és a végrehajtására vonatkozó rendelet (BM, 2015) MI rendszer specifikációt jelenleg nem tartalmaz. Az EU NIS 2 irányelv [12] követelményei alapján tervezett új nemzeti szabályozás tervezet esetében is hasonló a helyzet (BM, 2024). Megjegyzendő, hogy a magyar szabályozás alapjául szolgáló amerikai általános elektronikus információbiztonsági követelményrendszer ehhez hasonlóan szintén nem tartalmaz MI rendszerre vonatkozó szűkítéseket (US, 2020).

Logikus következtetés, hogy nemzetközi szabványok megjelenése várhatóan irányelvek, megközelítések szempontjából segítséget nyújthat, de a rendelkező ismeretek alapján hatékony megoldásnak egyedül *a meglévő elektronikus információbiztonsági keretrendszer pontosítása* mutatkozik. E mellett megállapítható a személyes adatok védelmével kapcsolatos kérdés kiemelt szerepe is, így *a meglévő adatvédelmi keretek pontosítása szintén prioritást képező feladat*.

Az EU szintű követelmények alkalmazása (mint például a NIS 2 és a CER[13] irányelvek, a DORA[14] rendelet) kötelező tagállami feladat az MI rendszerek területén is, illetve fontos hatásokat fog kifejteni a magyar jogszabályokban történő, az MI rendszere

[12] EU Network and Information Security Directive, 2022/2555
[13] CER: Resilience of Critical Entities, 2022/2557
[14] DORA: Digital Operational Resilience Act, COM/2020/595 final

üzemeltetésének szabályozásával kapcsolatos változások átvezetése is, kielemelt figyelemmel a magas kockázatú MI rendszerekre.

A kontroll alapú megközelítés mellett említendő egy másik szabályozási szemlélet. Az Amerikai Egyesült Államok 2024-es törvényjavaslata intézményi alapokkal kezdi meg az MI rendszerek üzemeltetésének biztonságossá tételét. Az MI Biztonsági Központ fő feladata a *sérülékenység kutatás*, az MI *biztonsági esemény adatbázis kialakítása és üzemeltetése* (beleértve „majdnem" ügyeket is) az *MI RED team irányelv*[15] fejlesztés és az MI *biztonsági események fejlesztési fázisban történő jelentések fogadása* (US, 2024).

Összefoglalás

Az áttekintett források alapján kijelenthető, hogy az MI rendszer és szolgáltatás fejlesztési kérdések mellett már megjelentek az elektronikus információbiztonsággal, kiberbiztonsággal kapcsolatos alapvető kérdések.

Általánosítható tapasztalat, hogy az MI rendszer jellemzők felbukkanása, kiemelése (pl. megbízhatóság, adatvédelem, emberközpontúság) mellett megerősített szempont *a meglévő*

[15] RED team módszertan: védelmi eljárás, az adott elektronikus információs rendszer tervezett, szisztematikus támadása a sérülékenységi pontok feltárása és azok kiaknázása érdekében, ami alapot biztosít a védelmi rendszabályok pontosításához.

nemzetközi normák, jogszabályok alkalmazásának kötelezettsége, így az MI rendszerrel kapcsolatos új kérdések a jelenleg tapasztalható szempontok alapján nem szülnek új üzemeltetési és biztonsági eljárásokat, hanem *a meglévő eszközök pontosításának* útját követik (az MI rendszer nem kaphat felmentést népszerűsége, vagy korszerű szolgáltatás portfóliója miatt).

Az MI rendszerek esetében is alapvető kérdés *a rendszerek funkciók szerinti azonosítása*, *fenyegetés alapú besorolása*, ami megalapozza az alkalmazott védelmi rendszabályok, eljárások *pontosíthatóságát*, *testre szabását*. Az *életciklus megközelítés* alkalmazása segíthet a feladatok és felelősségek lehatárolásában, illetve a kockázat alapú megközelítés támogatást nyújthat az MI rendszerek alkalmazása és szervezetbe történő integrálása során.

A nemzetközi szabványok, ajánlások kockázatmenedzsment oldalon még *nem adnak részletes támogatást vagy kontroll javaslatokat*, ezen a területen változások várhatók a jövőben, legalább általános irányelvek szintjén.

Alapvető biztonsági kérdés *a szükséges mértékű emberi felügyelet biztosítása*, ami az autonóm fegyver rendszerek esetében érthető a „veszélyes üzemmód” miatt. Egyszerűbb esetben is szükség van arra a tájékoztatásra, hogy az MI rendszerrel kommunikáló ügyfél probléma esetén hogyan tudja elérni az üzemeltető humán támogatást.

A honvédelmi ágazatnál látható az MI rendszerek, szolgáltatások sokrétű felhasználási lehetősége. Ez megalapozza azt a következtetést, hogy nem az „MI rendszer” szolgáltatását hanem *MI rendszerek nagyszámú üzemeltetését és MI rendszer szolgáltatások elérését célszerű alapul venni a technikai sokszínűség és az eltérő eljárások sokaságának tudomásul vételével együtt*.

A fentiek alapján megállapítható, hogy az MI rendszerekre vonatkozó szabályozás, ajánlások és egyéb, az alkalmazáshoz szükséges támogatások kialakulása megkezdődött.

A honvédelmi ágazatnál az MI rendszerek biztonságával kapcsolatos kérdéskör feltűnése nem csak a horizonton várható, hanem *napi aktualitású kérdés*.[16]

A meglévő szabályozók (pl. védelmi rendszabályok, eljárások) pontosítása minden érintett szereplőnek alapvető feladata, melyet követni fog a *jogszabályok változásából adódó második hullám*, illetve a várhatóan megjelenő *szabványok, ajánlások áradata*.

Felhasznált irodalom

BM. (2015). 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre (...) vonatkozó követelményekről.

[16] Az adott MI rendszer típusától függően más kérdések is fontosnak tekintendők, mint az átláthatóság, rendelkezésre állás vagy az adatvédelem, mely kérdések összefonódhatnak és akár új szakterületi kapcsolódási pontok kialakítását is igényelhetik.

BM. (2024). Biztonsági osztályba sorolás és alkalmazandó védelmi intézkedések. Letöltés dátuma: 2024. 04 25, forrás: https://kormany.hu/dokumentumtar/biztonsagi-osztalyba-sorolas-es-alkalmazando-vedelmi-intezkedesek-min-rendelet

Copp, T. (2024). An AI-powered fighter jet took the Air Force's leader for a historic ride. What that means for war, May 3, 2024. Retrieved 05 05, 2024, from https://www.latimes.com/world-nation/story/2024-05-03/an-ai-powered-fighter-jet-took-the-air-forces-leader-for-a-historic-ride-what-that-means

Csáki, C. (2023). A mesterséges intelligencia elterjedéséből adódó kockázatok szisztematikus vizsgálata (fejezet), p. 27 – 50. *A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata, KNBSZ 2023, Budapest, ISBN 978-615-612 és és ISBN 978-615-6128-18-8 [PDF]*.

Edwards, B. (2024). Microsoft launches AI chatbot for spies, 5/7/2024. Letöltés dátuma: 2024. 05 10, forrás: https://arstechnica.com/information-technology/2024/05/microsoft-launches-ai-chatbot-for-spies/

ENISA. (2020). Artificial Intelligence Cybersecurity Challenges, ENISA, 2020. 12. 15. Retrieved 04 27, 2024, from https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

EU. (2018). Az Európai Parlament 2018. szeptember 12-i állásfoglalása az autonóm fegyverrendszerekről (2018/2752(RSP)), P8_TA(2018)0341.

EU. (2023). 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.

EU. (2024). REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives. Retrieved 05 29, 2024, from

https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf

Maggie Gray - Amy Ertan. (2021). Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment, NATO CCD COE. Retrieved 04 20, 2024, from https://ccdcoe.org/library/publications/artificial-intelligence-and-autonomy-in-the-military-an-overview-of-nato-member-states-strategies-and-deployment/

MSZ. (2018). 31000: 2018, Kockázatmenedzsment, irányelvek.

MSZ. (2023). MSZ/ISO/IEC 27001:2023, Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek. Követelmények.

NATO. (2023). The NCI Agency's new data science and AI tool receives security accreditation, 12 8 2023. Retrieved 04 26, 2024, from https://www.ncia.nato.int/about-us/newsroom/the-nci-agencys-new-data-science-and-ai-tool-receives-security-accreditation.html

Parlament. (2013). 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

SDI. (2024). THE MOST USEFUL MILITARY APPLICATIONS OF AI IN 2024 AND BEYOND, MARCH 15, 2024. Retrieved 04 20, 2024, from 2024, https://sdi.ai/blog/the-most-useful-military-applications-of-ai/

US. (2020). Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 R5, September, 2020. doi:https://doi.org/10.6028/NIST.SP.800-53r5

US. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, January 2023. Letöltés dátuma: 2024. 04 26, forrás: https://doi.org/10.6028/NIST.AI.100-1

US. (2023a). DoD Announces Update to DoD Directive 3000.09, 'Autonomy In Weapon Systems' Jan. 25, 2023. Retrieved 04 26, 2024, from https://www.defense.gov/News/Releases/Release/Article/3278076/dod-announces-update-to-dod-directive-300009-autonomy-in-weapon-systems/

US. (2024). Secure Artificial Intelligence Act of 2024. Retrieved from BAG24561 (senate.gov)

Az MI kiberbiztonsággal kapcsolatos fontosabb kérdéseinek vizsgálata

(Lehet a megfoghatatlant megközelíteni és a biztonságáról beszélni?) ☺

Nemzetközi Katonai Információbiztonsági Konferencia

Budapest, 2024. 05. 09.

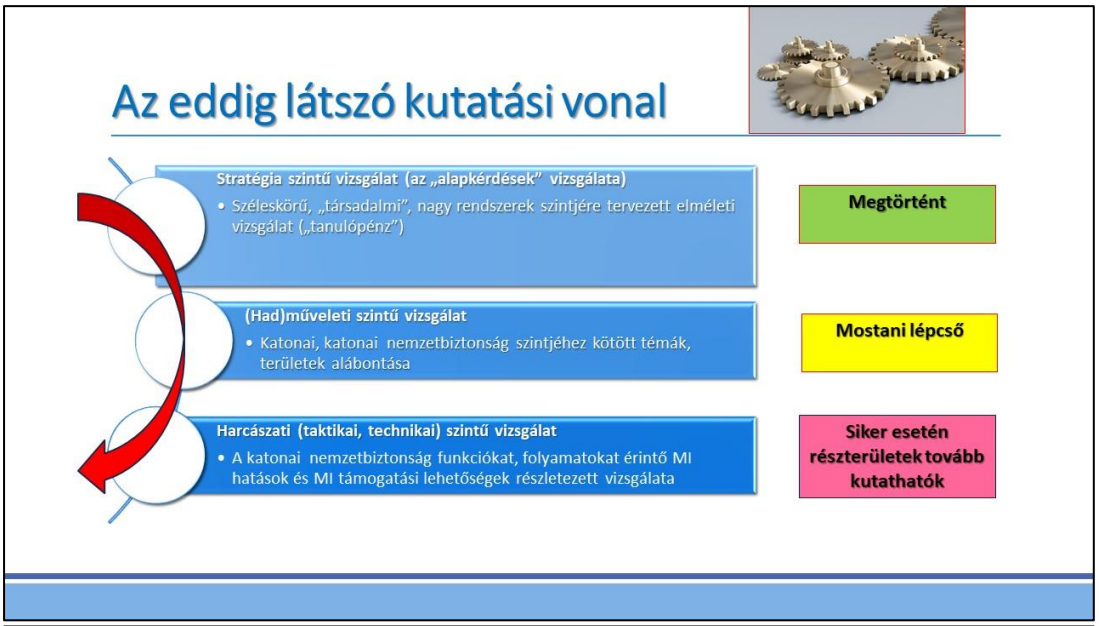
Dr. Kassai Károly

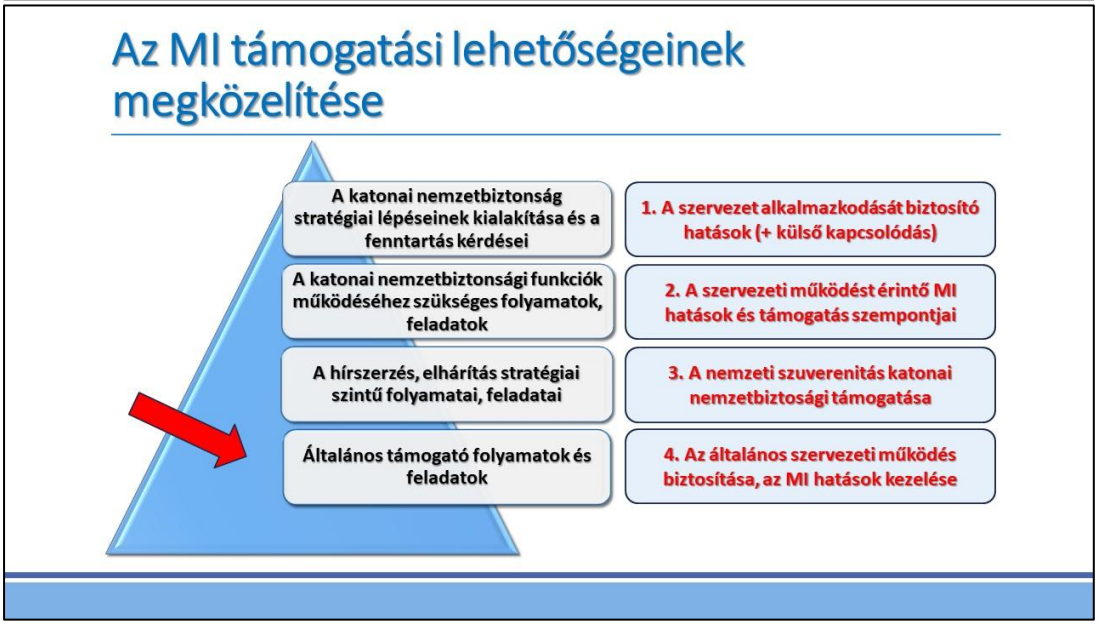
Tartalom

Kell-e 2026(?)-tól MI IBSZ-t írni Magyarországon? ☺

- Kutatási előzmények és háttér
- Erőteljes lehatárolás
- Kockázatalapú megközelítés
- Eddigi tapasztalatok

- Az előadás a KNBSZ ***mesterséges intelligencia (MI) hatásainak specifikus vizsgálata*** (2024-2025) kutatási terv,
- Páll-Orosz Piroska, Kassai Károly: ***Az elektronikus információs rendszerek, szolgáltatások szervezeti szintű, kiberbiztonsági szempontú felkészítési feladatainak körvonalazása az MI hatások hatékony kezelése érdekében*** című kutatási programhoz kapcsolódik


Az eddig látszó kutatási vonal
Stratégia szintű vizsgálat (az „alapkérdések" vizsgálata)
• Széleskörű, „társadalmi", nagy rendszerek szintjére tervezett elméleti vizsgálat („tanulópénz")
Megtörtént
(Had)műveleti szintű vizsgálat
• Katonai, katonai nemzetbiztonság szintjéhez kötött témák, területek alábontása
Mostani lépcső
Harcászati (taktikai, technikai) szintű vizsgálat
• A katonai nemzetbiztonság funkciókat, folyamatokat érintő MI hatások és MI támogatási lehetőségek részletezett vizsgálata
Siker esetén részterületek tovább kutathatók


Az MI támogatási lehetőségeinek megközelítése
A katonai nemzetbiztonság stratégiai lépéseinek kialakítása és a fenntartás kérdései
1. A szervezet alkalmazkodását biztosító hatások (+ külső kapcsolódás)
A katonai nemzetbiztonsági funkciók működéséhez szükséges folyamatok, feladatok
2. A szervezeti működést érintő MI hatások és támogatás szempontjai
A hírszerzés, elhárítás stratégiai szintű folyamatai, feladatai
3. A nemzeti szuverenitás katonai nemzetbiztosági támogatása
Általános támogató folyamatok és feladatok
4. Az általános szervezeti működés biztosítása, az MI hatások kezelése

MI = rendszerszerű gondolkodás és nem csak MI (matematikai) modell

- **EU megközelítés**
  - Tanító adatbázis, teszt adatbázis, (adatátvitel), tanuló MI rendszer, üzemeltetett MI rendszer
- **ENISA MI szelektálás**
  - ***MI kiberbiztonság***, MI a kiberbiztonság támogatásában, MI kártékony (ellenséges) használata
  - **Kiemelt katonai szempont: a támadó kiber infrastruktúra védelméről is gondoskodni kell!**
- **Az MI információ rendszer szerinti megközelítése (Csáki)**
  - technológia (szoftver), adatok (történeti, valós – klb. formátumok), folyamatok (fejlesztés, üzemeltetés), ember (szerepkörök szerint)
- **Kiegészítő szervezeti megközelítés**
  - Saját üzemeltetésű MI rendszer
  - MI rendszer szolgáltatásának igénybe vétele

Az MI katonai alkalmazása (top x)

- Katonai rendszerek (platformok)
- Stratégiai döntéshozatal
- Adatfeldolgozás és kutatás
- Harci szimuláció
- Célfelismerés
- Veszélyfigyelés
- Drónrajok
- Kiberbiztonság
- Közlekedés
- Sérültek ellátása és evakuálása

An AI-powered fighter jet took the Air Force's leader for a historic ride. What that means for war
2024. 05. 03.

Kockázat alapú megközelítés

- **EU AI Act**
  - **Tiltott**, **magas kockázatú**, **alacsony vagy minimális** kockázati kategóriájú MI megoldások
  - Emberi felügyelet biztosítása
  - Felügyelő hatóság, nyilvántartás, teszt és vizsgálat, EU adatbázis
- **EP állásfoglalás (MI, robot)**
  - **emberi vezérlésű megoldás** szükséges az autonóm fegyver rendszerek esetében
  - **tesztelés** szükségessége
- **US DoD Directive 3000.09 Autonomy in weapon system, 1. 2. a.**
  - Az autonóm és félig-autonóm fegyver rendszerek: a parancsnokoknak, kezelőknek **megfelelő szintű döntései lehessenek** az alkalmazáskor (use of force)
  - **A kiber képességekre nem vonatkozik a direktíva**
- **ENSZ ösztönzés (2024. 03.)**
  - Felhívás: nemzeti szabályozási és felügyeleti rendszerek kialakítása, **besorolás**, vizsgálat, teszt, **sérülékenység** azonosítás és csökkentés, **tudatosság** erősítés, hatékony védelmi rendszabályok, szellemi termékek védelme…

Az eddig érzékelhető biztonsági követelményekről…

- **Kezdődő szabványosítási lépések láthatók, pontos követelmények nem**
  - Új: ISO MI előszabványok, NIST Risk Management fw,
  - Meglévő: az ISO/MSZ 27001/2/5, ISO/MSZ 31000, US SP 800-53 v.5 MI „hullámai” még nem érzékelhetők
- **A meglévő szabályozási eszközökön keresztül kell az MI üzemeltetést és biztonságot szabályozni**
  - Meglévő EU követelmények: NIS 2 irányelv, CER irányelv, DORA irányelv
  - Meglévő nemzeti követelmények: Ibtv, Kibertan.tv, Lrtv. és a végrehajtási rendeletek
    - **Ezeken a szabályozási területeken a nagy kockázatú MI esetek okozhatnak változásokat**

Biztonsági megközelítés

- Intézményi megoldás (US Secure Artificial Intelligence Act of 2024)
  - MI Biztonsági Központ (sérülékenység kutatás), MI biztonsági esemény adatbázis („majdnem" ügyek is)
  - MI RED team irányelv fejlesztés
  - MI biztonsági események fejlesztési fázisban történő jelentése
- **Az EU AI Act követelményei közvetlenül fognak érvényesülni hazánkban (rendelet)**
  - A szabályok, intézmények kijelölése történhet **már meglévő jogszabályban**
  - Vagy dedikált **új jogszabály** jelenik meg?

Összegzés

- **Az MI rendszer megjelenése** – hasonlóan a kialakulóban lévő kiberbiztonsági szabályozással – **NEM jelent felmentést** a korábbi kötelezettségek alól
  - a meglévő nemzetközi jogszabályok, egyezmények alkalmazandók!
- Az MI rendszerek **funkcionalitás szerint besorolandók**, ami rendszabályok, követelmények kialakítását támogatja
  - **Életciklus szemlélet**
  - **Kockázat alapú megközelítés szükségessége**
- **Az emberi felügyelet** jelenleg kulcsfontosságú kérdésként kezelendő
  - Különös figyelem az autonóm és félautonóm fegyver rendszerekre
  - **Az MI ügyfelének lehetőséget kell adni, hogy a „mögöttes" humán támogatással kapcsolatba léphessen**
- **Kezdeti szabványok, ajánlások megjelenése** már azonosítható
  - **Az MI részletes biztonsági szabályozás támogatás később várható, most feladat a meglévő rendszabályok alkalmazhatóvá tétele**

Köszönöm a figyelmet!

A részletek zöme még a felszín alatt! ☺

Legyenek az MI rendszerek biztonságban!

Források

- A mesterséges intelligenciára és a robotikára vonatkozó átfogó európai iparpolitika Az Európai Parlament 2019. február 12-i állásfoglalása a mesterséges intelligenciára és a robotikára vonatkozó átfogó európai iparpolitikáról (2018/2088(INI))
- An AI-powered fighter jet took the Air Force's leader for a historic ride. What that means for war, https://www.latimes.com/world-nation/story/2024-05-03/an-ai-powered-fighter-jet-took-the-air-forces-leader-for-a-historic-ride-what-that-means-for-war
- Artificial Intelligence Cybersecurity Challenges, ENISA, 2020. 12. 15, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
- Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, January 2023, https://doi.org/10.6028/NIST.AI.100-1
- Csáki Csaba: A mesterséges intelligencia elterjedéséből adódó kockázatok szisztematikus vizsgálata (fejezet), p. 27 – 50. In: A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata, KNBSZ 2023, Budapest, ISBN 978-615-6128-16-4 és ISBN 978-615-6128-18-8 [PDF], p. 37.

