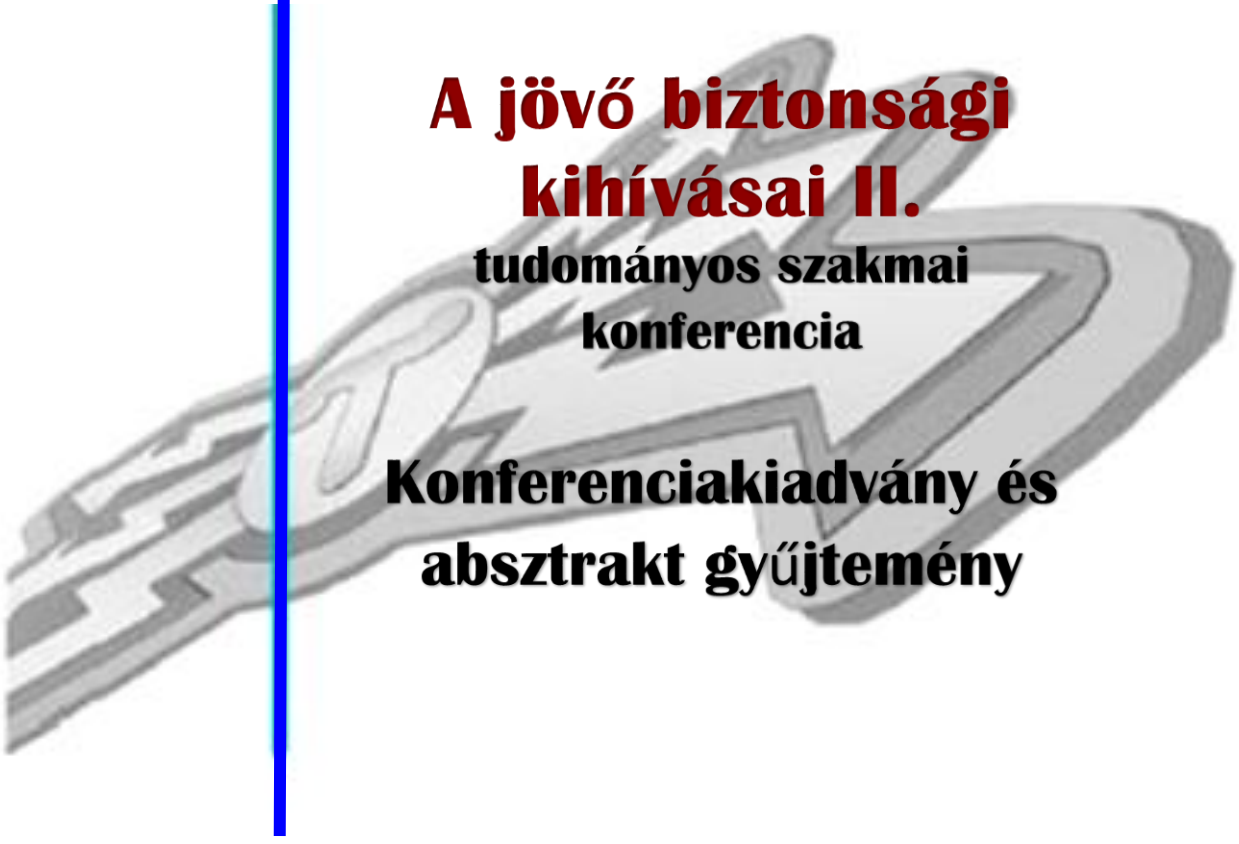
HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2022



A jövő biztonsági kihívásai II.

tudományos szakmai konferencia

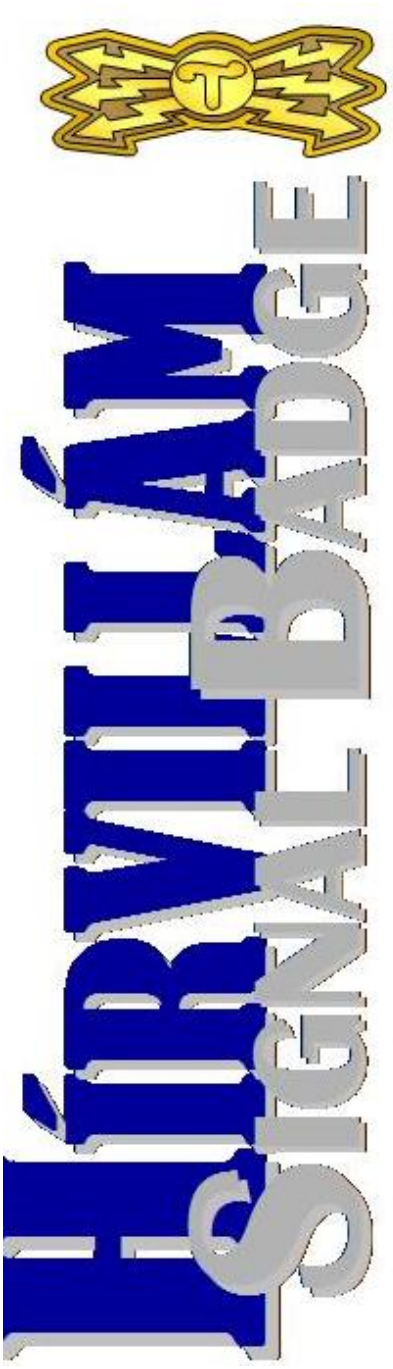
Konferenciakiadvány és absztrakt gyűjtemény

2022. november 17.

HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem, Híradó Tanszék tudományos időszaki kiadványa

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

Budapest, 2022



HU ISSN 2061-9499

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

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

2022. november 17-én a Puskás Tivadar Műszaki Szakkollégium, valamint a Hírközlési és Informatikai Tudományos Egyesület Információbiztonsági Szakosztálya által megrendezésre került az „A jövő biztonsági kihívásai II.” című szakmai tudományos konferencia. A konferencia alapvető célja egy tudományos szakmai fórum biztosítása a kutatási eredmények bemutatása, ismeretterjesztés, továbbá kapcsolatépítés céljából a téma iránt érdeklődök, a hadtudomány területén kutatást folytatók számára. A konferencián összesen 19 kutató, doktorandusz, mester- és alapszakos hallgató mutatta be kutatási eredményeit, melyek közül jelen kiadványban a szerzők hozzájárulásával 12 került megjelentetésre.

Jelen kiadványban a szerkesztőbizottság az egyes előadásokhoz készített absztraktokat és előadásokat gyűjtötte össze, amelyeket nagyon nagy örömmel bocsájt rendelkezésre a Kedves Olvasóknak.

Budapest, 2022. november 17.

Dr. habil. Kerti András
a Szerkesztőbizottság
elnöke

A konferencia programja

A jövő biztonsági kihívásai II. konferencia		
2022. 11. 17. Oktatási Központ, IV. emelet, 415		
Időpont	Előadó neve	Előadás Címe
09:50-10:00	O-415: Konferencia megnyitása	
I. szekció: Szekcióvezető: Dr. Tóth András, Dr. Farkas Tibor		
10:00-10:20	Krasnyánszki Brúnó	Az Orosz Föderáció kiberhadviselési műveleteinek változása a különböző konfliktusok során
10:20-10:40	Vattai Eszter	Az OSINT katonai vonzatai
10:40-11:00	Molnár Anna	A műveleti NATO harca a közös biztonság jegyében
11:00-11:20	Sipos Ákos	Háborús propaganda / propaganda háború
11:20-11:40	Bálint Áron	Italy's Military Development and Security Co-operations
11:40-12:00	Prilenszky András	Magyarország világűr politikája a 21. században
12:00-12:30	Szünet	
II. szekció: Szekcióvezető: Dr. Magyar Sándor, Orbók Ákos		
12:30-12:50	Dub Máté	Oroszország és az álhírek terjesztése
12:50-13:10	Schiller Gábor	Liman és Herszon
13:10-13:30	Kugler Péter	Békeműveletek és kognitív reziliencia
13:30-13:50	Székely Lóránd	Az okos eszközök és a vezetés kapcsolata
13:50-14:10	Nimsz Vivien	Az ellátási láncok kiberbiztonsági kihívásai a munkavállalók aspektusából
14:10-14:30	Laska Pál	Cinemeducation, avagy új utak keresése a biztonságtudatossági oktatásban
14:30-15:00	Szünet	
III. szekció: Szekcióvezető: Dr. László Gábor, Dr. Bányász Péter		
15:00-15:15	Tóth András	The applications of the Cloud of Things in the defence sector

15:15-15:30	Bús Nikolett Katalin, Magyar Sándor	The role of Security Operations Centres in supporting cyber security
15:30-15:45	Kerti András	Security of unclassified information
15:45-16:00	Ináncsi Mátyás	Social media sentiment of the russian-ukranian conflict
16:00-16:15	Bús Nikolett Katalin	Information security incident management- In a Hungarian company's programme
16:15-16:30	Sz. Podmaniczky Katalin	A kontrollrendszer a védelem szolgálatában
16:30-17:00	Konferencia zárása	

Krasnyánszki Brúnó: Az Orosz Föderáció kiberhadviselési műveleteinek változása a különböző konfliktusok során

Absztrakt

Empirikus szekunderkutatásomat arról készítettem, hogyan változtak meg az Orosz Föderáció fegyveres testületeinek kiberhadviselési műveletei az idő folyamán. A kutatásom első szakaszában tanulmányoztam a kiberhadviselési műveleteket és kialakítottam egy osztályozási sémát kutatásomhoz amelyhez a Nemzetközi Szabványügyi Szervezet (ISO) Nyílt rendszerek Összekapcsolása (ISO 35.100 - OSI) szabványt vettem figyelembe és az OSI 7 osztályába soroltam be a műveleteket függően attól, hogy az adott műveletet melyik térben hajtották végre. Kutatásomban megvizsgáltam a számomra négy legfontosabb mérföldkőnek ítélt kiberműveleteket. Ezek a 2007-es Észtország elleni kibertámadás (itt az Oroszok csak a kibertéren keresztül okoztak kárt), a 2008-as Grúz konfliktus (hibrid hadművelet melynek során alkalmaztak kiber, információs, gazdasági, diplomáciai és kinetikus eszközöket is!), a 2014-es Krími konfliktust (ami szintén hibrid hadművelet volt) és végül a jelenlegi (2022) Orosz-Ukrán konfliktust. Ezen konfliktusok kapcsán gyűjtöttem össze a nyilvánosan rendelkezésre álló adatbázisokból a támadások mennyiségét, típusát, intenzitását és minőségét. Melyet osztályoztam és statisztikát készítettem, hogy ezeket elemezni tudjam.

Konferencia előadásom során igyekeztem bemutatni, hogy mennyi aspektusa van a kiberműveleteinek kezdve a hagyományos informatikai műveletekkel (korábbi nevén Számítógép-hálózati hadviselés), majd az információs műveletek különböző aspektusait mutattam be a kiber műveleti térben.

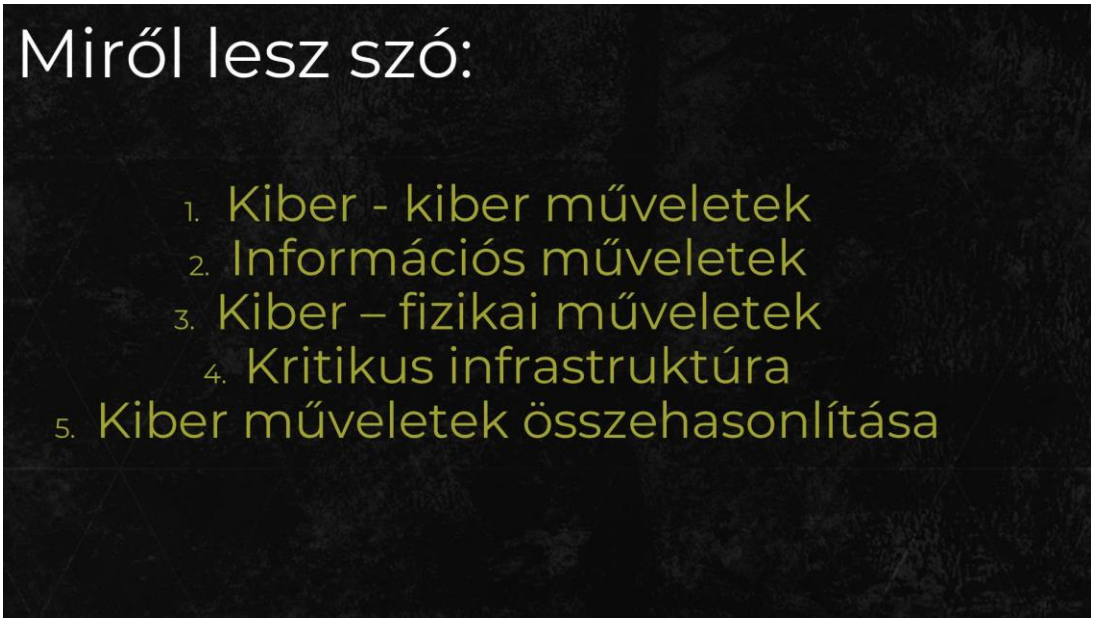
Előadásom során igyekeztem továbbá szemléletesen bemutatni a vizsgált konfliktusokat és konzekvenciáit a kiberműveletek szemszögéből.

Konklúzió:

Az Orosz Föderáció a vizsgált műveleti térben (kibertér) 2022-ig nagyon hatékony tudta alkalmazni a kiberműveleteit egymagában és kinetikus/hibrid eszköz tárát támogatva, de a jelenlegi konfliktus során hullámzó teljesítményt tud csak nyújtani. Ez eddigi ismereteim szerint nagyban köszönhető Ukrajna szövetségeseinek, akik felkészítették az ilyen támadásokra való védekezésre.

Kulcsszavak: Kiberhadviselés, Orosz Föderáció, Kiber – Fizikai műveletek, Információs műveletek, változás


Az Orosz Föderáció kiberhadviselési műveleteinek változása a különböző konfliktusok során
Krasnyánszki Brúnó
ORCID: 0000-0002-5672-4919
PUSKÁS TIVADAR
MŰSZAKI SZAKKOLLÉGIUM
NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY
NEUMANN JÁNOS SZAKKOLLÉGIUM


Miről lesz szó:
1. Kiber - kiber műveletek
2. Információs műveletek
3. Kiber – fizikai műveletek
4. Kritikus infrastruktúra
5. Kiber műveletek összehasonlítása

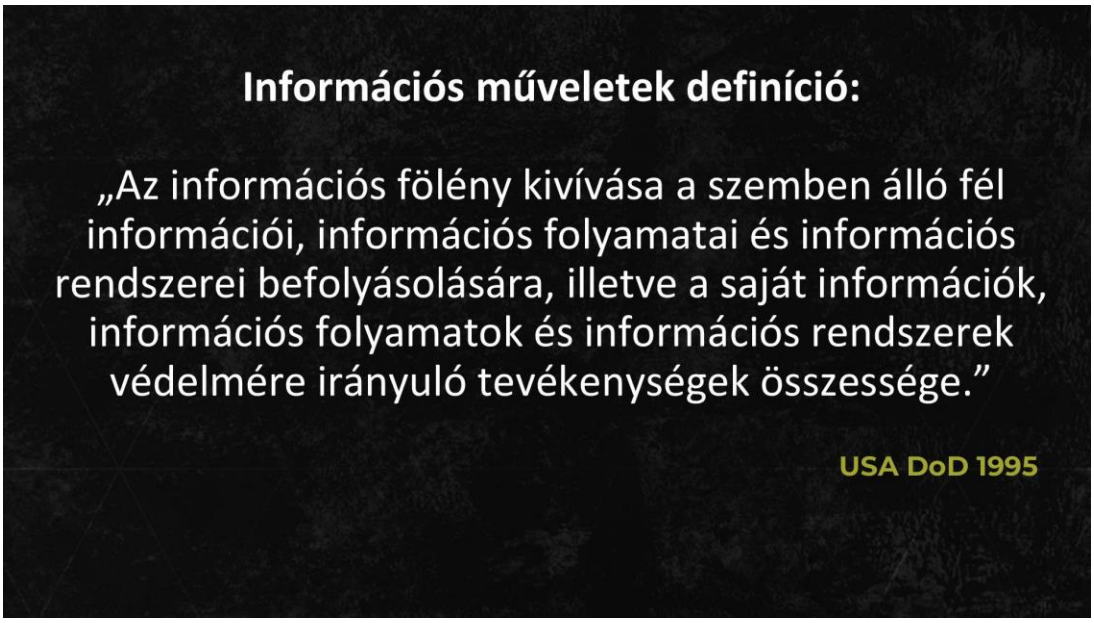
„Így aki igazán ért a hadviseléshez, úgy töri meg az idegen sereget, hogy nem vív csatát vele; úgy foglalja el az idegen városfalat, hogy nem ostromolja meg; úgy semmisíti meg az idegen fejedelemségeket, hogy nem tart sokáig (a háború). S minthogy a (kölcsönös) sértetlenség által igyekszik győzni az égalattiban, a fegyverek alkalmazása nélkül is biztosítani tudja magának az előnyöket. Ez a csellel való támadás törvénye!”

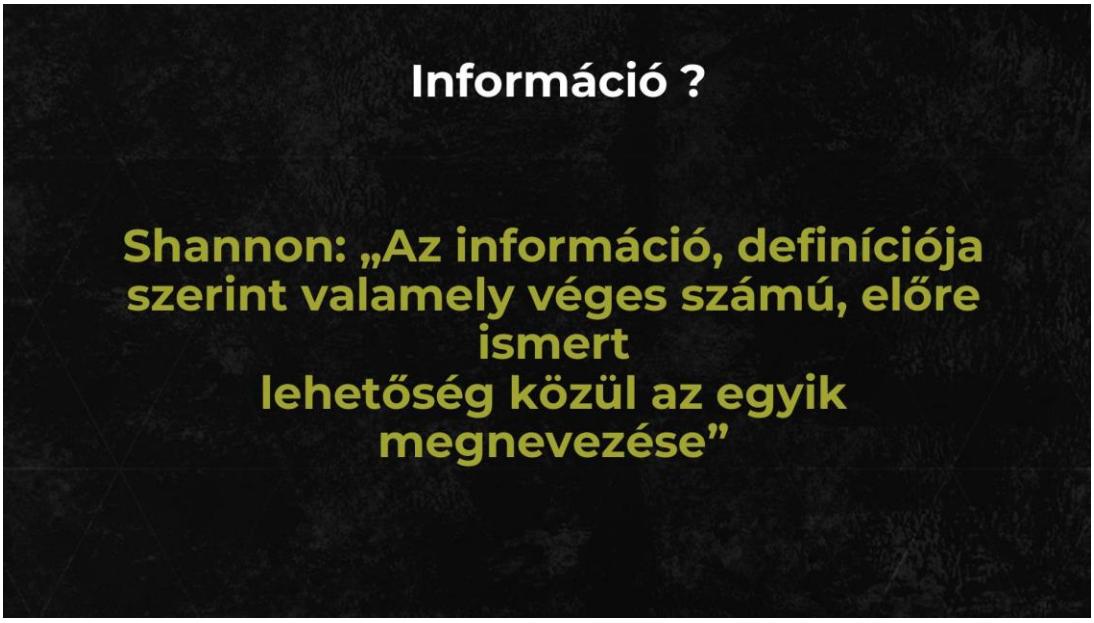
Szun Ce
A Háború Művészete

Kibertér definíció:

Felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva.

