HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2022

Új típusú kihívások a biztonságban

tudományos szakmai konferencia

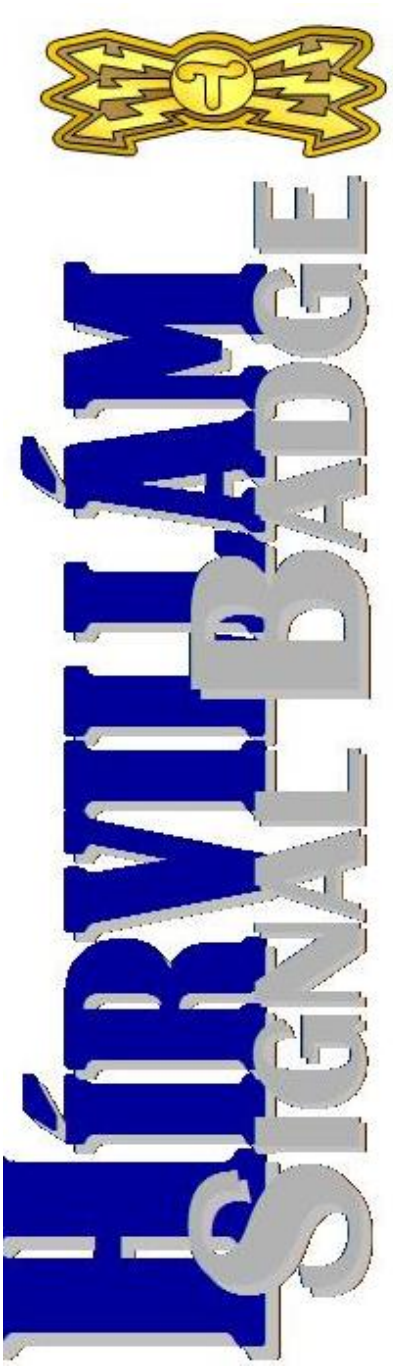
Konferencia kiadvány és korreferátum gyűjtemény

2022. február 28.

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



Felelős kiadó/Editor in Chief
Dr. Fekete Károly

A konferencia szervezőbizottsága, illetve a kiadvány szerkesztőbizottsága/Editorial Board

Elnök/Chairman of the Board
Dr. habil. Kerti András

Főszerkesztő/Co-ordinating Editor
Dr. Tóth András

Tagok/Members
Dr. Bányász Péter
Dr. habil. Farkas Tibor
Dr. Horváth Zoltán
Kirovné Dr. Rácz Réka
Dr. László Gábor
Dr. Magyar Sándor
Orbók Ákos
Szűcs Attila

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. január 20-21 között a Puskás Tivadar Műszaki Szakkollégium, a Hírközlési és Informatikai Tudományos Egyesület Információbiztonsági Szakosztálya, valamint a Magyar Hadtudományi Társaság Kápolnai Pauer Ifjúsági Klubja által megrendezésre került az Új típusú kihívások a biztonságban című szakmai tudományos konferencia. A konferencia alapvető célja egy évente megrendezésre kerülő tudományos szakmai fórum biztosítása a kutatási eredmények bemutatása, ismeretterjesztés, valamint kapcsolatépítés céljából. A konferencián összesen 33 kutató, doktorandusz, mester- és alapszakos hallgató mutatta be kutatási eredményeit, melyek közül jelen kiadványban a szerzők hozzájárulásával 33 került megjelentetésre, olyan területeket érintve, melyek veszélyeztetik napjaink biztonsági környezetét.

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

Budapest, 2022. február 28.

Dr. habil. Kerti András
a Szerkesztőbizottság
elnöke

A konferencia programja

ÚJ TÍPUSÚ KIHÍVÁSOK A BIZTONSÁGBAN **Nemzetközi tudományos - szakmai konferencia** *(2022. január 20.)* Oktatási központ, O-114-115 MULTI	
08:55-09:00	**MEGNYITÓ** **Dr. Tóth András**
Elnökség: **Dr. Magyar Sándor, Dr. Bányász Péter** **PANEL I.**	
09:00-09:15	**Dub Máté:** *A PET-ek befogadásának mérhetősége, és az információbiztonság növelésének kapcsolata*
09:15-09:30	**Katona Gergő:** *Az autonóm járművek kiberbiztonsági aspektusa*
09:30-09:45	**Tóth Rebeka:** *Biztonsági tesztelés a felsőoktatásban*
09:45-10:00	**Hankó Viktória:** *Nők az IT biztonsági szektorban - egy kvalitatív kutatás eredményeinek elemzése*
10:00-10:15	**Botan Renáta:** *Cyberbullying az online játékokban*
10:15-10:30	**Pajor Fanni:** *Okos otthonok biztonsági kihívásai*
10:30-10:45	**Molnár Ákos Ádám:** *Álhírek a koronavírus tükrében*
10:45-11:00	**Sz. Podmaniczky Katalin:** *Információs kockázatok*
KÁVÉSZÜNET	

Elnökség: **Dr. habil. Kerti András, Kirovné Dr. Rácz Réka** **PANEL II.**	
11:30-11:45	**Nyári Merse:** *Hibrid hadviselés - régi eszközök új köntösben*
11:45-12:00	**Schiller Gábor:** *Kína összfegyvernemi zászlóaljai kétéltű és szárazföldi műveletekben*
12:00-12:15	**Kugler Péter:** *A Kínával kapcsolatos narratíva és infodémia, az új hidegháború kapujában*
12:15-12:30	**Epresi Ádám:** *A Biden-adminisztráció Tajvan-politikája*
12:30-12:45	**Bellus Bálint:** *A műholdromboló fegyverek napjainkban*
12:45-13:00	**Baji Raik Martin:** *A 3D nyomtatott lőfegyverek nemzetbiztonsági kockázatai*
13:00-13:15	**Kárpáti Zalán:** *Nukleáris erők és a XXI. század*
13:15-13:30	**Pulai Bence:** *A 2021-es lengyel-fehérorosz határkonfliktus*
EBÉDSZÜNET	
Elnökség: **Dr. habil. Farkas Tibor, Dr. Tóth András** **PANEL III.**	
14:00-14:15	**Fülöp Bence:** *Armageddon hadművelet*
14:15-14:30	**Lux Benjámin:** *Kárpátalja geopolitikája a XX. század első felében*
14:30-14:45	**Kiss András László:** *"Aki bújt, aki nem", avagy a digitális terepmintákról*

14:45-15:00	**Korcsik Kristóf:** *A magyar-csehszlovák lakosságcsere és hatásai napjainkban*
15:00-15:15	**Vattai Eszter:** *Az infokommunikációs technológiák térhódítása, és annak hatása napjainkra*
15:15-15:30	**Baglyos Sándor:** *IT biztonsági auditálás (online)*
15:30-15:45	**Kiss Márton:** *Az emlékezetpolitika, mint a biztonsági kihívás a 21. századi Európában (online)*
15:45-16:00	**A konferencia zárása** **Dr. Tóth András**

ÚJ TÍPUSÚ KIHÍVÁSOK A BIZTONSÁGBAN **Nemzetközi tudományos - szakmai konferencia** *(2022. január 21.)* Zártkörű - Online	
08:55-09:00	**MEGNYITÓ** **Dr. Tóth András**
Elnökség: **Dr. Horváth Zoltán, Orbók Ákos** **PANEL I.**	
09:00-09:20	**Dr. Magyar Sándor:** *Az elektronikus információs rendszerek (EIR) fejlődése a kibertérben*
09:20-09:40	**Dr. Kerti András:** *Információbiztonsági tudatosság*
09:40-10:00	**Dr. Farkas Tibor:** *Electronic information systems today: mobile communications*
10:00-10:20	**Dr. László Gábor:** *Infodémia*
10:20-10:40	**Dr. Bányász Péter:** *A COVID-al kapcsolatos érzelmek vizsgálata Magyarországon*
10:40-11:00	**Szűcs Attila:** *Biztonsági kihívások a mesterséges intelligencia katonai alkalmazásában*
KÁVÉSZÜNET	
Elnökség: **Dr. László Gábor, Szűcs Attila** **PANEL II.**	
11:20-11:40	**Dr. Tóth András:** *Hálózatba kapcsolat harctéri eszközök (IoBT)*
11:40-12:00	**Kirovné Dr. Rácz Réka:** *A szélsőséges időjárási események okozta károk társadalmi költsége*

12:00-12:20	**Dr. Horváth Zoltán:** *Rejtjelezést és adatrejtést megvalósító programcsomag*
12:20-12:40	**Bús Nikolett Katalin:** *Információbiztonsági stratégia alkotás*
12:40-13:00	**Németh Attila:** *Drón detektálás, drón elhárítás kihívásai*
13:00-13:20	**Ináncsi Mátyás:** *Nyílt információ kérdésköre a közösségi média vonatkozásában*
13:20-13:30	**A konferencia zárása** **Dr. Tóth András**

Dub Máté: A PET-ek befogadásának mérhetősége, és az információbiztonság növelésének kapcsolata

Korreferátum

Korunk információs társadalmának, és az infokommunikációs technológiák ugrásszerű fejlesztésének és elterjedésének „köszönhetően" a biztonságban egy új típusú kihívásként jelent meg az egyének privátszférájának megfelelő szintű védelme, mely egyaránt hatással lehet az otthoni környezetünk, magánszféránk -, illetve munkahelyünk biztonságára.

A privátszférát erősítő technológiák (PET-ek) egy megoldást nyújthatnak a felhasználók tudta és beleegyezése nélkül begyűjtött, akár algoritmusok által elemzett és ismeretlen, harmadik fél számára továbbított adatok védelmével kapcsolatban. Ezen adatok jogszerű és szakszerű védelme azért is kiemelt fontosságú, mivel a felhasználók akár több ezer szempont szerint is profilozhatók, – ugyan általában csak a hirdetések kapcsán megjelenő profitmaximalizáció érdekében, – viszont ezen információk illetéktelen kézbe kerülése esetén kiváló nyersanyagot biztosíthatnak a humán-alapú támadások sikeres végrehajtásához.