Források 2

- DoD Announces Update to DoD Directive 3000.09, 'Autonomy In Weapon Systems' Jan. 25, 2023, https://www.defense.gov/News/Releases/Release/Article/3278076/dod-announces-update-to-dod-directive-300009-autonomy-in-weapon-systems/
- DoD Directive 3000.09 Autonomy in weapon system
- Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, United Nations A/78/L.49, 11 March 2024
- THE MOST USEFUL MILITARY APPLICATIONS OF AI IN 2024 AND BEYOND; https://sdi.ai/blog/the-most-useful-military-applications-of-ai/
- Top 8 Applications of Artificial Intelligence in Military in 2023; https://aihints.com/artificial-intelligence-in-military-ai-applications-in-military/
- Secure Artificial Intelligence Act of 2024; BAG24561 (senate.gov)
- Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 R5, https://doi.org/10.6028/NIST.SP.800-53r5

Sandor Magyar[1]: The role of security operation centres in the age of artificial intelligence

Correferatum

The rapid development of digitalisation is challenging not only individuals but also organisations. For an organisation to survive or perform its tasks, it needs significant IT support. As more and more systems support everyday work and information technology develops, the focus on information security and cyber security is increasing.

Emerging disruptive technologies - such as artificial intelligence, quantum computing, autonomous devices - are radically transforming our lives. The value generated by information technology will also have a growing impact on the revenues of organisations and even on the economies of countries.

The business continuity of organisations, their data assets and their reputation now depend on the IT domain. Prevention is a very important element of cybersecurity, but the detection and response capabilities provided by SOC must also be ensured at a high level. Without a SOC, organisations are at significant risk, partly due to

[1] ORCID: 0000-0002-6085-0598

the fact that preventive measures may not be sufficient, especially in the area of zero-day vulnerability exploitation.

The SOC is a centralised cyber organisational element responsible for detecting and responding to cyber threats in real time to prevent and manage incidents. With continuous monitoring of log data from IT networks and systems, attack detection is now an essential security function for organisations. The SOC works with information from three sources, which are log data, network traffic, endpoint protection (AV[2], EPP[3], EDR[4]). The SOC naturally identifies the characteristics of attacks by analysing their characteristics, i.e. when, how and why the attack was successful.

Security operations centres play a crucial role. They are indispensable for the protection of data assets and the availability of electronic information systems.

The triad of people, processes and technology is very closely interlinked in the case of security operations centres. If we do not have all three of these, we will not have adequate security against threats from cyberspace.

The development of SOC is essential, but achieving this capability cannot be achieved in a very short time. Strategic planning from the

[2] AV antivirus
[3] EPP Endpoint Protection Platforms
[4] EPP Endpoint Protection Platforms

organisational side has a very important role to play, which is linked to the risk appetite of the management. Until full SOC capability is achieved, the risks taken by senior executives are at a much higher level.

Emerging and disruptive technologies are not only the challenges of the future, but also of the present. These technologies can enrich the toolbox of both the offensive and defensive sides, and therefore a great deal of energy must be invested in research and development that can counter the lag in the field and identify future risks to which defence mechanisms must be tuned.


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
THE ROLE OF SECURITY OPERATION CENTRES IN THE AGE OF ARTIFICIAL INTELLIGENCE
Sándor MAGYAR
associate professor


Agenda
• Changing environment
• Challenging services
• Design of SOC
• Important areas os SOC
• Conclusion

Changing environment

- Increasing number of electronic information systems.
- Unavoidable smart systems.
- With all this comes a rising number of users, hardware and software, and therefore risks.
- The complexity of handling the rise of digitalisation from the point of view of cyber security is increasing.
- Identifying and managing threats from cyberspace.
- The growth of cyberspace operations against critical infrastructures.
- Emerging and disruptive technologies.

Source: Microsoft Copilot
https://copilot.microsoft.com/

Why do you need a SOC?

- It is no longer a question of whether organisations and individuals will suffer cyber attacks in the future, but rather the value of the damage.
- The most effective way to protect against cyber-attacks is proactive protection.
- Many forms of protection are possible, but the SOC and the people working in it are the last line of defence.

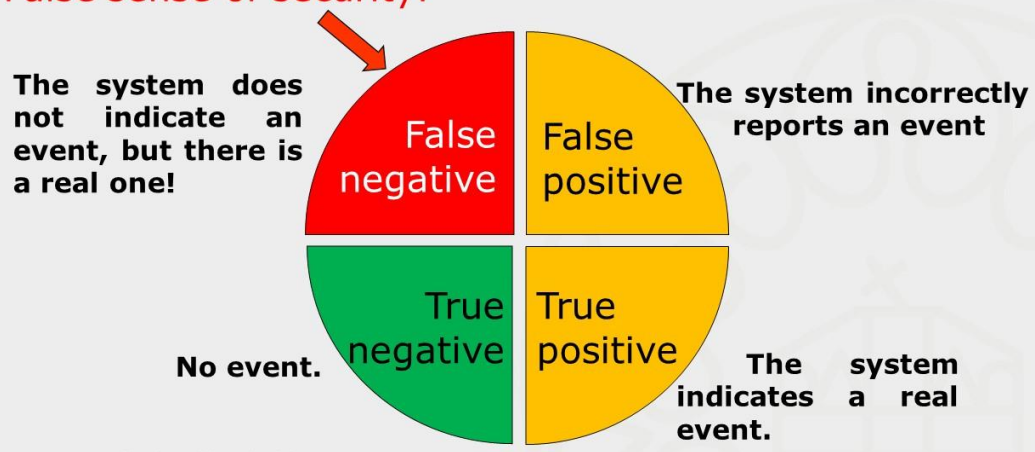
Source: Microsoft Copilot
https://copilot.microsoft.com/

Challenging services

- Cybercrime-as-a-Service (CaaS)
- Malware-as-a-Service (MaaS)
- Disinformation-as-a-Service (DaaS)

Without SOC!
False sense of security!

CATEGORIES OF FAULTS

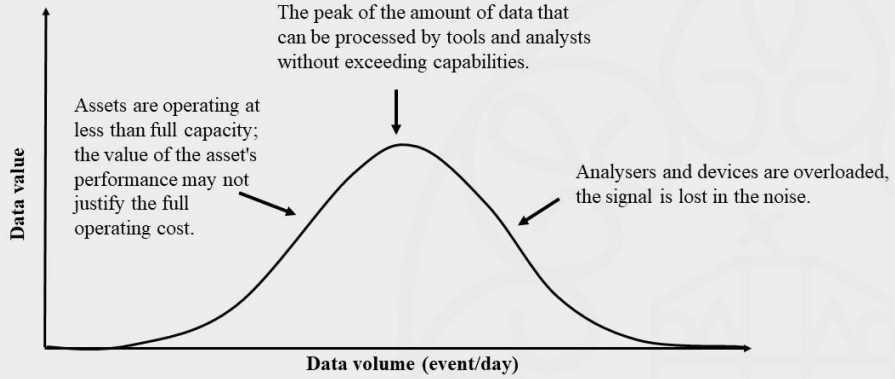


Forrás: saját szerkesztés

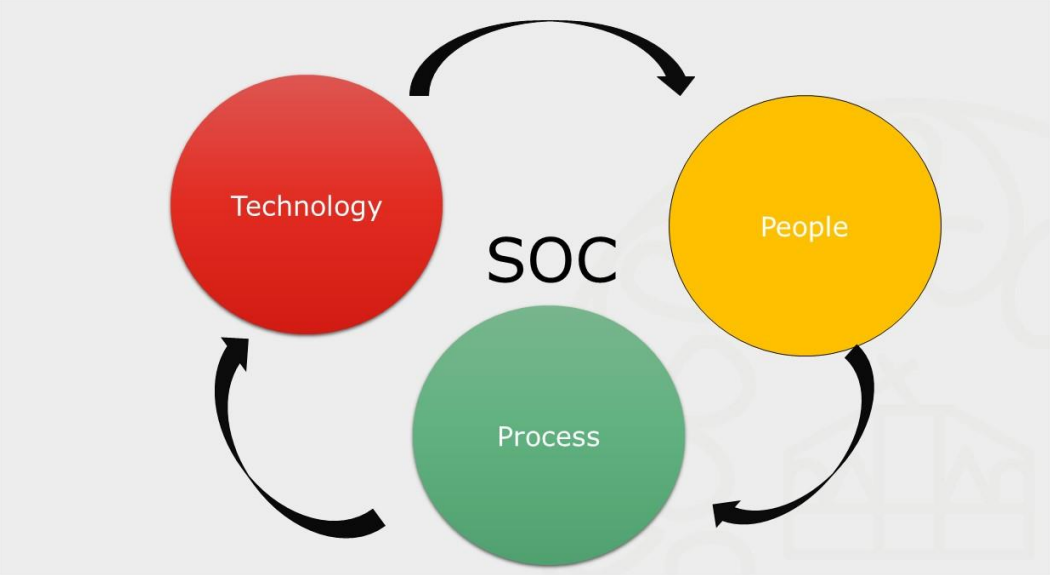
Design of SOC

- The SOC capability can be achieved by:
  - Using Security Operations Centres as a Service (SOC as a Service).
  - To deploy a Security Operations Centre.
  - Develop a hybrid SOC by combining the above two solutions.

The balance between data volume and data value



ZIMMERMAN, Carson. Ten Strategies of a World-ClassCybersecurity Operations Center. mitre. org. 2014. p.: 38



The contribution of AI to skills

- Processing large amounts of information.
- Reducing false positive alarms.
- Facilitate the work of analysts.
- More efficient attribution.
- Reducing response times.
- More efficient software testing.
- Improved anomaly detection.

Conclusion

- Without SOC, organisations are exposed to significant risk, partly because preventive measures may not be sufficient, especially in the area of exploiting zero-day vulnerabilities.
- A SOC is not just a technical toolkit, or a set of trained professionals, or processes, but a complex system of these that deliberately complement each other.
- Building an effective SOC capability can be developed in a phased approach with the right timing and strategy.
- The " developments " are continuous on the offensive side, generating competitive pressure on the defensive side.
- AI requires new competencies from employees.

References

- Schinagl, S, Schoon, KC & Paans, R 2015, A Framework for designing a Security Operations Centre (SOC). in Secure Cyberspace in 21st Century. Proceedings of the Hawaii International Conference on System Sciences (HICSS). Institute of Electrical and Electronics Engineers (IEEE), Hawai, Hawaii International Conference on System Sciences (HICSS), 8/01/15., 2015., http://www.computer.org/csdl/proceedings/hicss/2015/7367/00/7367c253.pdf. letöltés: 2023.10.20.
- A SANS 2021 Survey: Security Operations Center (SOC), https://www.sans.org/white-papers/sans-2021-survey-security-operations-center-soc/, letöltés: 2023.10.20.
- Security Operations Maturity Model LogRhythm's guide to assessing and improving the maturity of your security operations, https://logrhythm.com/solutions/security-operations-maturity-model/, letöltés: 2023.10.20.
- Scheidler Balázs, A SOC alapja a logelemzés múlt és jövő, EIVOK-36 SOC-ok aktuális kérdései Tudományos – Szakmai Konferencia, 2023., konferencia előadás., https://www.hte.hu/documents/10180/4864448/Scheidler+Bal%C3%A1zs_EIVOK-36.pdf, letöltés: 2023.10.20
- Hámornik, Balázs Péter, and Csaba Krasznay. 2017. "Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics." ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE 16 (3): 73–92. doi:10.32565/aarms.2017.3.5.
- M. Saraiva and N. Coelho, "CyberSoc Implementation Plan,"2022 10th International Symposium onDigital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
Thank you for your attention!

Imre Dobák[1]: The potential use of crowdsourcing in times of conflict

Correferatum

The phenomenon of crowdsourcing is increasingly emerging in the international scientific literature, both in the context of cyberspace-related information and communication environments and in addressing security threats and challenges. For many people, crowdsourcing is a little-known method, but it is also an invisible part of our daily lives. Originally linked to business thinking, the idea of collaborative, distributed use of resources (or even outsourcing certain workflows) has quickly emerged in the security field.

One of the key elements of the method is the use of external resources (basically human resources) to achieve a given goal, which can be directed towards gathering information from participants or even using the expertise of these participants. To understand the essence of the crowdsourcing method, simply think of a security event (e.g. an earthquake) where people in the area have accurate and up-to-date partial information about the event, which, when aggregated, can provide a more accurate overview of the security event and can also help to manage it effectively. Yet it is perhaps most widely encountered in commonly used route planning solutions, where users can formulate their opinion of a

[1] ORCID: 0000-0002-9632-2914

given traffic situation by sharing their information (e.g. traffic jam indication).

Regarding the security-related uses of the method, several main types can be identified based on international examples and literature.

1. The area of cybersecurity: think of the big bounty projects, not unknown in software development and testing, where vulnerability testing is done by using the open environment instead of internal staff. This allows a much larger human resource to be involved, often with financial rewards offered by the companies involved as a motivating factor.

2. Cybersecurity and awareness: members of society who are directly exposed to vulnerabilities can use their information to raise awareness and security-conscious attitudes by sharing their information on a community/crowdsourcing platform, which can result in a common knowledge base.

3. Security incident-related information gathering: in a targeted application of the method, the users of the method (e.g. authorities) request information from those who are in the geographical area and have accurate information about the security incident. Examples often include crowdsourcing

solutions for managing forest fires, floods, and natural and man-made disasters. They also include the targeted, organized collection of digital evidence related to security incidents, which can increase the amount of information by broadening the scope of participants and can also contribute to increasing the accuracy of information. The organized, centralized approach, over and above the sharing of information on social platforms - whether contradictory or creating misunderstandings and panic - can help to effectively manage a critical situation. If we look at practical examples of international security issues, we can see examples of widespread use of this method, whether in the context of chatbot applications created by Ukrainian agencies during the Russian-Ukrainian war to help signal military activities, or in the documentation of war damage.

4. Involving human resources for "expert" purposes: in some cases, crowdsourcing actors may not have sufficient human resources/expertise to investigate a given topic, so civil society actors with appropriate skills may be involved on a voluntary basis in the implementation of a crowdsourcing task. A well-known example in the security context is the missing Malaysia Airlines flight MH370 from Kuala Lumpur to Beijing (2014), where millions of people volunteered to join a crowdsourcing platform (Tomnod) created for this purpose to

help with a fast review of satellite imagery covering an area of more than 1 million square kilometers.

5. A little-known, progressive direction to be explored is the applicability of the method for forecasting purposes. Based on the literature, their main aim is to explore the possibility of predicting future events related to security and national security, based on the collective wisdom of the participants.

However, in addition to the many advantages of crowdsourcing (efficient use of human resources, possibility to reduce response times, possibility to obtain relevant information, and last but not least, cost reduction), several limitations of the method must be taken into account. The method is essentially based on the voluntary nature of the participants, so willingness to participate and motivation are important. A further key aspect is that, unlike information shared on social media platforms, the security of participants and the protection of their data must be guaranteed, regardless of the form of the platforms, and efforts must be made to minimize distortions and increase the credibility of the data.

Looking to the future, we can expect crowdsourcing to become even more important through social networking platforms and other info-communication tools that involve a wide range of participants, and to open up new applications and directions for their use in the security of society. The phenomenon of crowdsourcing is increasingly encountered in the international academic literature,

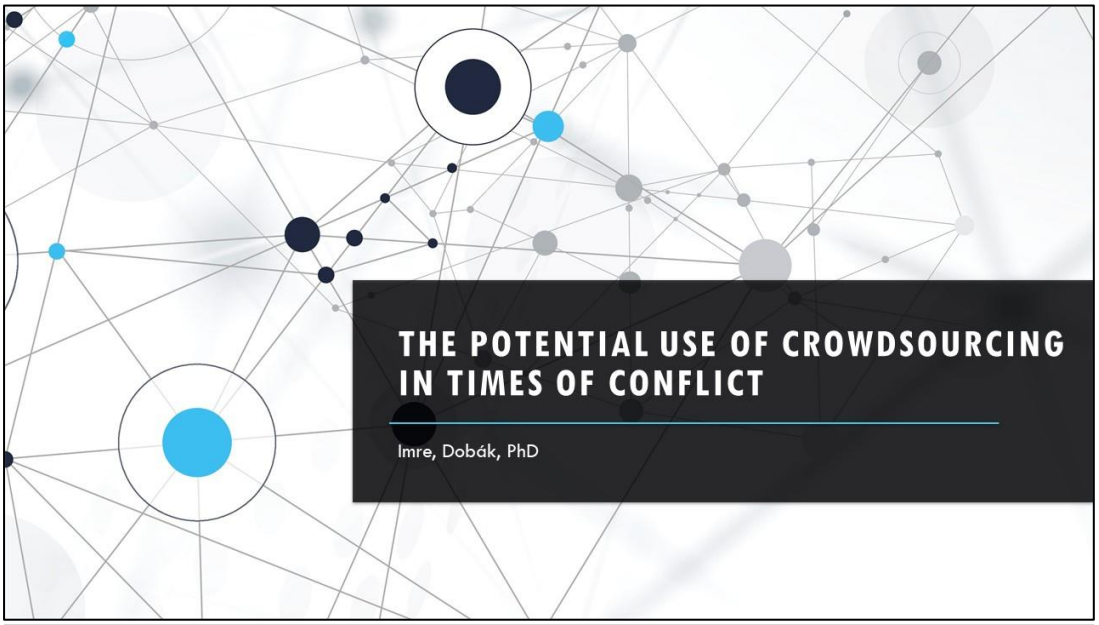
both in the context of cyberspace-related info-communications environments and in addressing security threats and challenges. For many people, crowdsourcing is a little-known method, but it is also an invisible part of our daily lives. Originally linked to business thinking, the idea of collaborative, distributed use of resources (or even outsourcing certain workflows) has quickly emerged in the security domain.

Sources:

- Xia, H., McKernan, B. Privacy in Crowdsourcing: a Review of the Threats and Challenges. Comput Supported Coop Work 29, 263–301 (2020). https://doi.org/10.1007/s10606-020-09374-0
- Annalisa Merelli: Using crowdsourcing to search for flight MH 370 has both pluses and minuses, March 15, 2014. https://qz.com/188270/using-crowdsourcing-to-search-for-flight-mh-370-has-both-pluses-and-minuses
- Dobák Imre – Kenedli Tamás: Információszerzési tendenciák és kihívások a kibertérben rejlő lehetőségek és a mesterséges intelligencia viszonylatában, Military and Intelligence Cybersecurity Research Paper, 2023/3. 2-41. https://shorturl.at/lrzAK
- Kiran Sridhar, Ming Ng, Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties, Journal of Cybersecurity, Volume 7, Issue 1,

2021, tyab007, https://doi.org/10.1093/cybsec/tyab007

- Esberg, Jane, and Christoph Mikulaschek. "Digital Technologies, Peace and Security: Challenges and Opportunities for United Nations Peace Operations."United Nations Peacekeeping 7 (2021).
- Paul Burke: The issues in the collection, verification and actionability of citizen-derived and crowdsourced intelligence during the Russian invasion ofUkraine, 2022, СТРАТЕГІЧНА ПАНОРАМА СПЕЦІАЛЬНИЙ ВИПУСК 2022 https://doi.org/10.53679/2616-9460.specialissue.2022.09.



WHAT IS THE CROWDSOURCING?

- Collaborative, distributed "work„
- Distributed outsourcing of partial work processes
- Leveraging the knowledge and expertise
- Those who want and can participate in the process based on their skills, expertise and opportunities (in a given situation, field).


WHAT IS THE „CROWDSOURCING"?


TYPES (ADVANTAGE - DISADVANTAGE)


ITS RELATIONSHIP WITH THE SECURITY ENVIRONMENT


EXAMPLES

THEORETICAL APPROACH

- It is not a new phenomenon
- The issue has been researched in the literature for more than 15 years (Jeff Howe 2006)
- Widely used in economic and business fields
- Its spread was accelerated by cyberspace
- In the field of security, even national security, its visibility has recently increased

AS A SECURITY TOOL? /1

Cybersecurity

Bug bounty programs

Software companies

AS A SECURITY TOOL? /2

Security

Security incidents sharing

AS A SECURITY TOOL? /3

Security

Crowdsourced traffic data

AS A SECURITY TOOL? /4

Security

Security awareness campaign

AS A SECURITY TOOL? /5

Security

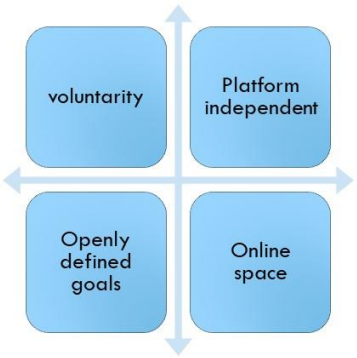
Collective intelligence

KEY ELEMENTS (1) - WHERE?

- Humanitarian crisis, Floods, Forest fires,
- Crisis management - Coordination,
- Supporting the work of law enforcement authorities and government bodies,
- Transfer of digital evidence etc.

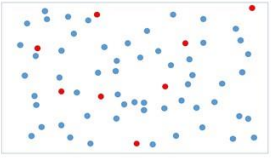
KEY ELEMENTS (2) - WHO?

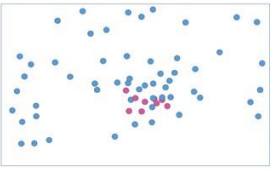
- Those human sources who can make a meaningful contribution to the result
- Volunteering
- Not platform-dependent
- Those who want and can participate in the process based on their skills, expertise and opportunities (in a given situation, field).