Kovács László
A KIBERTÉR VÉDELME


Információs műveletek definíció:
„Az információs fölény kivívása a szemben álló fél információi, információs folyamatai és információs rendszerei befolyásolására, illetve a saját információk, információs folyamatok és információs rendszerek védelmére irányuló tevékenységek összessége.”
USA DoD 1995


Információ ?
Shannon: „Az információ, definíciója szerint valamely véges számú, előre ismert
lehetőség közül az egyik megnevezése”

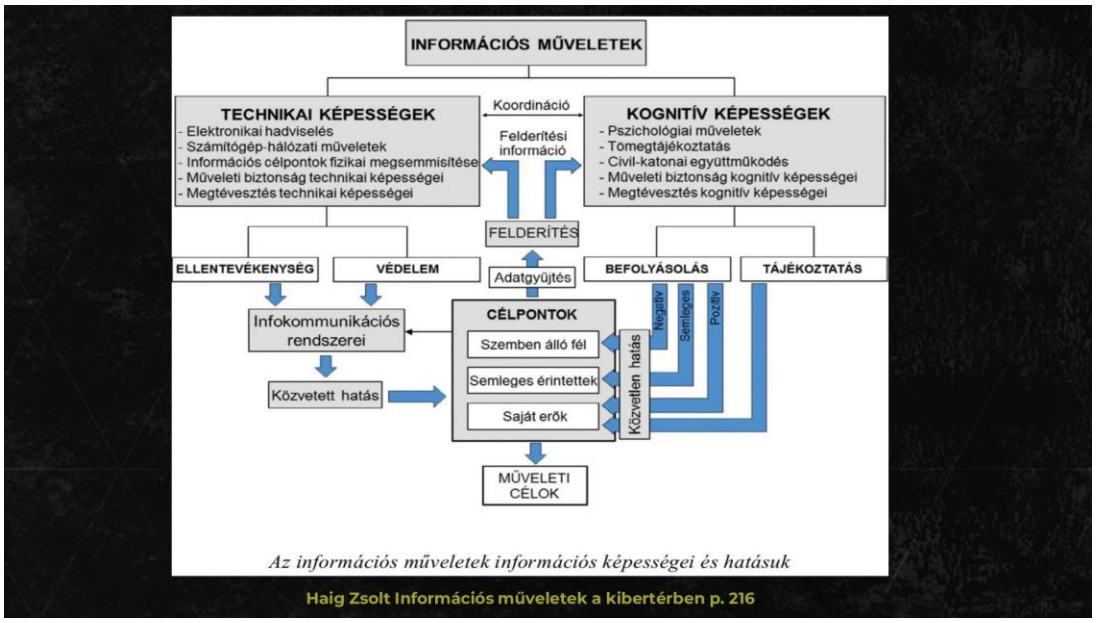

Propaganda
Fehér
Fekete
Szürke


Álhírek?
Félre tájékoztatás
Kontextus manipuláció
Dezinformáció

Entrópia

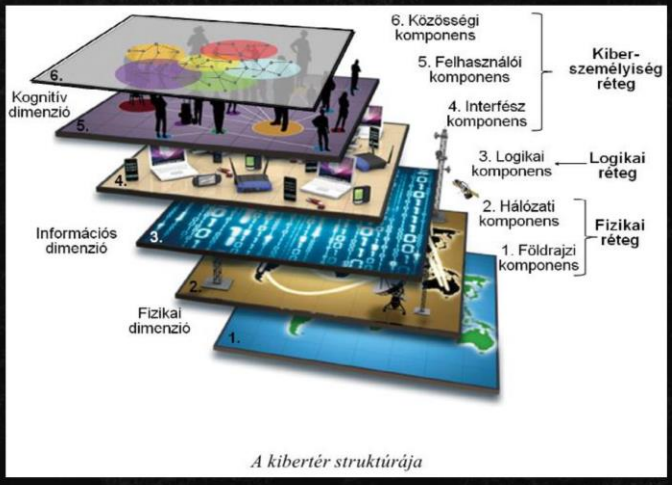
„A bizonytalanság mérőszáma”

„A rendszer rendezetlenségének foka”



Az információs műveletek információs képességei és hatásuk

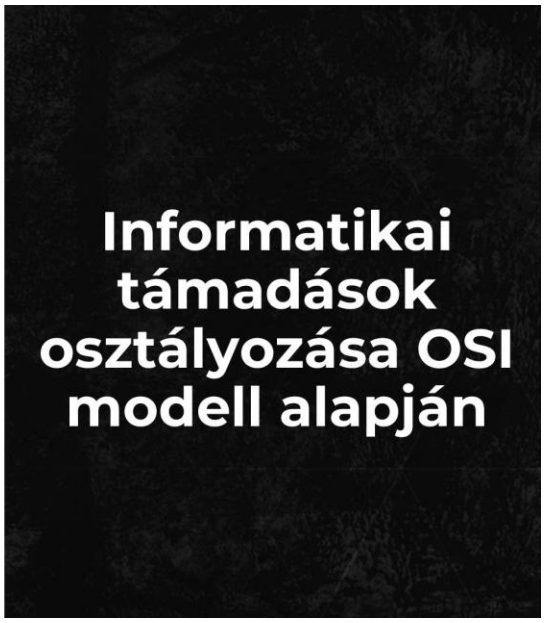
Haig Zsolt Információs műveletek a kibertérben p. 216

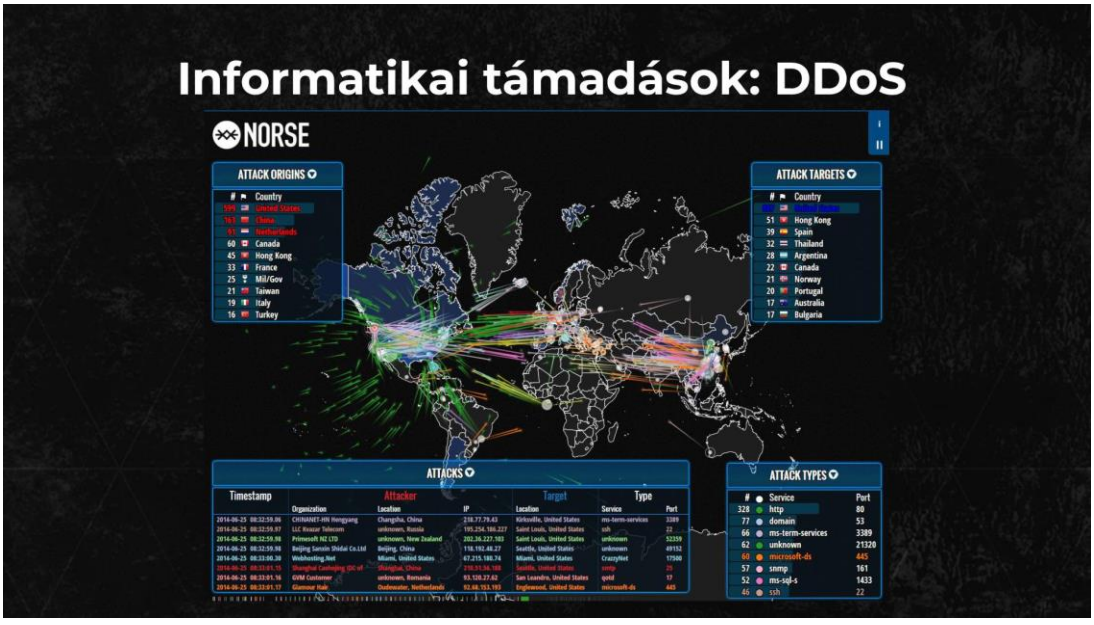


A kibertér struktúrája

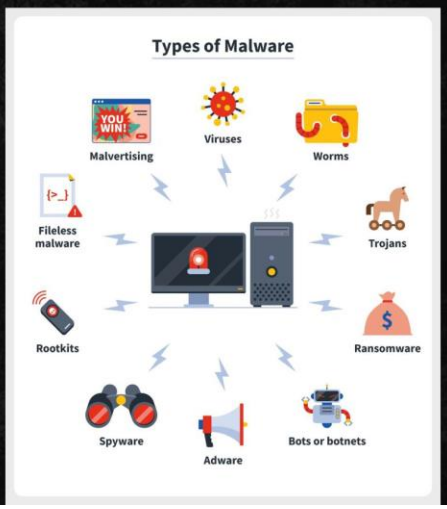
Haig Zsolt Információs műveletek a kibertérben p. 231


OSI Model
Host Layers
Process
Device/Protocol
7
Application
Network process to end-user application
SMTP/ DNS/ HTTP/ HTTPS/ FTP
End-User Layer
6
Presentation
Data representation and encryption
JPEG/ GIF/ TIFF/ HTML/ DOC
Syntax Layer
5
Session
Interhost communication
NFS/ RPC/ SQL/ RTP
Sync and send to ports
4
Transport
End-to-end connections and reliability
TCP/ UDP/ SPX
TCP
Media Layers
Process
Device/Protocol
3
Network
Path determination and logical addressing
IP/ ICMP/ PX
Packets
2
Data Link
Physical addressing
PPP/ SLIP
Frames
1
Physical
Media, signal and binary transmission
Hub
Physical Structure

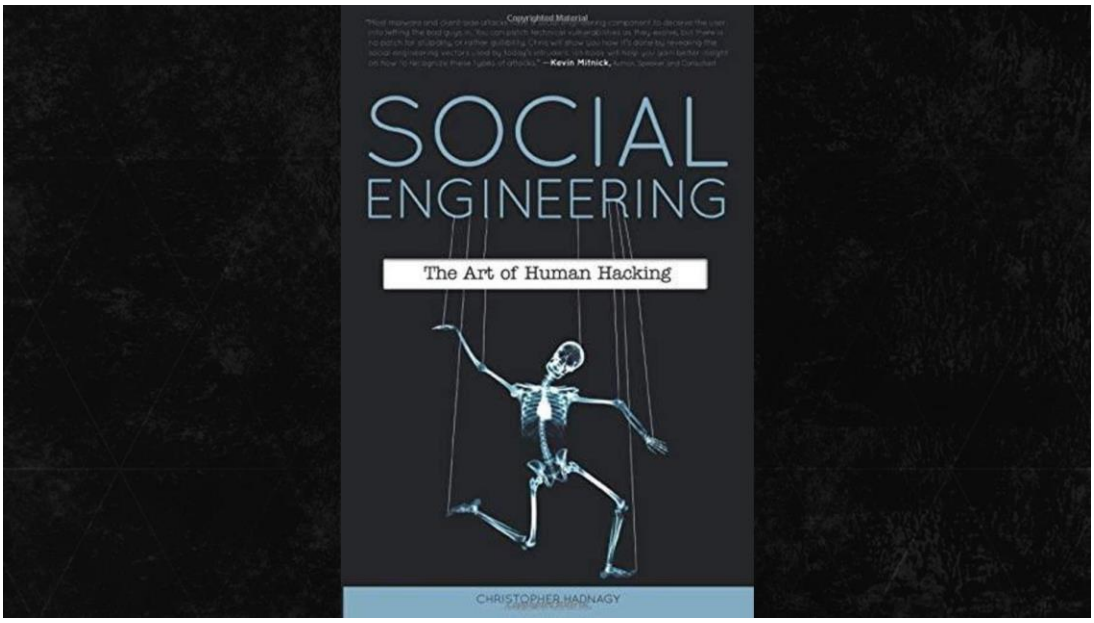

Informatikai támadások osztályozása OSI modell alapján

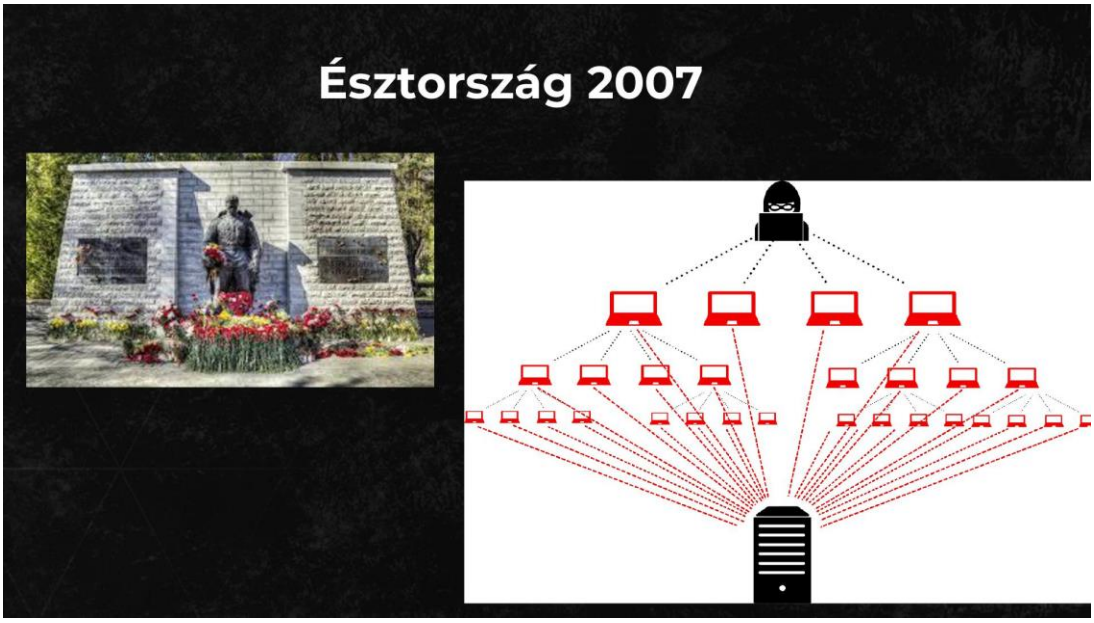

Informatikai támadások: DDoS
NORSE
ATTACK ORIGINS
Country
60 Canada
45 Hong Kong
33 France
25 Mil/Gov
21 Taiwan
19 Italy
16 Turkey
ATTACK TARGETS
Country
51 Hong Kong
39 Spain
32 Thailand
28 Argentina
22 Canada
21 Norway
20 Portugal
17 Australia
17 Bulgaria
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
ATTACK TYPES
Service Port
328 http 80
77 domain 53
66 ms-term-services 3389
62 unknown 21320
60 microsoft-ds 445
57 snmp 161
52 ms-sql-s 1433
46 ssh 22