A PET-ekre összességében tehát a megfelelő szintű egyéni és vállalati információbiztonság megteremtésének egyik alappilléreként tekinthetünk. Az előadás középpontjában mind ezekből adódóan az a kérdéskör szerepel, hogy az egyének a saját magánszférájuk védelmének érdekében milyen lehetőségeket alkalmazhatnak, és azok használatának, „befogadásának" milyen

főbb tényezői vannak? Ezek közé elsődlegesen a ráfordított anyagi erőforrások, az implementáláshoz szükséges idő és energia, valamint a szükség esetén elsajátítandó kompetencia tartozik, és sikeres befogadásról pedig abban az esetben beszélhetünk, ha bizonyos mértékben a korábban említett kategóriák közül valamennyit a felhasználó képes „rááldozni" a privátszférájának magasabb szintű védelme érdekében. Ezen tulajdonképpeni arányszám megállapítása pedig a munkáltató számára is fontos lehet, és azokat be is vezetheti többek között ajánlás, vagy szervezeti eszközökön kötelező jelleggel. A különböző jogszerűtlen adatkezelésekből, adatszivárgásokból, és kapcsolódó hiátusokból adódó, a munkavállalókat érintő sikeres kompromittációk ugyanis közvetlen módon érinthetik a szervezet biztonságát, hiszen a munkavállalók, vagyis a humán tényező, mint az információbiztonság leggyengébb láncszeme a statisztikák szerint kulcsszerepet játszat tudta és akarata ellenére is egy sikeres támadás végrehajtásában.

NEMZETI KÖZSZOLGÁLATI EGYETEM LUDOVIKA

INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

Új Nemzeti Kiválóság Program

PUSKÁS TIVADAR

A PET-EK BEFOGADÁSÁNAK MÉRHETŐSÉGE, ÉS AZ INFORMÁCIÓBIZTONSÁG NÖVELÉSÉNEK KAPCSOLATA

ÚJ TÍPUSÚ KIHÍVÁSOK A BIZTONSÁGBAN – 2022. 01. 20.

DUB MÁTÉ
PUSKÁS TIVADAR MŰSZAKI SZAKKOLLÉGIUM
MAGYAR HADTUDOMÁNYI TÁRSASÁG

KONZULENS: DR. BÁNYÁSZ PÉTER

Az előadás az Innovációs és Technológiai Minisztérium ÚNKP-21-2-II-NKE-70 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

Előadás felépítése

1. Téma aktualitása
2. Probléma megfogalmazása
3. Mik azok a PET-ek?
4. Az otthoni és a munkahelyi környezet kapcsolata
5. Bevezetés kérdésköre
6. Összegzés

Téma aktualitása

- Információs társadalom → Információkezelés kérdése + Alá-fölé rendeltségi viszony ← Információs túlhatalom problémája.
- Szolgáltatók és webhelyek adatkezelési általános hozzáállása és adatvédelmi **hiátusok**.
- **Profilozás** problémaköre – profitmaximalizáció (marketing- és hirdetési tevékenység); valamint az adatszivárgás kockázata.
- Humán-alapú támadások ← A támadók helyzete, motivációi és lehetőségei.

Probléma megfogalmazása

- A megfogalmazott kihívásokból adódó új kockázat kezelése;
- Információbiztonság szerepe;
- Védelem prosperálásának lehetőségei (?) → **PET-ek (Privátszférát erősítő technológiák)**;

\+ **Kiberhigiéniát erősítő** és **digitális lábnyomot minimalizáló** lehetőségek.

Privacy enhancing technologies

- PET-ek fogalma:

- *„A PET olyan **információs** és **kommunikációs technológiák** gyűjtőfogalma, amelyek **megerősítik** az egyén **magánéletének védelmét** egy **információs rendszerben** azáltal, hogy megakadályozzák a személyes adatok **szükségtelen** vagy **jogellenes** felhasználását, vagy olyan **eszközöket** és **beavatkozási lehetőségeket** kínálnak, amelyek **növelik az egyén ellenőrzését személyes adatai felett**."*

- *„A PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs privacyt a **személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi**, és így **megakadályozza a személyes adatok szükségtelen** vagy **nemkívánatos kezelését**, **anélkül**, hogy **csökkentené az információs rendszer funkcionalitását**."*

PET-ek rendszertana

- Felhasználó oldali technikák;
  - Nyomkövetés-elleni (ad-blockerek, pop-up tiltók és digitális ujjlenyomat minimalizálók).

- Szerver oldali technikák;
  - Adatok eltüntetése / semlegesítése / helyettesítése.

- Csatorna oldali technikák
  → Felhasználók és szerver közti kommunikációs- védelmi megoldások.
  - Biztonságos kommunikációk biztosítása (kliens-oldali és végponti titkosítás);
  - „Megbízható harmadik fél" ← Anonimitás / Pszeudonimitás.

A PET-ek alapvető kritériumai

1. **Anonimitás**:
   Az adatok **nem összekapcsolhatók** meghatározott személyekkel.
2. **Pszeudonimitás**:
   Van alany, de annak **kiléte nem ismert**;
   Pl. több fedőnév, álprofil, virtuális személyiség.
3. **Megfigyelhetetlenség**:
   Harmadik fél **kizárása**;
   Pl. észlelhetetlenség biztosítása nyílt hálózat használatakor.
4. **Összeköthetetlenség**:
   Jogosulatlan harmadik fél kizárása a kapcsolatteremtésből;
   Az alany szokásainak és **profilozásának** megakadályozása;
   Pl. adott oldal használatakor a megelőző vagy soron következő használt oldalak megfigyelésének letiltása.

A PET-ek csoportosítása

1. **Szubjektumorientált** PET-ek:
   - Középpontban az **alany**;
   - Azonosítás megszüntetése / korlátozása;
   - Egyaránt vonatkozik tranzakciókra és rögzített adatokra;
   - Pl. egyszerhasználatos azonosítók, digitális fedőnevek.

2. **Objektumorientált** PET-ek:
   - Középpontban az **eszköz**;
   - „Digitális ujjlenyomatok” kizárása;
   - Pl. telefonálási szokások naplózása.

A PET-ek csoportosítása

3. Tranzakcióorientált PET-ek:

- Az alany **tevékenységének** / **visszafejthetőségének** / **követhetőségének** védelme / megakadályozása;
- Hálózati tranzakciók során;
- Módszer: bejegyzések törlése, adatláncolatok feldarabolása;
- Pl. automatikus kitöltések automatikus törlése.

4. Rendszerorientált PET-ek:

A három csoport rendszerbe történő szervezése.

LEHETŐSÉGEK, PÉLDÁK

„Zero knowledge proofs”

- Nulla-tudásalapú-igazolás-támogatás;
- Személyazonosság-ellenőrzésre;
- Személyes adatok megadásának helyettesítésére;
- Tranzakciók során;
- Egyedi / személyes kriptográfiai megoldások:

Két fél közül az egyik fél úgy tud megbizonyosodni egy másik fél „állításáról”, hogy annak nem szükséges felfedniük személyes adataikat.

„Szisztematikus adatkészletek”

- Kiegészítés a különböző adatvédelmi megoldások mellett párhuzamosan;
- Mesterséges adatgyűjtést folytat a PET;
- Mintákat rendszerez, azokat szisztematikusan ismétel;
- Statisztikai jellemzőkre támaszkodik;
- Tulajdonképpeni való adatokat közöl, viszont:
- Ellehetetleníti a személy **valós** tevékenységének megfigyelését.

„Helyi feldolgozás”

- Alkalmazások, adatok és szolgáltatásoknál;
- Hálózatok végpontjain található központosított csomópontokból történő „adatmentesítés” / kiürítés.
- Helyi feldolgozás = adatminimalizáció;
- Csökkentett adatgyűjtés megvalósul: központosított szolgáltatásokban gyűjtött / megőrzött adatok; felhő-alapú tárolásban gyűjtött / megőrzött adatok kapcsán.
- Optimális nagy sebességet igénylő eszközök / rendszerek kapcsán.

Az otthoni és a munkahelyi környezet kapcsolata

- Profilozás → Humán-alapú támadások → Egyének kompromittálása;
- Megjelenik a szervezeti szint;
- A kitettség a „hozzáférés” kapcsán definiálható.
- Különbség az erőforrásokban → Lehet válasz PET-ek alkalmazása?
- Fő kérdések:
  - Kockázatokkal arányos?
  - Pénz / idő / energia?
  - Lehatárolható-e az alkalmazás a munkavégzés helyére / idejére?
  - Hogyan mérhető?

  +További lehetőségek!

Bevezetés kérdésköre

- Védelem prosperálása?
- **Kampányok** / **szoftveres** védelem / **tudatosítás** / **szabályzók**;
- Kiber-higiénia erősítése; Digitális lábnyom csökkentése;
- **Privacy-by-design** megoldások (GDPR-szellemében): (Beépített adatvédelem → Szervezetek és rendszerek kialakításakor / kezdetekor megvalósított adatvédelmi megoldások). → Adatvédelemi szempontok nem csak formai, hanem implementált jelleggel!

- **TAM** (TAM 1-3) – és **UTAUT** (UTAUT 1-2) modellek: *(technológia elfogadás – technológia elfogadás és -használat egységesített elmélete).*

Összegzés

- Információs társadalom → IKT → Megjelenő új típusú kihívások;
- Profilozás veszélyei;
- Humán-alapú támadások.

- PET-ek kulcsszerepe a védelemben.

- Otthoni és munkahelyi környezet kapcsolata;
- Az egyén és a munkáltató lehetőségei;
- A megfelelő „arány” meghatározása;
- **Kockázatokkal arányos védelem** megteremtése.

- A „befogadás” vizsgálata mindkét kategóriában.

Felhasznált szakirodalom

- Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. Journal of Network and Computer Applications, 102807. doi:10.1016/j.jnca.2020.102807
- Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. Computers & Security, 53, 1–17. doi:10.1016/j.cose.2015.05.002
- Gan, M. F., Chua, H. N., & Wong, S. F. (2019). Privacy Enhancing Technologies Implementation: An Investigation of Its Impact on Work Processes and Employee Perception. Telematics and Informatics. doi:10.1016/j.tele.2019.01.002
- Székely Iván, „A privátszférát erősítő technológiák” In: Dömölki, B (szerk.) Égenföldön informatika – az információs társadalom technológiai távlatai, Budapest, Magyarország: Nemzeti Hírközlési és Informatikai Tanács, Typotex Kiadó, (2008) pp. 419-433., 15 p.
- Tamara Keszey és János Zsukk, „Az új technológiák fogyasztói elfogadása. A magyar és nemzetközi szakirodalom áttekintése és kritikai értékelése”, Vezetéstudomány / Budapest Management Review 48 (2017. október 1.), https://doi.org/10.14267/VEZTUD.2017.10.05.