SUPPORT SECURITY

- Support for the work of government bodies
- Boston Marathon 2013 - a turning point
- Groups on Reddit and 4Chan join the search
- Cyber-vigilante communities have emerged in the online space
- Question of responsibility (disappears at „crowd")
- Main types…
- Basically two main directions (expert and information gathering)





RUSSIAN-UKRAINIAN WAR - CROWDSOURCING

- Ukrainian Security Service on STOP Russian War chatbot
- Ukrainian Police Narodnii mesnik / Avanger (Avenger) Bot)
- Ukraine, Ministry of Digital Transformation eVorogot (e-enemy) chatbot
  See: Diia digital e-administration

12

EXAMPLE FOR EXPERTISE

- An example for processing of already existing information:
  - Malaysia Airlines flight MH370 from Kuala Lumpur to Beijing, which disappeared in 2014.
  - Millions of people joined the created platform (Tomnod) to review more than 1 million square kilometers
  - Voluntary contribution
  - Activity of a broad crowd of high-resolution satellite

13

ADVANTAGES VS. DISADVANTAGES

Advantages

- Reducing Reaction Time,
- Enhancing Information Accuracy,
- Economic, Social and Human Benefits,
- Manpower, expertise and innovation,
- Cost savings.

Collective
- Knowledge and expertise of the crowd

Scale
- Large number of contributors help the identification

Time
- Continuous / monitoring

14

ADVANTAGES VS. DISADVANTAGES

Disadvantages

Work discreetly on of the security of the participants' personal data (anonymity for the external observer)

Sensitive boundaries: e.g. protecting people's privacy (see. social willingness to use Covid online application)

Accuracy and authenticity (the possibility of deliberate deception or innocent error) - the effects of these can even be neutralised by other data

The necessary limit to the activity of the "crowd".

15

CONCLUSION

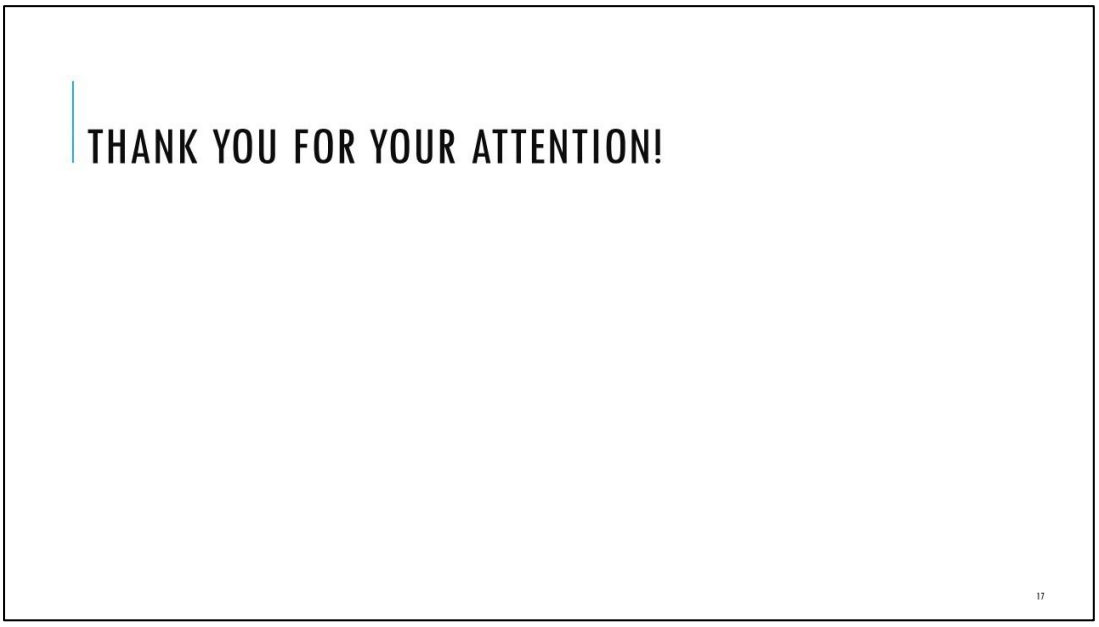
Could be significant even with the rise of "AI„ (?)

Technology and human resources relations

Development of skills

Specific aspects

1. Target group definition
2. Centralisation
3. Voluntarity of joining (e.g. collecting evidence.)
4. Credibility
5. Motivation
6. Cyberspace - online indispensability
7. Security of participants (anonymity)
8. Minimising distortions


THANK YOU FOR YOUR ATTENTION!
17

András Tóth[1]: The impact of advanced ICT solutions on command and control systems, from an information security perspective

Correferatum

Introduction

Recent military operations have highlighted the significant impact of advanced intelligence, surveillance, and reconnaissance (ISR) systems and information communication technologies (ICT) on command and control systems. Military leaders are committed to gathering as much relevant information as possible during operations. However, new technologies are required to outpace the enemy more than traditional methods. The attainment of information superiority is paramount in information operations and is fundamental to the success of military endeavors.

Military information communication technologies and their main components

Advanced technologies that can analyze the surrounding environment in real-time and rapidly share information are pivotal for acquiring pertinent data. In the context of military operations, the main components of military information communication

[1] ORCID: 0000-0001-6098-3262

technologies play a pivotal role in ensuring the efficient exchange of crucial information and intelligence. The following military information communication technologies and their main components are essential for this purpose.

Network infrastructure

- Sensor networks
- Wired networks
- Wireless networks
- Secure communications
- Space-based systems

Information sharing

- Intelligence, Surveillance and Reconnaissance (ISR)
- Data management
- Real-time data
- Need-to-Know principle
- Information flow control

Command and control systems

- Command centres

- Communication networks
- Data fusion and analysis tools
- Decision support software

Key components

- Cybersecurity
- Electronic warfare
- Interoperability
- Situational awareness
- Artificial Intelligence (AI) and Machine Learning
- Umanned systems
- Redundancy and resilience
- Encryption

They are indispensable for facilitating seamless and effective information flow across diverse military operations.

Transformation in command and control systems

The advancement of contemporary technologies in warfare necessitates a transition of command and control systems from network-centric to data-centric warfare. The transition is also

significantly better suited for handling multi-domain operations effectively and efficiently. To optimize command posts, it is imperative to diminish reliance on physical assets and amplify data utilization. This entails prioritizing information acquisition, analysis, and utilization to drive decision-making and enhance operational efficacy. Furthermore, maximizing engagement with commanders is fundamental to effective command posts, facilitating seamless communication, collaboration, and strategic alignment. By emphasizing these facets, command posts can bolster their capacity to adapt, respond, and make well-informed decisions within dynamic and intricate operational terrains.

Information security perspectives

In this transformation, information security assumes paramount significance. The safeguarding of sensitive data and the mitigation of cyber threats are imperative for the maintenance of operational integrity. Implementing robust security measures is essential to uphold the confidentiality and security of information, thereby fortifying the effectiveness of command posts in accomplishing their objectives. Moreover, consistently updating security protocols and comprehensive risk assessment procedures are pivotal in enabling command posts to navigate potential threats proactively. Investing in continual training and education for personnel in cybersecurity best practices serves to fortify command posts against the evolving landscape of cyber risks, enhancing their resilience.

Conclusion

Advanced Intelligence, Surveillance, and Reconnaissance (ISR) systems, alongside Information and Communication Technology (ICT), are pivotal in military operations, providing a framework for efficient information exchange and intelligence gathering. These cutting-edge technologies ensure seamless information flow across operations and also aid in transitioning command and control systems from a network-centric approach to data-centric warfare. Moreover, they emphasize prioritizing information acquisition, analysis, and utilization. Equally critical is establishing robust information security measures to safeguard the confidentiality and integrity of sensitive data and effectively mitigate cyber threats.

Acknowledgment

Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development, and Innovation Fund, financed under the TKP2021-NVA funding scheme, financed under the TKP2021-NVA funding scheme.

References

Beagle, M.; Slider, J. C.; Arrol, M. R. (2023): The Graveyard of Command Posts. In: Military Review, source: https://www.armyupress.army.mil/Journals/Military-

Review/English-Edition-Archives/May-June-2023/Graveyard-of-Command-Posts/

Li, Y.; Liu, Q. (2021): A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. In: Energy Reports, Volume 7, 2021, p. 8176-8186, ISSN 2352-4847, DOI: https://doi.org/10.1016/j.egyr.2021.08.126

Monzon Baeza, V.; Concha Salor, L. (2023): New Horizons in Tactical Communications: An Overview of Emerging Technologies Possibilities. In: TechRxiv, August 29, 2023. DOI: https://doi.org/10.36227/techrxiv.23993016

Toth, A. (2021): Cloud of Things Security Challenges and Solutions. In: 2021 Communication and Information Technologies (KIT), DOI: https://doi.org/10.1109/KIT52904.2021.9583760

Toth, A.; Farkas, T. (2023): Opportunities and Directions for the Evolution of Command and Control Systems in the Context of Multi-domain Operations. In: Vojenské reflexie, XVIII. 3, p. 59 – 73, ISSN: 1336-9202 DOI: https://doi.org/10.52651/vr.a.2023.3.59-73

Tunnicliffe, A. (2019): The next frontier of military communications. In: Army Technology, source: https://www.army-technology.com/features/future-military-communications/

Velastegui, N.; Pavon, E.; Jacome, H.; Torres, F.; Pico, M. (2022): Technological advances in military communications systems and

equipment. In: Minerva, 3(8), p.61-73. DOI: https://doi.org/10.47460/minerva.v3i8.65

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

The impact of advanced ICT solutions on command and control systems, from an information security perspective

Andras TOTH, PhD

International Scientific Conference on Military Information Security

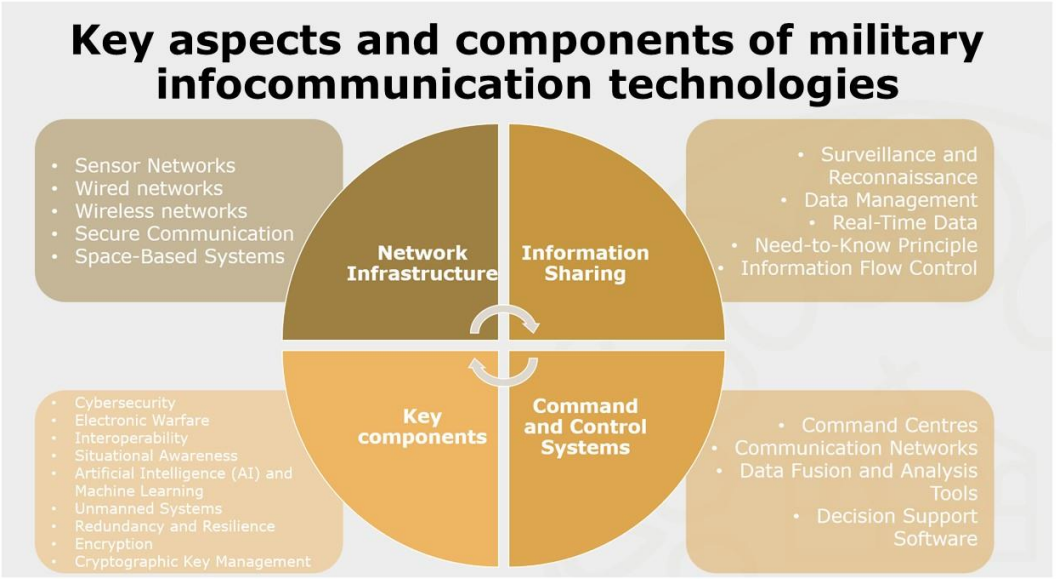
09th May 2024

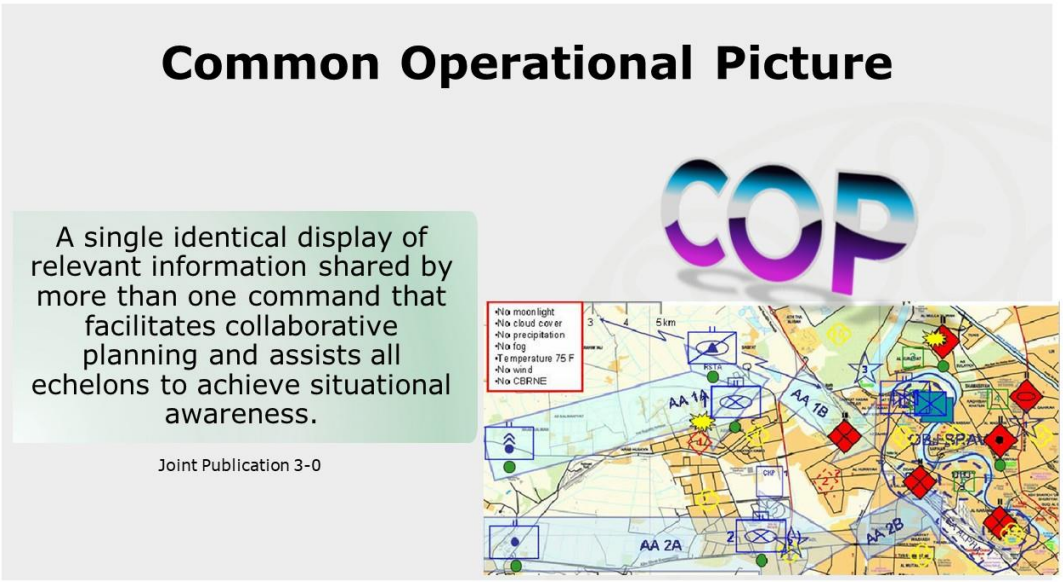
Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development, and Innovation Fund, financed under the TKP2021-NVA funding scheme, financed under the TKP2021-NVA funding scheme.

The concept of information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

Joint Publication 3-13


Key aspects and components of military infocommunication technologies
Sensor Networks
Wired networks
Wireless networks
Secure Communication
Space-Based Systems
Network Infrastructure
Information Sharing
Surveillance and Reconnaissance
Data Management
Real-Time Data
Need-to-Know Principle
Information Flow Control
Cybersecurity
Electronic Warfare
Interoperability
Situational Awareness
Artificial Intelligence (AI) and Machine Learning
Unmanned Systems
Redundancy and Resilience
Encryption
Cryptographic Key Management
Key components
Command and Control Systems
Command Centres
Communication Networks
Data Fusion and Analysis Tools
Decision Support Software

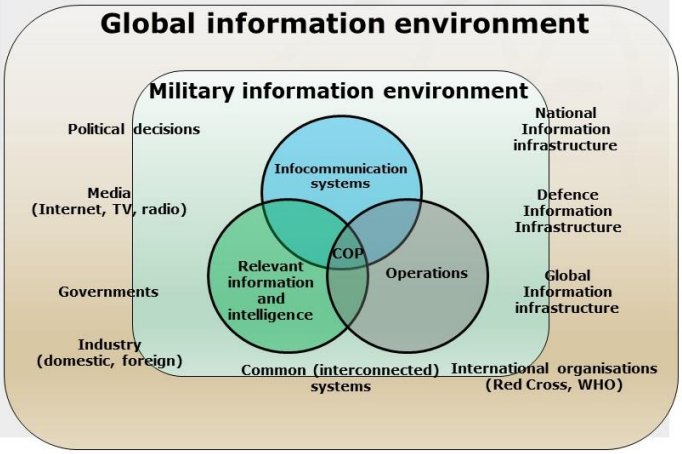

Common Operational Picture
A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness.
Joint Publication 3-0
COP
AA 1A
AA 1B
AA 2A
AA 2B

Common operational picture in information operations

Infocommunication tools are the means that enable commanders and their tribes to...

- Monitor the current situation;
- Integrate and synchronize operations;
- Coordinate multidimensional support;
- Update weapon systems targeting parameters;
- Be able to manage close-in, depth, and rear operations as a single operation.

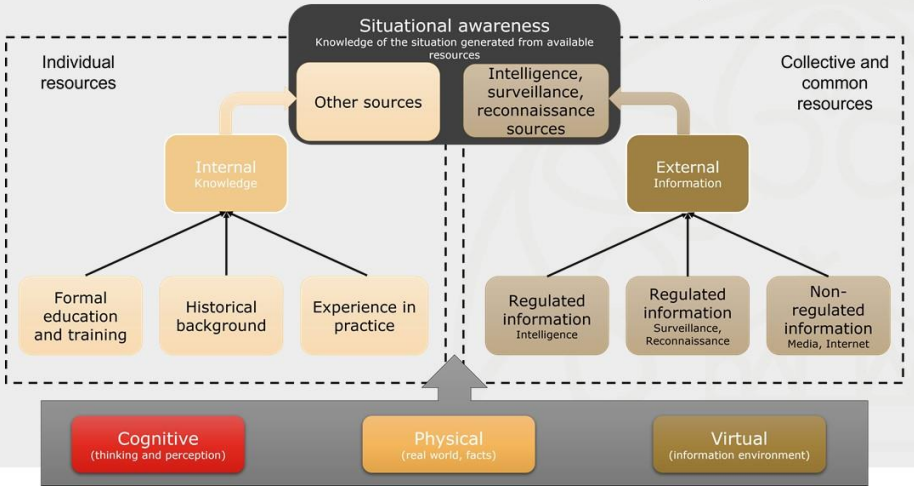
Effective commanders focus on relevant information and intelligence requirements and manage their intelligence cycle based on operational priorities. Advances in technology and open-source intelligence have facilitated this process. Successful integration of information operations requires battlefield intelligence preparation based on adversary capabilities and decision-making processes, focusing on current operations, capabilities, and vulnerabilities.



Situational Awareness

The ability of a person or organization to perceive, understand, and respond effectively to a situation. It involves understanding a circumstance, gathering and analyzing relevant information, and successfully making informed decisions to manage potential risks, threats, or events.

The relationship between situational awareness and information operations



Information Superiority

Information superiority refers to a situation in which, on the one hand, one of the combatants can acquire, process, and make available for decision-making information of significantly higher quality, quantity, and speed than the other in order to ensure the effective conduct of military operations, and, on the other hand, it reflects a situation in which the same party is more effective than the enemy in transmitting information to its own and the enemy's society, international organizations and public opinion, in order to influence their minds in their favor.

To gain and maintain information superiority

There are three equally important aspects of gaining and maintaining traditional information superiority, such as:

01 obtaining information on the factors influencing the commander's decision, which include the situation of the opposing party, the situation of his own forces, and the battlefield environment;

02 exploit and protect their own information capabilities; and

03 blocking the information capabilities of the other party.

Haig Zsolt: Információs műveletek a kibertérben. 2018

Infocommunications systems and information superiority

Command posts

Lt. Gen. Milford "Beags" Beagle, U.S. Army

&

Brig. Gen. Jason C. Slider, U.S. Army

&

Lt. Col. Matthew R. Arrol, U.S. Army

„ our command posts will be places where our leaders go to **die**."

Lt. Gen. Milford "Beags" Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol: *The Graveyard of Command Posts*. Army University Press (2023)

Imbalance between command and control requirements

The current command and control dilemma reflects an imbalance in the functional requirements of the command points to be both **efficient** and **survivable**.

Command posts have evolved over time to provide the best means to control units and sub-units in the chaos of war, to **make good decisions faster than the enemy**, and **to increase effectiveness** by leveraging the experience and leadership of the commander.

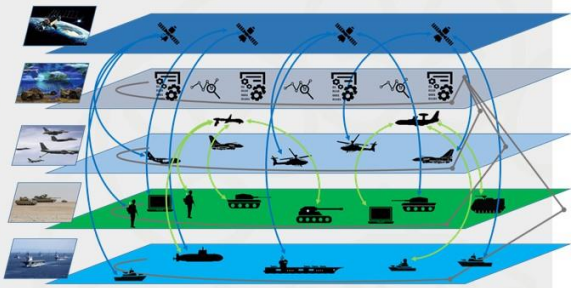
However, the unsatisfactory demand for **decision-support information** to enable **situational awareness** and **command visualisation** has only increased over time, resulting in an imbalance in functional requirements.

Command post in multi-domain operations

Armies need to transform their command and control systems so that the principles of **multi-domain operations** (MDO) are embedded at all levels of warfare.

Headquarters need to become more **flexible**, **mobile** and **resilient**, while not sacrificing effectiveness.

A better approach is needed to facilitate multidimensional command and control, with short-term objectives and an objective end state optimised for large-scale combat operations.



Four requirements for optimising command posts

Recognizing the challenges of the current environment, the MDO stresses that the command posts, as an element of the command and control system, should follow the principles of agility, alignment, resilience, and depth.

Optimizing the command posts requires reducing the reliance on the physical dimension (assets), increasing the use of the information dimension (data), and maximizing the ability to interact with the human dimension (commanders).