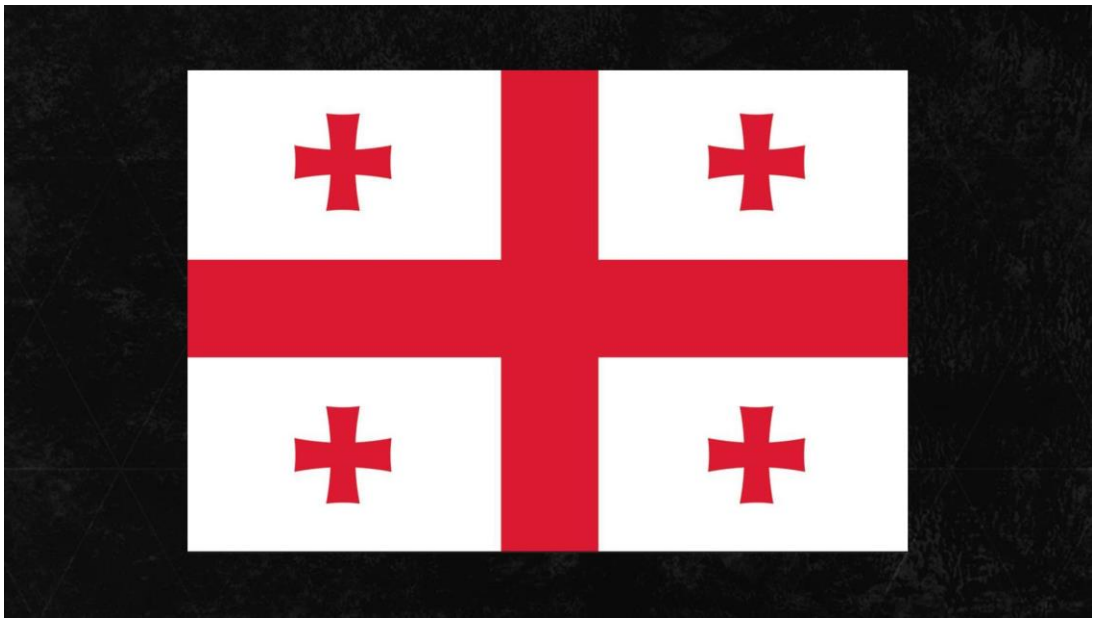
Informatikai támadások: malware

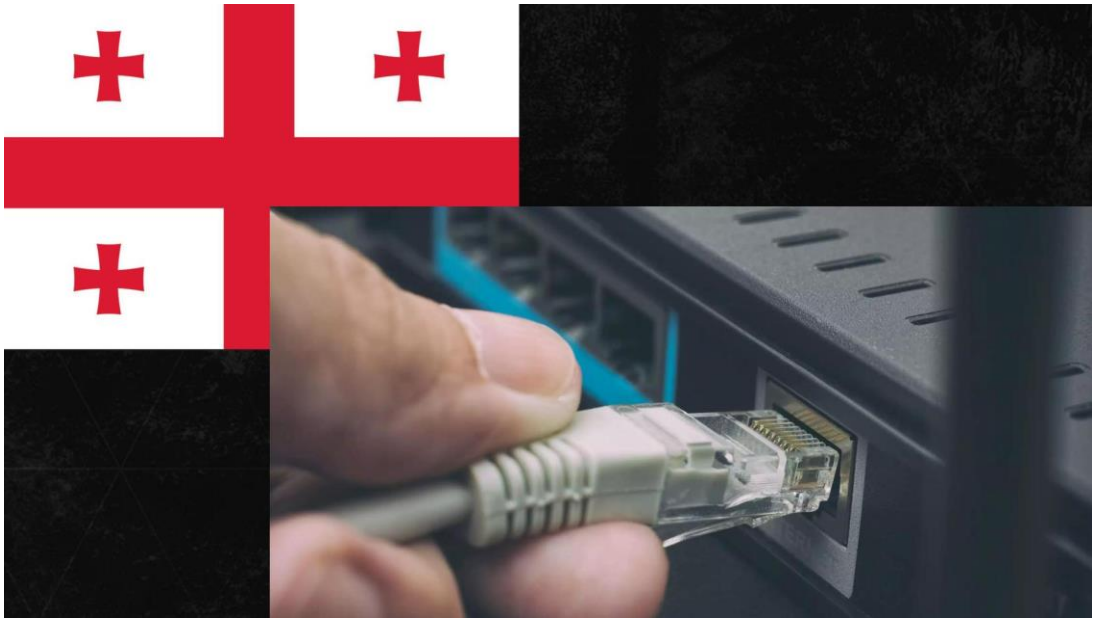


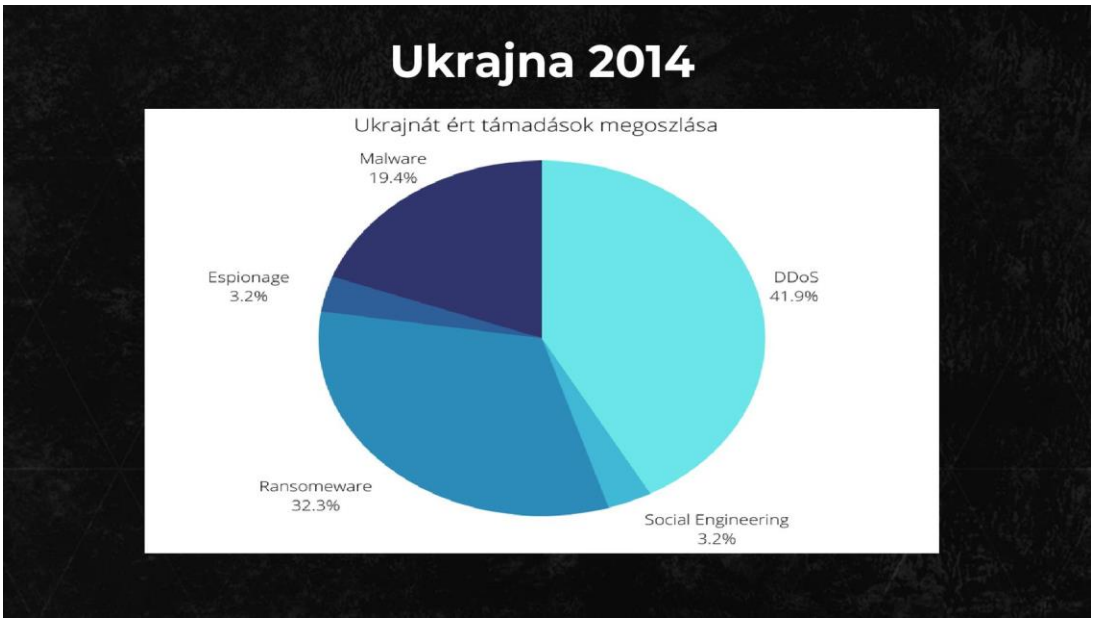
Informatikai támadások: ransomeware

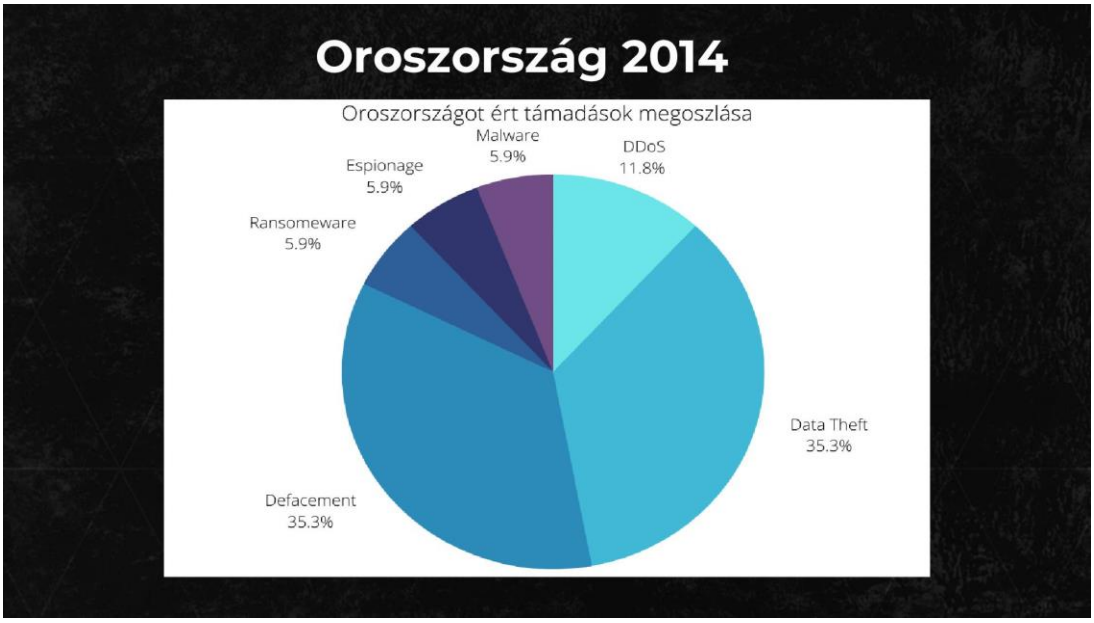

Copyrighted Material
SOCIAL
ENGINEERING
The Art of Human Hacking
CHRISTOPHER HADNAGY


Észtország 2007





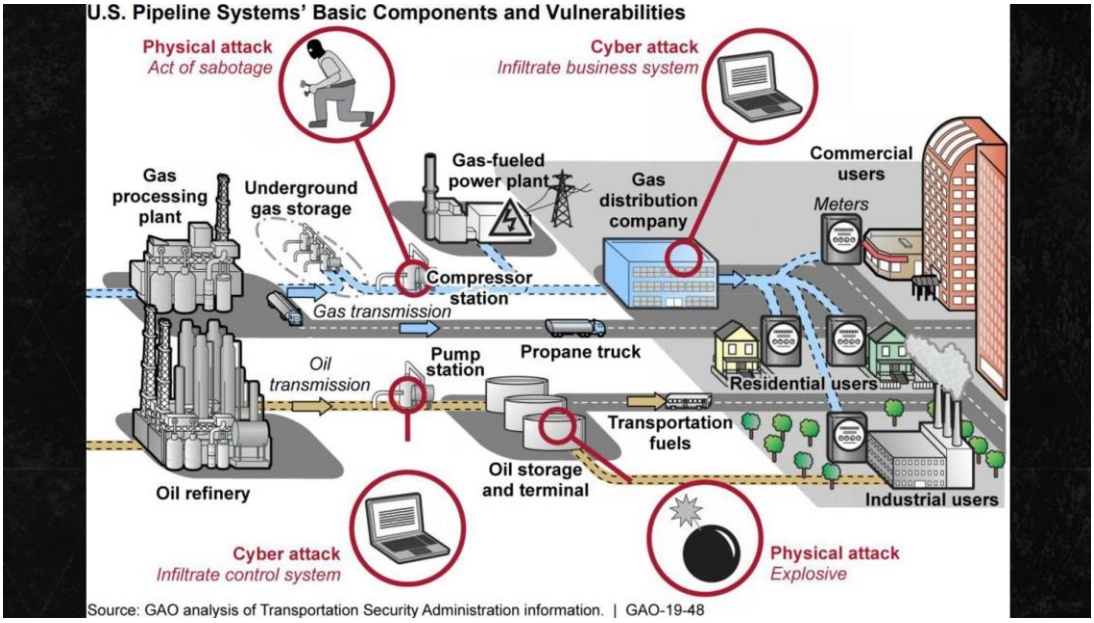

Ukrajna 2014
Ukrajnát ért támadások megoszlása
Malware
19.4%
Espionage
3.2%
DDoS
41.9%
Ransomeware
32.3%
Social Engineering
3.2%

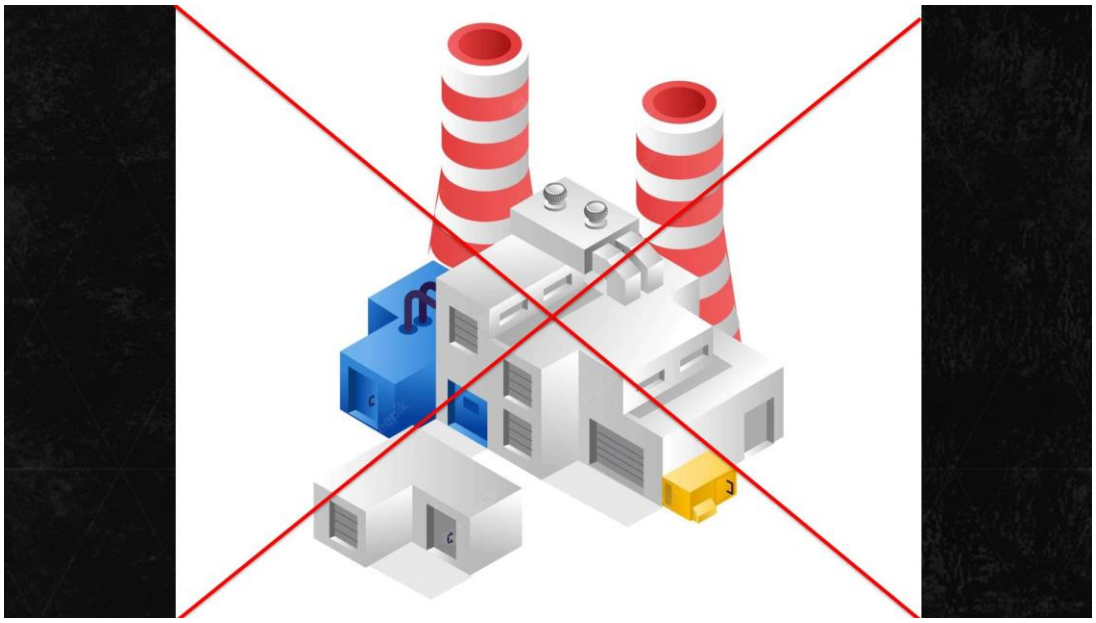

Oroszország 2014
Oroszországot ért támadások megoszlása
Malware
5.9%
DDoS
11.8%
Espionage
5.9%
Ransomeware
5.9%
Data Theft
35.3%
Defacement
35.3%

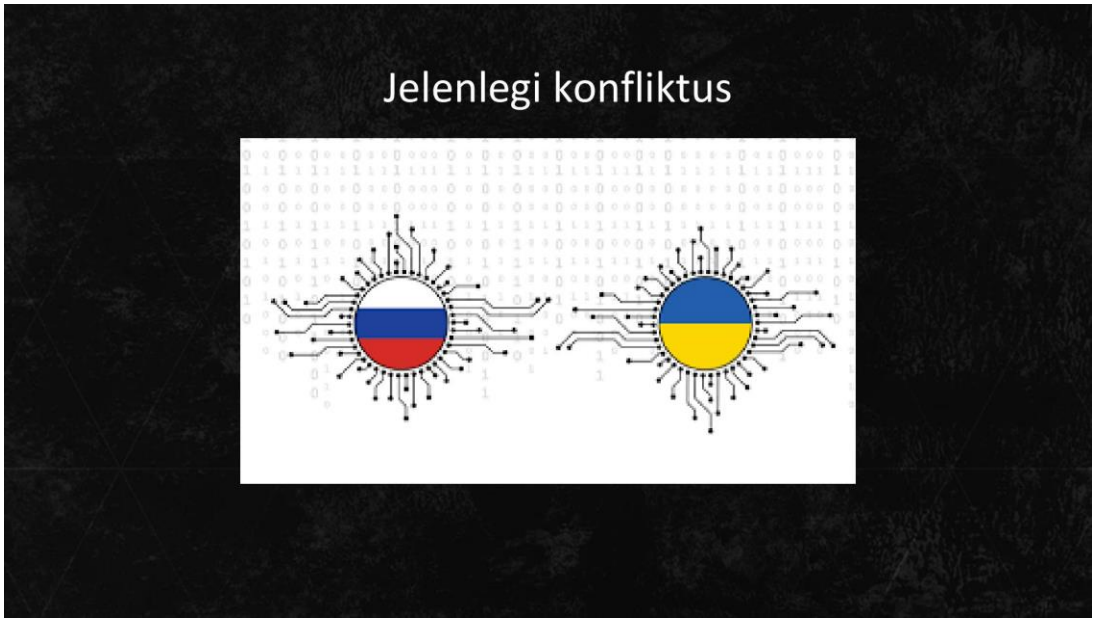

Ukrajna 2014

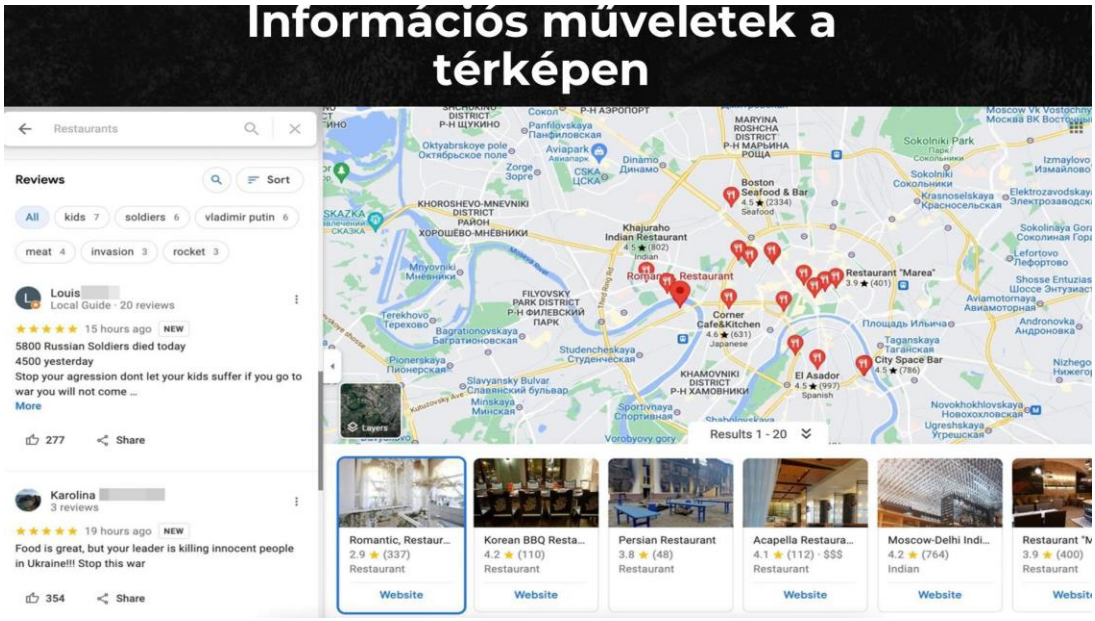

Web Browser
Web Defacement Attacks


Essential Critical Infrastructure Workers
Communications
Chemical
Critical Manufacturing
Commercial Facilities
Dams
Defense Industrial Base
Energy
Emergency Services
Financial
Food & Agriculture
Government Facilities
Healthcare & Public Health
Transportations Systems
Information Technology
Water
Nuclear Reactors, Materials & Waste
CISA
cisa.gov

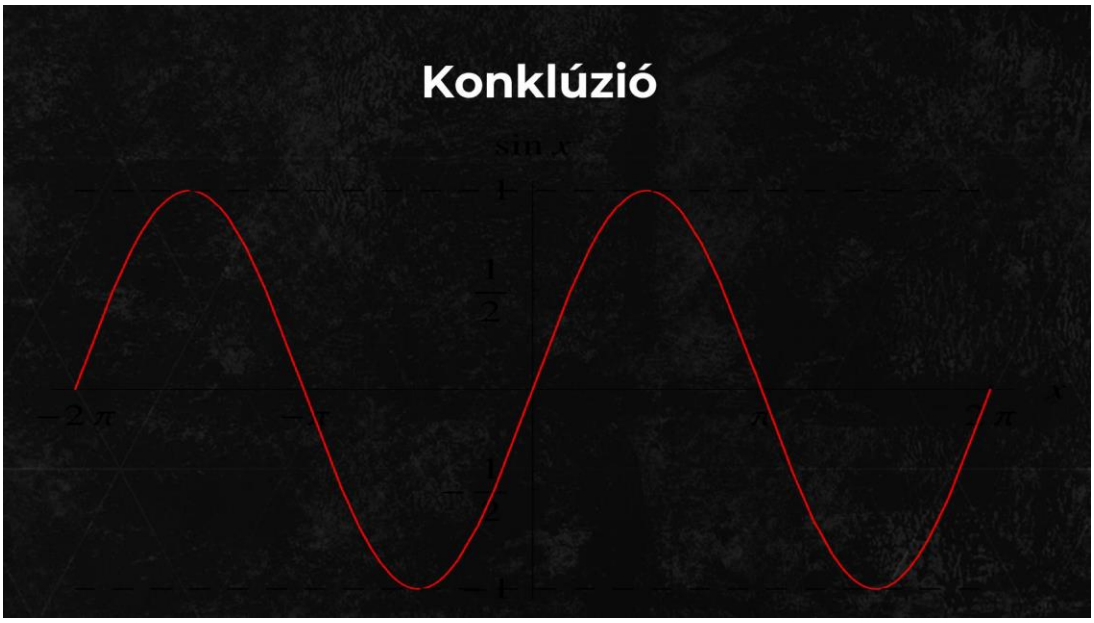

U.S. Pipeline Systems' Basic Components and Vulnerabilities
Physical attack
Act of sabotage
Cyber attack
Infiltrate business system
Gas processing plant
Underground gas storage
Gas-fueled power plant
Gas distribution company
Commercial users
Meters
Compressor station
Gas transmission
Oil transmission
Pump station
Propane truck
Residential users
Transportation fuels
Oil storage and terminal
Oil refinery
Industrial users
Cyber attack
Infiltrate control system
Physical attack
Explosive
Source: GAO analysis of Transportation Security Administration information. | GAO-19-48




Jelenlegi konfliktus


Információs műveletek a térképen
Restaurants
Reviews
Sort
All
kids 7
soldiers 6
vladimir putin 6
meat 4
invasion 3
rocket 3
Louis
Local Guide · 20 reviews
15 hours ago NEW
5800 Russian Soldiers died today
4500 yesterday
Stop your agression dont let your kids suffer if you go to war you will not come ...
More
277
Share
Karolina
3 reviews
19 hours ago NEW
Food is great, but your leader is killing innocent people in Ukraine!!! Stop this war
354
Share
Results 1 - 20
Romantic, Restaur...
Korean BBQ Resta...
Persian Restaurant
Acapella Restaura...
Moscow-Delhi Indi...
Website


ЭЛЕКТРОТРАНСПОРТ
РОССЕТИ
ЭЛЕКТРОТРАНСПОРТ
CCS


Konklúzió
sin x
1
1/2
−2π
π
x


Myth Buster
AI Varázslat
AI Kiber fegyver
AI Defenzív alkalmazása

FELHASZNÁLT IRODALOM

[1]https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/200 8-factsheet-cyber-defence-en.pdf Elérés: 2022.11.10 17:28:45
[2] Muriets Murimi Cyber Warfare Assess of Russia p. 14 https://www.academia.edu/9689387/Cyber_Warfare_Assess_of_Russia Elérés: 2022.11.10 19:38:15
[3] Baezner, Marie (2018): Cyber and Information warfare in the Ukrainian conflict, Version 2, October 2018, Center for Security Studies (CSS), ETH Zürich.
[4] Dr. Bányász Pérter Háború a kibertérben - kiberbiztonsági események az orosz-ukrán háborúban2022.10.06 18:00
[5]Haig Zsolt Információs műveletek a kibertérben Dialóg Campus Kiadó, 2018
[6] Ludovika Szabadegyetem - Dr. Kovács László dandártábornok (2022.03.08.)
[7]https://www.shacknews.com/article/131606/amzn-aws-ukrainedata-migration elérés: 2022.11.11. 21:25:36


Forrásaim:
https://www.google.com/search?q=OSI&tbm=isch&tbs=isz:l&hl=hu&sa=X&ved=0CAIQpwVqFwoTCPDmw-
KLtPsCFQAAAAAdAAAAABAN&biw=1271&bih=440#imgrc=oZI3Khk7uOY2ZM
https://www.google.com/search?q=ddos&&tbm=isch&ved=2ahUKEwiu95Pxy7T7AhUbwLsIHd2IAfIQ2-
cCegQIABAA&oq=ddos&gs_lcp=CgNpbWcQAzIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBAgAEB4yBAgAEB4yBAgAEB4y
BAgAEB4yBAgAEB4yBAgAEB46BAgjECc6CAgAEIAEELEDOggIABCxAxCDAVDSCFiKDGD8DGgAcAB4AIABdIgBigOSAQM0LjGYAQC
gAQGqAQtnd3Mtd2I6LWItZ8ABAQ&sclient=img&ei=UNV1Y66PBJuA7_UP3ZGGkA8&bih=440&biw=1271&hl=hu#imgrc=mlPHaNPVeEj
5pM
https://now.symassets.com/content/dam/norton/global/images/non-product/misc/tlc/in-post-01-types-of-malware.png
ocsia.im/media/brjepqkn/ransomware-banner.png
https://www.google.com/search?q=estonia+cyber+attack&tbm=isch&ved=2ahUKEwig4byozbT7AhUNt6QKHfHJCjkQ2-
cCegQIABAA&oq=estonia+cyber+attack&gs_lcp=CgNpbWcQAzIHCAAQgAQQEzIHCAAQgAQQEzoECCMQJzoGCAAQBxAeOgQIABAe
OgUIABCABDoECAAQQzoLCAAQgAQQsQMQgwE6CAgAEIAEELEDOggIABAIEB4QE1C-
CIi8IGCcIWgAcAB4AIABZ4gB5wuSAQQyMC4xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=0NZ1Y6C5H43ukgXxk6vIA
w&bih=431&biw=1271&hl=hu#imgrc=4KMk3H1Lw5Z7oM
https://cyberarms.files.wordpress.com/2014/06/real-time-hacker-map-2.png
https://websitesecuritystore.com/wp-content/uploads/2021/07/web-defacement-attacks-examples.svg
https://www.cisa.gov/sites/default/files/inline-images/ECIW%20honeycomb%20graphic_tw-02%20850px.png
https://www.gao.gov/assets/gao_blog/inline/4_8.pnghttps://www.nato.int/docu/review/files/3650.jpg
https://www.google.com/search?q=pull+out+internet+cable&tbm=isch&ved=2ahUKEwjrlqbe0bT7AhWSNuwKHc7fDWYQ2-
cCegQIABAA&oq=pull+out+internet+cable&gs_lcp=CgNpbWcQAzoECCMQJzoICAAQCBAeEBNQyApYoRFgnRJoAHAAeACAAU2IAck
FkgECMTCYAQCgAQGqAQtnd3Mtd2I6LWItZ8ABAQ&sclient=img&ei=c9t1Y6uRCJLtsAfOv7ewBg&bih=440&biw=1280&hl=hu#imgrc=
hLkflUp3Pofu3Mhttps://iea.imgix.net/1f05e7ce-3c0d-433c-a473-
5525d97c34d0/shutterstock_210379843.jpg?auto=compress%2Cformat&fit=min&q=80&rect=468%2C0%2C3744%2C3744
https://www.online-tech-tips.com/wp-content/uploads/2019/06/google-maps-write-review.png
https://helios-i.mashable.com/imagery/articles/00yqnhfQJ3f78rqrHIZNNNv/images-4.fill.size_2000x1042.v1646174678.jpg

Vattai Eszter: Az OSINT katonai vonzatai

Absztrakt

Jelen kutatómunkám a nyílt forrású információszerzés (Open Source Intelligence – OSINT) témakörét taglalja, civil és a katonai aspektusokat bemutatva.