Katona Gergő: Az autonóm járművek kiberbiztonsági aspektusa

Korreferátum

A beépített technológiai megoldások és a vezeték nélküli képességek elterjedésével a mai járművek már nem elszigetelt mechanikus gépek. Egy összekapcsolt rendszer részévé válnak, amelyben folyamatosan kommunikálnak a járművek egymással és a forgalom irányítási központtal egyaránt. Ezen összekapcsolt adatok halmazát nevezzük intelligens közlekedési rendszernek. Ez a rendszer képes támogatni az autonóm közlekedés jövőbeli bevezetését és a mesterséges intelligencia használatával jelentősen javítani lehet a közlekedés biztonságát, hatékonyságát és fenntarthatóságát. Az intelligens közlekedési eszközök megjelenése azonban új biztonsági kérdéseket vet fel, amik az egész rendszert potenciális célponttá teszik a kiberbiztonsági támadásoknak, amelyek mind a közlekedés biztonságát, mind pedig az emberi életet veszélyeztethetik. Mára már számos olyan támadást lehet azonosítani, amely az egyes járművek intelligens rendszerelemeinek sérülékenységeit használják ki. Ezen támadások céljaikban is eltérőek tudnak lenni, az egyszerű információ szerzésen át, az autó működésképteleségének elérésén keresztül, egészen a jármű irányításának befolyásolásáig bezárólag.

Eladás menete

- I. A téma aktualitása
- II. Tudományos probléma meghatározása
- III. A kutatás célja
- IV. Tervezett módszertanok
- V. Hipotézisek
- VI. Eddigi eredményeim
- VII. Továbblépési lehetőségek

I. A téma aktualitása

- Autonóm közúti közlekedés
- Autonóm kötöttpályás közlekedés
- Autonóm drón közlekedés

II. Tudományos probléma meghatározása

- A közlekedési eszközök egyre több vezetést segítő rendszert alkalmaznak, amelyek befolyásolják a jármű működését.
- A közlekedést mint kritikus infrastruktúra ágazatot az intelligens és autonóm járművek biztonsági kihívásai nagyban befolyásolják.

III. Kutatás célja

- Egy átfogó kép kialakítása a fő biztonsági kérdésekről és az intelligens közlekedési eszközök irányítási rendszerét akadályozó különféle támadásokról.
- Egy biztonságos rendszer kialakításához a kutatásom elemzést fog nyújtani a meglévő megoldásokról, és kiemeli azok erősségeit és korlátait.
- Kérdőíves felmérés segítségével képet alakítok ki az autonóm közlekedés elfogadásának szintjéről hazai népesség körében.

III. Kutatás célja

- Az autonóm közúti közlekedési eszközök egyik rendszerelemére ki fogok alakítani egy biztonsági keretrendszert, amely reflektál a feltárt fenyegetések releváns csoportjára.

IV. Tervezett módszertanok

- Interjú a hazai kiberbiztonsági szakértőkkel
- Kérőíves felmérés
  - SPSS: kereszttábla elemzés, Kruskal-Wallis-próba

V. Hipotézisek

H1: A biztonságos autonóm közlekedés kialakításához szükséges egy központi közlekedési irányítási rendszer.

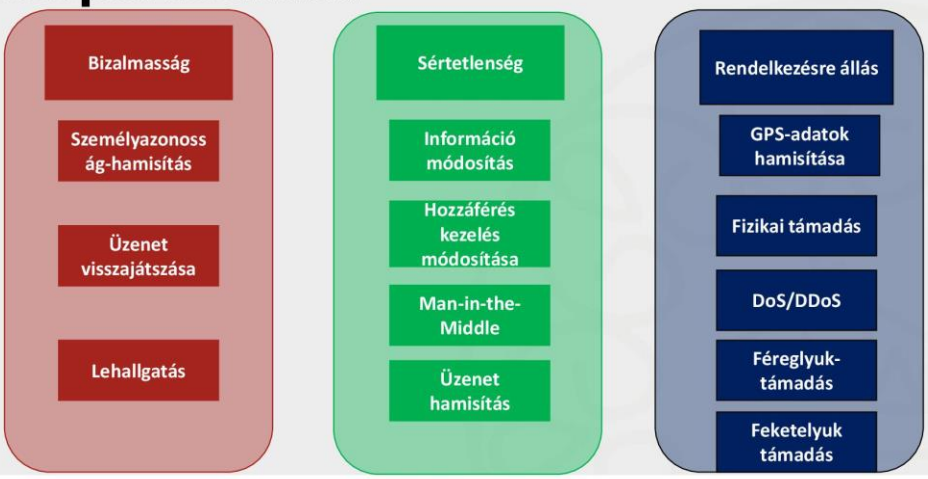
H2: Az intelligens közeledési eszközök biztonságával szemben bizalmatlanok az emberek.

H3: Kapcsolat mutatható ki az autonóm közlekedés definíciójának helyes meghatározása és az iskolázottság foka között a kitöltők körében.

VI. Eddigi eredményeim

- Felmérésre kerültek az autonóm autók és drónok rendszerelemei.
- Megkezdtem a felmérését az egyes rendszerelemek kitettségeinek.
- Azonosítottam azon szabványokat és ajánlásokat, amelyeket figyelembe fogok venni a keretrendszer kialakítása során.

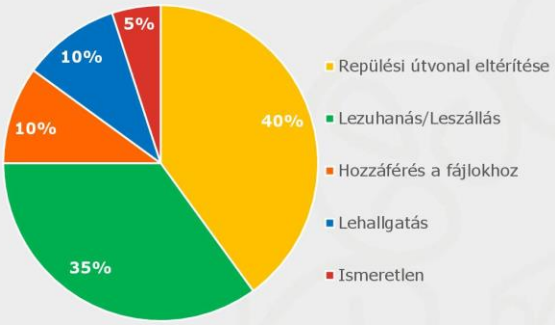
VI. Drónok kihívásainak csoportosítása



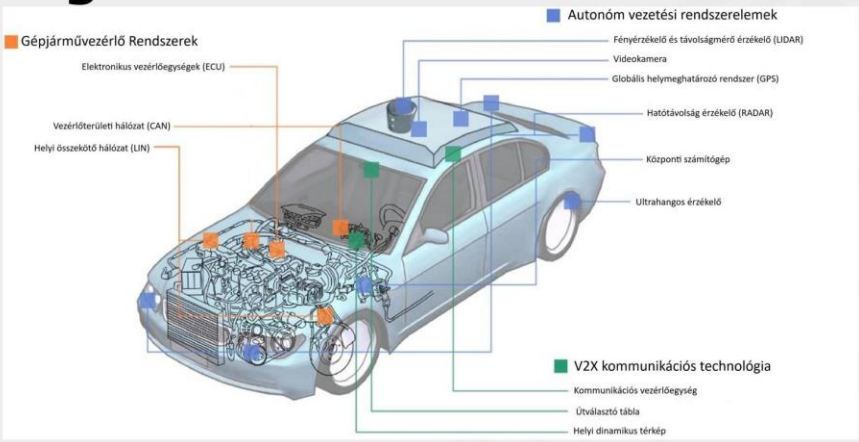
VI. Drón támadások céljainak csoportosítása

- Repülési útvonal eltérítése
- Lezuhanás/Leszállás
- Hozzáférés a fájlokhoz
- Lehallgatás

VI. Drón támadások céljainak csoportosítása



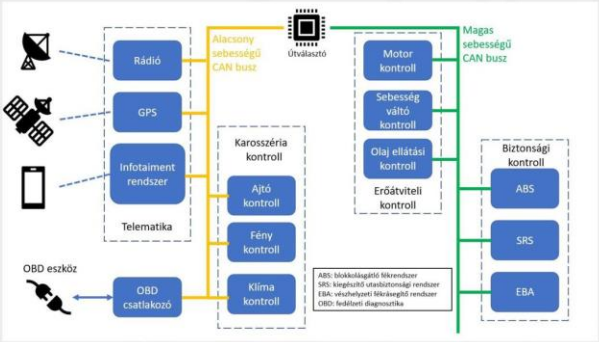
VI. Autonóm autók elemeinek meghatározása



VI. Az autonóm autók kihívásai

Gépjármű vezérlő rendszerek

- **Elektronikus vezérlőegységek** újraprogramozása
- Broadcast átvitel használata
- Rossz protokoll végrehajtás
- A CAN protokollokkal való visszaélés
- Titkosítás hiánya



VII. További lépések

- Autonóm autók biztonsági kihívásainak további tanulmányozása a másik kettő alrendszer esetében.
- A meglévő kérdőívekből a megfelelő kiválasztása

Felhasznált irodalom

- Biddlestone, Scott, és Keith A. Redmill. „A GNU Radio based testbed implementation with IEEE 1609 WAVE functionality”. 2009 IEEE Vehicular Networking Conference (VNC), 2009. október, 1–7. https://doi.org/10.1109/VNC.2009.5416372.
- „IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages”. IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), 2016. március, 1–240. https://doi.org/10.1109/IEEESTD.2016.7426684.
- Kim, Kyounggon, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, és Huy Kang Kim. „Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense”. Computers & Sec urity 103 (2021. április 1.): 102150. https://doi.org/10.1016/j.cose.2020.102150.
- Muha, Lajos, és Csaba Krasznay. Az elektronikus információs rendszerek biztonságának menedzselése. Budapest: Nemzeti Közszolgálati Egyetem, 2018.
- Pliatsios, Dimitrios, Panagiotis Sarigiannidis, Thomas Lagkas, és Antonios G. Sarigiannidis. „A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics”. IEEE Communications Surveys Tutorials 22, sz. 3 (2020. thirdquarter): 1942–76. https://doi.org/10.1109/COMST.2020.2987688.


Köszönöm a figyelmet!
katona.gergo@uni-nke.hu
uni-nke.hu

Tóth Rebeka: Biztonsági tesztelés a felsőoktatásban

Korreferátum

Napjainkban komoly szakember hiányt tapasztalhatunk globálisan az informatikai szakterületeken, amely a sérülékenység vizsgálati szakemberek esetében is meghatározó problémát okoz. Bár az új nemzeti stratégiák megfogalmazzák azokat az elvárásokat, ami szerint növelni kell Magyarország kiberbiztonsági képességeit – adott esetben offenzív képességek kialakítását is – azonban az állami szférában tapasztalható párhuzamos fejlesztések komoly kihívással kénytelenek számolni a piaci szféra munkaerő elszívó ereje okán. A kutatás alapvető célja felmérni azokat az elméleti és gyakorlati oktatási módszertanokat, releváns Capture The Flag platformok, sérülékenységvizsgálati módszertanok, tantárgyi és tanfolyam tematikák, amelyek adoptálásával növelhetők a hazai felsőoktatásban résztvevők kiber-higéniai képességeik, illetve a technológiai kompetenciái.