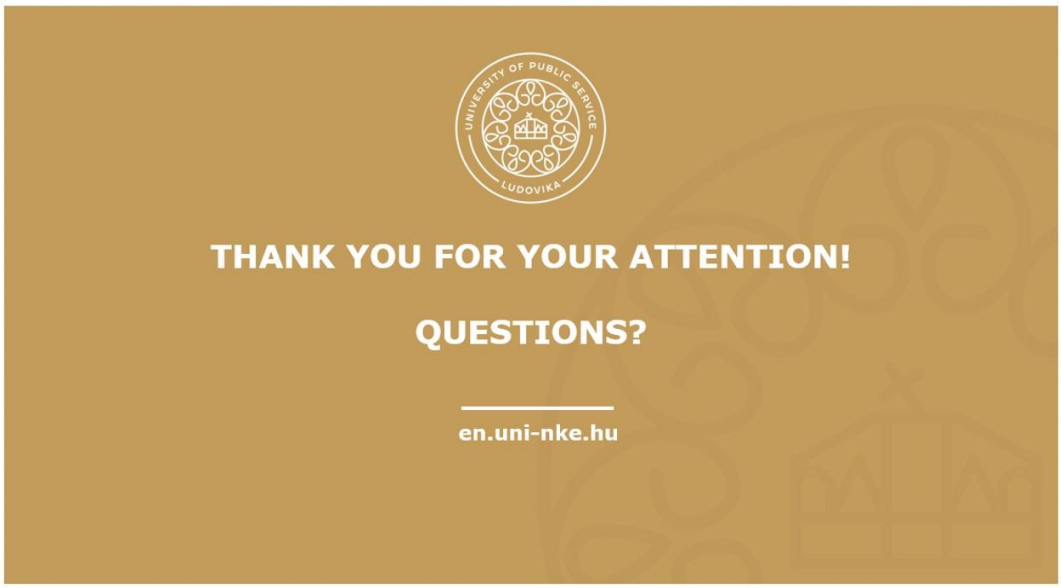
Examining these four principles will help determine what it means to develop an acceptable, reliable, and comprehensive command post that is effective and survivable in high-intensity operations against a powerful adversary.

Solutions

- Data-centric command posts will replace network-centric ones and rely on data development, security, and operations engineers.
- This approach allows commanders to fine-tune their command and control systems based on unique operational requirements and managerial preferences.
- Command posts must eliminate the physical placement of anything they provide "as a service" (aaS) to remain survivable.
- The aaS approach outsources the burden of proprietary maintenance and enables rapid adoption of new technologies and mobility.
- Reliance on the information dimension reduces the need to consolidate staff in one location and increases survivability.

Conclusions


OSINT & SOCMINT are the new RECCE?
Facebook
Telegram
X
Reddit
TikTok
Tinder
Bei Plünderungen gestohlen: Ukrainer tracken Airpods und Smartphones in Belarus – das könnte einen Vorteil im Krieg bringen
Russian troops leave Mariupol and head to other sectors of the front.
1254/
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 kamerájában vette észre, hogy az épület mellett orosz katonák telepítenek rakétákat, és rájött, hogy a házát valószínűleg búvóhelyként akarják használni.
Awareness at all levels, everywhere, for everyone


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA
THANK YOU FOR YOUR ATTENTION!
QUESTIONS?
en.uni-nke.hu

Gábor Knapp: Some vulnerabilities of global positioning systems

Correferatum

In my presentation I would like to introduce some basic thoughts those come up while during and in connection to my PhD research I studied about the vulnerabilities of global positioning system navigation like jamming during the electronic warfare attack.

The actuality of my presentation can we find in almost all military used device or vehicle, whose integrate global positioning systems to conduct and support operations. One-man military personnel, aircrafts, armoured personnel carriers, tanks, operations rooms of headquarters rely and base their decision on the information that can source from global positioning systems.

In the recent days news told about the necessary steps of Finnair, that they had to cancel the only commercial flights between Helsinki and Tartu due to the possible warning of jamming the onboard positioning systems. Such jamming was experienced in the whole Baltic region in the past that affected next to the military use of aircrafts also the civilian ones. However, there was no evidence that who was behind those actions, the civilian authorities decided to ground the planes for a while.

My research covers a bit wider area than the presented one, but common areas are global positioning, the vulnerabilities and the use

of such equipment by military personnel also. I try to focus on those common areas to receive inputs to my research.

As mentioned before independently if they are used by military or civilian due to the fact that the system use common segments vulnerabilities to civil systems are also the same in case of military systems. Therefore, we have to miss the so-called defensive cover or restricted access to military equipment. And also, in the contrary, if the military systems can be attacked, also the civilian ones have to face with the same problem like the Estonian jamming example shows.

While attacking the global positioning systems we have to differentiate among the different segments of global positioning systems, like space segment, control stations and user segmented end devices like global positioning system receivers. Both those segments can be, but in different ways and to different degree affected during the phase of their use. During development, producing and operating phases each has its own vulnerability that could be the target of attackers. Starting from the far side space segment can be influenced either via the malfunction of onboard control devices, or influence the use of the controllers of the correction engines. While we look to the controller segment, master or control stations has devices where the attacker can try to get access therefore intervene into to use of the system. Maybe the user segment can be the most difficult to attack, due to the wide various

type of the devices. But I think this kind of wide spectrum also has the wide range of vulnerability, what if found can be used on other devices too. Therefore, I think we can identify big responsibility on the manufacturers of global positioning system components.

If we investigate how to influence the use of global positioning system devices we have to think to the two main element that is responsible for controlling this kind of systems. We have to influence the computing capacity or we have to interfere into the availability of the transfer network.

My intention was while I prepared this presentation to underline what kind of parallels and differences I can highlight just for starting discussions and common brainstorming among the audience according to the electronic warfare and cyberspace operation. I just listed a couple upcoming ideas those I thought to well-known and understandable for everybody. Both operations are done in the virtual, non-visible space that can have some experienced effect in the physical space also. From both approach by using the vulnerability that will have an effect to the dependency from information. Those will influence the decision making negatively, what harms the superiority too. After this parallel and equality proving thesis, let's see the opposite, a difference showing opinion. While the electronic warfare tools can have an effect without direct access to the source, or to the wireless transmitted information, to intervene into those flow by cyber means we have to have at least

one physical access to any element of the network. Those contains also the access to wireless data transferring device, or any other IT component that runs the system.

To defend the relevant own global positioning system element or component I think the possible defensive countermeasures can be the following. As from the beginning of the planning, producing, implementing, operating the systems we have to introduce hardening options of the systems by technological development. Also, a proper way could be to integrate independent Global Navigation Satellite System (GNSS) based systems to enhance accuracy and flexibility. We cannot forget to about the fancy buzzword security awareness that has to also elaborated and enhance both on the side of users and also on operators to reduce the risk of jamming vulnerabilities.

As for the way ahead and finishing the presentation I identified some thoughts in the connection of my research. I will investigate the effects of the vulnerability through a complex approach. During the research I will look into details and look for the parts of IoT systems that can identified as the smallest, but harmful element from the global positioning system vulnerability perspective. I will check for possible factors that can influence the degree of integrity.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Some vulnerabilities of global positioning systems

Gábor KNAPP PhD student
National University of Public Service
Faculty of Military Science and Officer Training
Doctoral School of Military Engineering

Topic's processed during the presentation

- Actuality references
- Short overview of the global position systems
- Parallels and differences between the vulnerabilities of EW and cyberspace operations
- Possible defensive measures
- Way ahead

2

Actuality references

Source: Internet

3

Actuality references

POLITICS | ESTONIA

GPS jamming in the Baltic region: Is Russia responsible?

Konstantin Eggert
05/05/2024

Estonia and Lithuania have accused Russia of interfering with air traffic navigation in the region. Experts see it as part of Moscow's hybrid war against NATO. Will the security alliance respond?

Source: https://www.dw.com/en/gps-jamming-in-the-baltic-region-is-russia-responsible/a-68993942

4

The connection of the presentation to the vulnerabilites of positioning of IoT systems in the area of defence sector own research

#global_positioning

#vulnerabilities

#military_use

5

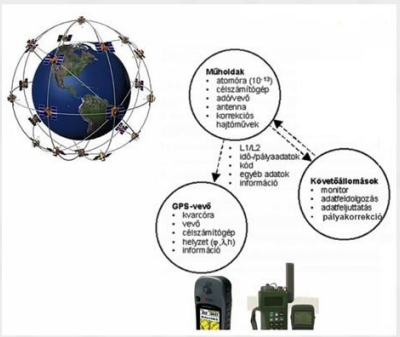
Short overview of the global position systems, problems I.

- Military vs. civilian systems
- 3D positioning, providing correct time (synchronisation, time measurement)
- Possible option to intervene during development phase, producing and operating
  - Space segment:
    control devices, controller of the correction engine's
  - ...

6

Short overview of the global position systems, problems II.

- Possible option to intervene during development phase, producing and operating
  - …
  - Control segment (access?) devices
  - User segment (GPS receivers)

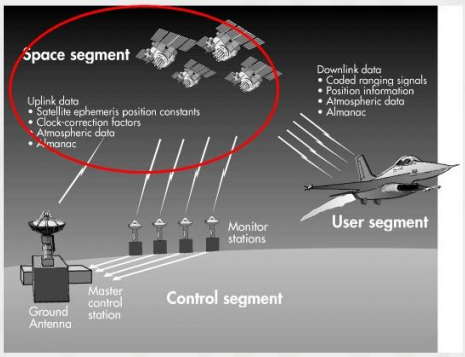


Source: Prof. Dr. Haig Zsolt
EW attack: Jamming of GPS navigation DSME presentation
2024.03.28.

7

Short overview of the global position systems, problems III.

- Responsible for controlling of a GPS system:
  - Use of computing capacity;
  - Availability of the transfer network.



Source: https://images.app.goo.gl/hAFQhwk5PKZHJuGr6

8

Parallels and differences between the vulnerabilities of EW and cyberspace operations*

- Operations done in the virtual, non visible space can have some effects experienced in the physical space also.
- Both vulnerability has effect to the dependency from information.
- Effect with or without access.

** without any need of completeness*

9

Possible defensive measures

Hardening of positiong systems by technological development.

https://infinidome.com/the-rising-threat-of-gps-jamming-impacts-and-solutions/

Integrating independent GNSS based systems to enhance accuracy and flexibility.

Enhance security awareness both on the side of users and also on operators to reduce the risk of jamming vulnerabilities.

https://www.linkedin.com/pulse/understanding-gps-jamming-attacks-impacts-mitigation-strategies-gqwhc

10

Way ahead
in the connection of my research

To investigate the effects of the vulnerability through an complex approach.
To look into details and look for the parts of IoT systems that can identified as the smallest, but harmful element from the global positioning system vulnerability perspective.
Check for possible factors that can influence the degree of integrity.

11

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Thanks for your attention

+36306856643
knapp.gabor@hm.gov.hu

Ferenc Fazekas[1]: Challenges of C2 in multidomain environment

Correferatum

Military activities are planned and directed through a well-established command and control system. Command and control is the main function of the military commander and the staff, thus it is important to continuously review and upgrade the existing processes. The planning and management of military operations are done by applying operational art. According to the actual NATO terminology stated in the Allied Joint Doctrine AJP-01(F), the operational art is the employment of forces to attain strategic and/or operational objectives through the design, organization, integration and conduct of strategies, campaigns, major operations and battles. The operational art is not fully intuitive, it has scientific foundation as it uses the scientific methods and principles of planning, and applies the tenets laid down in the doctrine. But the operational art also depends on the personal skills of the commander and staff, such as their skill, knowledge, experience, creativity and judgement. The combination of these two distinct parts makes it being an ’art’, as the outcome depends on subjective knowledge and experiences that vary from individual to individual.

[1] ORCID: 0000-0001-7409-1054

The roots of the science behind the operational art can be traced far back in the history, but there's an actual point when military thinkers started to designate a special mental attribute that makes the difference between good or bad commanders. This attribute was called „coup d'oeil" in French, literally meaning „glance" or „quick look". It signified that a quality officer could decide the application of the force on the given terrain by first glance due to the „coup d'oeil" he possesses. In the 19th century coup d'oeil was thought to be an attribute that everybody had in different degrees. It could be increased and enhanced through training and experience, but everybody has an upper limit, the better officers' limit was higher.

As science increasingly came into play in military leadership theory, different approaches were born, all aimed to improve decision-making. One improvement can be traced back to the works of John R. Boyd, who based on his own experiences as fighter pilot constructed a combat decision-making model of four steps: the observe, orient, decide and act steps. This so-called OODA loop serves as the base of the model of the present NATO approach of the decision-making process, the Operations Process. The core of the main activities of the Operations Process is the leadership that directs the activities of plan, prepare and execute.

The commander in the middle of these activities may apply the philosophy of mission command that has several tenets and principles to make it work properly. The superior commander's clear

and concise intent drives the activities which have to be facilitated by mutual understanding and trust. The ultimate goal is to have timely and effective decisions through decentralized execution.

These aforementioned principles and guidelines are based on the best practices of the past, but the modern operational environment creates brand new challenges that may initiate a change in the existing methods. Some of these factors are: the multidomain threats, the complex terrain, the defence systems getting more effective, the new technologies – such as Artificial Intelligence – being utilised, and the information as a weapon. The evolving operational environment enabled a new concept for planning and executing operations, the so-called multidomain operations. This new paradigm is the enhancement of the previous joint operations and requires extensive cooperation and information management from the own force. The concept builds on the effects-based operations in a way that it plans and coordinates the activities of the force through achieving synchronised effects that may disrupt or overload the enemy decision-making system. Activities executed by domain-specific forces create simultaneous effects that affect enemy forces, organizations, or individuals.

In order to achieve the desired effects the different activities have to be coordinated in a way that ensures that the own forces keep or retain the initiative. Making acceptable decision faster than the enemy is called decision superiority, and it makes impossible for the

enemy to make effective reactions to our activities. Decision superiority, or in other terms, „getting inside of the enemy OODA loop" is desirable, but in a constantly evolving environment it is hard to achieve, as the enemy also utilizes modern technologies and approaches. In this aspect Artificial Intelligence can be an enabler or even a game changer. There are several studies that deal with the possible improvements for the command and control system, one of them is the concept of the Mosaic Warfare. According to this human-machine cooperation will be intense in the staff and the field as well: the commanding human exercise machine-assisted control over manned and unmanned units. The OODA loop in this case will accelerate and become shorter, while the activities of the own force focuses on disrupting the enemy's orientation.

The transformation of the command and control system seems to be inevitable: the theoretic framework is changing, the weight of information is increasing, the tenets of mission command are fading and getting more difficult to achieve in a multidomain environment. The readily accessible large volumes of data enables precise real-time common operational picture solutions that give new tools to the commanders to exercise command and control over their units. All of these factors prompt changes in the required attributes of the commanders, and the notion of „coup d'oeil" still remains valid in a modernized form: commanders have to have „digital coup d'oeil" to effectively apply all the digital tools available to them in order to maintain the decision superiority and operations security.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Challenges of C2 in multidomain environment

LTC Ferenc FAZEKAS
UPS FMSOT Faculty of Military Strategy, assistant lecturer
fazekas.ferenc@uni-nke.hu

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

SUPPORTED BY THE ÚNKP-23-3-II-NKE-5 NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY FOR CULTURE AND INNOVATION FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND

Új Nemzeti Kiválóság Program

Operational art
NATO's approach

The employment of forces to attain strategic and/or operational objectives through the design, organization, integration and conduct of strategies, campaigns, major operations and battles.

Operational art combines the science of planning and the guidance from the tenets of doctrine with the skill, knowledge, experience, creativity and judgement of commanders and staff.

Operational art

A classical idea: coup d'oeil

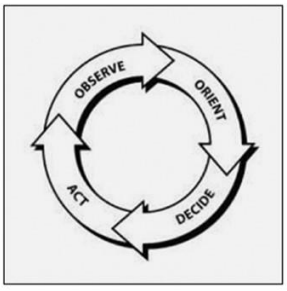
Jean-Charles de Folard

Carl von Clausewitz

Antoine-Henri de Jomini

C2 of military operations

Decision cycle



John R. Boyd

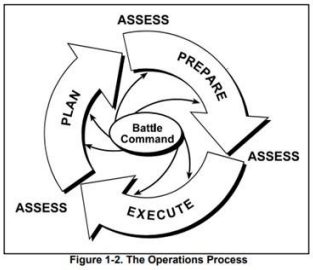


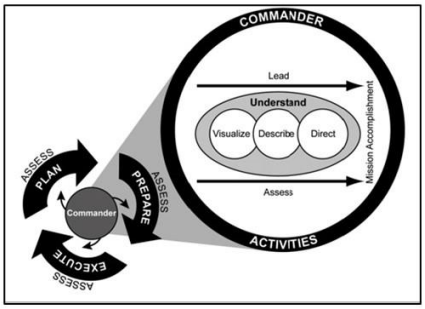
Figure 1-2. The Operations Process

C2 of military operations

The philosophy of mission command

Basic tenets and principles:

- Clear and consice commander's intent;
- Mutual understanding between subordinates and commanders;
- Two-way trust;
- Timely and effective decisions;
- Decentralized execution.



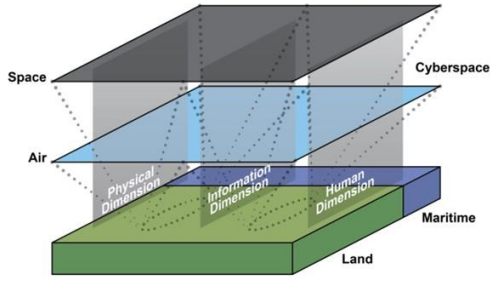
The modern operational environment

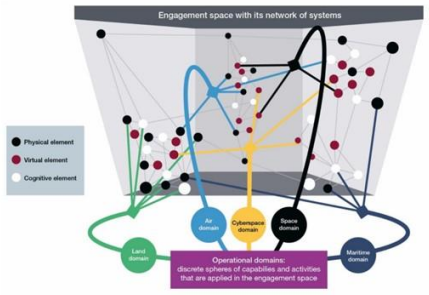
Potential threats getting more dangerous

- Multi-domain threats;
- Operations in complex terrain (built-up areas, cities);
- Hybrid approaches;
- Modernization and proliferation of WMD;
- Effective defence systems;
- Information as weapon;
- Emergence of weapons utilising new or upgraded technologies.

Concept of multidomain operations

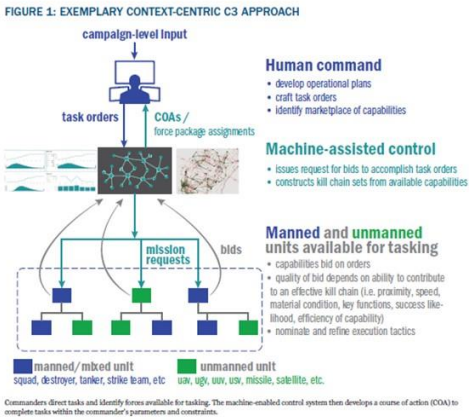
Increasing complexity

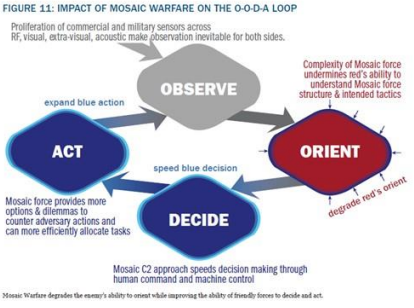




Challenges in C2

A possible solution - mosaic warfare





Challenges of the present and future

Transforming planning and C2

- The theoretic frame of decisionmaking changes;
- Human-machine trust and understanding;
- Information overload / loss;
- Possibility of decentralization changes;
- „Tactical Generals”;
- Digital coup d’œil required.

Thank you for you attention!

Viktor Szulcsányi[1]: Opportunities and challenges in analysing the actions of cyber threat actors

Correferatum

Introduction

There is a threat actor behind every cyber attack, however, identifying the perpetrator of these harmful activities keeps remaining of the most challenging objective of a daily life of cyber security experts. In order to effectively prepare for and defend against these complex cyber operations executed by either a hacktivist group or a state-sponsored APT group, first we need to understand the motives behind such attack and know every possible attack surface and vector that could be used during a potential breach of an IT infrastructure we would like to protect.

In my presentation, I tried to summarize the general characteristics of the activity of the attack groups, the current trends seen in the latest cyber attacks, as well as the technical details that help to detect the activity. I also presented multiple opportunities for data collection regarding the indicators of a cyber attack.

Current trends in the activity of threat actors

[1] ORCID: 0009-0003-7946-6312

Cyber threat groups are becoming more and more sophisticated and fact goes hand-in hand with the necessity of constant development in detection capabilities as well. Cyber security experts are facing newly emerging threats regularly and this will continue to be one of the biggest challenges for defending an organization's IT infrastructures.

APT groups are carefully planning each and every operation which enables them to be quick at adapting and reacting to new vulnerabilities or applied security measures. During the preparation phase of an attack, an actor would monitor the exploitable attack vectors or attack surface of an organization for a relatively long period, even for several months in order to increase the effectiveness of the cyber operation.

A continuous increase can also be identified in the field of cooperation between formerly independent cyber threat actors. This tendency is even expanding to cooperation between nation states, which makes the identification process of a potential breach more and more difficult. These actors are frequently using shared services for resource optimization reasons as well.

Opportunities for identifying actors behind an attack

Several factors can play a significant role in categorization and identification, such as the timing, the possible motivation, or the technical details of the attack.

In this presentation, I present the analysis of the activities of attack groups from the technical aspect. Instead of searching for occasional textual comments, errors, and typos in the source code of a malware, it is advisable to search for or create a general signature that can be used in all cases for a specific group. The TTPs defined by the MITRE ATT&CK Framework is meant to serve this exact purpose. As for signature-based identification, it could be relying on two main components: TTPs and IOCs.

The use of TTPs can outline the given group relatively reliably, but it is a source of information that is more difficult to filter. On the other hand, IOCs are significantly easier to identify, however, time is of critical importance in this case, since it is possible that the compromised or attacker-related infrastructure used during the attack was only under the control of the attacker for a few days or a few hours, and before and after the event it belonged to a legitimate service. For this reason, it is not necessarily reliable as IOCs are rarely reused, although it is definitely recommended to filter or monitor them through cybersecurity solutions.

Identifying certain characteristics of an APT group can be executed in multiple ways, based on different types and procedures of data collection and analysis, which I will explain in detail with a few examples later in my presentation.