Kutatási módszereim közé tartozott a szakirodalmak feldolgozása, a nyomtatott formában elérhető hazai szakirodalmak mellett, a témakör aktualitásának megfelelően elektronikus formában elérhető magyar és idegen nyelvű forrásokat is felhasználtam.

Kutatásom célja, az OSINT eszközök és az infokommunikációs technológiák komplex vizsgálata katonai aspektusokban. Jelenleg csak nagyon szűk körben vizsgált terület hazánkban a nyílt forrású információszerzés, ennek megfelelően ez ösztönzött arra, hogy ezzel a területtel foglalkozzak, továbbá a szakirányom végett is szerettem volna a témát kifejteni, mivel információbiztonsági tiszt leszek, fontosnak tartom a megszerzett tudást kamatoztatni a jövőbeni beosztásom érdekében.

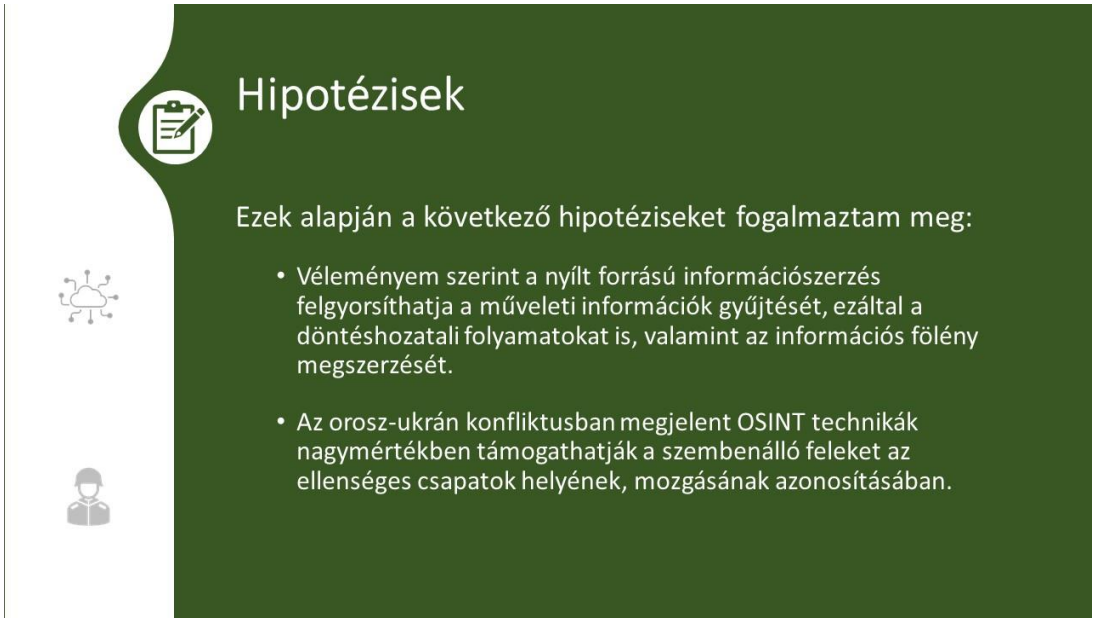
Az előzetes elemzéseim alapján (jellemzően nemzetközi szakirodalmak vizsgálatával) arra a következtetésre jutottam, hogy az OSINT tevékenységeknek egyre nagyobb hatása lesz a katonai műveletekre, így kiemelten fontosnak tartom egy ilyen irányú kutató-elemző munka végrehajtását. Mivel technológia fejlődése megteremtette azt a különleges helyzetet, hogy a felelőtlen, nem

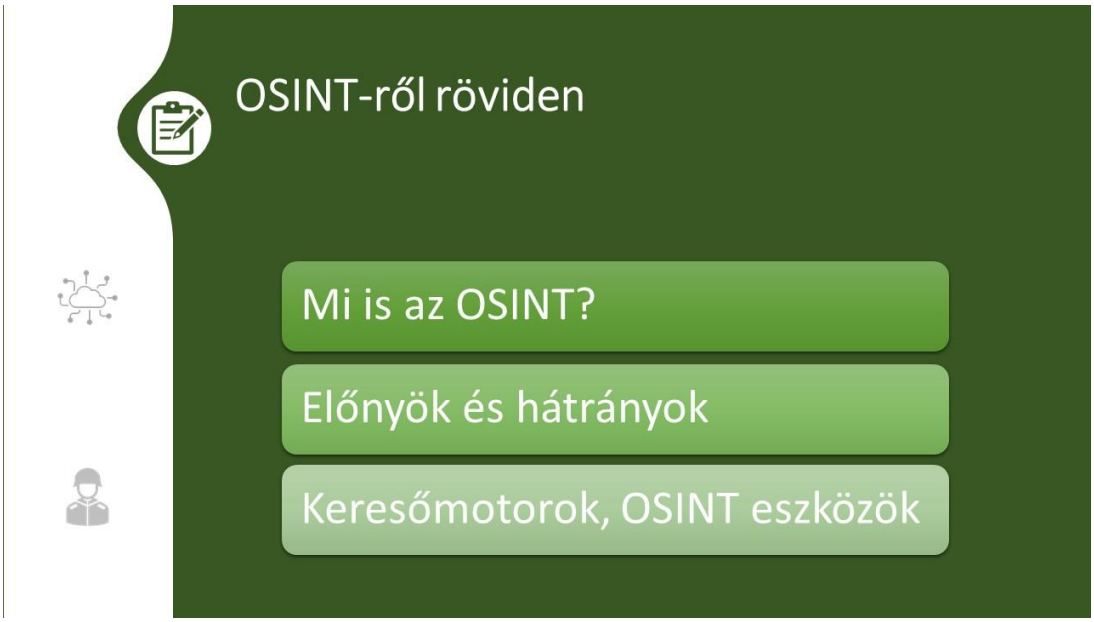
biztonságtudatos felhasználók nagyon könnyen lekövethetővé és lehallgathatóvá válnak.

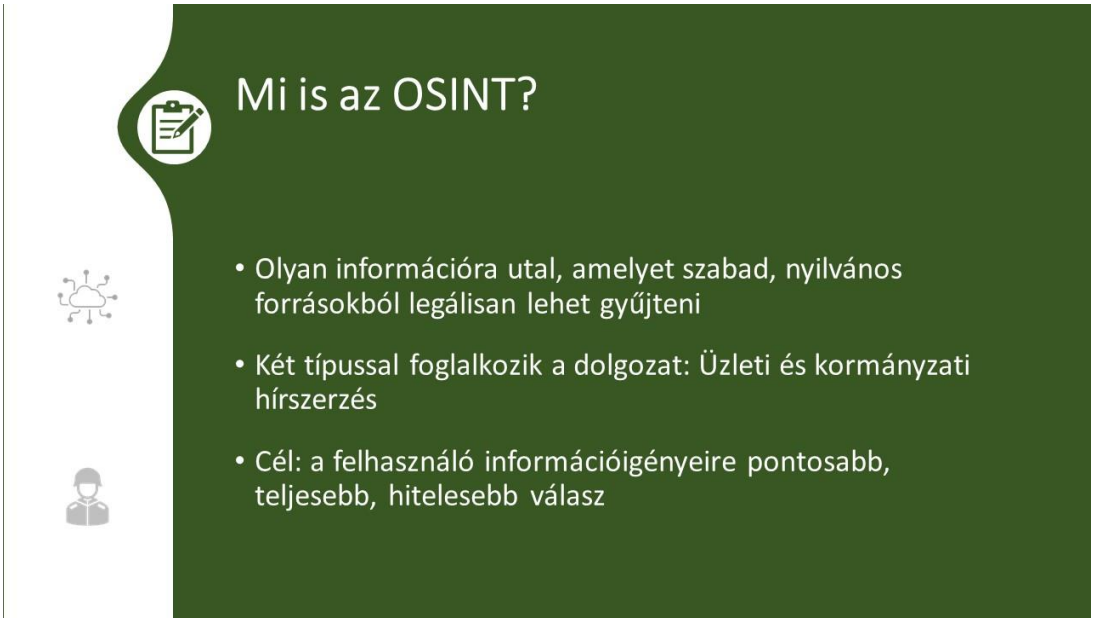
Összegzéseként kijelenthetem, hogy sikerült választ találnom a kutatási kérdéseimre, felépítenem egy olyan dolgozatot, amely tematikusan meghatározza az összefüggéseket az OSINT és a hadsereg között. Remélem, hogy a munkám több emberhez elér majd, és betekintést nyerhetnek a nyílt forrású információszerzés katonai lehetőségeibe.

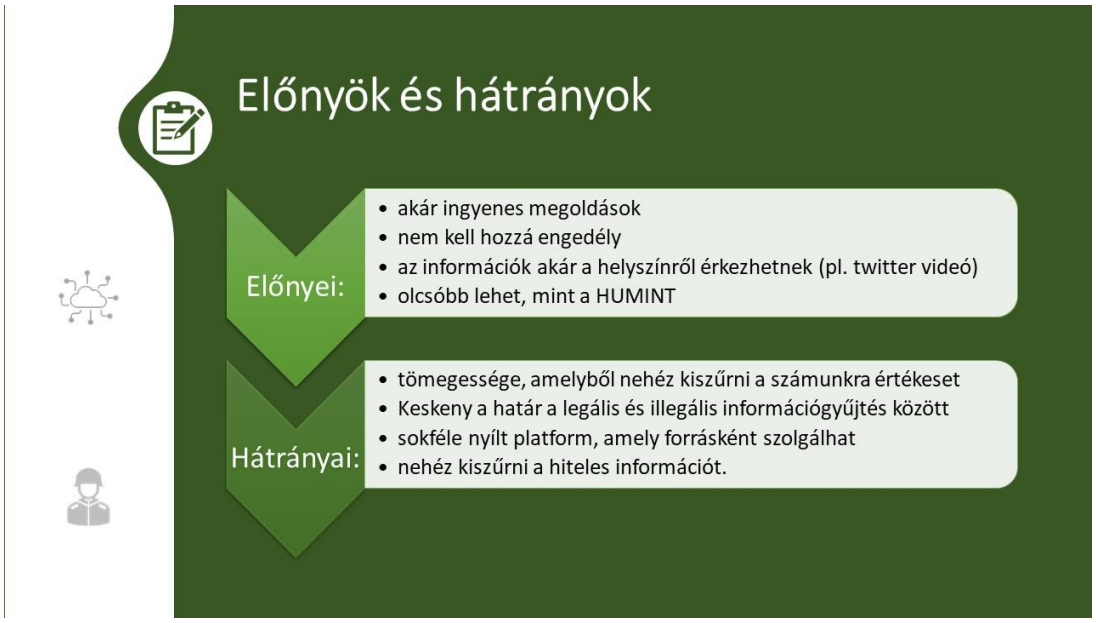
Kulcsszavak: OSINT, nyílt forrású információszerzés közösségi média, orosz-ukrán konfliktus


Az OSINT katonai vonzatai
A kibertér és a nyílt forrású információszerzés kapcsolata
OSINT-ról röviden
A nyílt forrású információszerzés kapcsolata a hadsereggel
Készítette: Vattai Eszter
Innovációs és Technológiai Minisztérium ÚNKP-22-1-I-NKE-34 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült


Hipotézisek
Ezek alapján a következő hipotéziseket fogalmaztam meg:
• Véleményem szerint a nyílt forrású információszerzés felgyorsíthatja a műveleti információk gyűjtését, ezáltal a döntéshozatali folyamatokat is, valamint az információs fölény megszerzését.
• Az orosz-ukrán konfliktusban megjelent OSINT technikák nagymértékben támogathatják a szembenálló feleket az ellenséges csapatok helyének, mozgásának azonosításában.


OSINT-ről röviden
Mi is az OSINT?
Előnyök és hátrányok
Keresőmotorok, OSINT eszközök

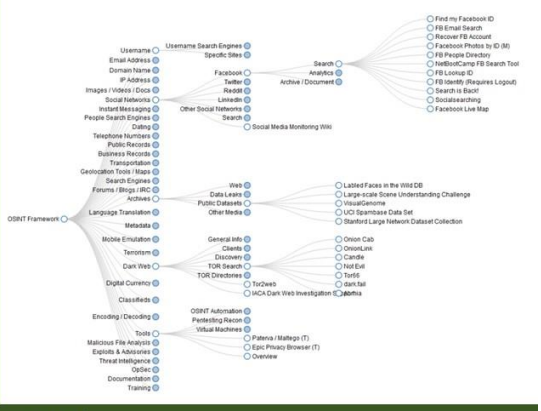

Mi is az OSINT?
• Olyan információra utal, amelyet szabad, nyilvános forrásokból legálisan lehet gyűjteni
• Két típussal foglalkozik a dolgozat: Üzleti és kormányzati hírszerzés
• Cél: a felhasználó információigényeire pontosabb, teljesebb, hitelesebb válasz


Előnyök és hátrányok
Előnyei:
akár ingyenes megoldások
nem kell hozzá engedély
az információk akár a helyszínről érkezhetnek (pl. twitter videó)
olcsóbb lehet, mint a HUMINT
Hátrányai:
tömegessége, amelyből nehéz kiszűrni a számunkra értékeset
Keskeny a határ a legális és illegális információgyűjtés között
sokféle nyílt platform, amely forrásként szolgálhat
nehéz kiszűrni a hiteles információt.


Keresőmotorok, böngészők
Google
Alerts
DuckDuckGo
Bing
Images
Nemzetközi keresőmotorok
I Search From
Web archívum
TOR
Keresőmotor gyűjtemények
FTP keresés

OSINT eszközök

- osintframework.com
- Open Source Intellligence Tools and Resources Handbook



- Maltego
- Recon-ng
- The Harvester
- Shodan
- Mitaka
- Intelligence X
- DarkSearch.io

A kibertér és a nyílt forrású információszerzés kapcsolata

- Az etikus hackelés
- A közösségi média szerepe a nyílt forrású információszerzésben
- A nyílt információszerzés szerepe a kibertámadásokban
- Geolokációs információgyűjtés

Az etikus hackelés

- Mi is az a hackelés?
- Black és white hat hacker

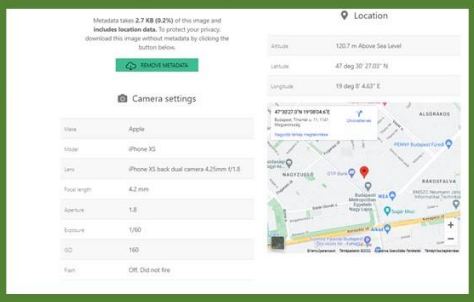
White hat hacker (etikus)	Black hat hacker (nem etikus)
Felhatalmazással rendelkezik	Nincs felhatalmazása
Tevékenységét szerződések szabályozzák	Tevékenysége illegális
Célja a biztonsági rések javítás miatti felfedése	Célja a biztonsági rések kijátszása, haszonszerzés
Munkaszerűen végzi tevékenységét	Hobbiként vagy anyagi érdek alapján végzi tevékenységét
Tevékenysége szabályozott	Tevékenysége szabályozatlan

A nyílt információszerzés szerepe a kibertámadásokban

Az információk keresésére az alábbi megoldások lehetnek:

- személyes megkeresés;
- kuka átvizsgálás;
- internetes információgyűjtés;
- megfigyelés;
- hagyományosan publikált anyagok;
- telefonos információgyűjtés.

Geolokációs információgyűjtés



Segíthetnek a geolokációs információgyűjtésben.

- műholdképek
- nyilvános kameraképek
- légifelvételek
- földrajzi koordináták
- geoinformációs rendszerek és szoftverek
- tematikus térképek
- épületek kutatása

A nyílt forrású információszerzés kapcsolata a hadsereggel

Az OSINT szerepe a nemzetbiztonsági szervezeteknél

Az orosz-ukrán háború OSINT vonatkozásai

Az OSINT szerepe a nemzetbiztonsági szervezeteknél

Az információszerzést pedig az alábbi hírszerzési ágak végzik:

- emberi erőforrásokkal folytatott hírszerzés (HUMINT);
- rádióelektronikai felderítés (SIGINT);
- nyílt forrású hírszerzés (OSINT);
- képfelderítés (IMINT);
- mérés és jelmeghatározó hírszerzés (MASINT);
- kiberhírszerzés (CYBINT).