BIZTONSÁGI TESZTELÉS
A FELSŐOKTATÁSBAN
Rebeka Tóth


Tudományos probléma
DIGITALIZÁCIÓ UGRÁSSZERŰ NÖVEKEDÉSE ÉS A KIBERBIZTONSÁGI TUDATOSSÁG HIÁNYA
KIBER-HIGÉNIA
FOLYAMATOS VÁLTOZÁS, FEJLŐDÉS A KIBERBIZTONSÁGI VÉDELMI ÉS A TÁMADÓI
SZAKEMBER HIÁNY (ÁLLAMI TERÜLETEN NAGYOBB)
KÜLÖNBÖZŐ TERÜLETEK, ELTÉRŐ KOMPETENCIÁK (SZAKSPECIFIKUS KOMPETENCIÁK SZÜKSÉGESEK)
INFORMÁCIÓDÖMPING

Kutatási célkitűzések

Elméleti módszertanok felmérése
- OWASP módszertan és checklist
- Nagyvállalati módszertan
- Tantárgyi tematikák

Gyakorlati módszertanok felmérése
- Online oktató platformok
- Biztonsági tesztelési riport elemzése

Új oktatási platform karakterisztikáinak meghatározása
- Versenyképes tudás
- Hiányzik az állami és piaci szféráról

Központi kérdések

A GAMIFICATION ÉS A VERSENGÉS NÖVELNÉ A MOTIVÁCIÓT?

MILYEN KARAKTERISZTIKÁK RENDELKEZZEN AZ ÚJ PLATFORM?

SZÜKSÉGES-E A JELENLEGI PLATFORMOK JAVÍTÁSA?

Várható eredmények

- KÉPZÉS SPECIFIKUS KOMPETENCIÁK MEGHATÁROZÁSA
- ELMÉLETI ÉS GYAKORLATI OKTATÁSMÓDSZERTAN, ILLETVE TARTALOM KIALAKÍTÁSA
- KIBERBIZTONSÁGI SZAKSPECIFIKUS KÉPZÉSI KERETRENDSZER KIALAKÍTÁSA

Fejlesztési lehetőségek

- FELSŐOKTATÁSI GYAKORLATI MÓDSZERTAN
- RIPORT, JELENTÉS ÍRÁSA
- INFORMÁCIÓS, ALACSONY ÉS KÖZEPES HIÁNYOSSÁGOK
- TUDÁSMEGOSZTÁS ÖSZTÖNZÉSE (WRITEUP, WALKTHROUGH)

KÖSZÖNÖM A FIGYELMET!

Q&A

Hankó Viktória: Nők az IT biztonsági szektorban - egy kvalitatív kutatás eredményeinek elemzése

Korreferátum

Az információs társadalom korában az információvédelem és a kiberbiztonság kiemelt fontossággal bír. A két terület között átfedés azonosítható, így nem lehet teljesen elkülönülten kezelni őket. Ebből fakadóan a pályát választó szakemberállomány határait is nehéz megállapítani. Emellett a pályát választók számának alakulása, összetétele aktuális kérdéseket vet fel. Az előadás során kifejezetten a női munkavállalók IT biztonsági szektorban betöltött szerepére kerül a hangsúly. Ezen belül is kiemelt figyelmet fektetve a korábbi, valamint a jelenlegi trendekre például a pályaválasztás, bemenetel és pályaelhagyás alakulására. A munkaerőpiaci helyzet feltárása mellett az előadás második pilléreként jelenik meg a felsőoktatási hallgatók motivációja. Különös tekintettel, hogy milyen arányban, milyen háttérrel vagy éppen milyen motivációval választják a szektort mind a hazai, mind pedig a nemzetközi hallgatók. Továbbá harmadik pillérként a hazai és nemzetközi szervezetek jelenléte, tevékenysége is megjelenik. Magyarország esetében kiemelendő a WITSEC (Women in IT Security) szervezet munkája. Az előadás keretében a kiemelt hangsúlyt kap a tevékenységük bemutatása.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Új Nemzeti Kiválóság Program

PUSKÁS TIVADAR

Nők az IT biztonsági szektorban - egy kvalitatív kutatás eredményeinek elemzése

Hankó Viktória

Új típusú kihívások a biztonságban

2022.01.20.

AZ INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM ÚNKP-21-2-II-NKE-46 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁGI PROGRAMJÁNAK SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.

Előadás felépítése

I. *Téma aktualitása*
II. *Tudományos probléma*
III. *Kutatási célkitűzések*
IV. *Hipotézisek*
V. *Kutatási módszer*
VI. *Eredmények*
VII. *Összegzés*

I. Téma aktualitása

1 Prekoncepció

2 Felmérések

3 Mentorálás

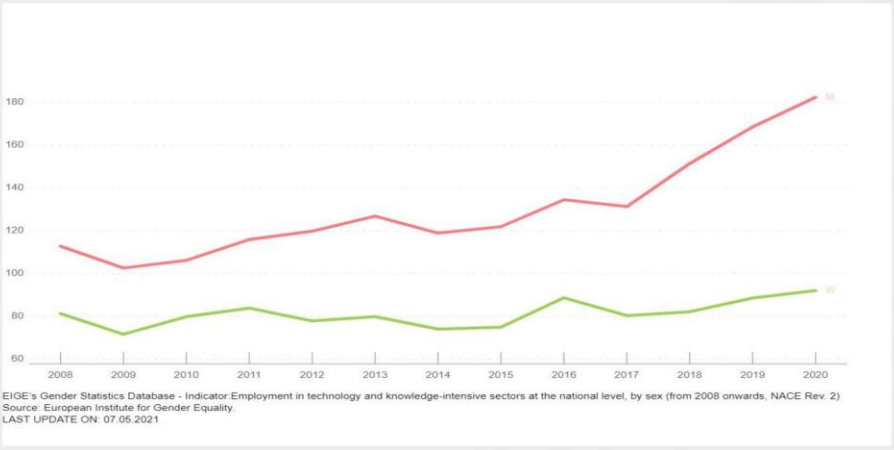
I. Téma aktualitása

10-15%

17%

25%

I.
Téma aktualitása



EIGE's Gender Statistics Database - Indicator:Employment in technology and knowledge-intensive sectors at the national level, by sex (from 2008 onwards, NACE Rev. 2)
Source: European Institute for Gender Equality.
LAST UPDATE ON: 07.05.2021

II. Tudományos probléma

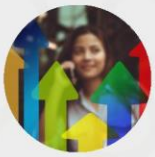
- Terminológia
- Egyenlőtlen munkaerőpiaci helyzet

III. Kutatási célkitűzések

Elhelyezkedés

Motivációk

WITSEC mentorprogram



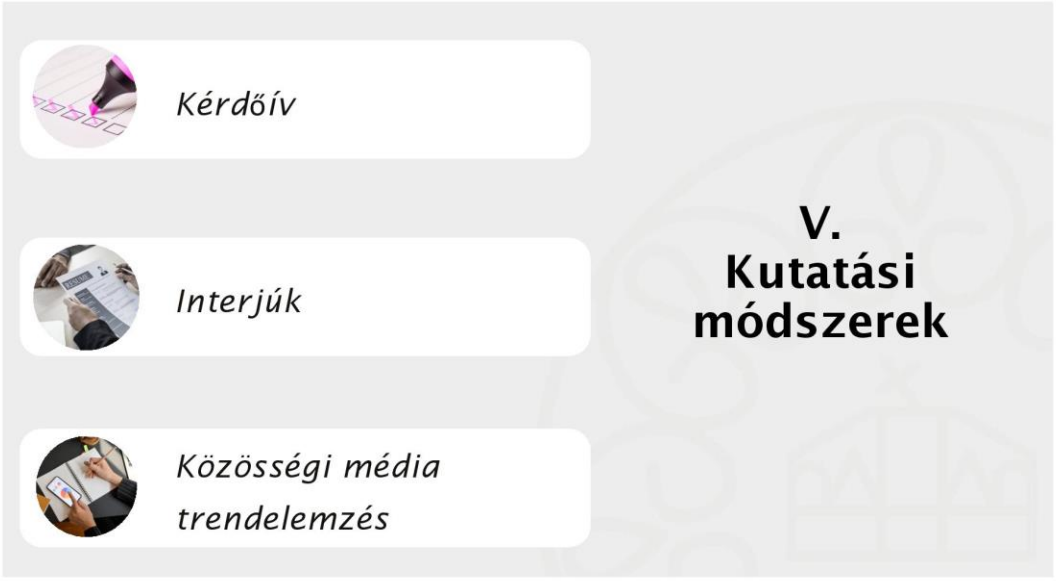
Trendek

IV. Hipotézisek

H1: A cégen belüli előmenetel a női dolgozók számára könnyebb, ha a szervezet vezetője nő.

H2: A felsőoktatási hallgatók motivációjában az ismeretségi kör befolyása a legjelentősebb tényező.

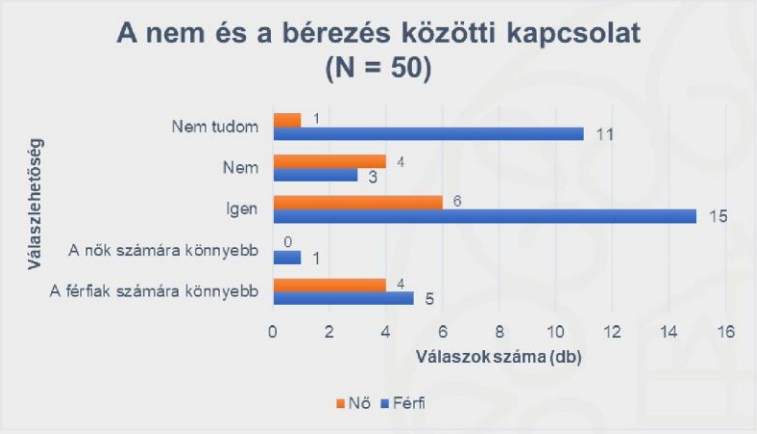
H3: A WITSEC mentorprogram résztvevői elkötelezettebbek a szakmai fejlődés mellett.