In November 2023, the cybersecurity company Kaspersky released a summary report on the activities of Asian APT groups, identifying

the detailed signatures that were detected during the attacks these threat actors carried out. The signatures range from the IP addresses, domains and other indicators used to the TTPs associated with each step of the attack process defined by the Unified Kill Chain. This summary report focuses on multiple threat actors operating in Asia and from the thorough analysis of recent cyber attacks related to these actors, the threat intelligence group of the company was able to drew a few important conclusions about how they operate. In my presentation, I would like to present a few examples of what characteristics can be determined from analysing the activity of an APT group. [1]

Based on the report, several methods and procedures are being used by these actors in the phase of establishing persistence. One certain signature, however, appears as a recurring element more often, in almost every attack carried out by Asian APT groups. This signature is a combination of multiple TTPs, including the creation of a windows service, DLL side-loading and process hollowing.

Process hollowing is a technique used by attackers to replace a piece of legitimate code running in memory with malicious code. DLL side-loading is a form of DLL hijacking, when an attacker loads a malicious, but legitimate looking, renamed DLL file into a vulnerable application. The vulnerability is due to the use of a partial file path, where the operating system starts searching for the referenced DLL in a predetermined order, and the attacker places the malicious file

ahead of the actual, legitimate built-in DLL file in this particular order.

Although the signatures defined in this report could be copied or specific to multiple threat actors, it could provide a starting point in analysing a cyber attack, along with the other indicators used by the given attacker.

Possible methods to gain valuable information

The continuously evolving cyber landscape is the reason why finding new, effective and even unorthodox ways of gaining valuable information became a necessity. The analysis and processing of threat and malware reports published is still useful, but lacks proactivity as it focuses on using information about a cyber attack that has already occurred for defensive measures. Therefore using intelligence operations against the possible attackers, especially threat groups sponsored by a nation-state is becoming more and more crucial for maintaining the security of our key IT infrastructures.

A possible solution for this problem could be considering the usage of virtual HUMINT capabilities besides the more general approach of OSINT and SOCMINT operations. Although the latter two are skills that can be developed more easily, mainly hacktivist groups publish information about their current targets and if APT groups are our main concern, there will be little to no information available about

future attacks. However, through an effective virtual HUMINT operation, even advanced hacker groups could be infiltrated and that potentially provides access to critical information about the given group's further actions in preparation.

Another interesting method for data collection is utilizing the vast information available through malware databases. Searching malware databases, obtaining specific samples and analyzing them in detail could be a good starting point when analyzing the activities of attack groups.

Malware databases are available as a paid service or publicly as well. The disadvantage of these is that usually we are working with bulk data, and most of the time preliminary analysis result or categorization is not available. However, paid services could already contain preprocessed, categorized data, which is more useful for collecting information about a certain threat actor.

Unfortunately, reverse engineering malware samples is a more difficult activity to automate, so it turns out to be an extremely resource-intensive task for even a medium-size company.

The usage of deception techniques, namely honeypots however could still be a viable option for analysing the activities of cyber threat groups, despite the fact that it may also require significant human resources to process the collected information. Implementing deception techniques could provide more targeted

and detailed information about the activities of threat groups than the previously mentioned methods if it is executed optimally.

Challenges in the near future

The field of cybersecurity is expected to be ever-changing. This phenomenon could be both a challenge and an opportunity as well. From the defending side, it would seem more difficult however to adapt to the constantly changing signatures of attacks or the newly emerging threats. The increasing demand for deep technical analysis of each complex attack could chip away the resources from an organization's day-to-day activities, like maintenance, code development or other equivalently important tasks.

Although there is a moderate evidence of the spread of artificial intelligence usage in the activities of APT groups, the challenge related to AI-supported cyber attacks or defensive capabilities remains a priority for the next few years of cybersecurity. [2]

Conducting regular vulnerability scans and continuously developing the incident management process could be useful and is always recommended to mitigate the possible attack vectors in an IT infrastructure, but most of the time the measures mentioned above are still not sufficient enough together to evade a potential cyber attack. [3]

The necessary legal basis and possible consequences of attributing a cyber attack are currently unclear and in my opinion will still

remain in obscurity, however, the issue of the former could be partially solved by detailed, strict regulation. [4]

References

[1] Kaspersky Threat Intelligence (2023), Modern Asian APT Groups – Tactics, Techniques and Procedures, Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/09055246/Modern-Asian-APT-groups-TTPs_report_eng.pdf (Accessed 8 May 2024)

[2] Dijk A. (2021), "Detection of Advanced Persistent Threats using Artificial Intelligence for Deep Packet Inspection," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, pp. 2092-2097, doi: 10.1109/BigData52589.2021.9671464.

[3] Magyar S., Szulcsányi V. (2023), "The importance of cyber defense exercises to increase resilience", In: Tastanbekov M.; Ağayev E., 1. BİLSEL INTERNATIONAL EFES SCIENTIFIC RESEARCHES AND INNOVATION CONGRESS, Izmir, Turkey, pp. 607-615.

[4] Finlay L, Payne C. (2019), "The Attribution Problem and Cyber Armed Attacks", American Journal of International Law, AJIL Unbound, Vol. 113, pp. 202-206., doi:10.1017/aju.2019.35

Keywords: threat, APT, cyber threat intelligence, honeypot

Opportunities and challenges in analysing the actions of cyber threat actors

Viktor Szulcsányi

Table of contents

Recent trends in cyber attacks

- Organized, state-sponsored cyber threat groups and emerging threats
- Quick adaptation and reaction to the applied cybersecurity measures and new vulnerabilities
- Formerly independent, now increasingly cooperative groups
- Continuous monitoring of attack vectors for the effective preparation of cyberspace operations
- Using shared services is becoming more frequent (Cybercrime-as-a-Service)

Signature-based categorization

- MITRE ATT&CK – TTP-s
  - Relatively reliable
  - Previously identified attack methods are often being reused
  - Harder to detect
- IOC-s
  - Significantly easier to identify
  - Not necessarily reliable
  - Typically not reused

Signature-based categorization

Asian APT groups

- Based on a summary report issued in November 2023
- Narrowed list, specifically with elements experienced during the activities of the attack group
- They usually do not resort to destructive methods at the end of the attack
- Global activity
- SIGMA rules

Signature-based categorization

Asian APT groups- Gaining persistence

- Several, but one outstanding method that is typical for the group
  - T1543.003 – Create or Modify System Process: Windows Service
  - T1574.002 – Hijack Execution Flow: DLL Side-Loading
  - T1055.012 – Process Injection: Process Hollowing
- Step 1: Delivery of harmful DLL and DLL hijacking vulnerable but legitimate executable file
- Step 2: Create and start a Windows Service pointing to a legitimate file
- Step 3: Process Hollowing is used to create a new process and load malicious code into memory through it
- Step 4: Hide activity behind the svchost.exe process
- Result: A continuously running process with elevated privileges that an attacker can access at any time

Data collection and analysis methods

CTI + Intel

- OSINT
- SOCMINT
  - Mainly hacktivist groups publish information about their current targets
- HUMINT
  - Colonial Pipeline -2021
- Analysis and processing of Threat and Malware reports

Data collection and analysis methods

Malware DB

- Public service, available for free
- Paid service
- Bulk, uncategorized and categorized, processed data
- Extremely resource-intensive solution with an uncertain return value

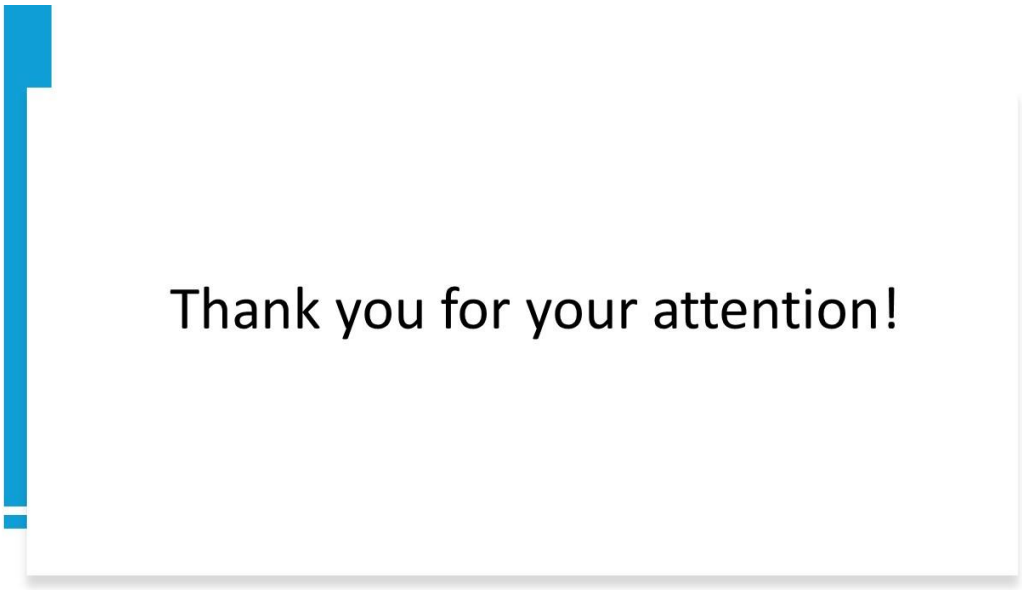
Data collection and analysis methods

Deception techniques

- Public service, deployable, available for free
- Paid or self-hosted service
- Monitoring the use of "leaked" credentials (Honeytoken)
- It may also require significant human resources
- It can provide more targeted and detailed information about the activities of threat groups than the previously mentioned methods

Future challenges and difficulties

- Constantly changing signatures
- New emerging threats
- Increasing cooperation between cyber threat actors
- Automation, spread of AI usage
- Increasing demand for technical analysis
- Legal difficulties of threat attribution
- Prevention is essential, but it would never provide complete protection


Thank you for your attention!

Attila József Busa[1]: The place and role of the cyber security trainings in the Hungarian Defence Forces

Correferatum

Cyber security is one of the most sensitive areas of security science today. This area of information security is becoming prominent not only in the military but also in civilian life. This conference paper presents the role and development of cyber security training in the military.

In the following few lines, it will be shown how cyber security has become a substantially important security area since the early 2000s. In 2007, Tallinn, the Estonian capital, was the site of a major cyber-attack, which became known as the first major cyber-attack. At the heart of the crisis were cyber-attacks on Estonia, which completely paralysed the country with a successful offensive on government and economic targets. The background to the events was the Estonian government's announcement that it would move the Bronze Soldier monument from the centre of Tallinn to a military cemetery on the outskirts of the city. Following this, the Russian hacker group Killnet is believed to have launched a coordinated cyber-attack against Estonia. The attacks also left many government and business websites, as well as online banking systems, completely paralysed. Following the cyber-attack, NATO

[1] ORCID: 0009-0009-6167-2154

allied nations joined forces to help Estonia, which had been plunged into the digital dark ages. Thanks to this united effort, the country has leapfrogged two generations of digital progress. The role of cyber defence was enhanced by this event, and in 2008 the NATO Cooperative Cyber Defence Centre of Excellence was established in the Estonian capital Tallinn, where the development and training of cyber defence-specific training in NATO began. Initially, the centre received major support from the United States and Israel, and later 32 other countries from around the world joined the list of sponsors.

The next milestone was the emergence of the Stuxnet worm in 2010. This cyber-attack was directed against Iran's nuclear program and specifically targeted industrial systems used by Siemens. Stuxnet was one of the first known cases of a cyber-attack targeting real physical systems and had a major impact on the industrial processes involved.

At the 2016 NATO Summit, the Heads of State and Government unanimously declared their commitment to making cyberspace an operational domain, and accordingly adopted it as the fourth operational dimension (alongside land, air and sea). Interestingly the space only became the fifth operational domain after that, in December 2019. To strengthen cyber defences, the NATO member states need to develop a new cyber defence strategy and strengthen their cyber resilience. Subsequently, cyber defence training will start to be developed at a strategic level in several nations. Building on

the national defence cyber security training institutions established in neighbouring European countries, Hungary has also started to organise such training in 2018.

The 2020 National Security Strategy also called for the strengthening of cyber capabilities, and the 2021 National Military Strategy also supported the creation of a new Cyber and Information Operations Centre.

The Cyber and Information Operations Centre of the Hungarian Defence Forces (HDF CIOC) was established in early 2022 by merging the Military Cyber Operations Centre of the Hungarian Defence Forces, the Civil-Military Cooperation and Psychological Operations Centre and the Electronic Incident Management Headquarters of the Budapest Garrison Brigade, in response to security challenges. The soldiers of this unit of the National Defence Forces are involved in the protection of the electronic information system of the Ministry of Defence and in the prevention of cyberspace threats every day of the year. Twenty-four hours a day, the staff of the centre is tasked with combating computer malware, ransom notes and malicious code. While there is never 100 percent protection, 21st century technology is in capable hands and can be relied upon to provide the right level of protection.

In the Centre, cyber training tasks are carried out by the Cyber Training Subdivision within the Training Division. In contrast to the international schools listed above, at the time of writing the Centre

is still only organising training courses in the defence sector in the country.

In the beginning, finding professional cyber security experts was a huge challenge; there are far fewer cyber security experts than needed and this is a global problem. One of the main considerations in the selection of professionals was the importance of 'reverse thinking' in this field, as both the attacker and the defender have to constantly look for loopholes and alternative solutions in this area of defence. The design of the training courses considered the didactical and methodological aspects of cyber security training in similar areas. The aim was to develop the "cyber capability" from scratch. Once the required capabilities had been defined, the training modules deemed necessary were developed.

The basic cyber security training modules have been defined as follows:

- Cyber-awareness,
- Cyber security practitioner,
- Cyber security management,
- Python programming,
- Ethical Hacking,
- Digital Forensic and Incident Response,

- Cyber security for military decision-makers,
- Cyber security for senior NCOs.

The technical development of the Centre and the replenishment of its specialised staff are ongoing. It seeks to attract the workforce with outstanding development opportunities in the Hungarian Defence Forces. The future objectives of the institution include the development of e-learning-based on-line training and the organisation of English-language training courses for NATO.

As a small digression, it is important to mention that for the first time in Hungarian public education, cyber awareness is introduced as a compulsory subject in the training of defence cadets, which provides students with an insight into the basic areas of cyber security and draws attention to the dangers of everyday cyberspace use.

The conference presentation shows that the role of cyber defence training institutions within NATO, and thus within Hungary, is key to responding effectively to modern cyber security challenges. These training institutions help Allies to develop their cyberspace skills, adapt rapidly to threats, and improve cooperation and information sharing, thus contributing to the security and resilience of NATO as a whole in cyberspace.

International Scientific Conference on Military Information Security

The place and role of the cyber security trainings in the Hungarian Defence Forces

Attila József, Busa
HDF Cyber and Information Operations Centre
Training Division,
Head of division

BRU Infosec Kft.
founding member, managing director

Óbuda University,
Doctoral School of Security Sciences,
2nd year PhD student

Draft

- Historical overview;
- The legal background;
- Cyber organisational improvements in the HDF;
- Cyber protection modules;
- Goals;
- Summary;
- Questions / Answers.

Historical overview

- 2007, Tallinn (concerted cyber attack);
- 2008, NATO Cooperative Cyber Defence Centre of Excellence, Est.
- 2010, Stuxnet;
- 2016, NATO Warsaw summit (making cyberspace an operational area);
- 2019, NCIA Academy - Oeiras;
- 2019, NATO School – Oberammergau;
- 2020, Cyber Security Training Centre of Excellence – Warsaw.

The legal background

- 1163/2020. (IV. 21.) government res. [The National Security Strategy] Point 101. „*Hungary considers cyber capabilities capable of endangering physical security or causing significant material damage as weapons, and their use as armed aggression, which can be responded to in physical space.*"
- Act CXL of 2021 3. § 24. „*operational area: the geographical area defined and designated in the operational plan and the airspace above it, as well as cyberspace,*"

Cyber organisational improvements in the HDF

- 2019 – Cyber Defence Perspective (separate theatre of operations, capability definition)
- 2019/2020 – "Cyber Academy", Szentendre
- 2020 – HDF Cyber Coordination Division
- 2021 – Preparing the integration of CYBER, CIMIC, PSYOPS and Event Management
- 2022.01.01 – Cyber and Information Operations Centre
- 2022.11.01 – Cyber Operations Command

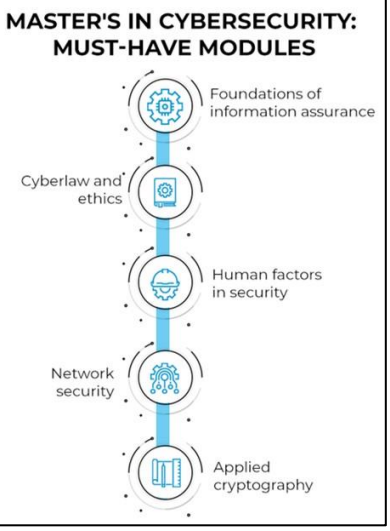
Cyber organisational improvements in the HDF

CYBER SECURITY EDUCATION

- Find experts.
- "Thinking backwards" is a PRIORITY. Attacks need to be analysed in order to design an appropriate defence.
- Examining the themes of NATO cyber defence training.
- Examining topics for civil cyber defence training.
- How to build a cyber defence specialism?
- Research into the most effective teaching methods.
- Create training modules.

Cyber security modules

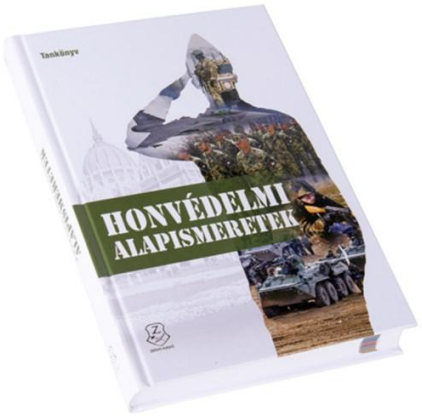
- Cyber-awareness
- Cyber security practitioner
- Cyber security management
- Python programming
- Ethical Hacking
- Digital Forensic and Incident Response
- Cyber security for military decision-makers
- Cyber security for senior NCOs



Goals

- Providing training throughout the government sector.
- Processing experiences from participation in national exercises.
- Design e-learning training courses (cybersecurity maturity assessment).
- Continuous improvement for the future.
- LLL

Read more



Summary

The role of cyber defence is of paramount importance at international and national level. But protection should not be left to professionals alone. All users must be aware of the cyber threats they face and do their utmost to use cyberspace consciously.

Solution

„No defence can replace common sense!”

Any questions?

Resources

- 1163/2020. (IV. 21.) korm. h. [Nemzeti Biztonsági Stratégia]
- 2021. évi CXL. törvény [Hvt.]
- Szenes Zoltán: Elrettentés és védelem a NATO új haderőmodellje http://real.mtak.hu/160782/1/HT_32_2_3-17.pdf (letöltve: 2023.11.13.)
- Kiss Zoltán: Honvédségi Szemle , Zrínyi Kiadó, Budapest 147 évf. 2019. / 2. szám
- Jamie Shea: Resilience: a core element of collective defence. NATO Review, 3. 30/03/2016. http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm (letöltve: 2018.04.16)
- MH KIMK – Cyber Academy: I. modul tananyag (Busa A. J., Rácz O., Umhauser B.), Szerk.: Busa A. J., Szentendre, 2022.
- Honvédelmi alapismeretek tankönyv (Almási L., Balog P., Berkecz G., Busa A. J., Drót L., dr. Eleki Z., Fekete A., dr. Kállai A., Kalmár I., Mihályi L., Nyulászi T., Szűcs P., dr. Tálas P. H., Tóth G., Zentai K.), Zrínyi Kiadó, Budapest, 2023.

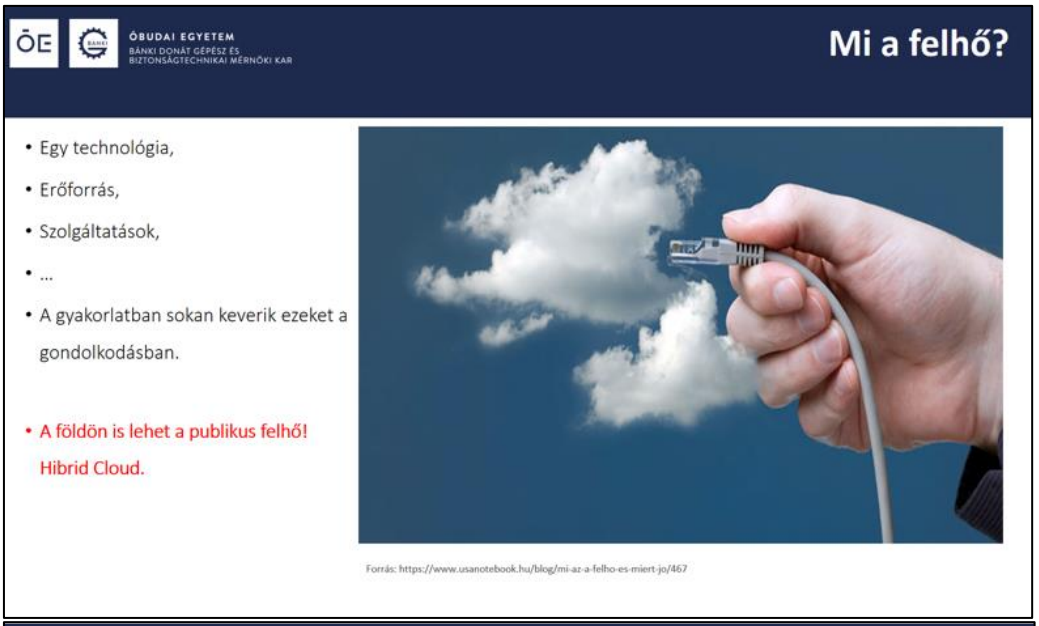
Thank you for your attention!