Az orosz-ukrán háború OSINT vonatkozásai

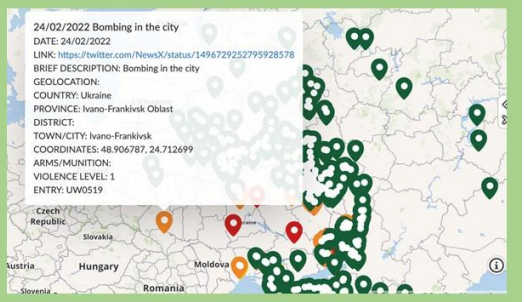
HUMINT, OSINT eszközei

Különleges erők, mélységi felderítők

Csapatfelderítés, drónfelderítés

Az orosz-ukrán háború OSINT vonatkozásai

- A Russia-Ukraine Monitor Map a Center for Information Resilience (CIR) cég térképe
- Térképen látható információk ellenőrizve vannak



Az orosz-ukrán háború OSINT vonatkozásai

- Joker DPR csoport feltörte a Delta programot
- Parancsnoki-irányítási program, melyben az összes baráti és ellenséges adat szerepel és frissül

Összegzés

- Ahhoz, hogy a legtöbbet hozzuk ki az OSINT-ből, részletes elemzésre és a használat követelményeinek megértésére van szükség.
- A katonai műveleteket, az a fél nyeri, aki több releváns információval rendelkezik

- az orosz-ukrán háború egy kitűnő példa volt az 1. számú hipotézisem alátámasztására, hiszen ott is megnyilvánult, mennyire meg tud változni egy hadszíntér, ha nem kívánt információ kerül fel az internetre.
- 2. számú hipotézisemmel kapcsolatban szintén, hiszen több olyan példát ismerhettünk meg mi is a közösségi médiából, amely alátámasztotta, hogy bizonyos csapatok úgy mértek csapást az ellenségre, hogy előtte a közösségi médiából tájékozódtak

Felhasznált források

- Deák Veronika: A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során – Hadmérnök, XIII. évfolyam 3. szám – 2018. szeptember 393. oldal
- Dobák, Imre: OSINT – Gondolatok a kérdéskörhöz, NEMZETBIZTONSÁGI SZEMLE (ONLINE) 7 : 2 pp. 83-93. , 11 p. (2019)
- Nemzetbiztonság elmélete a közszolgálatban - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), III. Az információgyűjtésről általában (Dobák Imre), 99. oldal
- Nemzetbiztonsági alapismeretek - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), A nemzetbiztonsági szolgálatok (Dezső Lajos), III. fejezet, 100. oldal
- S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016, pp. 860-867, doi: 10.1109/ASONAM.2016.7752338.
- Szabó Károly: Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről; NEMZETBIZTONSÁGI SZEMLE 7. évfolyam (2019) 2. szám 68–82. • doi: 10.32561/nsz.2019.2.6
- T. Aichner és mtsai., „Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019”, Cyberpsychology, Behavior, and Social Networking 24, sz. 4 (2021): 215–22, https://doi.org/10.1089/cyber.2020.0134.

Felhasznált források

- https://bluebird.hu/mennyit-ernek-az-etikus-hackerek/; letöltve: 2022.11.05.
- https://creepy.en.softonic.com/; letölve: 2022.11.08., fordította: szerző
- https://maphub.net/Cen4infoRes/russian-ukraine-monitor
- https://restofworld.org/2022/osint-viral-ukraine/; letölve: 2022. 05. 26. fordította: szerző
- https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/; letöltve: 2022. 11. 10., fordította: szerző


Az OSINT katonai vonzatai
Köszönöm a megtisztelő figyelmet!
Készítette: Vattai Eszter
Elérhetőség:
Email: vattaieszter2001@gmail.com
Mobil: +36/30-4899246

Bálint Áron: Italy's Military Development and Security Co-operations

Abstract

The instability in the world is growing and the international security is deteriorating. With the 2022 Russian invasion of Ukraine many countries realised that their current defence capacity and capability is not enough and started the development of their military through the acquisition of military equipment. A Mediterranean middle power, the Italian Republic has been progressively reforming and developing its military since 2013. In 2012 Minister of Defence Giampaolo Di Paola prepared the law of 2012 n. 244, which allowed the overall reorganisation of the structure of the Italian military and the acquisition of new instruments through a report-the Multiannual Programmatic Defence Document (DPP)- that the minister yearly prepares for the Parliament. In the DPPs a vast amount of information can be found regarding the state of the Italian military, the ongoing and planned R&D programmes in the field of defence, and the Peace Support Operations (PSO) that she participates in. In these strategic documents one can also read about how the Italians perceive the recent occurrences in the world. Italy also partakes in a number of security and defence co-operations, of which some are within the European Union's (EU) integration, while others are intergovernmental organisations, and co-operations independent of the Union. Within the framework of the Common Security and

Defence Policy, the EU can launch PSOs to stabilise different regions. The Organization for Joint Armament Co-operation (OCCAR) has been developing some of the most advanced European military equipment, like the Airbus A400M military transport aircraft, or the Eurodrone unmanned aerial vehicle. Finally, in 2022 Mario Draghi resigned ending the 67th cabinet of Italy. Fratelli d'Italia won the 2022 Italian elections and Giorgia Meloni became the first female prime minister of Italy.

Keywords: Italy, Peace Support Operations, CSDP, OCCAR, Giorgia Meloni

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

PUSKÁS TIVADAR

Italy's Military Development and Security Co-operations

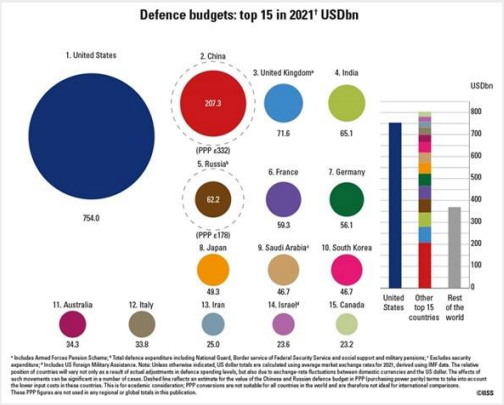
Áron BÁLINT
University of Public Service - Faculty of Military Science and Officer Training
international security and defence policy BA
Jövő biztonsági kihívásai II.

Agenda of the Presentation

- Italy, the middle power
- The Multiannual Programmatic Defence Document
- The DPP of 2022
- Security and defence co-operations
- The 2022 Russian invasion of Ukraine
- Conclusion

[1]

Italy: a Mediterranean Middle Power



- The 8th most developed economy with 2100 billion $ in 2021
- Is the NATO's 4th strongest member state
- Has the 3rd largest gold reserves with 2452 tonnes

[2]

The Multiannual Programmatic Defence Document (DPP)

- In 2012, Minister of Defence Giampaolo Di Paola prepared a law that allowed the reorganization of the military
- Since 2013, a sum of 10 documents have been prepared by the Ministers of Defence
- The DPPs evolved through the decade and now besides being easier to consume, they consist of 3 main, well-structured sections

The DPP of 2022

- The investments in defence plays a fundamental role in supporting Italy's international position
- Italy continues to participate in many peace support operations
- 2022 programmes cost approximately 15,500 m€

[3] Own edit

[3]

[4]

Security and Defence Co-operations

[5]

- Italy participates in a number of co-operations regarding security and defence
- Some of these European co-operations are: CSDP, EDA, OCCAR
- A 6th generation fighter jet is being developed by a consortium called „Team Tempest”

[6]

- Some OCCAR programmes have been completed and the instruments are already used by the armed forces

The 2022 Russian Invasion of Ukraine

- On 24 February 2022, the Russian Federation invaded Ukraine
- Prime Minister Mario Draghi declared state of emergency because of the war in Ukraine
- The Brothers of Italy won the elections on 25 September 2022

[7]

Conclusion

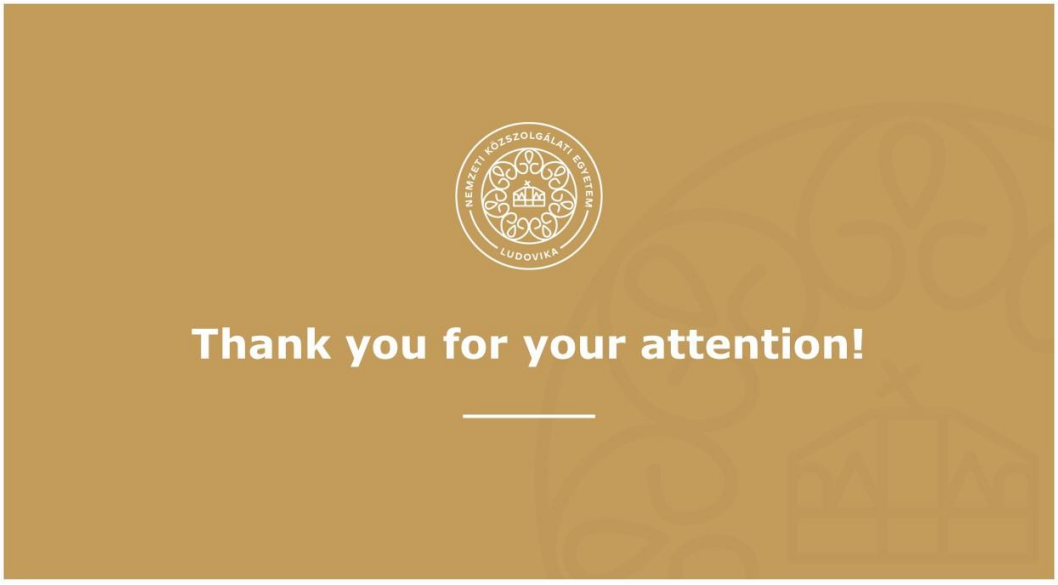
- Italy is progressively increasing the defence budget to be able to cope with the growing instability in the world
- She takes part in a decent amount of peace support operations on 3 continents
- She also co-operates with other European nations in the R&D of defence instruments
- In 2022 Prime Minister Mario Draghi had to resign, ending the 67th cabinet of Italy

Literature Cited

- Axe, David, 'Italy's Extra Aircraft Carrier Could Become A Floating Space Base', *Forbes* <https://www.forbes.com/sites/davidaxe/2021/03/17/italys-extra-aircraft-carrier-could-become-a-floating-space-base/> [accessed 18 November 2022]
- 'European Defence Agency Mission', *Default* <https://eda.europa.eu/who-we-are/Missionandfunctions> [accessed 17 November 2022]
- 'Giorgia Meloni Appointed as Italy's First Female Prime Minister', *Euronews*, 2022 <https://www.euronews.com/2022/10/21/giorgia-meloni-set-to-be-appointed-italys-first-female-prime-minister-despite-berlusconi-t> [accessed 17 November 2022]
- 'Gold Reserves by Country 2021', *World Gold Council* <https://www.gold.org/goldhub/data/gold-reserves-by-country> [accessed 14 November 2022]
- 'Italian PM Mario Draghi Offers Resignation after Coalition Falls Apart', *BBC News*, 14 July 2022, section Europe <https://www.bbc.com/news/world-europe-62171284> [accessed 17 November 2022]
- Lettig, Daniele, 'Italy Declares State of Emergency over Russia-Ukraine War', *Www.Euractiv.Com*, 2022 <https://www.euractiv.com/section/politics/short_news/italy-declares-state-of-emergency-over-russia-ukraine-war/> [accessed 17 November 2022]
- Lyman, Eric J., '"Their Absence Will Be Felt": Italy Fears Economic Hit as Russians Stay Away', *The Guardian*, 7 April 2022, section World news <https://www.theguardian.com/world/2022/apr/07/italy-economy-russian-tourists-ukraine> [accessed 17 November 2022]
- 'Meloni: How Will Italy's New Far Right PM Handle the Climate Crisis?', *Euronews*, 2022 <https://www.euronews.com/green/2022/09/30/giorgia-meloni-everything-we-know-so-far-about-the-new-italian-pms-climate-views> [accessed 17 November 2022]
- Molnár, Anna, *AZ EURÓPAI UNIÓ KÜLKAPCSOLATI RENDSZERE ÉS ESZKÖZEI* (Dialóg Campus Kiadó, 2018)
- 'NATO Member States Military Ranking (2022)' <https://www.globalfirepower.com/countries-listing-nato-members.php> [accessed 14 November 2022]
- 'Report for Selected Countries and Subjects', *IMF* <https://www.imf.org/en/Publications/WEO/weo-database/2022/April/weo-report> [accessed 14 November 2022]
- 'Royal Air Force Tempest', *Royal Air Force* <https://www.raf.mod.uk/> [accessed 17 November 2022]
- Takács, Lili, and Anna Molnár, 'Italy: An Aspiring Mediterranean Middle Power Wavering between Bilateralism and Multilateralism', *Estudos Internacionais: Revista de Relações Internacionais Da PUC Minas*, 8.2 (2020), 47–69 <https://doi.org/10.5752/P.2317-773X.2020v8n2p47-69>
- 'The Common Security and Defence Policy | EEAS Website' <https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en#8784> [accessed 17 November 2022]
- 'What Does OCCAR Do? | OCCAR' <https://www.occar.int/21-what-does-occar-do> [accessed 17 November 2022]

Source of the Figures

1. BullionStar Singapore. „From Gold Trains to Gold Loans – Banca d'Italia's Mammoth Gold Reserves". Accessed: 15 November 2022 https://www.bullionstar.com/blogs/ronan-manly/banca-ditalia-gold-reserves-trains-loans/.
2. IISS. „Military Balance 2022 Further Assessments". Accessed: 15 November 2022 https://www.iiss.org/blogs/analysis/2022/02/military-balance-2022-further-assessments.
3. DPP_2022-2024". Accessed: 15 November 2022 https://www.difesa.it/Il_Ministro/Documents/DPP_2022_2024.pdf.
4. „La Portaerei Garibaldi e Trieste". Accessed: 18 November 2022 http://www.aviazione-italiana.it/Aviazione%20Navale%204.html.
5. „Royal Air Force. „Royal Air Force". Accessed: 17 November 2022 https://www.raf.mod.uk/.
6. „Programmes | OCCAR". Accessed: 18 November 2022 https://www.occar.int/our-work-programmes.
7. „Giorgia Meloni". Accessed: 16 November 2022 https://en.wikipedia.org/w/index.php?title=Giorgia_Meloni&oldid=1122299210.


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
Thank you for your attention!

Schiller Gábor: Liman és Herszon

Absztrakt

A 2022. október 2-án véget érő limani offenzíva során és azt követően számos politikai változás ment végig az Oroszországi Föderációban. Az orosz hadviselő fél feleszmélt az ukrán támadó műveletek hatására, hogy céljai elérésére több erőforrást kell a háborúra fordítania. Érdekeik biztosításának érdekében változtattak a műveleti vezetés struktúráján, a „Különleges Hadművelet" élére Szergej Szurovikint állították, aki olcsó irányból importált Shahed-136 drónok segítségével megkezdte az ukrán energetikai infrastruktúra támadását, ezzel hivatalosan is anyagháborúvá változtatta a hadszíntér jellegét. Az Oroszországi Föderáció fegyveres erői több szempontból is tehermentesültek, 300 ezer tartalékost mobilizáltak, a Wagner csoport aktívabban kezdett részt venni a háborúban, valamint kiemelkedő szerepet kapott az orosz fél narratívájában. Az Oroszországi Föderáció önként kivonult Herszonból, az egyetlen elfoglalt nagyvárosból, melyet orosz magterületnek nyilvánítottak, egy 100 ezer négyzetkilométeres elcsatolt terület részeként. A kivonulás minden bizonnyal számos orosz életet mentett meg. 30 ezer fő ellátására mindössze 2 vasúti híd volt elérhető, így fenntarthatatlannak ítéltetett a lokális védelem. A kivonulás azonban nem zajlott hibátlanul, értékes nehézfegyverzet maradt hátra, működőképes mi-24-esek, emellett modern gyalogsági felszerelés. A kivonulás szervezettsége sem volt

megfelelő, számos orosz katonának a Dnyeperen kellett átúsznia vagy civil járműveket használnia, hogy el tudja hagyni a térséget. Ezen események a háború rövid távú stagnálásához vezettek pár lezáratlan védelmi kérdést kivéve, például a Kinburn-félsziget védelmét – viszont hosszú távon a konfliktus eszkalációját okozták.

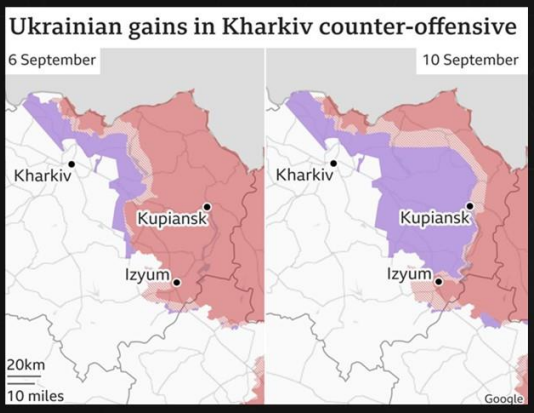
Kulcsszavak: Liman, Herszon, Szergej Szurovikin


Liman és Herszon
Schiller Gábor


Források, kutatás
Térképek: militaryland.net, deepstatemap.live
OSINT: Telegram (Intermarium TV, Bellum Acta, ATF – Anti Terror Force, Intel Slava Z, Kyiv Independent)
defensepoliticsasia.com
liveuamap.com
oryxspioenkop.com

Krízis az Oroszországi Föderációban

- Harkov, Izjum
  - Egy hónap visszavonulás
- Jelentése potenciális oroszpárti offenzívákra
  - Nincs kiszögellés, csak frontális lehetőségek
- Vezetés
  - Szergej Szurovikin kinevezése
- Mobilizáció
  - 300000 fő + Wagner Csoport



Bekerítés Limanban

Védelem helyzete

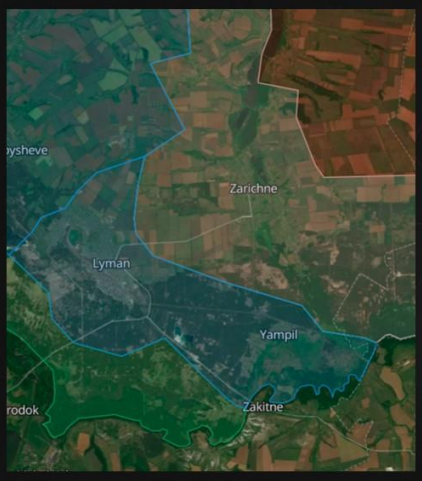
ATGM felszereltség, harckocsizó osztályok, kevés lőszer

Támadó felkészültsége

Fáradó egységek, lendület megőrzésének kísérlete

Végkifejlet

Hadifoglyok száma kérdéses, offenzíva megállítása bármi áron

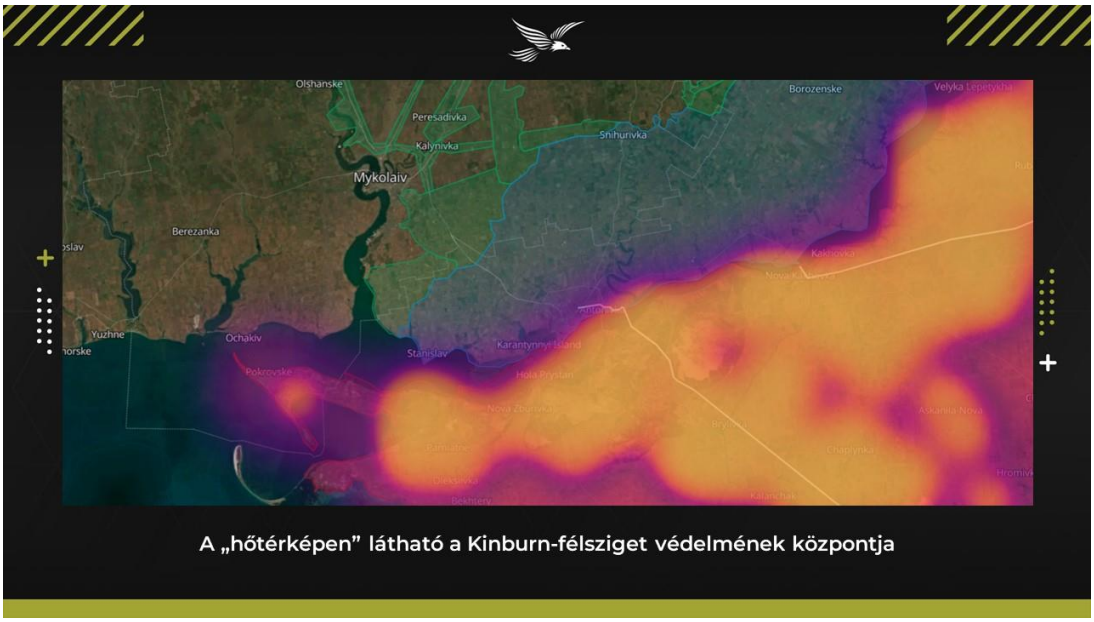


Herszon evakuálása

- Miért
  - Logisztika nehézségei pl. HIMARS miatt
- Miért most
  - Saras időszak
- Vitatható sikeresség
  - Hátramaradt fegyverzet, halottak