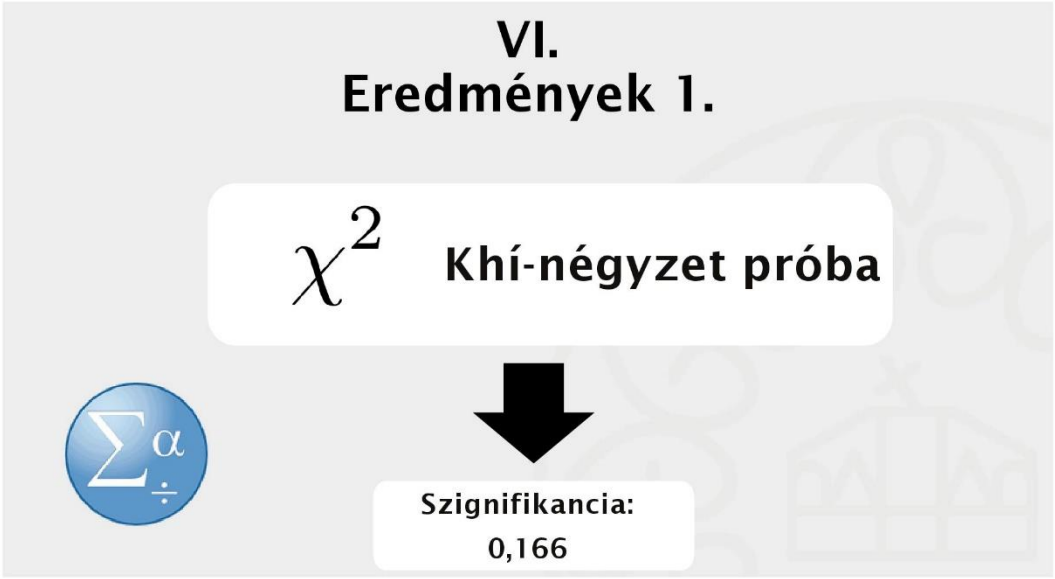

Kérdőív
Interjúk
Közösségi média trendelemzés
V.
Kutatási módszerek


VI.
Eredmények 1.
Kérdőív
1.
Demográfia
2.
Motiváció
3.
Környezet

VI.
Eredmények 1.

VI.
Eredmények 1.




VI.
Eredmények 1.
χ^2
Khí-négyzet próba
Szignifikancia:
0,166


VI.
Eredmények 2.
1. Fogalom
2. Választás oka
3. Elégedettség
4. Jövő
5. Várakozás
6. Kompetenciák
7. Ajánlás
8. Szakterület összetétele
9. Ösztönzés
10. Célok

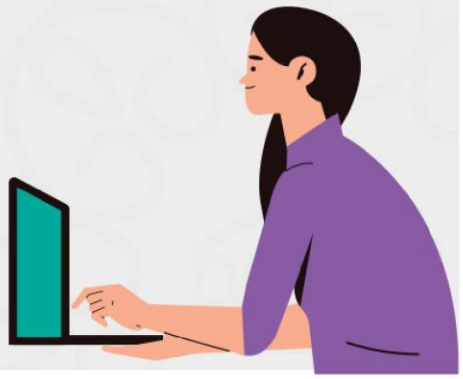
VI.
Eredmények 3.

WITSEC

- Szakmai, tudományos tevékenység
- Mentorálás
- Tudatosítás

VII.
Összegzés

- Összefüggés
- Hatások



Felhasznált források

- *Képes Gábor: Nők és az informatika, 2022. https://njszt.hu/hu/news/2022-01-10/nok-es-az-informatika*
- *VG: Tárt karokkal várja a nőket az IT-szektor, 2021. https://www.vg.hu/vilaggazdasag-magyar-gazdasag/2021/08/tart-karokkal-varja-a-noket-az-it-szektor-1*
- *Calitz, André & Cullen, Margaret & Fani, Duduetsang. (2020). The Influence of Culture on Women's IT Career Choices. Lecture Notes in Computer Science. 12067. 345-357. 10.1007/978-3-030-45002-1_30.*
- *BCS Women in IT, 2014. https://www.bcs.org/policy-and-influence/bcs-women-in-it-2014/*
- *WITSEC weboldal, https://www.witsec.hu/hu*

Botan Renáta: Cyberbullying az online játékokban

Korreferátum

21. században a technológia térnyerése magával hozta a többszemélyes játékok kialakulását és elterjedését. Kiszélesedése azonban itt még nem ért véget. A járványhelyzet okozta lezárások következtében robbanásszerűen nőtt a gamerek száma. Ezek hatására az online játékok felhasználói között sokszor tapasztalható a cyberbullying, vagyis az internetes zaklatás széleskörű jelensége. Amennyiben cyberbullyingról beszélünk, beszélhetünk áldozatokról, valamint zaklatókról. Az előbbi esetében egy-egy ilyen zaklatás pszichésen maradandó károkat okozhat, pláne ha az áldozat kiskorú, míg az utóbbinál sokszor csak a szórakozás lehet a motivációs tényező. A legtöbb szakirodalom azt mondja, a legjobb védekezés ez ellen a megelőzés. Vajon mit tehetnek a játékfejlesztők és a szülők ennek érdekében? Érdekes kérdést vet fel az is, hogy vajon mennyire jellemző hazánkban az internetes zaklatás az online játékok vonatkozásában, illetve melyik korosztályt érinti a leginkább, és ez hogyan oszlik meg a nemek között. Demográfiai szempontok figyelembevételével milyen körülmények hatására válik valakiből zaklató, és milyen hatást gyakorol az áldozatokra egy ilyen helyzet. Mindezen szempontok vizsgálatát egy kérdőíves felmérés segíti elő, amely segítségével meghatározható, hogy milyen tényezők játszanak szerepet a cyberbullying alakulásában.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR

Cyberbullying az online játékokban

Botan Renáta
Kiberbiztonsági Msc I. évfolyam
Új típusú kihívások a biztonságban 2022.01.20.

Előadás felépítése

1. Téma aktualitásai
2. Tudományos probléma
3. Kutatási célkitűzések
4. Védelmi megoldások
5. Kutatási módszertan
6. Eredmények
7. Összegzés

[1]

1. Téma aktualitása


[2]


[3]

Játékok folyamatos fejlődése

↓

Többjátékos mód

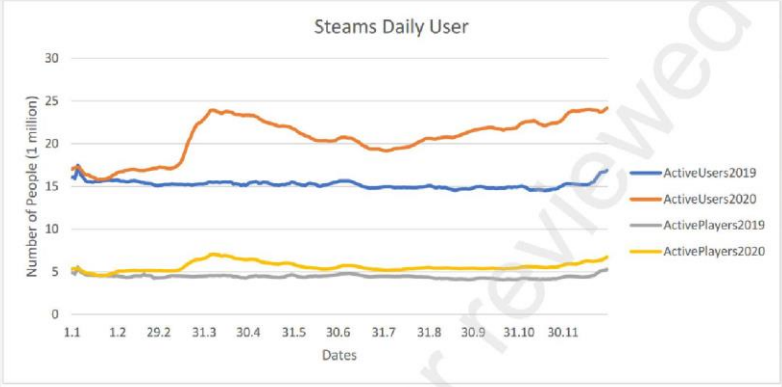
Korona vírus járvány

↓

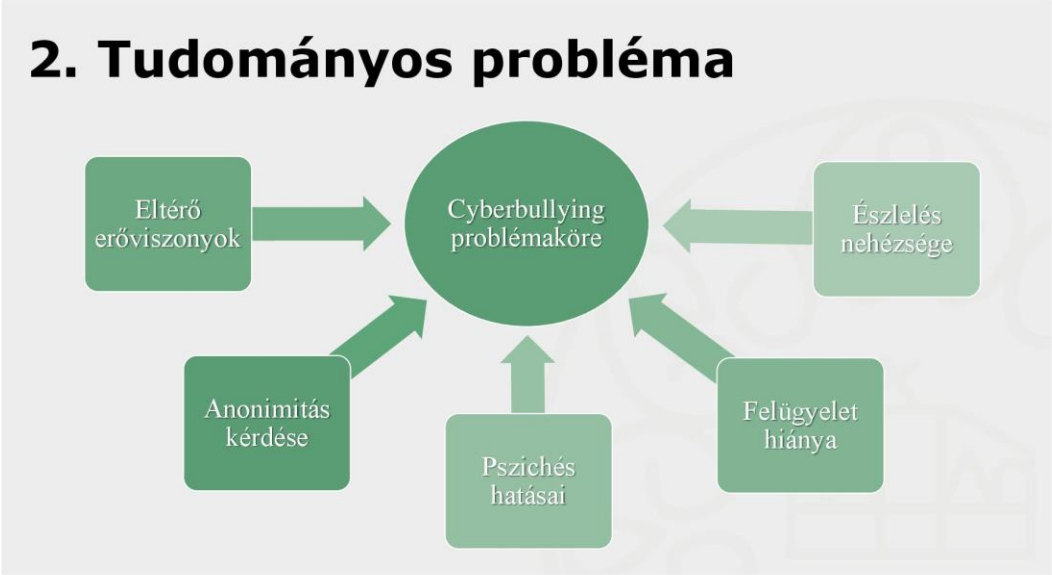
Széleskörű elterjedés

→ **Cyberbullying** ←

1. Téma aktualitása



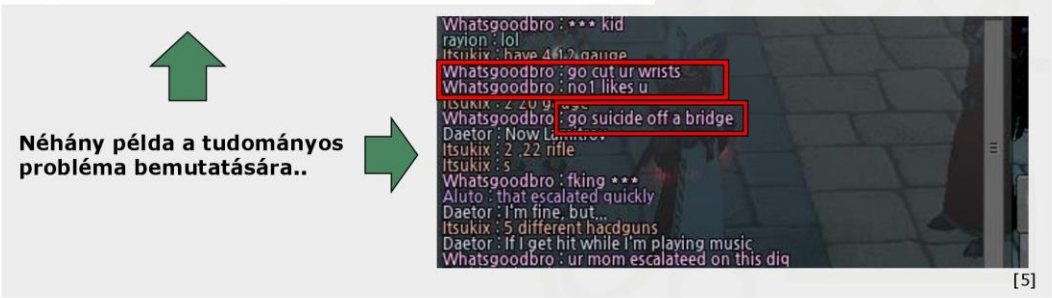
(Data Taken from SteamDB)


2. Tudományos probléma
Eltérő erőviszonyok
Cyberbullying problémaköre
Észlelés nehézsége
Anonimitás kérdése
Pszichés hatásai
Felügyelet hiánya


NiP nuke joined the room.
NiP nuke: Ihope
NiP nuke: you
Mamboox joined the room.
Grand Marshal joined the room.
Prince Discharge: BRONZE V
Prince Discharge: omg
NiP nuke: get cancer and die fucking trash jews, i will gass your famailies
Xiaolaro: i think
Send

[4]