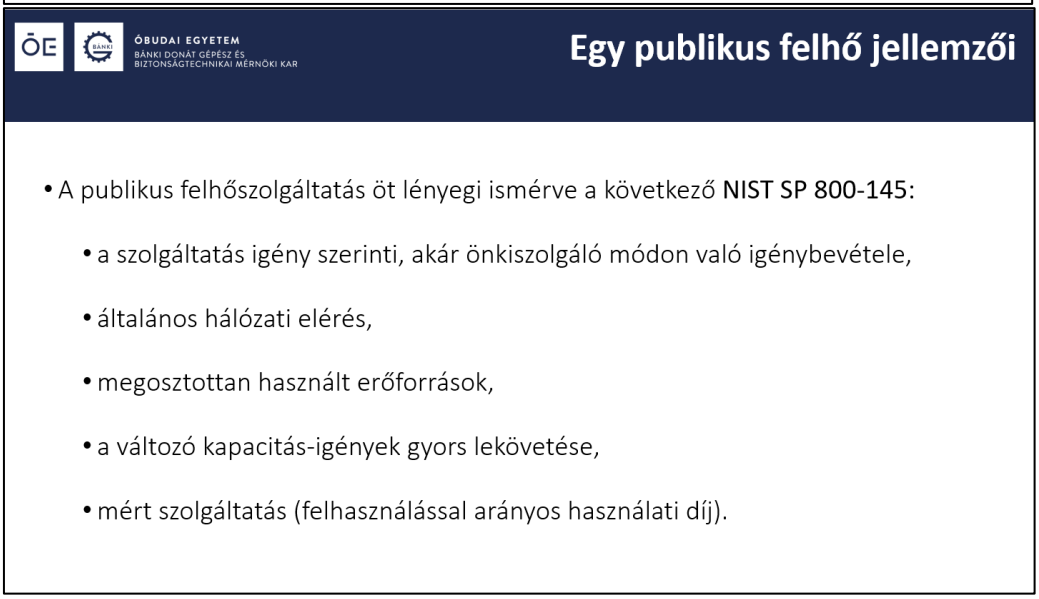
Oláh István: Egy publikus felhőszolgáltatás biztonsági kontrolljai egy pénzintézetnél

Egy publikus felhőszolgáltatást lehet-e a hazai jogszabályok szerint auditálni kérdésben nem egységes a szakma válasza. A konferencián résztvevőknek is feltettem a kérdést. Nem volt aki szerint a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szempontrendszere szerint egy audit elvégezhető lenne. Az előadásomban egy javasolt módszertant mutattam be erre.

Egy felhő alapfogalmai és felelősségi rendszere

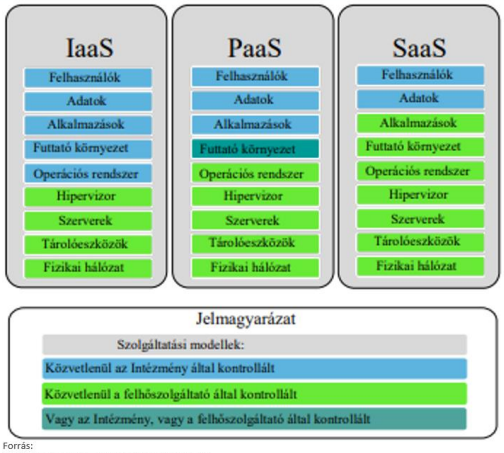
Az alapok tisztázását, felelősségi rendszerét a 2; 3; 4; 5, diákon mutattam be.





ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

A publikus felhő felelősségi határai



Forrás:
https://www.mnb.hu/letoltes/4-2019-felho.pdf

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Kontrollok a felhőben?

Egy adat szempontjából érdektelen, hogy:

- User hoston,
- Server hoston,
- Storageon,
- Fentiek virtuális verzión,
- Szalagon,
- Lemezen,
- Hordozható adathordozón,
- Mobil eszközön,
- .....
- A Felhőben,

Van.

A védelemnek egyenszilárdnak, és kockázatokkal arányosnak szükséges lennie!

Egy felhő logikai kontrolljai

A BM rendelet szerinti logikai kontrolljai szerinti audit lépéseit a 6; 7; 8; 9; 10, ismertettem.

Kutatási eredmény, az öt lépéses kontroll módszertan

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Ibtv. Megfelelés kontroll szinten- I

- A bemutatott eset a Microsoft Azure plafromra értelmezett, de az öt lépés minden publikus felhőszolgálatónál elvégezhető,
- Az AzPolicyAdvertizer/semicolon lapon az Azure policydefiníciók összefoglalása található meg. Az Azure védelmi profilok egyes adatai innen kerülnek az Azureba,
- **Első lépésként** célszerű „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet kontrolljait NIST azonosítóval összerendelni, pl:

BM rendelet			NIST
3.3.10.10.	A munkaszakasz zárolása	3.3.10.10.1. Az érintett szervezet: 3.3.10.10.1.1. meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést; 3.3.10.10.1.2. megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.	AC-11

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Ibtv. Megfelelés kontroll szinten- II

- **Második lépésben** a NIST kód alapján az audit dokumentumokban megkeresni az adott kontrollt:

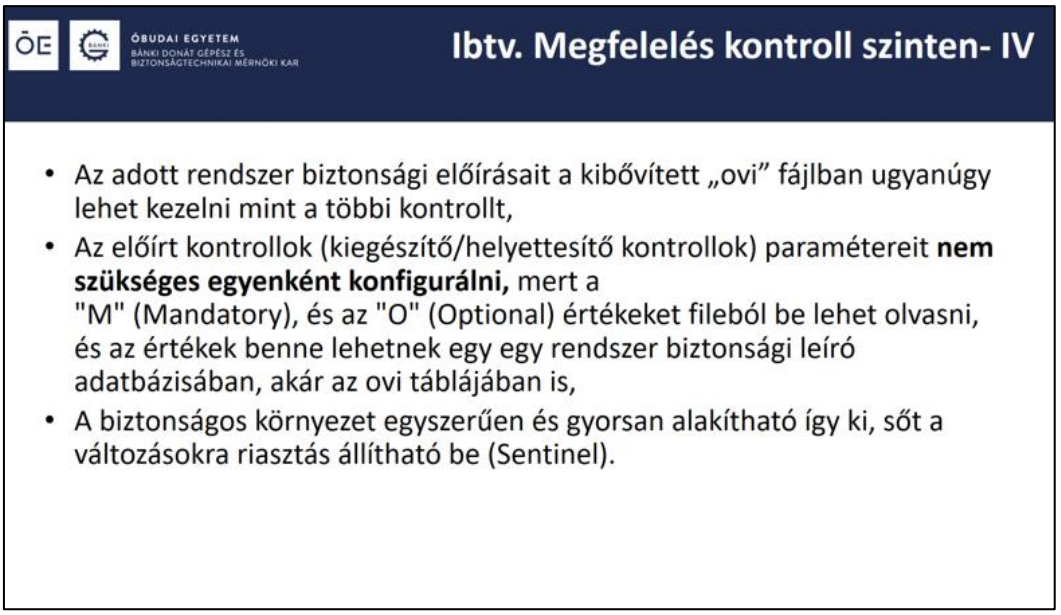
		NIST
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

- **Harmadik lépésben** a kontrollal kapcsolatos előírás értékelése következik megfelel, vagy nem felel meg **lehetőség szinten**: IGEN!

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Ibtv. Megfelelés kontroll szinten- III

- **Negyedik lépésben**, az adott kontroll kialakítását szükséges előírni egy EIR biztonsági rendszertervében,
- **Ötödik lépésben** az pl. Azure-ban az adott rendszere az érvényesítő paramétereket hangolni szükséges, azaz az alapbeállításokat kontrollonként végig kell gondolni, és a hangolást elvégezni,
- Amennyiben nem lehet közvetlen a kontrollt kialakítani, akkor kiegészítő kontrollokat szükséges előírni,
- Az előíró jellegű lépések a forráshelyről pl. excel exportot alkalmazva úgy végezhetők el könnyedén, hogy egy „üres OVI” táblába az összerendelési logikát bevisszük, azaz az ovi táblát egy felhős + *„füllel”* látjuk el.


ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR
Ibtv. Megfelelés kontroll szinten- IV
• Az adott rendszer biztonsági előírásait a kibővített „ovi” fájlban ugyanúgy lehet kezelni mint a többi kontrollt,
• Az előírt kontrollok (kiegészítő/helyettesítő kontrollok) paramétereit **nem szükséges egyenként konfigurálni,** mert a "M" (Mandatory), és az "O" (Optional) értékeket fileból be lehet olvasni, és az értékek benne lehetnek egy egy rendszer biztonsági leíró adatbázisában, akár az ovi táblájában is,
• A biztonságos környezet egyszerűen és gyorsan alakítható így ki, sőt a változásokra riasztás állítható be (Sentinel).

Egy felhő fizikai kontrolljai

A fizikai kontrollokkal kapcsolatos gondolataim a 11; 12; 13; 14, diák tartalmazzák.

Kutatási eredmény, a publikus felhőszolgálató adatközpontjára az igénybevevő szervezet fizikai kontrolljait alkalmazni szükséges.

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Az adatközpont szemlélet a fizikai biztonságra ?

- Egy publikus felhőszolgáltató műszaki épültei **ugyanúgy a szervezet működési fizikai tere, mint a saját épületek, saját adatközpontja a védelem szempontjából.**
- A fizikai kontroll, és az objektumbiztonsági előírásokat a szolgálatóra is érvényesíteni szükséges.
- Amennyiben ez nem lehetséges, kiegészítő kontrollt szükséges alkalmazni!

		BM rendelet	NIST
3.3.8.5.2.	Kriptográfiai védelem	Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán.	MP-5

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

NIST MP-5

MEDIA TRANSPORT

- Control: The organization:
  - a. Protects and controls [Assignment: organization-defined types of information system media] during transport **outside of controlled areas using** [Assignment: organization-defined security safeguards],
  - b. Maintains accountability for information system media during transport outside of controlled areas,
  - c. Documents activities associated with the transport of information system media,
  - d. **Restricts the activities associated with the transport of information system media to authorized personnel.**

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

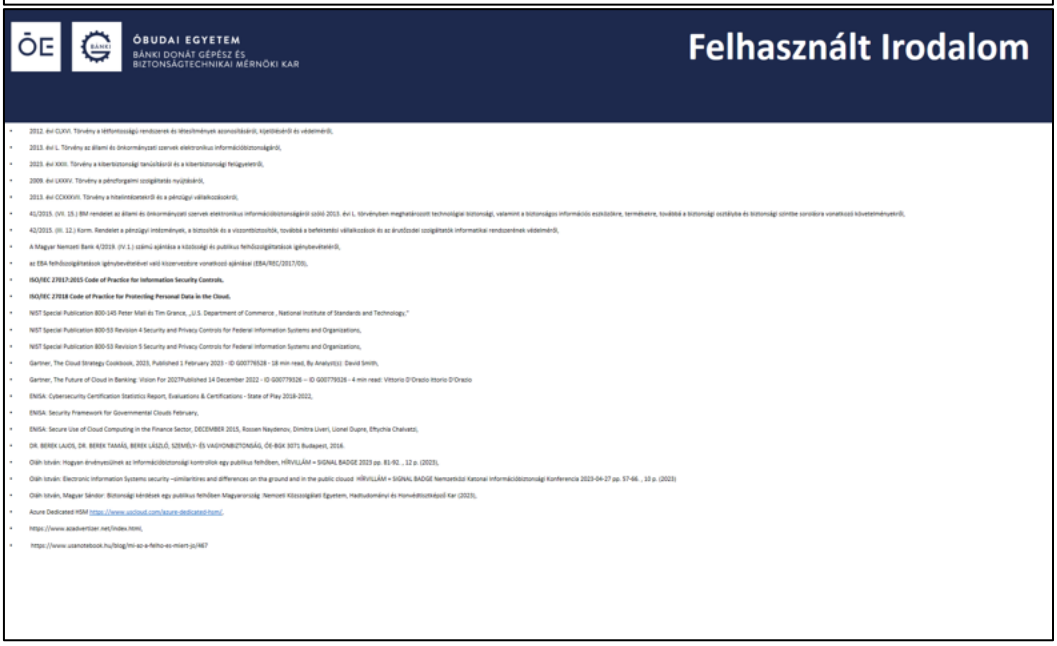
A KULCSOK a KULCS!

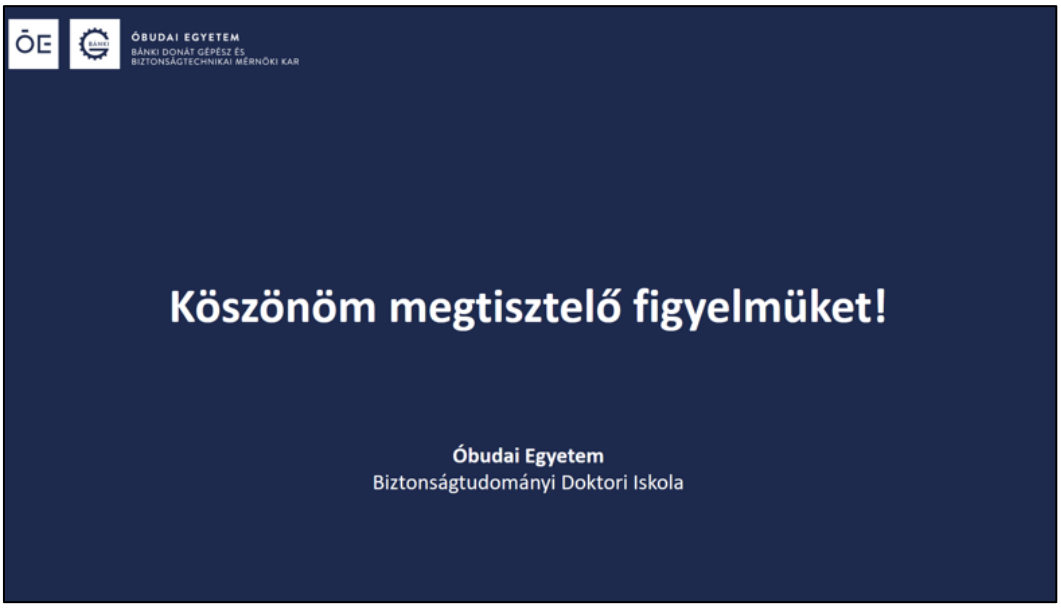
- Lehetőség szerint ne a szolgálató eszközein képezzük a kulcsokat, mert a maradványinformációkra is gondolni érdemes,
- A kulcsmenedzsment legyen szabályozott, zárt,
- A kulcsokhoz a felhő szolgáltató ne férjen hozzá!
- Az adatnak valahol ott kell lennie natívan! Ha máshol nem a memóriában, ezért mindent naplózni szükséges!
- HSM!
  - szoftveres (memória probléma),
  - hardveres (jellemzően drága!).

Forrás:
https://www.uscloud.com/azure-dedicated-hsm/

Záró gondolatok és irodalom jegyzék

A felhasznált irodalmat és a záró gondolatot a 15; 16; 17, diák tartalmazzák.




ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR
Köszönöm megtisztelő figyelmüket!
Óbudai Egyetem
Biztonságtudományi Doktori Iskola

Péter Stranszki: The need to develop information security awareness

Correferatum

In the last nearly 35 years, the Internet has gone through leaps and bounds. In the early 90s, only the privileged could access it and - from today's point of view - only relatively few websites could be browsed, and those who had an email address could use it for electronic communication. The most of the Internet users at that time largely did not even think that the Internet could be the scene of harmful activity.

Nowadays, there is almost no person who is not connected to the Internet in some way and at some level. On the Internet, anyone can read news, communicate, do official business, bank or shop from the neighboring village or the other side of the world. Internet communication has become an essential part of our everyday life.

In parallel, the telecommunications sector also developed, call centers were created and the possibility of official contact through the telecommunications channel was created.

The age group that "experienced" the development of the Internet tried to keep up with the speed of development, while it is an integral part of the everyday life of young people. During this development process, almost exclusively the positive effects of the novelties were presented, the new services each solution offers, or

in what ways it is better than the current ones. Since the dangers of the Internet and impersonal communication were not presented, many people do not even think that any problems could arise.

However, the development constraint also has negative effects: individual software and applications were and are not sufficiently tested, and functionality and economy overshadow security. However, where there are security gaps, there will necessarily be those who intend to exploit them, and those who want to make a profit from them. On the one hand, cybercriminals try to take advantage of the security gaps left in this way, so that they can enter computers or computer networks and steal data from them, or just make the computer or network unusable.

Another group of abuses is when they deceive the user by directing them to a website similar to the original one and asking for data that can be used, e.g. access their bank account or by calling users and personalize a banks call center and ask users for their credit card details or ask them to transfer money to an account defined by the cheaters.

It can already be seen that the attackers will become more and more professional, pay more and more attention to the small details, and it will become more and more difficult to distinguish the real from the fake.

What can be done to ensure that, despite being connected to the Internet, we do not suffer damage?

The best defense against attacks exploiting security holes is to constantly update both devices and software as recommended by the manufacturer, thereby eliminating known security holes as soon as possible.

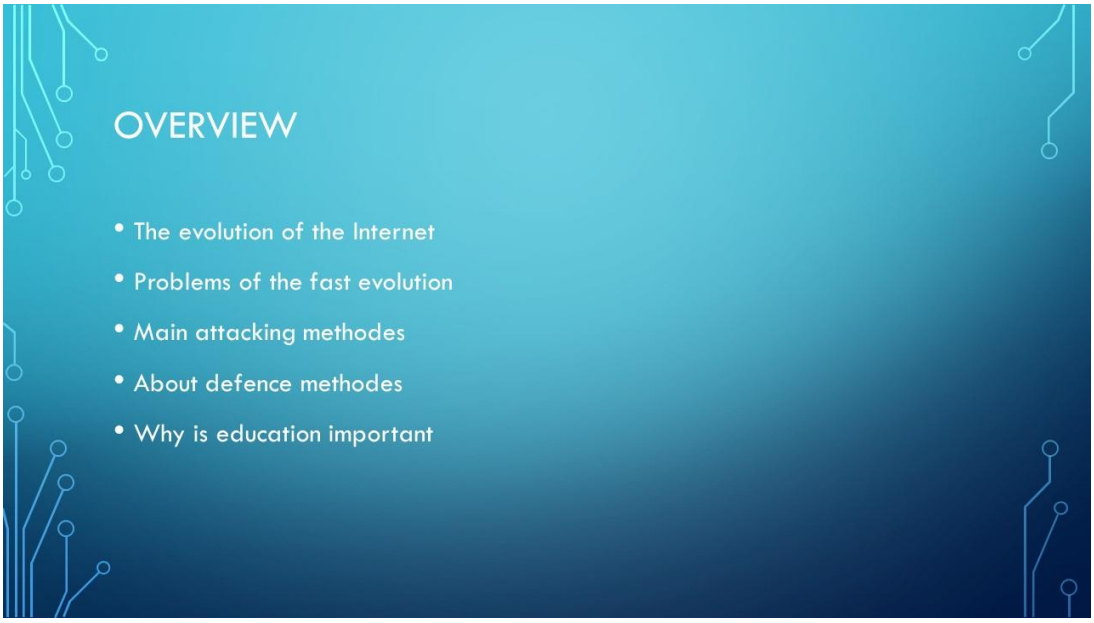
The best defense against fraud is to draw attention to the existence of this type of abuse and current trends.

It would be necessary to educate and explain clearly to everyone how the Internet works, what possibilities it has and for what reason and with which methods attackers try to obtain our data and what kind of behavior and security-conscious thinking anyone can do to protect their own data against these methods.

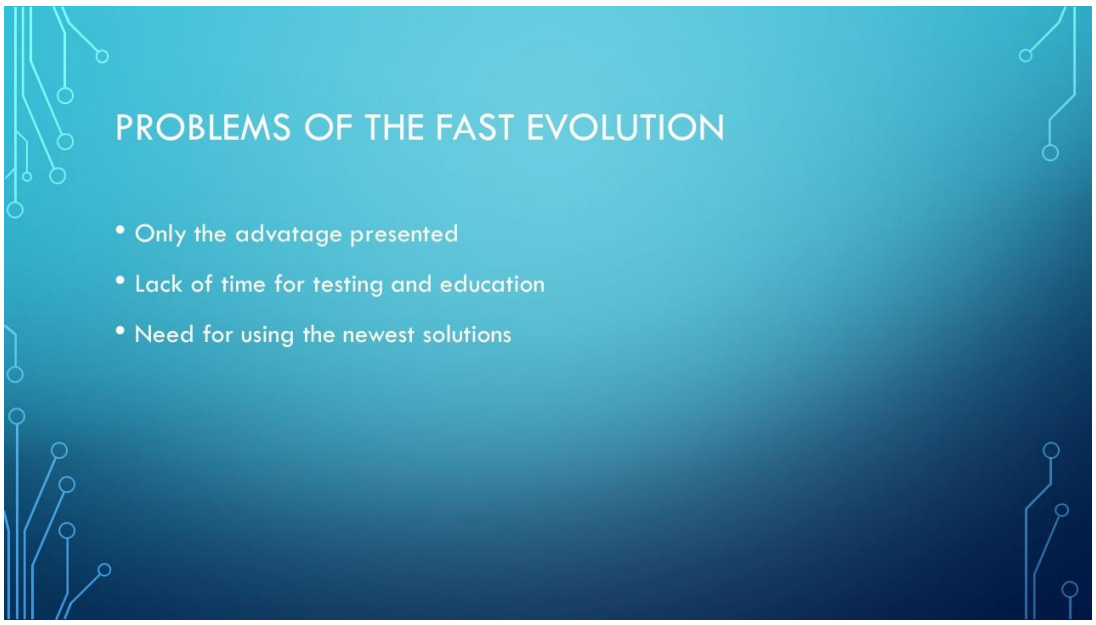
Several forms of these clarifications are possible, the simplest being perhaps regular information security awareness training, where current threats, their trends, the currently most common attack schemes and effective defense methods can be presented in general. In addition, the protection solutions and rules that users must and can do in order to reduce vulnerability can be dealt with in particular. Such an education can be an excellent opportunity in schools or workplaces, in addition to raising awareness campaigns general, everyday life, to present and repeat the special rules specific to the given institution and to emphasize the most important ones.