Ukrán SOF és tüzérség

- Kinburn-félsziget
  - Kitettség az ukrán tüzérségnek
- Biloberezhia Nemzeti Park
  - Logisztika ellehetetlenítése
- Védelem kérdése
  - Könnyen védhető part, előnytelen logisztikai adottságok



A „hőtérképen” látható a Kinburn-félsziget védelmének központja

A háború folytatása

Donyeck

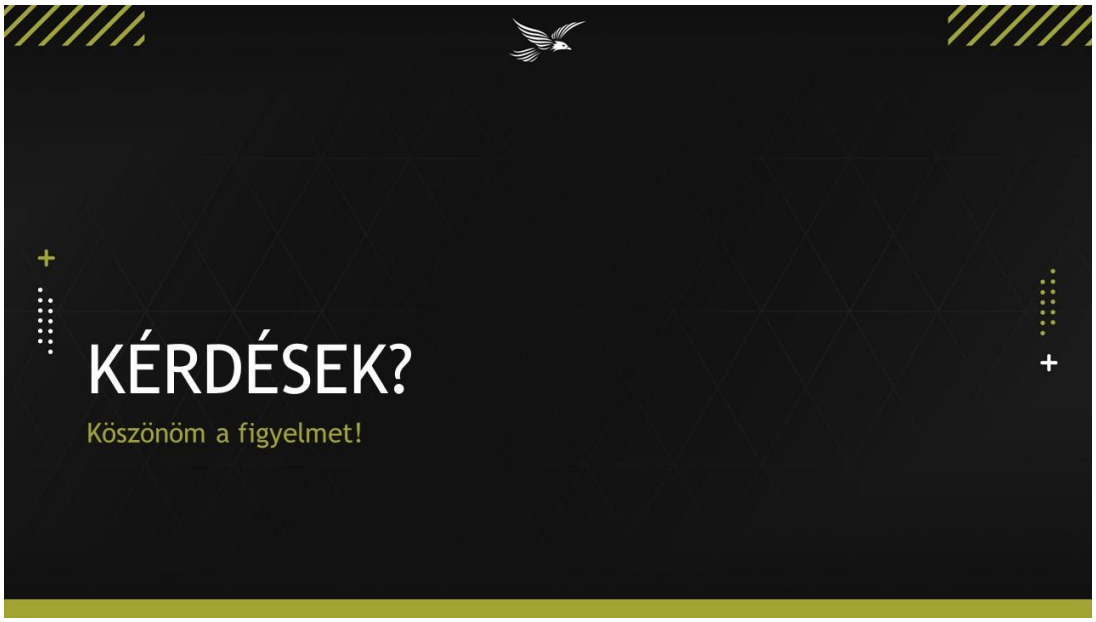
Fő frontvonal, erődített terület elleni offenzíva

Bakhmut

Lokációja fenyegeti az orosz logisztikát

Fehéroroszország

Új front nyitása kérdéses, elégtelen csoportosítás


KÉRDÉSEK?
Köszönöm a figyelmet!

Székely Loránd: Az okos eszközök és a vezetés kapcsolata

Absztrakt

A kutatásom során arra kerestem választ, hogy a vezetés és a vezetéselmélet hogyan változott meg az évszázadok során, és melyek azok a kihívások, melyekkel a vezetőnek szemben kell néznie napjainkban. Először meghatároztam, hogy mi is a vezetés a vezetéselmélet klasszikusai alapján és bemutattam, hogy a klasszikus vezetéselmélet képviselői hogyan hatottak a vezetésre. A vezetés meghatározása után a digitalizációról annak hatásairól a társadalomra majd a vezetésre gyakorolt hatásairól van szó, itt megemlítve a kiberteret, amely az egészet összefogja, a mesterséges intelligenciát, mint jelenleg is és a jövőben is nagy potenciállal bíró technológiát, illetve az okos eszközöket. Az okos eszközök olyannyira a mindennapjaink részévé váltak, hogy a társadalmunk már képtelen meglenni nélkülük, így a vezetés szempontjából is meghatározó a szerepük. Az okos eszközök számának alakulását vizsgálom napjainkig és a számuknak a becsült változását a jövőre nézve, mely növeli a kockázatukat a társadalomra nézve. A vezetés szempontjából kitérek azokra a főként negatív hatásokra, amelyek az okos eszközök és a digitalizáció hatására alakultak ki, illetve megpróbálok ezekre egy megoldást találni, amivel a vezető ezeket a problémákat kezelni tudja. Ennek hatására beszélek az egészséget támogató vezetést, mint egyik legmeghatározóbb és legfontosabb vezetési attitűdöt,

amely az alkalmazottak lelki egészségére figyel és ez által javítja az ők munkával való kapcsolatát.

Kulcsszavak: Digitalizáció, vezetéselmélet, egészséget támogató vezetés, okos eszközök

Az előadás tartalma

- A téma aktualitása
- Mit jelent vezetni?
- Klasszikus vezetéselmélet képviselői
- A digitalizáció
- A digitalizáció hatásai
- Az okos eszközök és a vezetés
- Egészséget támogató vezetés
- Összegzés

A téma aktualitása

- A digitalizáció jelenléte az életünkben
- A technológia ellenére a vezető szerepe megkérdőjelezhetetlen
- Az okos eszközök okozta veszélyek

„Egy hadsereg vezér nélkül semmit sem ér”
Bonaparte Napóleon

Mit jelent vezetni?

A vezetés:

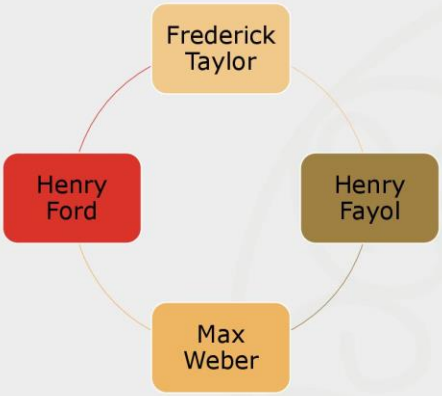
- Sajátos emberi tevékenység
- Társadalmi tevékenységi folyamat
- Emberek meghatározott csoportjában érvényesül

A vezető:

- Másokat befolyásol
- Meghatározza a célt
- Erőforrás-feltételek megteremtése

(Czuprák, Kovács, 2017)

A klasszikus vezetéselmélet képviselői:



A digitalizáció:

- Jason Bloomberg
  - analóg információ kódolása
    - Feldolgozás
    - Tárolás
    - Továbbítás
- Tér és idő eltörlése
  - Globalizáció

(Bloomberg, J. 2018)

[1]

A digitalizáció hatásai:

- A kibertér
  - Globális tartomány
  - Információs környezetben
- Mesterséges intelligencia
  - Nagy potenciál
  - Sokan félnek tőle
- Közösségi média:
  - Áldás és átok

[2]

Okos eszközök:

- A társadalom nincs felkészülve
- Veszélyek a felhasználókra nézve

Okos eszközök és a vezetés:

- Teleworking
- Home-office
- Technostress

[3]

[4]

Egészséget támogató vezetés:

Egészség megőrzése:
- Fizikai szempontból
- Lelki szempontból

A vezető felelőssége a munkaerő megőrzése

Munkahelyi stressz csökkentése
- Megfelelő munkakörülmények megteremtése
- Megbecsülés
- Elismerés

Maslow féle szükséglet piramis
(McLeod, S. 2007)

Összegzés:

- A klasszikusok még mindig aktuálisak
- A digitalizáció és az okos eszközök fontossága megkerülhetetlen
- A vezetői szerep fontossága

„Aki kimarad, lemarad”

(Csikósné Maczó, E. 2021)

Felhasznált képek:

[1] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.ciat.org%2Fciatblog-los-dilemas-de-la-digitalizacion%2F%3Flang%3Den&psig=AOvVaw3zmESNAMsIHbJ8TAPPzxrO&ust=1667588089882000&source=images&cd=vfe&ved=0CA0QjRxqFwoTCJDjt_PXkvsCFQAAAAAdAAAAABBX (letöltés ideje:2022.11.03.)

[2] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.searchenginejournal.com%2Fwhy-social-media-is-important%2F285809%2F&psig=AOvVaw2v5KdyYfGQzjBflEnj6SXd&ust=1667594177814000&source=images&cd=vfe&ved=0CA0QjRxqFwoTCNDR18jukvsCFQAAAAAdAAAAABAI (letöltés ideje:2022.11.03.)

[3]https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.dhrm.virginia.gov%2Fteleworking&psig=AOvVaw2FBI9Jk0jpPgskI1Me87YB&ust=1667652205432000&source=images&cd=vfe&ved=0CA0QjRxqFwoTCMifp97GlPsCFQAAAAAdAAAAABAa (letöltés ideje:2022.11.04.)

[4] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwhatfix.com%2Fblog%2Fbeat-workplace-technostress%2F&psig=AOvVaw2mwOPB_99L9gX6thNUnuQj&ust=1667652523117000&source=images&cd=vfe&ved=0CA0QjRxqFwoTCJD51_bHlPsCFQAAAAAdAAAAABAm

Felhasznált szakirodalom:

- Czuprák, O. and Kovács, G., 2017. *A szervezetvezetés elmélete*. Budapest: Dialóg Campus.
- Kulcsár Zs. (2014): Az integratív e-learning felé. http://bit.ly/2pa8mYF
- Prensky, M. (2001): Digital Natives, Digital Immigrants In: On the Horizon. (MCB University Press) 9, 5, October 1–6. DOI: 10.1108/10748120110424816, https://bit.ly/2ySL1ib .
- Csikósné Maczó, E. (2021). Aki kimarad, az lemarad?: A digitális munkarendre átállt oktatás megítélése a hátrányos helyzetű tanulókra nézve.
- McLeod, S. (2007). Maslow's hierarchy of needs. Simply psychology, 1(1-18).
- https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

KÖSZÖNÖM A FIGYELMET!

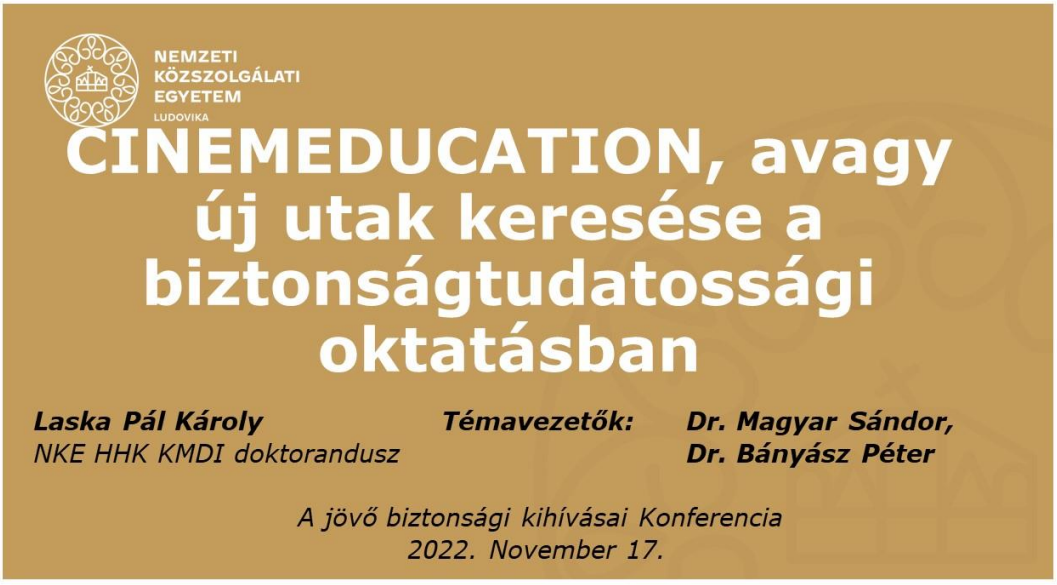
uni-nke.hu

Laska Pál Károly: Cinemeducation – avagy új utak keresése a biztonságtudatossági oktatásban

Absztrakt

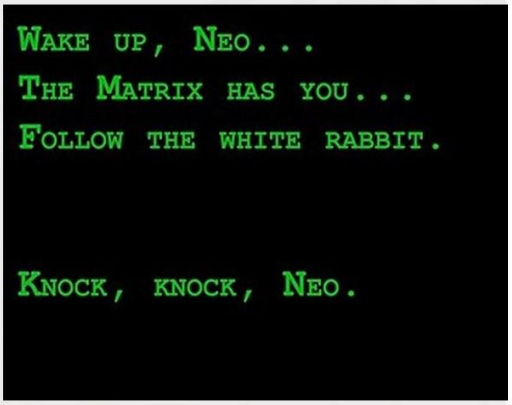
A fiatalok jelentős online kockázatoknak vannak kitéve. Az online csalások, a cyberbullying, az adathalászat szinte a mindennapok része – különösen a Nemzeti Közszolgálati Egyetem hallgatói számára fontos, hogy ezek ellen védekezzenek, hiszen néhány év múlva fontos államigazgatási, rendvédelmi, honvédelmi feladatokat fognak betölteni. Ezért kiberbiztonsági tudatossági oktatóanyagok felkészíthetik őket arra, hogy megvédjék magukat az online kockázatokkal szemben. A kutatás célja volt, hogy megvizsgálja a hallgatók kiberbiztonsággal kapcsolatos ismereteit és ehhez új módszert, az ún. Cinemeducationt használtuk, amely fikciós alkotások (mozifilmek, televíziós sorozatepizódok, stb.) segítségével mutatja be az adott kiberbiztonsági problémát. A hallgatók ezirányú ismereteinek vizsgálata során gamification módszert alkalmaztunk, ami a tudatossági viszonyok elemzésében is segített. A kísérleti pilot projekt azt mutatta, hogy az egyetemi hallgatók kiberbiztonsági tudatossága nem megfelelő szintű, a hallgatók átlagnál nagyobb része nincs tisztában azzal, hogyan védjék meg saját adataikat. Az új ismeretbővítési módszer hozzájárult, hogy a hallgatók biztonságtudatosabban viselkedjenek. Emellett a felmérés azt is jelezte, hogy a diákok nagyobb lelkesedéssel viszonyulnak a kiberbiztonsági kérdésekhez.

Kulcsszavak: kiberbiztonság, egyetemi hallgatók, Cinemeducation, Nemzeti Közszolgálati Egyetem



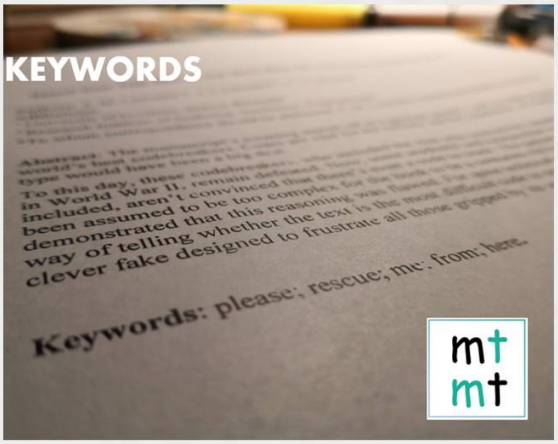
Kutatás előzményei

- TDK (OTDK)
- Struktúrált interjúk három szakterület
  - Tudomány - Dr. Krasznay Csaba
  - Oktatásfejlesztés, tartalomgyártás - Apertus Nonprofit Zrt.
  - Forgatókönyvírás - Szélesi Sándor
- Kérdőíves felmérés
- Kulcsszóelemzés
- Tudománymetria
- Hálózatelemzés



Tudományos probléma

- Mindenhol jelenlevő, folyamatosan változó kockázatok
- Alacsony tudatossági szint
- Változások az oktatásban



Problémák az oktatásban

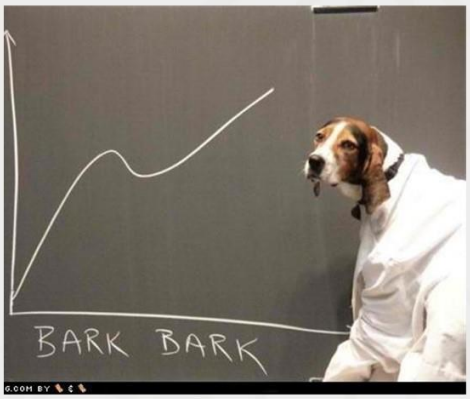
- Generációs különbségek
- Digitális bevándorlók, bennszülöttek
- Nem készít fel az új típusú fenyegetésekre
- NKE speciális feladatrendszere
- Képzési sajátosságok
- Szakfejlesztés: Kreatív Tanulás Program

Kutatási kérdések

- Milyen a kapcsolat a film és kiberbiztonság között?
- Filmek által növelhető-e a kiberbiztonsági tudatosság?
- Tudunk-e változtatni a viselkedésünkön, hogy biztonságosabban éljünk?

Kutatási módszerek

- Kulcsszó analízis (IMDB)
- Hálózatkutatás (IMDB)
- Fókuszcsoportos interjú
- Cinemeducation modell egy pilot projekten
- Gamification (Kahoot)

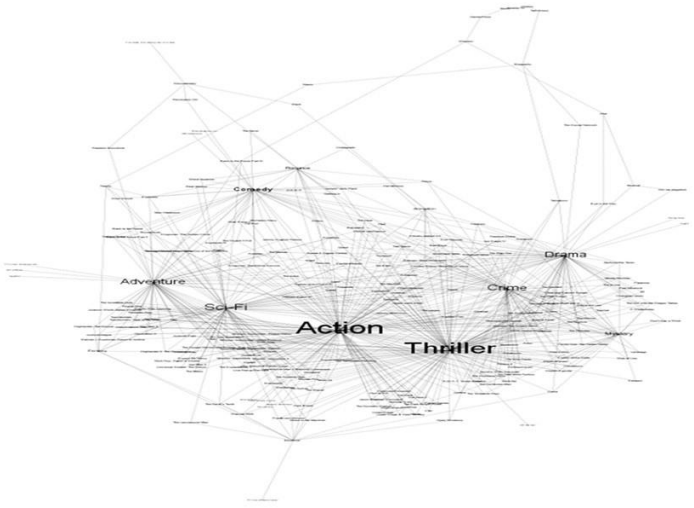


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Eredmények I.

Filmművészet és kiberbiztonság kapcsolata

IMDb adatbázis alapján: 942 filmből 2848 db műfajbesorolás



Hálózatkutatás - A kiberbiztonság témája leggyakrabban a thriller műfajban jelenik meg

Klasszikus hollywoodi dramaturgia

	Háborús játékok (1983)	Komputerkémek (1992)	Mátrix (1999)	Kardhal (2001)	Mr. Robot (2015)
A pozitív hős	tinédzser gamer	profi csapat vezetője	programozó és hacker	büntetett hacker	introvertált hacker
A megtámadott számítógép	katonai szimulációkat lejátszó szuperkomputer	önálló szakmai hálózatok	teljes virtuális tér	kormányzati adatbázis	közérdekű adatot tartalmazó vállalati szerver
A támadás módja	„hátsó kapu”	nyílt forráskódú kódolás	telefonvonalon keresztül	külső gépről végrehajtott támadás adott idő alatt	túlterheléses támadás
Utóélet	USA törvénymódosítás	„RSA- kódolás”	internet szerepéről szóló viták	külső okok miatt kevéssé jelentős	valószerű támadások bemutatása

A filmek főhősei a kor legmagasabb szintjén alkalmazzák a kiberteret

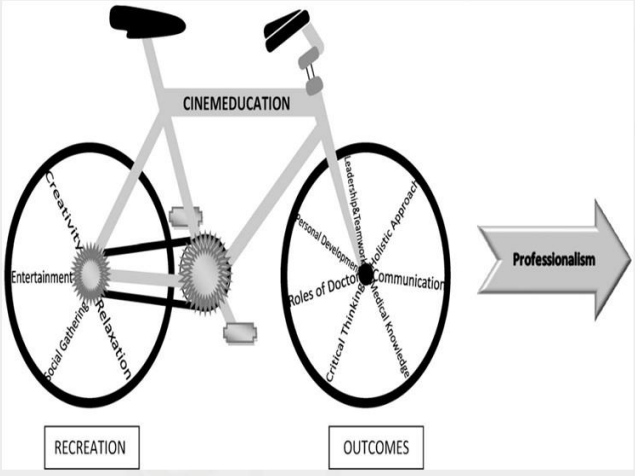
NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Eredmények II.