2. Tudományos probléma


Néhány példa a tudományos probléma bemutatására..
Whatsgoodbro : *** kid
rayion : lol
Whatsgoodbro : go cut ur wrists
Whatsgoodbro : no1 likes u
Whatsgoodbro : go suicide off a bridge
Itsukix : 2 .22 rifle
Itsukix : s
Whatsgoodbro : fking ***
Aluto : that escalated quickly
Daetor : I'm fine, but...
Itsukix : 5 different hacdguns
Daetor : If I get hit while I'm playing music
Whatsgoodbro : ur mom escalateed on this dig

[5]

3. Kutatási célkitűzések

4. Védelmi megoldások

A legjobb védelem a megelőzés

A mesterséges intelligencia moderálása csökkenti a verbális visszaéléseket a League of Legendsben - **Tribunal**

[6]

5. Kutatási módszertan

[7]

Cyberbullying elterjedtsége a 14-26 év közötti korosztályban Magyarországon

[8]

6. Eredmények

7. Összegzés

[9] 

[10]

- Fenyegetések
- Trollkodás
- Kirekesztés
- Zaklatás
- Gyűlöletbeszéd
- Fiókfeltörés

Felhasznált források

https://www.statista.com/statistics/1109979/video-game-console-sales-covid/
https://www.stopbullying.gov/cyberbullying/what-is-it
https://www.stopbullying.gov/cyberbullying/cyberbullying-online-gaming
https://cyberbullying.org/what-is-cyberbullying
https://www.cybersmile.org/news/ai-moderation-slashes-verbal-abuse-in-league-of-legends
https://www.sciencedirect.com/topics/social-sciences/cyberbullying
https://www.sciencedirect.com/science/article/pii/S0190740919304190

Felhasznált képek

[1] https://techcrunch.com/2015/10/31/the-history-of-gaming-an-evolving-community/?guccounter

[2] http://www.webgltutorials.org/how-do-you-become-a-game-developer/

[3] https://www.sapphirenation.net/effects-of-the-covid19-pandemic-on-the-gaming-industry

[4] [5] https://cyberbullying.org/league-legends-cyberbullying

[6] https://www.cybersmile.org/news/ai-moderation-slashes-verbal-abuse-in-league-of-legends

[7]https://www.iconfinder.com/icons/555942/online_survey_questionnaire_survey_web_survey_exam_icon

[8] http://getdrawings.com/spss-icon

[9] https://www.analyticsinsight.net/gaming-boom-in-covid-19-times-analysis-insights/

[10] https://kidshelpline.com.au/parents/issues/online-gaming-signs-your-child-may-be-bullied

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR

Köszönöm a megtisztelő figyelmet!

Molnár Ákos Ádám: Álhírek a koronavírus tükrében

Korreferátum

2019. decemberben Kína egyik tartományában, Wuhanban jelent meg a napjainkra már mindenki által ismert és azóta világjárvánnyá nyilvánított Covid-19. A vírussal együtt, azonban felerősödtek az álhírek és az ezzel kapcsolatos dezinformálás. Az álhírek és azok terjedése több csatornán is meg tud valósulni azonban ezek közül napjainkban a legerőteljesebben az online térben történik. 2020 tavaszán a World Health Organization az „infodemic" kifejezéssel, azaz amikor túl sok információ, köztük rengeteg megtévesztő jelenik meg egy járvánnyal kapcsolatban, mutatott rá, hogy nem csak a vírus, de a vele kapcsolatos dezinformáció, vagyis félreinformálás is ugyanolyan mértékben terjed a világon. Jelenleg még mindig ebben a korszakban élünk, a „post truth" árnyékában, amikor a különböző híreket gyakrabban hisszük el az érzelmi töltöttségük alapján, mint sem valóságtartalmuk vagy forrásuk alapján, jelentősen befolyásolva a társadalom informáltságát.

Kutatásom fő célja a koronavírussal kapcsolatos álhíreknek és érzelmek vizsgálata. Ezen belül az álhírek fajtáit, terjedését és hallgatóságra tett hatásait vizsgáltam. Online felületeken végzett kulcsszó elemzést alkalmazva az álhírek terjedését, annak ütemét és miértjét kutattam. Továbbá, kérdőíves elemzést alkalmazva vizsgáltam a világjárvánnyal kapcsolatos álhírekben való hiszékenységet, illetve aggodalmat, fenyegetettséget és fogékonyságot, utóbbi hármat összesítve észlelések néven

elemeztem. A kapott adatokat később különböző statisztikai módszerekkel vizsgáltam az IBM SPSS nevű programban. Az adatok alapján megállapítottam, hogy a vakcinákkal kapcsolatos álhírek kivételével, azok a Covid-19-cel kapcsolatos álhírek, melyek a vírus megjelenésekor voltak a legnépszerűbbek az első hullám idején voltak a legelterjedtebbek, szemben a többivel. Bebizonyítottam, hogy a vírus ellen megalkotott ellenanyagok megjelenésével és tömeges használatával a koronavírusos álhírek online megjelenése ismét megerősödött. Statisztikai elemzés során bebizonyítottam, hogy az álhírekben való hiszékenység alapján képzett csoportok összefüggést mutatnak a vírussal kapcsolatos érzékeléseikkel. Megállapítottam, hogy a különböző álhírekre adott válaszok összefüggnek az adott személyek oltakozási hajlandóságával.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR

Álhírek a koronavírus tükrében

Molnár Ákos
Ostrakon Szakkollégium

ON

Molnár Ákos

Előadásom felépítése

- I. Téma aktualitása
- II. Tudományos probléma
- III. Kutatási célkitűzések
- IV. Hipotézisek
- V. Kutatási módszertan
- VI. Eredményeim
- VII. Összegzés

I. Téma aktualitása

Post truth korszak
Koronavírus járvány
Infodemic

→ Problémák és veszélyek?

II. Tudományos probléma

III. Kutatási célkitűzések

IV. Hipotézisek

- **H1**: A koronavírus megjelenésekor legnépszerűbb álhírek az első hullám idején voltak a leginkább elterjedve, szemben a többi hullámmal.

- **H2**: A Covid-19 oltóanyagok megjelenésével a vírussal kapcsolatos álhírek megjelenése megerősödött az előtte lévő időszakhoz képest.

IV. Hipotézisek

- **H3**: Az álhírekre vonatkozó kérdésekre adott válaszok alapján képzett klaszterek szignifikáns összefüggést mutatnak az aggodalom, fenyegetés és fogékonyság kérdéseiben.

- **H4**: Az általam vizsgált álhírekre adott válaszok összefüggnek az adott személy oltakozási hajlandóságával.

V. Kutatási módszertan

- Közösségi média elemzés, szentiment analízis

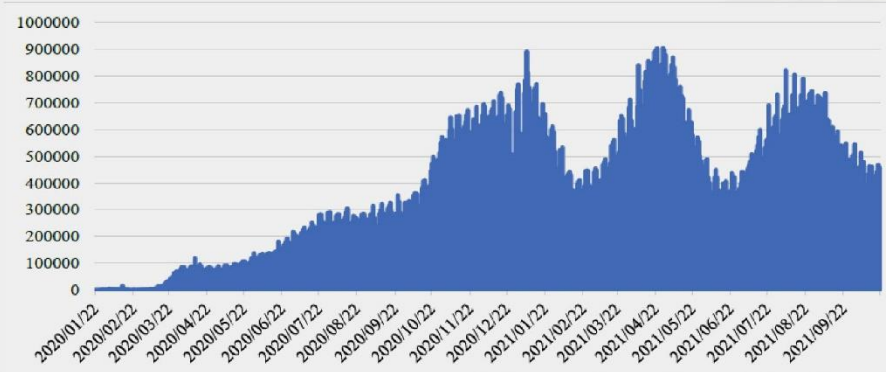
senti one

- Kérdőíves felmérés a Covid-19 vírussal kapcsolatos tudatosság és érzékelések felmérésére

SPSS

Covid-19 hullámok világszinten

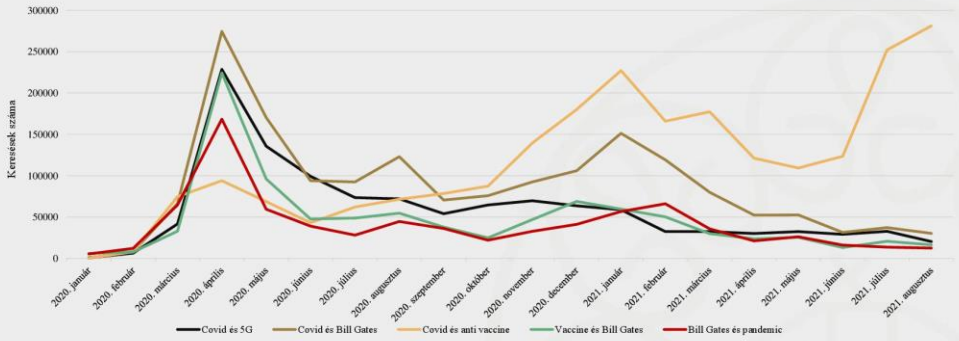
(n=1192592)



Napi új koronavírus megbetegedések száma világszerte 2020.01.22 - 2021.09.22 között (saját szerkesztés)

VI. H1: Legelterjedtebb álhírekkel kapcsolatos kifejezések megjelenése

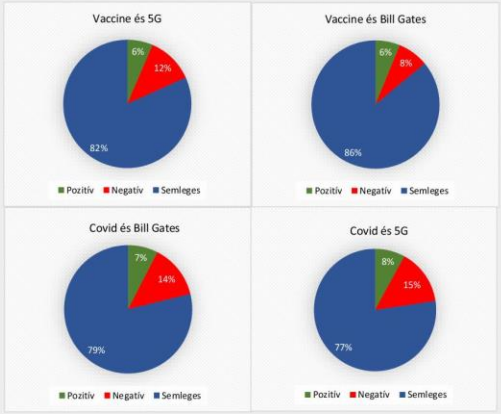
(saját szerkesztés)



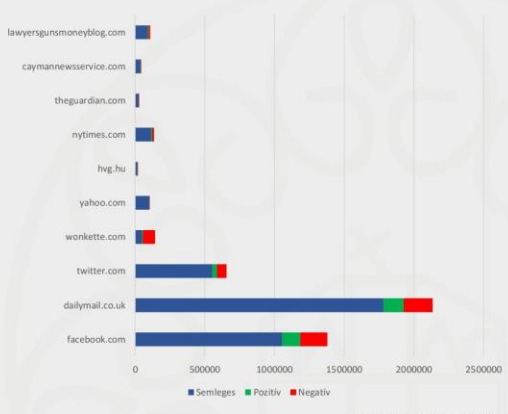
Koronavírussal kapcsolatos kifejezések keresései a Senti One program segítségével (saját szerkesztés)