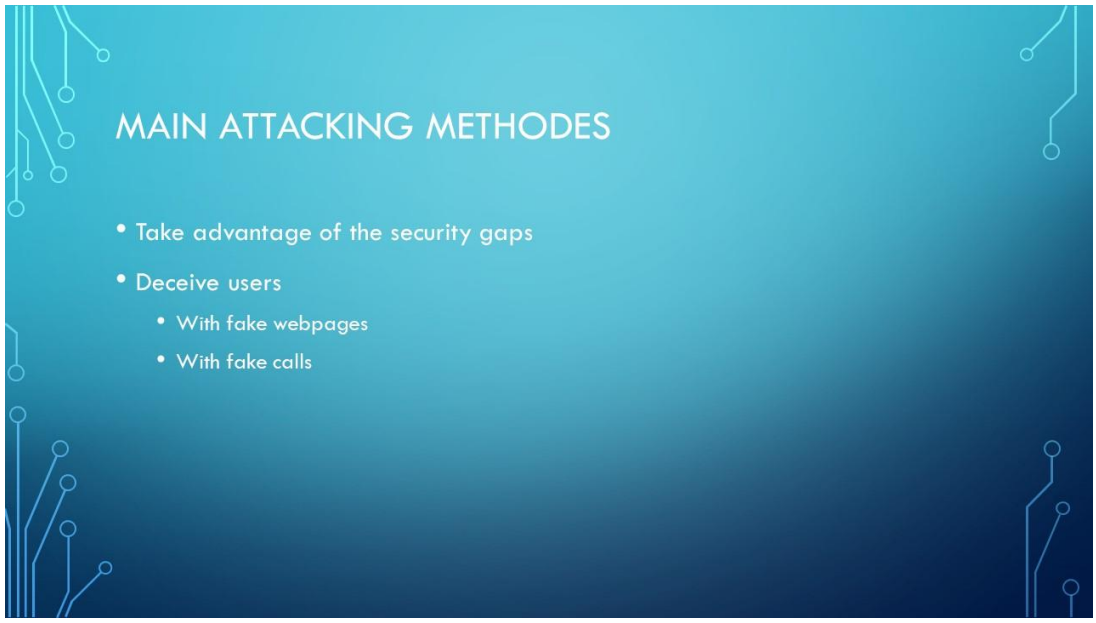
This type of education would be needed by all Internet users, regardless of age, gender, or education. Since some types of attacks have received more and more publicity in recent years, the media drew attention to the existence of this type of danger. This can be a good start, what can lead to a safer internet environment.

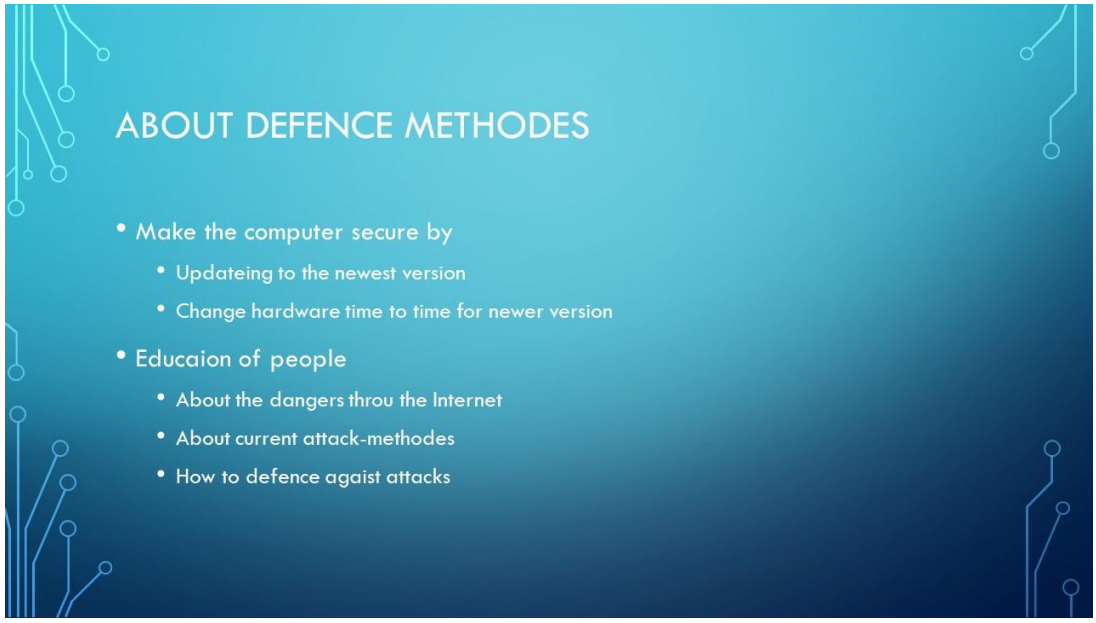

THE NEED TO DEVELOP INFORMATION SECURITY AWARENESS
PETER STRANSZKI

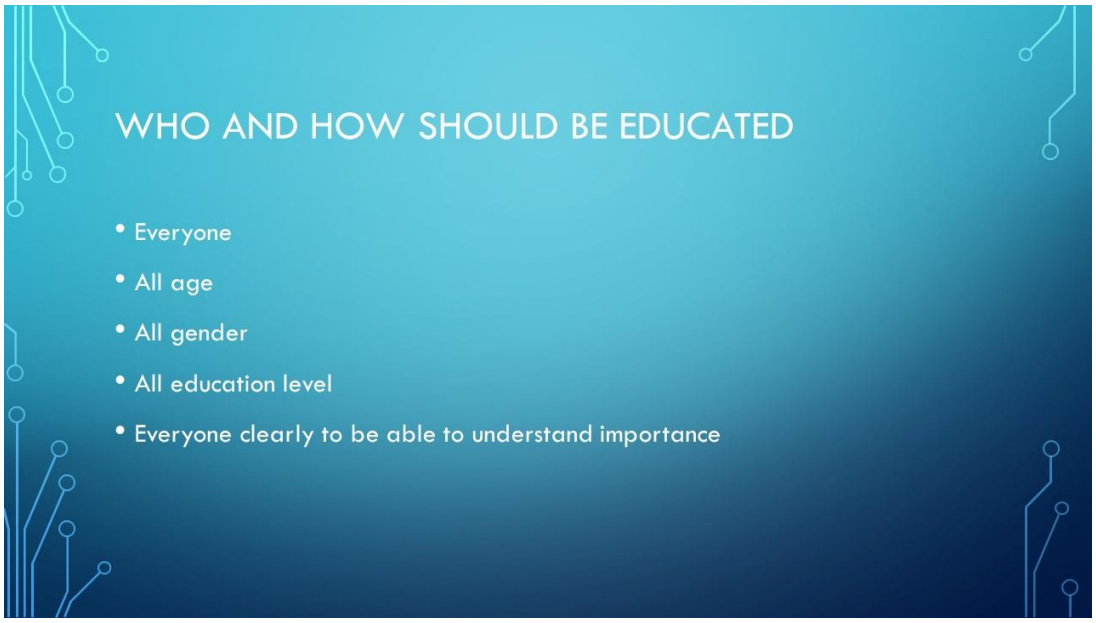

OVERVIEW
• The evolution of the Internet
• Problems of the fast evolution
• Main attacking methodes
• About defence methodes
• Why is education important

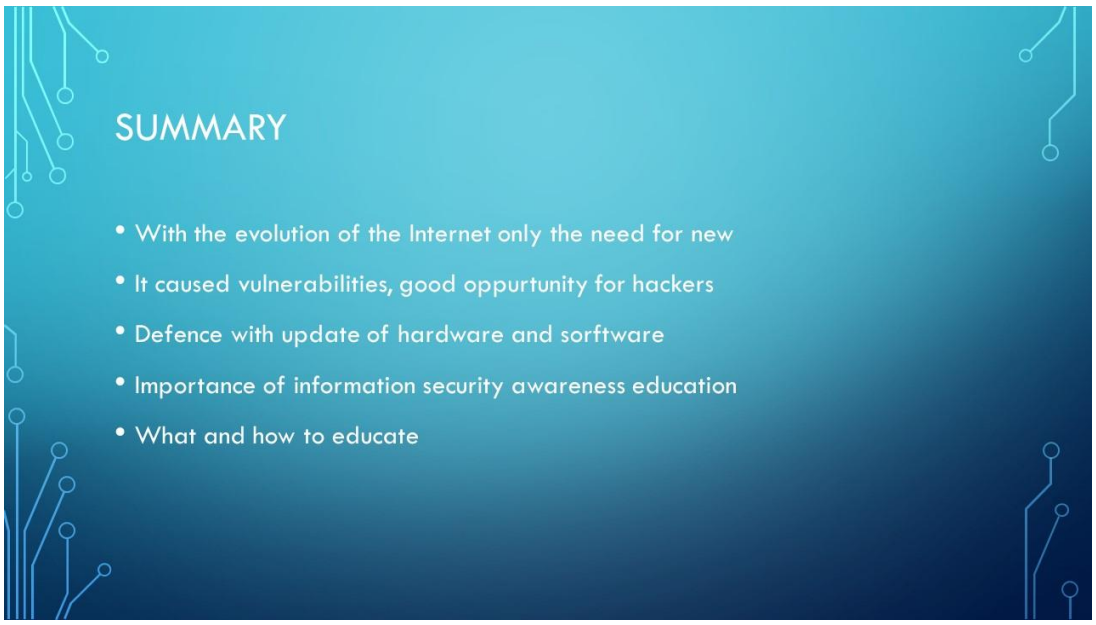

THE EVOLUTION OF THE INTERNET
• Early 90s:
• Only few websites
• Few email address owner
• Few information
• Nowdays:
• Lot of information
• Lot of public services (shop, bankig, communication, do official bussines)
• Part of everydays life

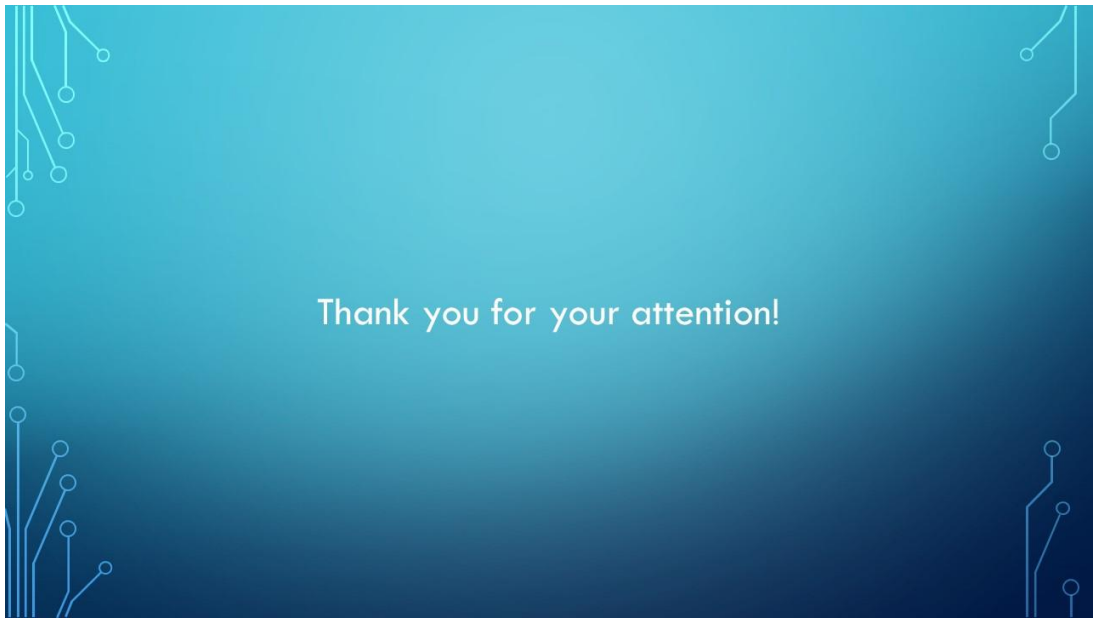

PROBLEMS OF THE FAST EVOLUTION
• Only the advatage presented
• Lack of time for testing and education
• Need for using the newest solutions


MAIN ATTACKING METHODES
• Take advantage of the security gaps
• Deceive users
• With fake webpages
• With fake calls


ABOUT DEFENCE METHODES
• Make the computer secure by
• Updateing to the newest version
• Change hardware time to time for newer version
• Educaion of people
• About the dangers throu the Internet
• About current attack-methodes
• How to defence agaist attacks


WHO AND HOW SHOULD BE EDUCATED
• Everyone
• All age
• All gender
• All education level
• Everyone clearly to be able to understand importance


SUMMARY
• With the evolution of the Internet only the need for new
• It caused vulnerabilities, good oppurtunity for hackers
• Defence with update of hardware and sorftware
• Importance of information security awareness education
• What and how to educate


Thank you for your attention!

Haya Altaleb[1], Zoltan Rajnai[2]: The Role and Impact of the Network Equipment Security Assurance Scheme (NESAS) in the 5G Era

Correferatum

The Network Equipment Security Assurance Scheme (NESAS) is a critical security assurance framework for the mobile industry, designed to standardize security assessments and evaluate equipment vendors, ensuring compliance with legal guidelines. This study provides an overview of NESAS, detailing its definitions, functions, and significance. Additionally, it explores the implications of the 5G digital revolution, addressing key concepts, associated risks, and potential enhancements. Furthermore, the study examines the European Union's cyber risk assessment, highlighting major threats, the 5G risk landscape, and recommended governmental actions. In light of the increasing need for robust security evaluation methods, the importance of maintaining secure telecom infrastructure and systems throughout their lifecycle is emphasized. This abstract underscores NESAS's benefits for network operators, equipment vendors, regulators, and the broader industry, advocating for diversified resources, continuous risk

[1] ORCID: 0000-0002-1442-4037
[2] ORCID: 0000-0002-9139-736X

assessments, and collaborative efforts between public and private sectors to mitigate cybersecurity threats effectively.

The rapid digital transformation across various sectors has significantly raised cybersecurity concerns. The proliferation of mobile devices, smart applications, IoT, AI, and cloud platforms has expanded the boundaries of security control. Identifying cybersecurity vulnerabilities and associated risks is essential, especially with the advent of 5G technology. This study investigates the advantages of 5G, new risk landscapes, system evaluations, and security management strategies, addressing the persistent challenge of cyber-attacks exacerbated by human errors.

NESAS, developed by 3GPP and GSMA, is a globally recognized security assurance framework that defines security requirements, test cases, and evaluation methodologies for network equipment. It ensures that network products meet stringent security standards, providing transparency and confidence to consumers and stakeholders. NESAS facilitates security by design, encouraging vendors to maintain high security levels throughout the product lifecycle.

5G represents a significant technological leap, promising enhanced speed and the realization of real-time cloud applications. However, it introduces new security challenges and risks. The 3GPP SA3 working group has identified 17 key security areas, including authentication, network slicing security, and privacy. Comparing 4G

and 5G, the latter offers improved security mechanisms but also presents unique vulnerabilities due to its advanced features and extensive connectivity.

The EU has conducted comprehensive cyber risk assessments, identifying hardware failures, software bugs, and human errors as primary threats. The 5G risk assessment emphasizes confidentiality, privacy, and the dangers of dependency on single suppliers. The EU certification framework, developed by the European Commission and ENISA, aims to enhance trust in digital products and services by establishing rigorous security standards and evaluation processes.

To date, NESAS has been accepted in 17 countries, reflecting its growing influence and the mobile industry's commitment to robust security practices. The adoption of NESAS helps streamline security requirements, reducing duplication of efforts and facilitating a cohesive approach to telecom security across different regions. By encouraging a culture of security by design, NESAS supports the industry's goal of maintaining high-security standards in an increasingly connected world.

The scheme's voluntary yet rigorous certification process, including third-party audits, ensures that network equipment complies with predefined security standards, making it a valuable tool for national security authorities and mobile operators alike. As the telecom landscape evolves with advancements like 5G, NESAS remains a

critical component in safeguarding network infrastructure against emerging threats.

The widespread acceptance and implementation of NESAS underscore its importance in driving global harmonization of telecom security standards, ultimately contributing to a more secure and resilient mobile communications environment.

This study underscores NESAS's pivotal role in securing the mobile industry, highlighting its impact on 5G security and the broader digital ecosystem. By standardizing security assessments and fostering collaboration between public and private sectors, NESAS enhances the resilience of telecom infrastructure. Future research should explore global adoption and comparative analyses of 5G policies to refine and expand security frameworks in the digital age.

Keywords: NESAS, cybersecurity, security certifications, 5G.

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

The Role and Impact of the Network Equipment Security Assurance Scheme (NESAS) in the 5G Era

Haya Altaleb, Prof. Dr. Rajnai Zoltan

Doctoral School on Safety and Security Science
Bánki Donát Faculty of Mechanical and Safety Engineering

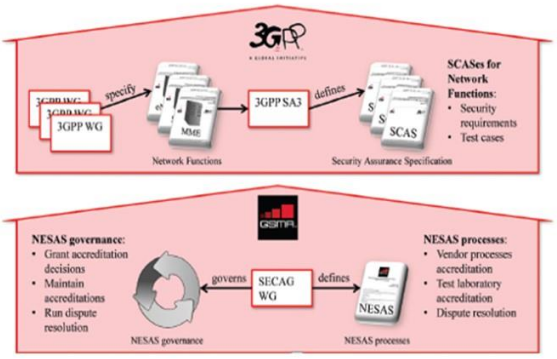
Main objectives of this research

- Overview NESAS definitions, explanation, importance, and benefits.
- The concepts of the 5G Digital Revolution, risk aspects.
- Discuss the European Union Cyber Risk Assessment over the recent years i.e. 5G risk assessment in the EU countries, and some suggestions about governments' action.
- The proper technique to produce security evaluation and guarantee telecoms infrastructure and systems throughout the offering lifecycle focusing on developing security systems in all sectors and businesses and maintaining the continuity of improvement.

Overview NESAS definitions, explanation, and importance

(NESAS) **The Network Equipment Security Assurance Scheme (NESAS) is a security assurance framework for improvements in the mobile industry** which was established as an action by the 3rd Generation joint Project (3GPP), standards associations for mobile Telecommunications, Global System Mobile Application (GSMA), international manufacturer association for mobile operators as shown in the Figure.

The 3GPP defines the security requirements of products and test cases, and it is specified in security assurance specifications (SCAS). GSMA represents the methodologies and requirements of vendor process security. In addition, it assigns auditors and lists test labs.



The Importance of NESAS

-Making network equipment security measurable and visible.

-Comprised of both technical aspects, expressed by equipment tests and organizational aspects.

-Primarily focused on legal and technical aspects of product development.

-Making the product's cybersecurity clear to customers surely will facilitate the purchases, and the cyber risk tolerance will be obvious to the buyers.

The Benefits of NESAS

For Network Operators: Raise confidence, increase transparency and provide background for use in procurement processes.

For Equipment vendors: lowers duplication of assurance and tests, Increases vendor ability to maintain security, reduces the load levels, and encourages comprehensive security across vendor community.

For Regulators and national security authorities: Funded totally by the industry, Consider a global scheme, a Cost-effective scheme with benefits that provide security gains, The ability to extend if needed, and reuse models to deliver security gains.

For The Industry: The level of security assurance of network equipment is visible and understandable, Across the vendor community, it encourages security by design culture and highlights vendor ability to achieve and maintain security levels, The cost of security is shared among vendors and across all operators, Security assurance scheme is accepted and funded by the industry, Single assurance scheme that is universally applicable. NESAS is designed to be updated when needed.

The concepts of the 5G Digital Revolution

5G digital revolution, considered a speed boost, allows the future smart city and connects the social division on digital transformation considering data as the new oil.

5G applications

- Mobile/Wireless systems.
- IoT and Machine-to-Machine (M2M)
- Network Functions Virtualization
- Intelligent Transport Systems
- Broadcasting.
- Securing AI.

The European Union Cyber Risk Assessment over the recent years

EU certification schemes contain a complete collection of technical conditions, criteria, and methods. Each EU scheme will define:

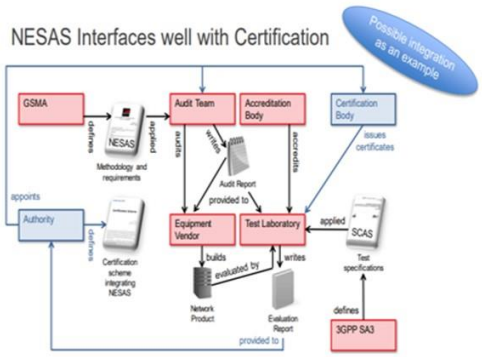
-The classifications for all products and services.

-The standards or technical characteristics.

-The evaluations process.

-The levels of assurance (basic, substantial, and high).

-The certificate will be accredited in all EU States for security purposes.