Filmművészet az oktatásban

„Cinemeducation” – modell: kapcsolat az oktatás és a filmek között

- Alkalmas adott jelenségek bemutatására
- Főszereplői a vizsgált terület különböző szintjein működnek
- A probléma időszerű és releváns



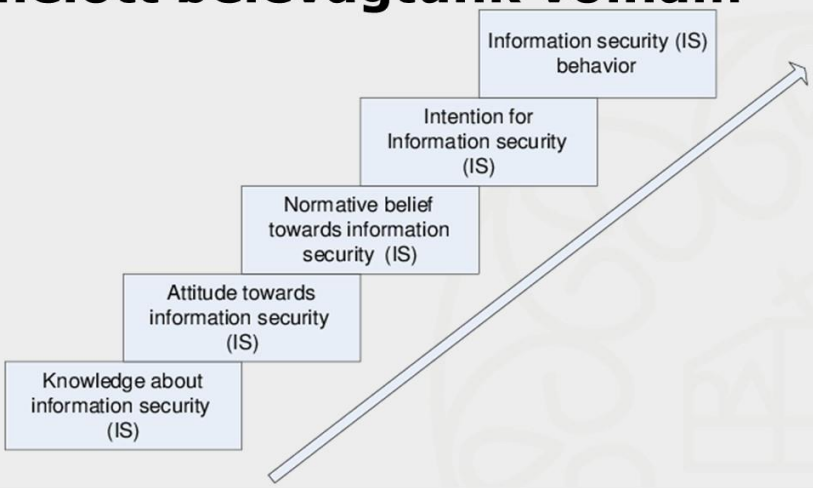
A kísérleti kurzus

- **„Jogok, kötelezettségek és a biztonság a virtuális térben”**
- Hétfő este 18.00-19.30,
- Demotiváció, fáradtság,
- 11 hallgató,
- Közigazgatás mesterszak, 4. szemeszter
- Előző félévben: Adatvédelem és kiberbiztonság a közigazgatásban című tárgyból kollokvium, hozzá tartozó szeminárium
- Kahoot óra elején kompetencia felmérés, óra végén visszamérés

Tematika és filmek

2019.02. 4-8.	Bevezetés (ismerkedés, követelmények, fókusz csoportos interjú)
2019.02. 11-15.	A kibertér biztonságpolitikai kihívásai: Háborús játékok, Mr. Robot, Skyfall
2019.02. 18-22.	A virtuális tér (cyberspace) fogalma: Zaklatás, Tron, Matrix
2019.02. 25-2019.03.1	A kiberhadviselés alapjai: Die Hard 4.0, Skorpió s01e01, Komputerkémek, Hackers
2019.03.4-8.	Támadási és védekezési sémák a virtuális térben műszaki szemszögből
2019.03. 11-15.	Megfigyelés: Snowden, A kör, Bourne Ultimátum, Bourne Rejtély
2019.03.18-22.	Megfigyelés társadalma: 1984, Black Mirror s03e01
2019.03.25.-29.	Kiberbűnözés: Blackhat, Kardhal, Hálózat csapdájában
2019.04. 1-5.	A virtuális tér problémáinak elemzése: Közellenség, Johnny English 3., Office Space, Nerve
2019.04. 8-12.	Információs műveletek: Black Mirror s01e01, Berlin Station s03e01
2019.04. 15-19.	Hacktivizmus: A WikiLeaks-botrány, Harcosok klubja, V mint Vendetta
2019.04. 22-26.	Húsvét
2019.04. 29-2019.05.3.	Social engineering: Black Mirror s03e03, Takedown
2019.05. 6-10.	Ember-gép interfész, AI: 2001 Űrodüsszeia, Különvélemény, Transzcendens, Ex-Machina, Black Mirror s01e03, s02e01
2019.5. 13-17.	Összefoglalás, zárás

Mielőtt belevágtunk volna…



… pár kérdés

Tudás

- Volt- e korábban kiberbiztonsággal kapcsolatos kurzusa?
- Mit jelent az Ön számára a kiberbiztonság kifejezés?
- Milyen védelmi megoldásokat ismer?
- Az utóbbi 5 évben milyen jelentős kiberbiztonsági incidensekről hallott?

Attitűd

- Alapvetően műszaki vagy humán területként értékeli a kiberbiztonságot? Miért?
- Biztonságtudatosnak tartja-e önmagát?

Jogszabály

- Milyen kiberbiztonsággal kapcsolatos jogszabályokat ismer?
- Mennyire ismeri a GDPR rendelkezéseit, bevezetésének körülményeit?
- Ismeri-e a szervezete informatikai biztonsággal kapcsolatos szabályzóit? Kiberbiztonsági incidens esetén kihez fordul?

… és még pár

Szándék

- Mennyire érzi célpontnak magát? Mint magánember? Mint a szervezet, ahol dolgozik, tanul? Mint ország?
- Volt-e mar áldozata kiberbiztonsági incidensnek? Ha igen, miképpen oldotta meg?
- Az élete melyik területén gondolja fontosnak a kiberbiztonságot? Magánélet, iskola, munka?

Viselkedés

- Milyen védelmi megoldásokat használ az eszközein?

Előzetes interjú tapasztalatai

- „Voltam korábbi kurzuson, de…”
- „Én nem vagyok elég fontos/érdekes”
- Hírek, még a mainstream hírek is felületesen ragadtak meg, ha egyáltalán…
- Az új megközelítés lelkesítő volt
- Történet, karakterek – döntési helyzetek, lehetőségek mérlegelése

Visszajelzés, korrekció

- „… azóta letakarom a webkamerám”
- Növekedett a biztonságtudatosság, az érzékenység
- Kahoot eredményei alátámasztották, hogy figyeltek az órán

- Jelenlegi kurzus kontrollcsoport

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

KÖSZÖNÖM A MEGTISZTELŐ FIGYELMET!

Kérdés?

laskapal@gmail.com

Tóth András: The applications of the Cloud of Things in the defence sector

Abstract

Today, Internet of Things (IoT) devices are widespread and are no longer limited to the private sector but also to the commercial, industrial and defence sectors. The volume of data they collect, the need for continuous availability and the need to make the best use of performance and resources make it advisable to connect these systems to cloud computing. This is called a Cloud of Things (CoT) approach, which provides solutions that deliver these capabilities.
In his analysis, the author has investigated the possibilities of applying IoT tools to the following elements of the defence sector:

- Law Enforcement;
- Military;
- Disaster Management;
- National Security.

He then examined the potential benefits of connecting each separate IoT ecosystem to a central cloud and the impact this could have on the operation of digital or smart governments.

Keywords: Internet of Things, Cloud of Things, defence sector, Law Enforcement, Military, Disaster Management, National Security


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
The applications of the Cloud of Things in the defence sector
Dr. Tóth András
A jövő biztonsági kihívásai II.
Konferencia
2022. november 17.
Supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the
ÚNKP-22-5-NKE-88 New National Excellence Program of the Ministry of Innovation and Technology
from the source of the National Research, Development and Innovation Fund."
Új Nemzeti Kiválóság Program


Agenda
I • Law Enforcement: Police Department
II • Law Enforcement: Prison Service
III • Disaster Management
IV • Military
V • National security
VI • Cloud of Things in the defence sector
VII • Conclusions

Law Enforcement: Police Department

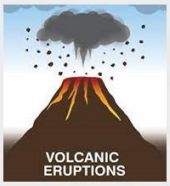
- On-Board sensors and detectors
- Radar detector
- License plate scanners
- Traffic signals
- Roadside cameras
- Traffic database
- Body camera
- Head up display
- Drones

Law Enforcement: Prison Service

- Environmental monitoring sensors and cameras
- Biometric jail management
- RFID-tracking
- Ankle monitors
- Suicide-alert sensors
- Fleet control of patrols and internal relocation vehicles

Disaster Management

- **Volcanic Disaster Management**
- **Forest Fire Disaster Management**
- **Flood Disaster Management**
- **Landslide Disaster Management**
- **Earthquake Disaster Management**
- **Victim Localization**







Military

- **Locators**
- **Cameras**
- **Sensors**
- **Radars**
- **Sonars**
- **RFID**
- **Short range military drones**
- **Lasers**
- **Sensors providing combat vehicle data**
- **Cameras**
- **Heart Rate Monitors**





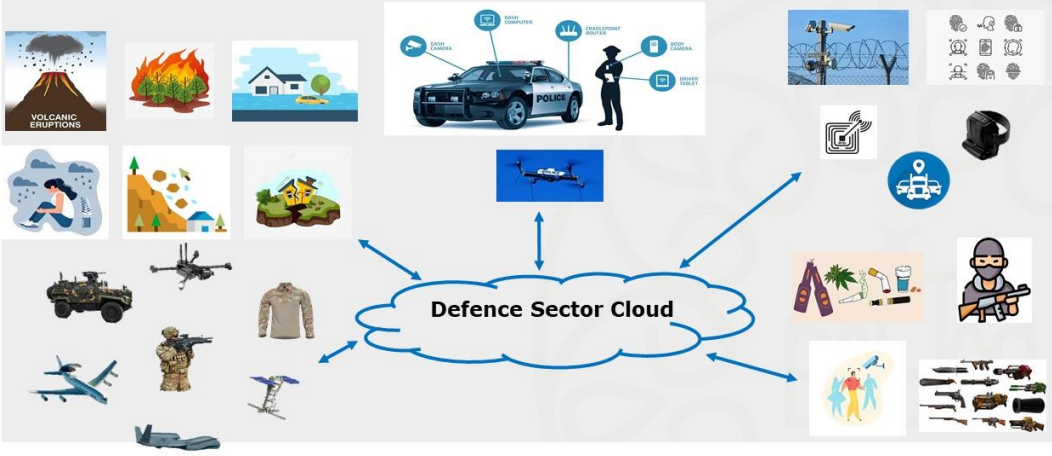


National security

- **Intelligence information gathering**
- **Monitoring organised criminal activities**
- **Tracking terrorist persons, organisations**
- **Tracing illegal drug and weapons trafficking**




Cloud of Things in the defence sector



Conclusions

- Scalability, high speed
- Continuous availability
- Efficient asset management
- Robust, comprehensive surveillance network
- Decentralised
- Easy information sharing with the right permissions
- Real-time information gathering

THANK YOU!

en.uni-nke.hu

Bús Nikolett Katalin, Magyar Sándor: The role of Security Operations Centres in supporting cyber security

Abstract

Today, there is a growing focus on digitalisation, and a growing dependence on IT systems. More electronic information systems means more hardware and software in the systems. The number of IT developments is increasing. Companies' efficiency is also increasing through IT systems. This development brings with it an increase in the number and volume of cybercrime, which must be followed up with appropriate action on the cyber defence side.
Cybersecurity can be enhanced in a number of areas. The PreDeCo principle areas of prevention, detection and correction have a crucial role to play in cyber security, none of which can be neglected.
The key function of the SOC is to detect and respond immediately to security threats and incidents and to manage and maintain the security state of an organisation.
Strategic decisions play a key role. Can the organisation develop and maintain an effective SOC or should it be used as a service? If it can be developed, what will be the milestones on the way to achieving an effective SOC?
The level of maturity of the organisation is very important in the case of SOC. The organisation need to assess the availability of the required technical equipment; the current organisational structure; the available human resources; the required IT training.

Security Operations Centres can be supported by a variety of security platforms. These include Security Information and Event Management (SIEM) systems, which are primarily responsible for collecting and analysing security-related data. Security Orchestration, Automation and Response (SOAR) platforms are used to automate and streamline the process of responding to security threats, and Extended Detection and Response (XDR) includes the collection and analysis of data from multiple sources.
Collaboration is an extremely important area for SOCs, which can help organisations share information and knowledge to achieve more effective protection. Particular attention should be paid to Indicators of compromise (IoC) and Tactics, Techniques, and Procedures (TTPs).

Kulcsszavak: Security Operations Centre, Security Information and Event Management, Security Orchestration, Automation and Response, XDR, IoC, TTPs

The role of Security Operations Centres in supporting cyber security

Nikolett Katalin BÚS, Sandor Magyar

Impact of IT systems penetration

- More electronic information systems:
  - Hardware;
  - Software.
- IT developments are increasing.
- Companies' efficiency increases through IT systems.
- Increased dependency on IT systems.
- Increase in the number and volume of cybercrimes.

PreDeCo

- Cybersecurity can be enhanced in a number of areas.
  - Prevention.
  - Detection.
  - Correction.

Security Operations Centres

- The key function of the SOC is to detect and respond immediately to security threats and incidents and to manage and maintain the security state of an organisation.

Strategic decisions

Strategic decisions play a key role.

Can the organisation develop and maintain an effective SOC or should it be used as a service?

If it can be developed, what will be the milestones on the way to achieving an effective SOC?

Maturity level

- The level of maturity of the organisation is very important in the case of SOC. You need to assess:
  - the available technical equipment;
  - the current organisational structure;
  - the available human resources (level 1-3);
  - the required IT training;
  - the suitability of the accommodation conditions
  - etc.

SOC platforms

- Security Information and Event Management (SIEM).
- Security Orchestration, Automation and Response (SOAR).
- Extended Detection and Response (XDR).

Cooperation, collaboration

- Collaboration is an extremely important area for SOCs, which can help organisations share information and knowledge to achieve more effective protection. Particular attention should be paid to Indicators of compromise (IoC) and Tactics, Techniques, and Procedures (TTPs).

References

- HÁMORNIK Balázs Péter: A Security Operations Center (SOC): A kiberbiztonsági csapatmunka és kihívásai, Hadmérnök, XIII. Évfolyam 2. szám – 2018. június. Pp.: 393-408. http://hadmernok.hu/182_27_hamornik.pdf
- Ötvös Antal: Rögzítendő jó SOCaaS OK, avagy jó gyakorlatok a kibervédelmi központokban. EIVOK-24. Szakmai Fórum, 2022.03.31. https://www.hte.hu/documents/10180/4737479/SOC.pdf

Thank You for your kind attention!

Kerti András: Security of unclassified information

Abstract

Many of the events of the Ukraine-Russia war in our neighbourhood have drawn attention to the importance of information security, including the security of unclassified (non-classifiable) information. In my next lecture I will discuss the basics of the protection of unclassified information. What misconceptions have I encountered on the subject. I will prove the necessity of protection in a logical way and finally I will propose possible ways to enhance the security of unclassified information.

Keywords: Fully open data, Non-public data, Classified data, information security, awareness raising activities

Scope of data processed in the public sector

- Personal data
- Public interest data
- Data of public interest
  - "Fully open data"
  - **"Non-public data"**
  - Classified data
    - Restricted
    - Confidential
    - Secret
    - Top secret

The "legal" aspects of protection

- Hungary
  - Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information
    - The body performing a public task must enable anyone to have access to the data of public interest, subject to the exceptions specified. Exceptions:
      - Classified data
      - **Restrictions on disclosure by law**
      - **Data used in the preparation of a decision**

The "legal" aspects of protection

- European Union
  - COM(2022)119 Final (REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information security in the institutions, bodies, offices and agencies of the Union)
    - three levels of non-classified information: public use, normal and sensitive non-classified;

The "legal" aspects of protection

- NATO
  - CM(2002)60 THE MANAGEMENT OF NON-CLASSIFIED NATO INFORMATION
    - NATO UNCLASSIFIED
      - Administrative markings
    - Information releasable to the Public

Why dont need to deal with it?

- Theses on information security ignorance:
  - Satellites see everything, no secrets from them
  - Information security is the job of the professionals (IT, IT specialist)
  - If it were important information it would be classified

A logical approach to the need for protection

- In other words, why the previous statements **are not true**.
  - Mosaic principle
  - The undeniable elements of critical infrastructure
  - The existence of open source detection

What is the disclosure?

- Disclosure: making data available to anyone (Act CXII of 2011)
  - Who is anyone?
    - My colleague?
    - Social media?
    - Public lecture?
    - A conversation on public transport?

Proposals for greater information security

- The security of non-public data can be improved:
  - Increased information security through awareness raising activities
  - Simplifying the classification process
  - Use of administrative markings based on the "need to know" principle

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu

Ináncsi Mátyás: Social media sentiment of the russian-ukranian conflict

Abstract

We see information being shared on social media constantly, especially when the conflict began, social media had a high role in sharing information. The baseline for this research is to show the user sentiment regarding the Russian-Ukrainian conflict. For this research, SentiOne social media analysis platform was used. The method for the research was social listening, from social listening the software is capable determining the user sentiment. Timeframe for the research was between 2022. 03. 01. and 2022. 11. 01.

Around 775 thousand results were analyzed, and these posts had a reach of 65 770 million users. The reach and mentions were slowly decreasing since March, with one exception: October. During October there was a clear bump in the slow decrease, this might have happened due to the Ukrainian counter-offense and territorial gain. Regarding the reach it is worth noting that from a social media perspective Facebook had the highest reach level, following it came surprisingly Instagram and TikTok.

Source distribution vise the top sources were Facebook and Twitter. By analyzing the results furthermore, we can see the top authors. Interestingly all the top authors were traditional media, which are represented in social media. New York Times, CNN, and The Guardian took the lead in top authors.

The big question is still the user sentiment, which was the focus of the research. How do the users feel about this conflict? What is their sentiment on social media? The results for user sentiment were overwhelmingly neutral. More than 85% of the analyzed posts were neutral, which makes sense in the information sharing role. The user sentiment has not changed a lot by time. The negative sentiment has decreased since March, but overall, the user feeling remained the same.

In summary we can say that the conflict had a high reach ratio, top authors remained traditional media and users overwhelmingly felt neutral in their posts during this conflict.

Keywords: Social media, Russian-Ukranian conflict, information sharing role, sentiment analyses

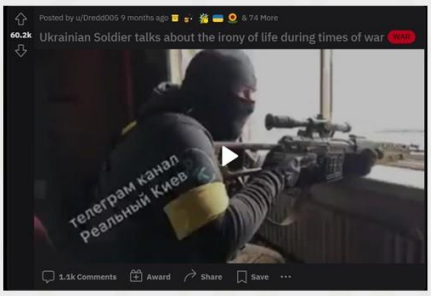
NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Social media sentiment of the russian-ukranian conflict

Ináncsi Mátyás – UPS: Military Science Doctorate school

I. Baseline of the research

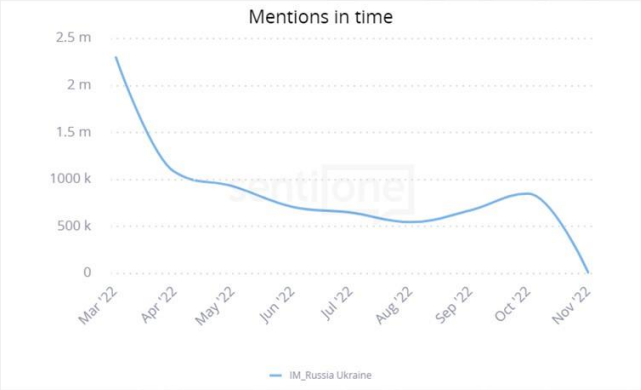
- The russian-ukranian conflict is highly shared on social media
- Quick wartime information sharing
- Research method:
  - SentiOne analysis of the user sentiment regarding the conflict
  - Timeframe
    - 2022. 03. 01 – 2022. 11. 01.