VI. Álhírek érzelmi alapú említései

(n=4649861)

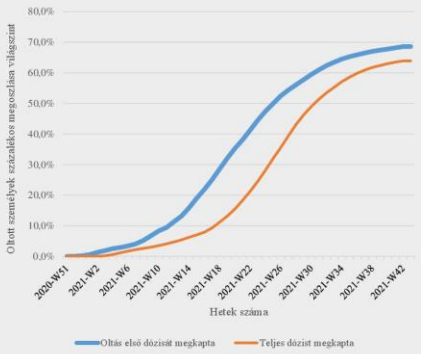


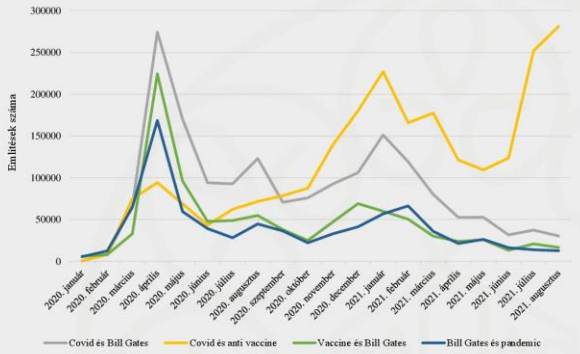
(saját szerkesztés)



(saját szerkesztés)

VI. H2: Oltóanyagok és álhírek terjedése közti kapcsolat



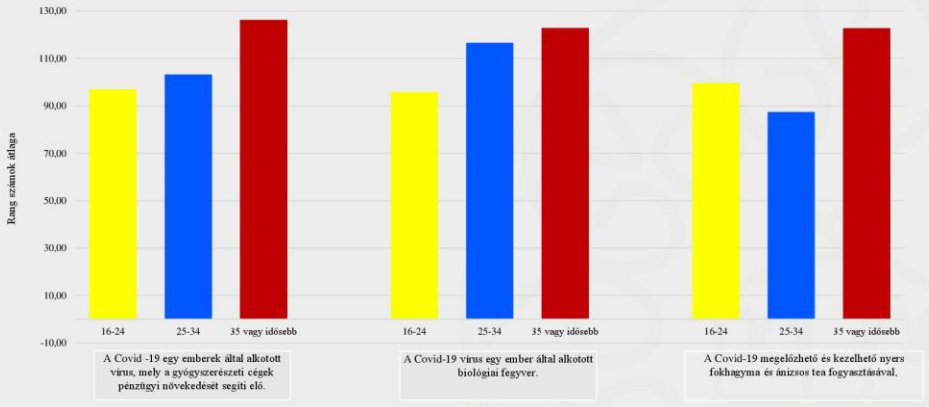


VI. Kérdőíves felmérés

- 202 fő kitöltő
- 64,4% nő
- 76,7% 16 és 24 év közötti
- 86,6% rendelkezik Covid-19 elleni védőoltással
- 136 fő tartja fenyegetésnek a járványt
- 117 fő nem aggódik miatta
- 190 fő jól informált a vírussal kapcsolatban

VI. Életkor és az informáltság összefüggése

(n=202)




VI. Informáltság és észlelések
(n=202)
Rang számok átlaga
120,00
100,00
80,00
60,00
40,00
20,00
0,00
informált
félreinformált
Mennyire tartja veszélyesnek a Covid-19 vírust?
Mennyire lenne veszélyes Ön szerint, ha a Covid-19 vírus elkezdene terjedni az Ön közösségében?
Mennyire lenne veszélyes a vírus a saját városára nézve, ha elkezdene terjedni Magyarországon?
Mennyire aggódik amiatt, hogy egy közeli ismerőse vagy rokona elkapja a vírust az elkövetkezendő hónapokban?
Mennyire aggódik amiatt, hogy esetleg egy új Covid-19 hullám tör ki a városában


VI. H3: Klasztercsoportok és észlelések
(n=202)
1. Klaszter
• 99 fő
• Jól informáltak
2. Klaszter
• 65 fő
• Kevésbé informáltak
3. Klaszter
• 38 fő
• Rosszul informáltak
Fogékonyság
Észlelések
Fenyegetés
Aggodalom

VI. H4: álhírek és oltakozási hajlandóság (n=202)

Kruskal Wallis elemzés	Szignifikancia szint		Cramer's V	
Álhírek	Oltott személyek	Fizetős vakcina	Oltott személyek	Fizetős vakcina
A Covid -19 egy emberek által alkotott vírus, mely a gyógyszerészeti cégek pénzügyi növekedését segíti elő.	0,000	0,648	0,00	X
A Covid-19 vírus egy ember által alkotott biológiai fegyver.	0,009	0,036	0,09	0,35
A Covid-19 vírus nem tud átterjedni a melegebb éghajlatú területekre.	0,043	0,972	X	X
A gyerekek nem tudják elkapni a Covid 19-et.	0,018	0,512	X	X
Az antibiotikum hatásos a Covid-19 megelőzésében és kezelésében.	0,797	0,157	X	X
A Covid-19 megelőzhető és kezelhető nyers fokhagyma és ánizsos tea fogyasztásával.	0,030	0,674	X	X
A legtöbb ember, aki elkapja a Covid-19 vírust, bele is hal.	0,199	0,749	X	X

VII. Összegzés

- T1: Az első hullám idején, azaz 2020 tavaszán legnépszerűbb álhírek, az első hullám idején voltak a legelterjedtebbek, szemben a többivel.
- T2: Az oltóanyagok megjelenésével, az álhírek online megjelenése ismét megerősödött.

VII. Összegzés

- T3: Az álhírekben való hiszékenység alapján képzett csoportok összefüggést mutatnak a vírussal kapcsolatos érzékeléseikkel.
- T4: A vírussal kapcsolatos álhírekben való hiszékenység összefüggést mutat az oltakozási hajlandósággal.

Források

- Koronavírus fertőzések száma világszerte: https://www.worldometers.info/coronavirus/
- SenitOne:https://sentione.com
- Világ lakosság Covid-19 védőoltás felvétele százalékban: https://qap.ecdc.europa.eu/public/extensions/COVID-19/vaccine-tracker

Felhasznált képek

- (1): https://abcnews.go.com/US/ways-spot-disinformation-social-media-feeds/story?id=67784438
- (2): https://sentione.com
- (3): https://worldvectorlogo.com/logo/spss-1

Sz. Podmaniczky Katalin: Információs kockázatok

Korreferátum

Az információkat, ezzel szoros összefüggésben az információbiztonságot érintő kockázatok egyre sokrétűbbek a számítástechnikai rendszerek, az elektronikus adattárolás, -feldolgozás és -megosztás térhódítása következményeként. A legnépszerűbb információbiztonsági kockázatok közé tartoznak a közösségi oldalak kezelése, a jelszavak megosztása, a jogosulatlan hozzáférés, a frissítési hibák, a lopás és elvesztés. Ezek mind az adatok megsemmisüléséhez, illetéktelen hozzáféréshez, időveszteséghez, az érdekek sérüléséhez vezethetnek.

A megelőző intézkedések ellenére mégis folyamatosak az incidensek, ezért nagyon fontos, hogy az információt úgy határozzuk meg, hogy a felhasználó bármikor felismerje. Alapvetés, hogy információ lehet bármi. Ezt szűkíti a fontosság és újszerűség, ami csökkenti az ismerethiányt és a bizonytalanságot. Növeli a kockázatot, hogy a mai korban az emberek az információt, az információszerzést és -birtoklást pótcselekvésként, önbizalmuk erősítésére, félelmeik csökkentésére is használják.

Az információ legveszélyesebb tulajdonsága, hogy lényegében minden annak számít, amivel változás érhető el. Ebben az értelmezésben komoly hatalommal bír az információ, illetve az is, aki az információt szolgáltatja.

A valódi veszély az, hogy a védendő információt vétlen vagy szándékos módon közlő nincs tisztában az információ kontextusával, jelentőségével, felhasználásának lehetséges következményeivel.

A tudatos visszaélések megelőzésére és elhárítására a legtöbb szervezet felkészült, de a személyi állomány nem akaratlagos veszélyeztetése jelentősen növeli a kockázatot.

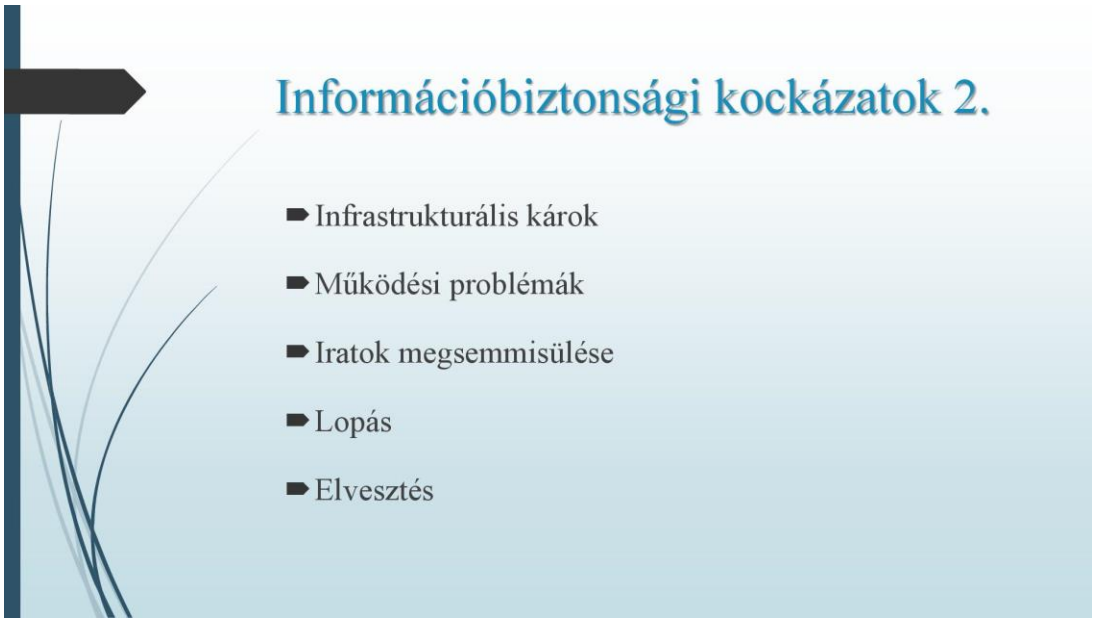
A védekezés legnagyobb és egyben legújabb kihívásai a mindent behálózó közösségi felületek, a rendszerek vétlen vagy szándékos sebezhetőségei és a kiszolgáltatottság.