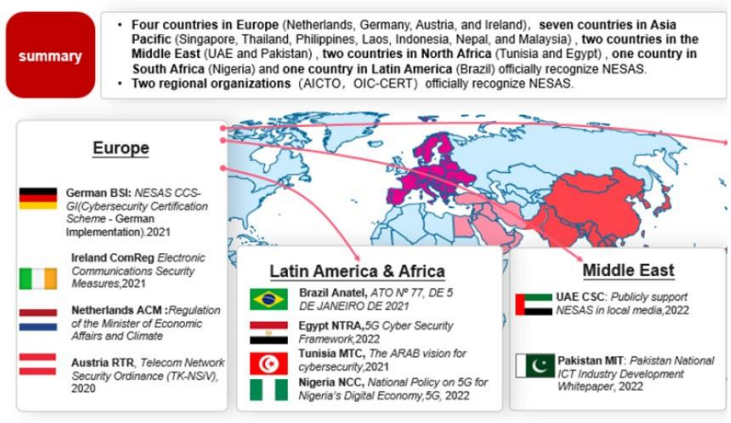
The importance of the Collaboration between the private sector and government

It's is essential for each critical infrastructure and that will enhance the relationship between the customers, the providers, and the suppliers.

In order To develop security systems in all sectors and businesses and maintain the continuity of improvement, the governments should focus on:

1. **Diversity of sources and not rely on one resource**; this will reduce the risk and improve intelligent networks such as 5G and fiber.
2. **Encouraging competition to ensure sustainability,** higher quality, innovation, creativity, and more concentration on cyber security.
3. **Identify the proper toolbox** for efficient risk mitigation and practical measurements and specify the certifications with suitable risk asses.
4. **Ensure testing for equipment, systems, and software**. Continuous risk assessment and program evaluation from different vendors and supply chains.
5. **Improve the industrial ability in equipment manufacturing**, laboratory testing, conformity evaluation, and cyber security systems, on the country's level.

NESAS recognition: completed official recognition in 17 countries



Conclusion

This Study presents a literature overview of the 5G roll-out and the Network Equipment Security Assurance Scheme (NESAS), which is considered an assessment framework for secure outcome development and lifecycle processes and delivers tests for the security evaluation of network equipment.

1. It facilitates the cyber risk tolerance to be obvious to the buyers.
2. Measuring security level is not easy to create a system beyond IoT to develop security certifications that need emerging technologies and cloud computing cooperation between different agencies.

Hopefully, in the future, it will be recognized globally by industry leaders as a baseline for security requirements, security assessments of network equipment, and evaluation of equipment vendors.


ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY
Thank You For Your Attention
@haya.altaleb
Lecturer and Researcher
@Obuda University
Safety and security science
Research Gate
Google Scholar
Linktree

Lourdes Ruiz S.: ICT and telecom Supply Chain, evolving threat Landscapes, countermeasures, and Solutions

Correferatum

Information and Communication Technology (ICT) supply chain expands and intertwines with the telecommunications sector. The landscape of cyber threats undergoes continuous evolution, presenting complex challenges to security practitioners and stakeholders. This abstract delves into the intricate relationship between ICT supply chain dynamics, telecom infrastructure, and the multifaceted threat landscape while exploring effective countermeasures and innovative solutions to mitigate risks.

The ICT supply chain serves as the backbone of modern telecommunications networks. It is global, complex, and interconnected. It comprises a global network of suppliers, manufacturers, vendors, and service providers. However, this interconnected ecosystem also introduces vulnerabilities.

The Telecom Supply Chain Threat landscape includes

- Geopolitical factors such as trade conflicts, country vendor restrictions, and natural disasters cause disruptions in the supply chain, uncertainty, and increased costs.

- Strict regulations increase compliance costs and prevent market access.

- Third-party reliance brings security, operational, legal, and financial risks, data breaches, and supply chain disruptions.

- Lack of security skills concerning data science, AI implementation, security operations, legacy network, standard development, etc.

- More connectivity implies a larger attack surface due to digitalization, cloud services, and IoT, which increases cybersecurity risks that affect customer and supplier assets.

Countermeasures:

- Securing IoT Devices

- Security education, formal or informal, offered to all the members involved in the supply chain, especially the most vulnerable customers.

- Network performance reliability, including threat forecasting, simulations, and modeling

- End-to-end visibility, traceability, vendor management monitoring, and requirement compliance in order to reduce third-party risks

- Build robust relationships within the mobile ecosystem actors, sharing information, best practices, and concerns about strengthening high-security levels.

- Supply chain resilience to face geopolitical threats, sourcing flexibility, and supplier diversification.

- Risk assessments and supply risk management programs

Conclusions

- ICT supply chain security is an ongoing concern among all supply chain participants. The risks associated with the supply chain need to be recognized and addressed due to the importance of connectivity and communication globally and for critical infrastructure security assurance.

- A holistic security approach comprising stakeholders, government, and regulators must approach the supply chain globally to formulate security frameworks and avoid fragmentation.

- A balance between connectivity and security is required to face the evolving threat landscape.

- Adaptation and resilience to new threats are vital for telecom companies to ensure security, build customer trust and loyalty, and aid regulation compliance.

- Environmental sustainability and ethical considerations, such as component traceability for equipment manufacturers, will provide a competitive advantage among digital businesses.

- A service-driven supply chain will be a differentiating aspect for increasing revenue.

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

ICT and Telecommunications Supply Chain: Threat Landscape and Countermeasures

Lourdes Ruiz S. PhD

Prof. Dr. Rajnai Zoltan

Agenda

- Telecom SC
- ICT SC
- Threats, Risks
- Solutions

2

ICT Supply Chain

ICT→ Consolidation of telecommunications, networks, and computer systems to facilitate the creation, exchange, management, process, and transmission of information

Telecom Blended into the ICT landscape → Enables data transfer within various applications, devices, and platforms

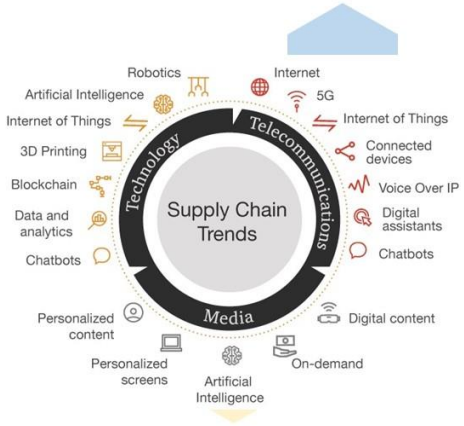
Supply Chain

- Different processes that transform raw materials and components into finished goods for end users.

✓ Global
✓ Complex
✓ Interconnected

- **Influences every aspect of modern life**

3



Telecom Supply Chain Threats

- Geopolitical Factors

Trade conflicts, country vendor restrictions, natural disasters, international cooperation → disruption SC, uncertainty and increased costs

- Regulatory Compliance

Strict regulations increase compliance costs , prevent market access

- Third party risks

SC global→ relies on different vendors, suppliers, contractors, service providers → security, operational, legal, financial risk, data breaches, SC disruptions

- Lack of security skills: **gap security knowledge**

(Data science, AI implementation, Security Operations, legacy network, standard development)

Presentation title 4

Threat Landscape (cont)

Cybersecurity

- **More connectivity**→ larger attack surface (digitalization, cloud services, IoT)
- **SC attacks:** combination of 2 or more attacks on the supplier, which are utilized to attack a target (another supplier or customer) to gain access to their assets.

Types of Attacks Customer	Customer Assets
Trusted Relationship: certificate, update, backup	Data: payment, documents, email, credentials, user activity, applications, location
Drive-by compromise: website malicious scripts	Intellectual property
Phishing: supplier impersonation	Software: customer product source code
Malware infection: ransomware, remote access trojan	Processes: internal, configuration
Physical or modification: hardware, physical intrusion	Bandwidth: DDoS, send spam
Counterfeiting	Financial: cryptocurrency, bank account, money transfer
	People: Position or knowledge

Types of Attacks Supply Chain	Supplier Assets
Malware Infection: spyware to gain access to employee credentials	Pre-existing software: web servers, app, cloud, monitoring systems
Social Engineering: phishing, fake apps, Wi-Fi impersonation	Software libraries
Brute-Force Attack: get SSH password or web login	Code
Software vulnerability exploit: SQL injection, buffer overflow	Configuration: firewall rules, URLs, passwords
Configuration vulnerability exploit: advantage of configuration issues	Data: suppliers, customers,
Open-Sources Intelligence (OSINT): look online for API keys, credentials	Processes: updates, backups, certificates
Counterfeiting	Hardware: chips, USB, etc.
Physical or modification: hardware, physical intrusion	People: access to data, infrastructure
	Other Suppliers

Countermeasures

- Connectivity: securing IoT devices
- Security education (formal , informal) : members SC, customers (most vulnerable)
- Network performance Reliability: threat forecasting, simulations, modeling
- End-to-end supply chain visibility, traceability (reduce third party risks), vendor management monitoring, requirement compliance
- Build robust relationships SC(stakeholders, operators, producers, etc.→ sharing information, best practices , concerns
- SC resilience: face geopolitical threats, sourcing flexibility, supplier diversification
- Risk assessments, supply risk management program

Conclusions

- ICT supply chain security is an ongoing concern among all supply chain participants.
- The risks associated with the SC need to be recognized and addressed due to the importance of connectivity and communication globally and for critical infrastructure security assurance
- ICT and Telecom are closely connected→ 5G network deployment makes integration seamless because it requires telecom infrastructure and ICT components
- **Holistic approach:** collaboration of stakeholders, government, regulators should approach the supply chain as global to formulate security frameworks.
- Connectivity and security balance
- Adaptation and resilience to new threats are vital for telecom companies to ensure high-security→ building customer trust and loyalty, aids regulation compliance
- Environmental sustainability and ethical considerations (component traceability equipment manufacturers) → competitive advantage among digital businesses.
- Service-driven supply chain will be a differentiating aspect for increasing revenue

7

Thank you

Yue Wu: Mobile Communication Evolution and the development of 5G in China

Correferatum

Mobile communication has evolved through four generations since 1980, leading to the current fifth generation, or 5G, which began development in 2012. Each generation marked significant technological advancements. 5G represents a transformative expansion in mobile technology, supporting a wider range of applications beyond traditional mobile voice and data. 5G integrates various use cases and is defined by the development of Long Term Evolution (LTE) or 4G, enhancing data speeds and network efficiency. New Radio (NR) technology and the 5G Core Network (5GCN) were introduced by the 3rd Generation Partnership Project (3GPP) in 2018, setting the standards for global mobile communication. These standards were designed to facilitate broader connectivity and include provisions for connecting non-3GPP networks. 5G development featured significant global milestones including the first 5G NR specifications by 3GPP in 2017, initial trials in China, and South Korea's successful 5G spectrum auction in 2018. The rollout faced challenges like COVID-19, which delayed the implementation of subsequent 5G standards like Release 17. A comprehensive literature review and content analysis were conducted to understand 5G standardization and China’s role in it,

utilizing resources from prestigious journals, official news, and governmental reports.

Standards are essential for security, interoperability, and strategic deployment of technologies globally. 3GPP plays a crucial role in developing these standards, which are vital for technological integration and address geopolitical and security considerations. Standards development involves a complex mix of negotiations among international stakeholders, including regulatory bodies, industry forums, and standard development organizations (SDOs).

China has significantly invested in 5G, leading globally in the number of 5G base stations. Chinese companies like Huawei are major contributors to 5G patents and standards. China's strategy extends to leadership roles in international standard-setting organizations, influencing global telecommunications standards. China's influence in standardization includes active contributions to ITU and 3GPP. From 2017 to 2021, China led many key ITU-T Study Groups, shaping 5G protocols and infrastructure. China's efforts aim not only at national but also at global standardization, affecting international policies and practices. The continuous evolution from 5G to future generations like 6G highlights the need for comprehensive strategies that encompass technological advancements and geopolitical aspects of telecommunications. China’s approach, emphasizing both technological leadership and

international collaboration, offers insights into the future of global mobile communications.

The future of mobile communication will be significantly influenced by the interplay of technology, policy, and international relations, with standardization playing a critical role. The shift from national to global strategies in telecommunications standardization underscores the importance of collaborative and innovative approaches.

China proactively advanced 5G technology by establishing the IMT-2020 Promotion Group in 2013 and later initiating the IMT-2030 for 6G. By 2021, China had deployed over 1.43 million 5G base stations, indicating rapid infrastructure development. The Chinese government aims to extend 5G coverage to rural areas and increase its global user base significantly by 2023. China leads in 5G development indicators such as publications, patents, and standard contributions. Despite this, the collaboration among Chinese patent holders is not as robust as that in the U.S., which is also a major player in 5G technology. Large Chinese companies dominate the standardization landscape, with significant contributions to the technical specifications managed by 3GPP. China's strategy in 5G standardization is to leverage its technological advancements and market size to influence international standards. It participates in mutual standardization recognition discussions and has established significant bilateral agreements to promote its standards

internationally. China also focuses on developing a new internet system under the "Decentralized Internet Infrastructure" to enhance network reliability and efficiency. China's involvement in ITU has been substantial, with Chinese representatives leading various study groups and contributing to the development of global 5G standards. The Standardization Administration of China synchronizes the implementation of national and international standards, facilitating China's influence in global standardization efforts.

In conclusion, China's leadership in 5G development and standardization positions it as a key player in the global telecommunication landscape, driving the adoption of its standards and technologies worldwide. This influence is expected to grow as China continues to advance.

5G STANDARDISATION: CASE STUDY IN CHINA

- YUE WU
- PROF. DR. RAJNAI ZOLTÁN

· Obuda University
- Doctoral School on Safety and Security Science;
- Donát Bánki Faculty of Mechanical and Safety Engineering

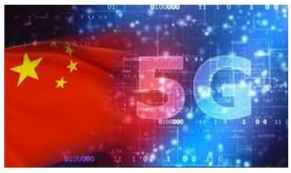
INTRODUCTION

- **2012-2015,** research stage in 5G; **2017,** initial 5G specification & test in China; **2019,** the 1st 5G mobile smart phone
- Standards - **hardware infrastructure & software** that runs on top of components, ensuring that various devices and equipment can work together in a **shared system**
- Determining the standards for the future generation network - **national security, individual safety, and the global deployment of equipment**
- the3rd Generation Partnership Project (3GPP) (**telecommunication organization**)-in charge one of international standards for telecommunication

METHODOLOGY

Secondary research methodology/literature review (recent years' research)

Content analysis



RESULTS

- The development of 5G in China
- 5G standardization in China

A. THE DEVELOPMENT OF 5G IN CHINA

1) THE **INFRASTRUCTURE AND DEPLOYMENT** OF 5G

2) THE **MAIN FORCES** OF 5G DEVELOPMENT

1) THE INFRASTRUCTURE AND DEPLOYMENT OF 5G

- **2016**, the Ministry of Industry and Information Technology (MIIT) – R&D tests for 5G technology
- **2019**, started deploying 5G networks - **2020**(690,000 5G base stations) – **2021**(1.43 million 5G base stations, over 60% of the worldwide total) – **2023**(3.37 million 5G base stations, 805 million 5G mobile phone users in China)
- **2021**, MIIT(promotion group in 2019)-plan preparations for the commercial launch of **6G** systems in 2030
- **2021-2025**, a focus on 5G technology in **industrial** settings, particularly in manufacturing, 10,000 5G factories
- **New infrastructure:** information infrastructure, integrated infrastructure, and innovation infrastructure

2) THE MAIN FORCES OF 5G DEVELOPMENT

- **Publications, patents, standard-essential patents (SEPs), and contributions to standards** are crucial factors that indicate the progress of technology development in 5G （China, US, Korea）
- Telecommunications **companies** - 5G-related technology and intellectual property (Huawei, **13.53%** of all global 5G patent families)
- **lack core patents,** resulting in a lower quality of innovation compared to the US; **level of collaboration** among Chinese patent holders is not as strong as it is in US
- weighted standard contributions: China>US>Sweden>Korea>Finland>Japan (**92%**)
- The biggest 5G technical 3GPP contributions and 5G approved technical 3GPP contributions are 21,799 globally (Huawei: 6,599)

HUAWEI

B. 5G STANDARDIZATION IN CHINA

1) CHINA'S **COMPETENCE** IN 5G STANDARDIZATION
2) CHINA'S EFFORT IN 5G STANDARDIZATION IN **ITU**
3) THE ROLE OF **STANDARDIZATION ADMINISTRATION** OF THE PEOPLE'S REPUBLIC OF CHINA
4) THE LAUNCH OF **5G LIGHTWEIGHT TERMINAL INDUSTRY STANDARDIZATION**
5) THE INTRODUCTION OF **DECENTRALIZED INTERNET INFRASTRUCTURE (DII)**

1) CHINA'S COMPETENCE IN 5G STANDARDIZATION

- **Leads** in 5G-related contributions to 3GPP
- pursuing **mutual standardization** recognition bilaterally or regionally
- **international standard-setting organizations** - Chinese representatives with qualitative and quantitative effects (the largest at the ITU, the 5th largest at the ISO, and making up 10% of all attendees at the IETF)

2) CHINA'S EFFORT IN 5G STANDARDIZATION IN ITU

- **2017 - 2021,** four primary ITU-T Study Groups (SG) were involved in addressing 5G-related matters: **5G issues associated with FG IMT-2020; transport network standards; evaluated energy efficiency and 5G; formulated standards for 5G-based network protocols**
- **SG 13:** China Mobile - IMT-2020 5G standardization efforts (184/731/1389) 中国移动 China Mobile
- **SG 15:** the **most focus of China** with 374 unique submissions (over last 10 yrs)
- **SG 5:** contributed 47% (**24**/**51**) of the 5G-related work items; **not** as significant compared to other study groups
- **SG 11**: **sole significant** contributor thus far

3) THE ROLE OF STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA

- **2001** – charge of all standards-related tasks in China
- **primary role** - manage and synchronize the implementation of national and international standards within China and for Chinese projects abroad (BRI)
- Standards 2035 - **new initiative** to review and extend national and international standards strategy:
  - highlights the significance of technical standards in promoting the growth and development of the country's economy.
  - outlines how these standards can be utilized to achieve China's ambitious geopolitical objectives.

4) THE LAUNCH OF 5G LIGHTWEIGHT TERMINAL INDUSTRY STANDARDIZATION

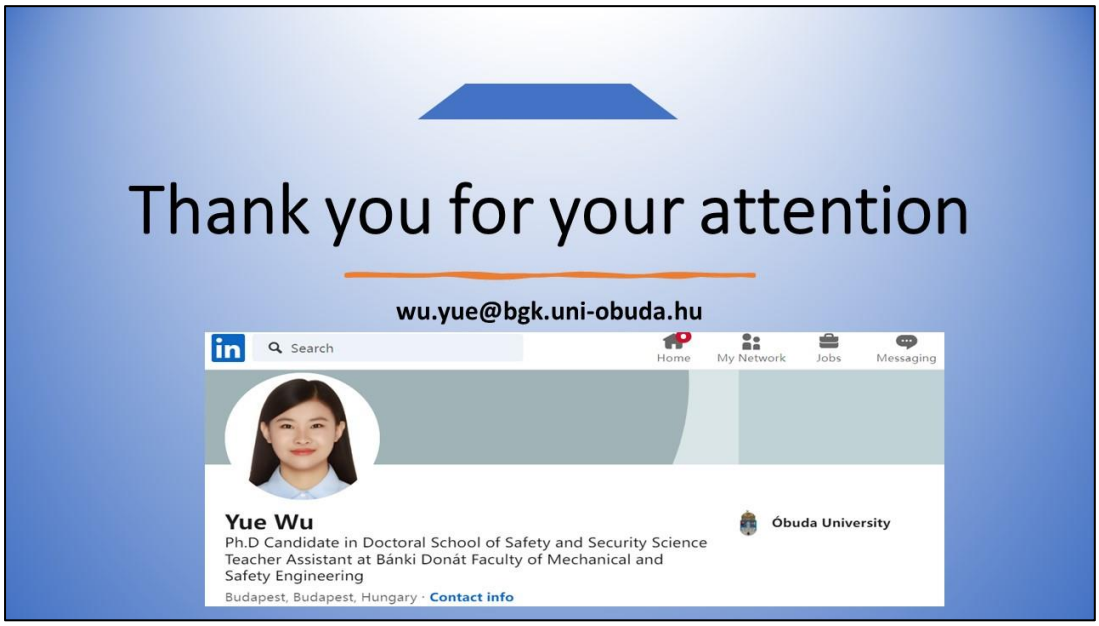
- 3GPP R17 standard includes the **5G Lightweight (RedCap) terminal technology** - industrial wireless sensors, video surveillance, and wearable devices, and is beneficial for the extensive commercial deployment of 5G networks
- simplify terminal design, optimize 5G system configuration and business processes, and achieve design goals like reducing terminal chip/module costs and power consumption. It can also create new business opportunities for scenarios like 5G industry applications.

5) THE INTRODUCTION OF DECENTRALIZED INTERNET INFRASTRUCTURE (DII)

- **2018** – Huawei - the concept of **"decentralized internet infrastructure"** (DII) - establish a trustworthy network by creating interconnected data logs (allows for the use of advanced tools like deep packet inspection and censorship)
- **2019** - Chinese delegations - "decentralized internet" model and its core technical components ("New IP")
- Three related technologies:
  - **Object identifiers (OIDs)**
  - **Distributed ledger technologies (DLT)**
  - **Network 2030**

CONCLUSION

- leading development of 5G **infrastructure** & guiding the early **standardization** of 5G protocols
- if China wants to exert influence in the standardisation space, it needs a complementary set of institutional, organisational, and negotiating skills **beyond an outstanding patent portfolio**, and higher quality of **innovation**


Thank you for your attention
wu.yue@bgk.uni-obuda.hu
Search
Home
My Network
Jobs
Messaging
Yue Wu
Ph.D Candidate in Doctoral School of Safety and Security Science
Teacher Assistant at Bánki Donát Faculty of Mechanical and Safety Engineering
Budapest, Budapest, Hungary · Contact info
Óbuda University

Published by the Signal Department of the Ludovika University of Public Service

www.comconf.hu

HU ISSN 2061-9499

***

University of Public Service
Signal Department
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15