Source:
https://www.reddit.com/r/ukraine/comments/tjyzsq/ukrainian_soldier_talks_about_the_irony_of_life/

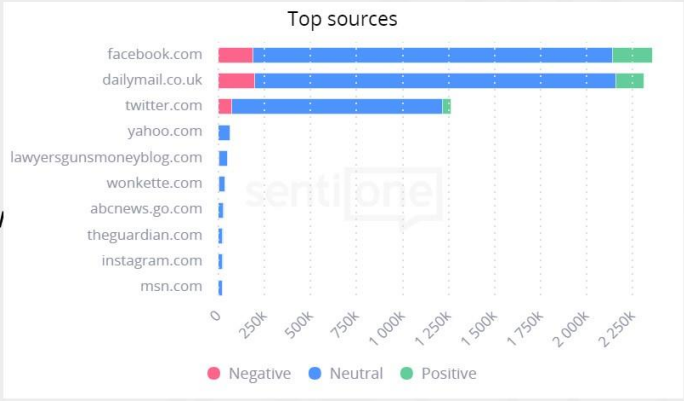
II. Social media reach of the conflict

- Clearly the beginning of the conflict had the highest reach
- October was a raise
  - The moment when Ukraine started major offenses



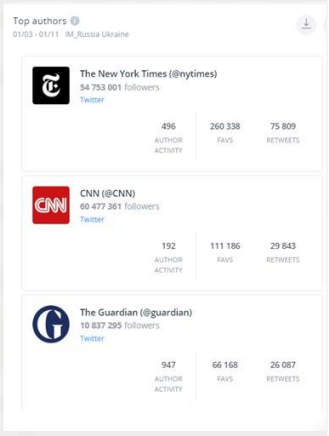
III. Source distribution

- Facebook, Dailymail and Twitter had the highest reach
- Reddit is not included
- Facebook has a low moderation level, which may assist information sharing, same applies to Twitter

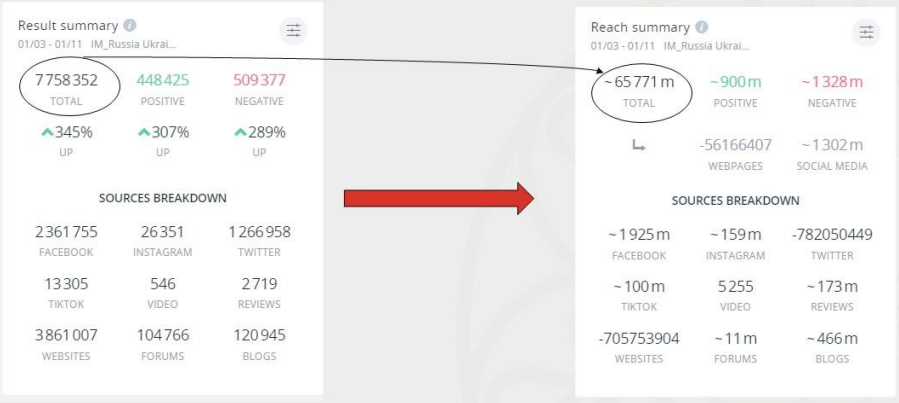


IV. Top Social media authors

- To no suprise traditional media is still strong, the top authors are traditional media which are represented in social media:
  - New York Times
  - CNN
  - The Guardian
  - Fox News
  - The Economist
  - Bloomberg
  - Reuters
- No non-news sites were part of the top author list

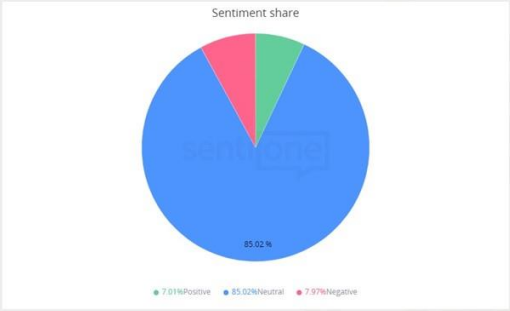


V. Result and reach connection



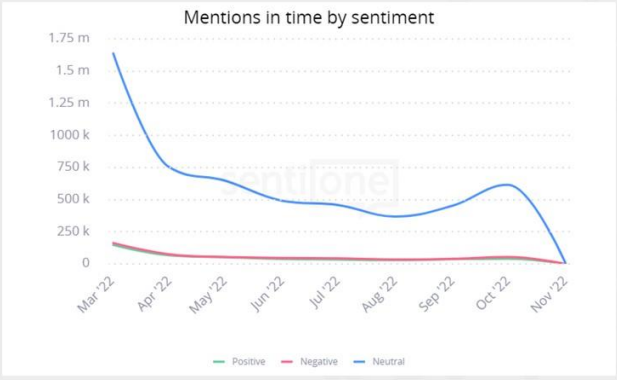
VI. And by timeframe?

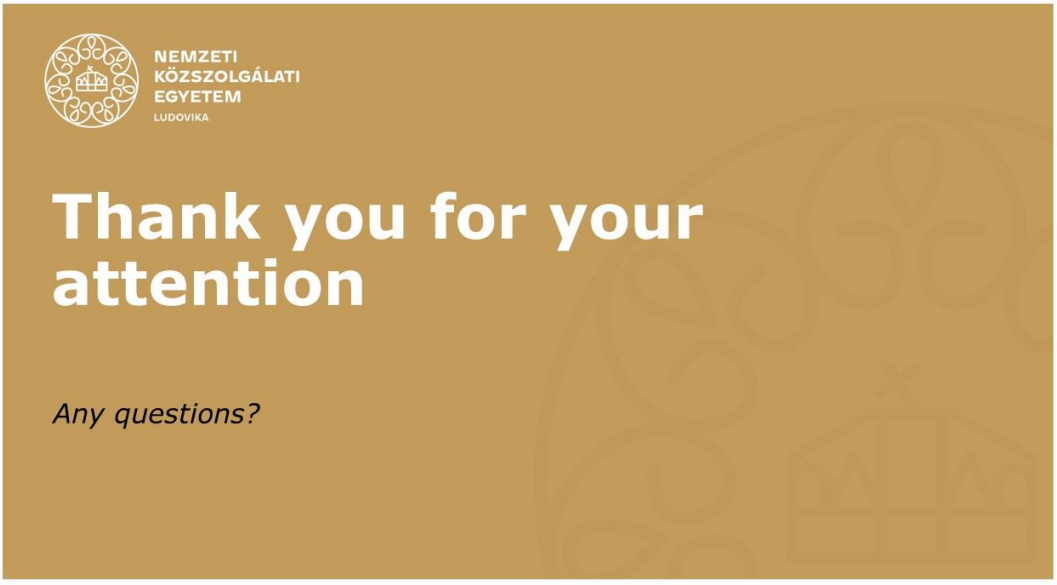
- So how did the responders react to the conflict?



V. User sentiment

- By timeframe we can see neutralness remained:




NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
Thank you for your attention
Any questions?

Bús Nikolett Katalin: Information security incident management- In a Hungarian company's programme

Abstract

Information security incident is defined by the Act L of 2013 on the Electronic Information Security of State and Local Government Bodies as a security incident: 'an unintended or unanticipated unique event or series of events that causes an adverse change or a previously unknown situation in an electronic information system, and as a result of which the confidentiality, integrity, authenticity, functionality or availability of the information carried by the electronic information system is lost or damaged.'

If the security incident involves personal data content, a data breach is detected. The term data breach is defined in the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information as 'a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or transmission of, or access to, personal data transmitted, stored or otherwise processed.'

Pursuant to Article 25/E(1)(j) of the Data Protection Act, 'the controller shall record the circumstances in which a personal data breach occurs in relation to the data it processes, the effects of the personal data breach and the measures taken to deal with it'.

The purpose of information security is to ensure the confidentiality, integrity and availability of the information handled. Information

security covers all events that occur during the life cycle of information (creation, access, handling, processing and destruction). In other words, information security goes beyond the provision of information systems and services.

In all cases, information security incidents should be documented, as fully as possible, in order to support the detection of the incident, to record the evidence necessary for subsequent possible prosecution and to improve the effectiveness of preventive measures.

Vulnerabilities related to the way systems, services, tools are designed or used present risks to employers. It is in the vital interest of employers to identify these vulnerabilities in order to prevent further security incidents or potential security incidents (and the associated losses).

Reported information security incidents should be investigated to determine the extent to which information security controls have been breached and whether the results of the investigation can be used to determine whether the reported incident falls into the category of an information security incident. If an information security incident is involved, a report shall be made immediately and the management of the information security incident shall be initiated and its impact and circumstances investigated.

In my presentation, I would like to describe the information security incident and incident management procedures in a Hungarian company's program.

Kulcsszavak: Information security, incident, incident management, vulnerabilities, investigation

Information security incident management- In a Hungarian company's programme

Nikolett Katalin Bús; Ph.D. student,
Óbudai University Doktoral School on Safety and Security Sciences,
e-mail: bus.nikolett@uni-obuda.hu, ORCID: 0000-0002-3069-4512

Objective

Information about an information security incident or event resulting from any incident or event should be communicated in an organised and controlled manner, as required by the owner, to the organisations and individuals competent to manage the information security incident or event, and to those who may be indirectly affected by the incident or event, as soon as possible.

Rules of Procedure

- Procedure for reporting information security incident that have occurred.
- A description of the handling process from the detection of the incident to the conclusion of its handling, with the definition of the associated tasks, responsibilities and accountabilities.
- Companies should be prepared to deal with an information security incident.
- Responsibility for preparing for and, if an incident occurs, managing the incident should lie with the relevant line managers, depending on the type of incident.

Reporting an incident

- **It is the responsibility of all employees to report any information security incident they become aware of to the appropriate persons without delay.**

In the event of an information security incident involving a business system:

- To be reported to the IT service provider, with the immediate supervisor and the company information security officer informed.

Physical security incident:

- To be reported to the CEO, with the immediate supervisor and the corporate information security officer informed.
- Other security incident:
- To be reported to immediate supervisor and to the Corporate Information Security Officer.

Incidents can be reported through various channels, such as e-mail, phone, in person. In all cases, the fastest and most direct communication channel possible should be used.

Receiving, recording, preliminary assessment of an incident

- The reception, recording and preliminary assessment of the incident is carried out by the competent staff member of the receiving department, depending on the type of incident, but the competent departmental manager is responsible for its implementation.
- The competent line manager receiving the notification shall record the incident in a documented form, which may be:

  a) e-mail

  b) a form completed via the web interface

  c) minutes

  d) voice note (in case of a report made in person or by telephone, if possible)

Receiving, recording, preliminary assessment of an incident

The documented notification must include the following information in all cases (in the case of unknown information, the "no information" flag applies):

a) the identity of the notifier: name, primary employer, title, contact details;

b) incident details: description of circumstances, exact time, location, cause, expected effect/consequence, expected course of action, action taken, persons notified;

c) information on the person who received the report: name, primary employer, position, contact details.

Evaluation of the incident

Once the incident has been recorded, it is the responsibility of the relevant line manager at the Company to assess and categorise the notification, but the relevant line manager is responsible for its implementation.

The final result of the categorisation of the notification may be as follows:

a) there is no real information security incident underlying the notification;

b) an information security incident;

c) information security incident.

Evaluation of the incident

If the incident is related to the processing of personal data, the identification and handling of the personal data breach will be further handled in accordance with the internal rules on personal data processing and data protection.

There may also be information security incidents that require the involvement of other stakeholders in their assessment. In such cases, an expert working group should be convened to carry out the categorisation.

Evaluation of the incident

Depending on the type of information security incident, the working group may consist of:

- in the case of an IT security incident, the IT service provider or the company operations
- for a physical security incident, the security service provider
- the Data Protection Officer in the event of a personal data breach
- in the case of other security incidents, the company's Information Security Officer, or representatives of other disciplines, depending on the incident, will form the investigation committee.

Initiate incident response

In the event of an incident, immediate action must be taken to rectify it. Where it cannot be excluded that an information security incident has occurred, particular care shall be taken to ensure that evidence is not compromised during the response.

Depending on the type of incident the responsible line manager shall be responsible for the response and for restoring the default protection level.

If the incident can be handled internally, the corporate information security officer shall coordinate its resolution and investigation.

Delimitation of assets involved, collection of evidence

The investigation of information security incidents can be started in parallel with the resolution of information security incidents. If necessary, the first step is to isolate the affected assets, which will allow the evidence to be preserved and collected in its original state.

Depending on the type of incident, the responsible line manager is responsible for the containment and collection of evidence. The collection of evidence shall be the responsibility of the relevant functional staff responsible for the management of the incident. Evidence collection may also be carried out by the company's Information Security Officer or by other parties (IT and security service providers) involved in the investigation.

Delimitation of assets involved, collection of evidence

Possible ways to collect evidence:

a) examination of log files on the systems under investigation

b) examination of IT devices (including smartphones) involved in the incident and their images

c) in case of reasonable suspicion, access to the electronic communications of the user involved in the incident (e.g. corporate correspondence, corporate chat or documents stored on a central server)

d) CCTV footage.

e) Witness interviews (data subjects, managers, experts)

Delimitation of assets involved, collection of evidence

When collecting and handling evidence, particular attention must be paid to compliance with the provisions of the GDPR. The information collected is strictly confidential and must be treated accordingly. Access to the information collected shall be restricted to the persons involved in the investigation and to the managing director and his/her authorised representatives.

The evidence gathered during the investigation of the incident shall be recorded in the minutes.

Closing the incident, taking minutes

The handling of an incident is considered closed when the incident has been responded to, prevented, the risk of further damage has been reduced to a negligible level, the collection and examination of evidence has been completed, the incident has been investigated, the necessary findings have been made by the experts and conclusions have been drawn.

The steps taken to deal with incidents requiring treatment, and the results of the investigation, should be documented and recorded by the relevant incident handler

Information security incident management post communication

If necessary (e.g. when an incident affecting all employees of the company occurs), the affected employees should be informed of the incident via e-mail or other IT systems (Intranet news, pop-up).

Prior to such notification, it is necessary to consider whether and to what extent the user affected by the incident needs to be informed of the incident (e.g. users need to be informed of a phishing attack, but not necessarily of a problem detected by a monitoring tool).

The report must contain information on the incident to the extent necessary and sufficient, and detailed sharing of incidents or test results is prohibited. It shall be the responsibility of the relevant line manager to provide the information.

Thank you for your kind attention!

Sz. Podmaniczky Katalin: A kontrollrendszer a védelem szolgálatában

Absztrakt

A globalizáció és a digitalizáció napjainkban olyan mértékű és irányú fejlődést generál, illetve kényszerít ki, ahol a dinamikusan változó biztonsági környezet egyre nagyobb felkészültséget és egyre rövidebb reakcióidőt vár el a védelmi tevékenységben résztvevőktől. Ennek csak a szükséges együttműködések megvalósítását és az eredményes koordinációt támogató működési környezet és eljárások kialakításával lehet megfelelni. Ezt biztosítja a kontrollrendszer részét képező kontrollkörnyezet, kockázatkezelés, kontrolltevékenységek, információs és kommunikációs rendszer, illetve a monitoring rendszer megfelelő kialakítása.

Az egyértelműen elhatárolt szerepek, a célok eléréséhez való hozzájárulás, illetve ezen belül a saját résztevékenység pontos ismerete alapvetően meghatározza a végrehajtás minőségét. A védelmi tevékenység – a tervezéstől a végrehajtás értékeléséig – megbízhatóbbá válik a résztvevők tudatosságának fokozása során. Ezt veszélyeztethetik a kapacitásproblémák, az időnyomás vagy egyéb havaria tényezők, ezért a nemkívánatos események bekövetkezésének megakadályozását, a vezető által kijelölt irányhoz való igazodást csak a folyamatba épített kontrollok képesek garantálni.

A vezetés által a célok elérése érdekében működtetett kontrollrendszer elemei minden tevékenységre vonatkoznak és biztosítják az elvárások teljesülését, valamint alkalmasak a változó környezet és az esetleges információs és kommunikációs zavarok esetén is biztosítani a működés folyamatosságát és a vezetői szándéknak megfelelő végrehajtást olyan módon, hogy az utólag is ellenőrizhető és értékelhető legyen.

Kulcsszavak: digitalizáció, kontrollrendszer, információs és kommunikációs rendszer, működésbiztonság

A jövő biztonsági kihívásai

A kontrollrendszer a védelem szolgálatában

Sz. Podmaniczky Katalin
NKE HHK HDI

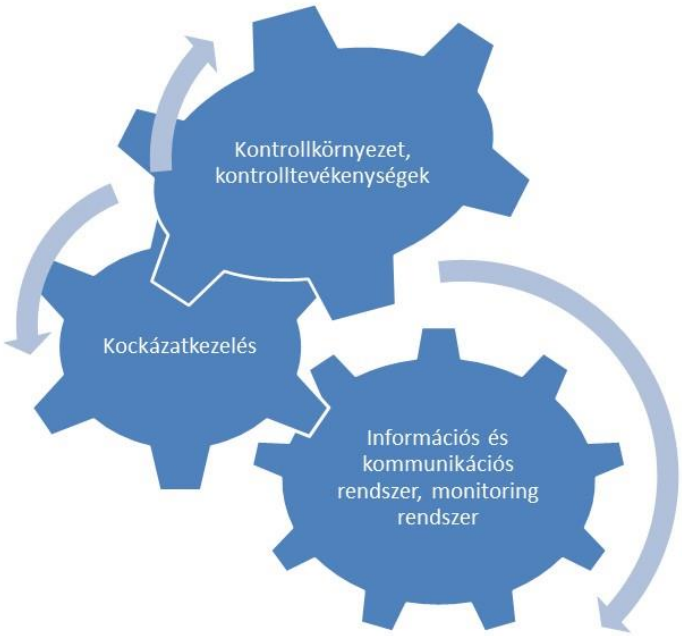
Új működési környezet: gyorsuló globalizáció és digitalizáció

https://www.coe.int/hu/web/compass/globalisation

https://autopro.hu/szolgaltatok/a-kisvallalkozasoknak-is-digitalizalni-kellene/211805


Kihívások 1.
Felkészültség
Specializálódás
Sokszereplős folyamatok
Együttműködés
Koordináció

Kihívások 2.


Kontrollkörnyezet, kontrolltevékenységek
Kockázatkezelés
Információs és kommunikációs rendszer, monitoring rendszer

A végrehajtás minősége

- Elhatárolt szerepek
- Hozzájárulás ismerete
- Tudatosság
- Egyértelmű vezetői elvárások
- Konkrét célok

- Kapacitásproblémák
- Időnyomás
- Havaria tényezők
- Információs és kommunikációs rendszer zavarai

Összefoglalás

Működésbiztonság

Végrehajtás zavartalansága

Váratlan helyzetek kezelése

Kiszámíthatóság

Felkészültség

Köszönöm a figyelmet!

Szerzőink figyelmébe

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

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

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

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

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

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

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

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

Az űrlapok a szerkesztőségnél szerezhetők be.

Megjelent az NKE HHK Híradó Tanszék gondozásában

www.comconf.hu
www.puskashirbaje.hu

HU ISSN 2061-9499

***

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