Információs kockázatok

Sz. Podmaniczky Katalin

Információbiztonság


Információbiztonsági kockázatok 1.
Közösségi háló, közösségi oldalak
Jelszavak közzététele
Jogosulatlan hozzáférés
Karbantartási hiba
Áramszünet


Információbiztonsági kockázatok 2.
Infrastrukturális károk
Működési problémák
Iratok megsemmisülése
Lopás
Elvesztés

De mi lehet a hiba?

Az információ 1.

- Információ:
  - bármi,
  - ami számunkra fontos,
  - újszerű és
  - csökkenti az ismerethiányunkat
- Információ:
  - pótcselekvés
  - önbizalom erősítő
  - félelmet elűző eszköz

Az információ 2.

- Információ:
  - informatika alapfogalma,
  - amelyre nincs egységes definíció

Információ minden,
ami képes más emberre hatni oly módon,
hogy ettől annak viselkedése megváltozzék.

Az információ lényege 1.

A bizonytalanság csökkentése


Az információ lényege 2.
Információ
vs.
Információ +
kontextus
jelentőség
felhasználás következményei


Védekezés
Kockázatok azonosítása és kezelése
Tudatos visszaélések kezelése
Legújabb kihívások:
Közösségi felületek
Kapcsolati háló
Vétlen vagy szándékos sebezhetőség
Kiszolgáltatottság
Információs túlterhelés → figyelmetlenség


Köszönöm a figyelmet!

Nyári Merse: Hibrid hadviselés - régi eszközök új köntösben

Korreferátum

Előadásom célja, hogy a politikai és a hibrid hadviselést összehasonlítsam, megvizsgáljam a két hadviselés jellemzőit, hasonlóságiat és különbségeit. A hidegháború során, illetve a Szovjetunió esetében már évtizedekkel korábban elkezdődött a politikai hadviselés folytatása.

A politikai hadviselés nem csak a potenciális előnyei miatt alakult ki, hanem amiatt is, mivel a két szuperhatalom, a Szovjetunió és az Amerikai Egyesült Államok olyan katonai képességekkel rendelkeztek, amik nem adtak lehetőséget egy nyílt háború kirobbanására. Egy ilyen háború mindkét fél számára csak veszteségekkel járt volna.

A kutatás során megvizsgáltam a politikai hadviselés jellemzőit. Kifejezetten koncentráltam az Amerikai Egyesült Államok és a Szovjetunió által folytatott politikai hadviselés tanulmányozására. Ezután megvizsgáltam, hogy bizonyos kutatók hogyan értelmezik a hibrid hadviselést, valamint milyen tevékenységek köthetőek ahhoz.

A kutatás során arra jutottam, hogy a politikai és a hibrid hadviselés között egyaránt találhatóak hasonlóságok és különbségek is. Hasonlóság például, hogy a hadviselések két atomhatalom között mennek végbe, továbbá az, hogy nem hagyományos eszközök kerülnek bevetésre. A célok is részben azonosak, azaz geopolitikaiak. Eltérés azonban, hogy jelenleg úgy néz ki, hogy a hibrid hadviselés csak Oroszország határmenti országaiban jelenik meg, mely

országokban nagy számban találhatók orosz nemzetiségű kisebbségek. Különbség továbbá, hogy míg a politikai hadviselés két pólusú világrendben, úgy a hibridhadviselés többpólusú világrendben, globalizált környezetben jelentkezik, emiatt részben az államok eszköztára is kibővült.

Előadás felépítése

- Bevezetés
- Politikai Hadviselés
- Hibrid hadviselés
- Hasonlóságok, különbségek
- Következtetés, előadás zárása

Bevezetés

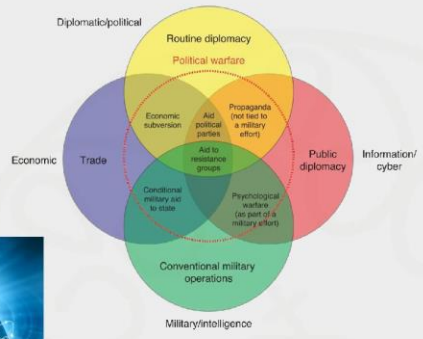
- Szun-ce: A háború művészete
- Hadviselés fejlődése: vonalharcászattól a második világháborúig

Politikai Hadviselés

- Nem hagyományos hadviselés
- Szovjetunió, cionizmus
- USA csak 1947-től

Politikai Hadviselés

- Geopolitikai érdekek domináltak
- Nem hagyományos eszközök
- Elrettentés szerepe

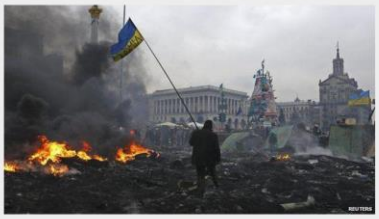


Hibrid hadviselés

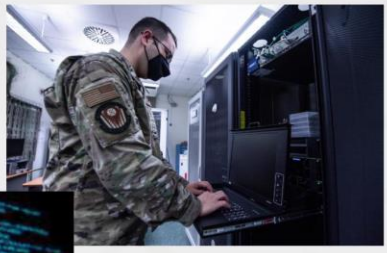
- Megváltozott világrend
- Nem hagyományos eszközök
- Elrettentés szerepe

Hibrid hadviselés

- Nincs hivatalos fogalma
- Ukrán válság
- Nagyhatalmi szembenállás, geopolitika



Hasonlóságok és különbségek


Következtetés


Kép források

- https://keletazsiafigyelo.blog.hu/2018/04/22/szun-ce_es_a_kinai_strategiai_gondolkodas
- 2-vilaghaboru.gportal.hu
- https://arsmilitaria.blog.hu/2020/05/26/mel_gibson_es_nagy_frigyes_veletlen_talalkozasa_egy_boncasztalon_avagy_mi_is_az_a_vonalharcaszat
- https://int.icej.org/media/biblical-stand-zionism-i
- https://lonelyplanet.nl/reistips-and-trends/manhattan-kgb-spy-museum
- https://flagmagazin.hu/nagyvilag/amit-a-cia-nem-vett-eszre
- https://wallpaperaccess.com/nuclear-blast
- https://www.rand.org/pubs/research_briefs/RB10071.html
- https://www.japantimes.co.jp/opinion/2019/10/20/commentary/japan-commentary/mixed-messages-nuclear-deterrence/
- https://www.thesun.co.uk/news/17341491/russia-invasion-ukraine-putin-ww3/
- https://www.bbc.com/news/world-europe-27308526
- https://www.geopolitica.ru/en/article/hybrid-warfare-hybrid-lawfare
- https://isdp.se/the-enemy-of-my-enemy-is-my-friend-russia-china-relations-in-the-face-of-u-s-china-tensions/
- https://www.onespan.com/blog/faux-hackers-who-hacked-word-hacking
- https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/
- https://www.bbc.com/news/world-europe-35578716

Irodalomjegyzék

- Kennan, George F.: The Inauguration of Organized Political Warfare [Redacted Version], History and Public Policy Program Digital Archive, April 30, 1948
- Codevilla, Angelo M.: POLITICAL WARFARE and PSYCHOLOGICAL OPERATIONS, National Defense University Press Publications, 1989, pp. 79-81.
- Hoffman, Frank: On not-so-new warfare: political warfare vs hybrid threats, Texas National Security Review, 2014.07.28., https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/
- Markey, Dell: What Did the USSR Do to Promote Communism in the Cold War?, The Classroom, 2018.06.25., https://www.theclassroom.com/did-ussr-promote-communism-cold-war-8040.html
- Richman, Evan: The Spy Who Came Into the Classroom Teaches at Boston U., New York Times, 1994.04.27., https://www.nytimes.com/1994/04/27/us/the-spy-who-came-into-the-classroom-teaches-at-boston-u.html
- Hoffman, Frank G.: Conflictin the 21st Century: The Rise ofHybrid Wars.Wars. p. 8., 2007
- Epstein, Edward Jay: Agency of fear: Opiates and political power in America, Verso, 1990.
- Korybko, Andrew: HYBRID WARS: THE INDIRECT ADAPTIVE APPROACH TO REGIME CHANGE, Moscow Peoples' Friendship University of Russia, 2015.
- Berzins, J. (2019). "Not 'Hybrid' but New Generation Warfare". in Howard, G. and Czekaj, M. (Eds.) Russia's Military Strategy and Doctrine. Washington, DC: The Jamestown Foundation.


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
Köszönöm a figyelmet!

Schiller Gábor: Kína összfegyvernemi zászlóaljai kétéltű és szárazföldi műveletekben

Korreferátum

Kína 21. századi külpolitikája 21. századi hadsereget igényel. A jelenlegi reformok során a vezető szerepet a Haditengerészet Tengerészgyalogsága vette fel. Az újítások legfrissebb hulláma 2017-ben indult meg, mely során Kína eltávolodik a Szovjet-mintájú hadseregcsoportok alkalmazásától, zászlóaljakra szervezi át szárazföldi és kétéltű haderejét. Az új összfegyvernemi, limitált nehézfegyverzettel rendelkező, gyors reagálású zászlóaljak a tengerészgyalogság tradicionális feladatai mellett háborús küszöb alatti műveletekben is bevethetők. Kiképzésüknek és a decentralizált támogató egységeiknek köszönhetően az ellenséges vonalak mögötti harctevékenység folytatására és a nehéz környezeti viszonyok közötti hadviselésre is képesek. A zászlóalj szintű reformok betekintést nyújtanak Kína hadászati képességeinek fejlődésébe és a hadviselés változásával kapcsolatos projekcióiba.

Kína összfegyvernemi zászlóaljai kétéltű és szárazföldi műveletekben

Schiller Gábor

2000es évektől napjainkig

- Elavult struktúra
- Újítási kísérletek kezdete
- 2017es átszervezés

Jelenlegi struktúra

- Felépítés
- Századok feladatai
- Századok jellemzői
- Külföldi inspiráció

Képességek

- Invázió előkészítése
- Többdimenziós hadviselés
- Gyorsreagálási képesség
- Összhaderőnemi együttműködés

Határok

- Csatahelikopterek hiánya
- Csak MANPAD
- Haditengerészeti függés
- Hiányos szállítóképesség

Feladatkör

- Szárazföldi erők komplementere
- Erőkivetítés
- Békeidő

Tajvani invázió esetén

- Komplementer szerep
- Különleges műveleti dandár
- Frontvonal mögötti zavaró tevékenység
  - Altisztképzés fontossága

Összegzés

- Reform folyamata
- Specializáció – univerzalitás
- Hely a változó világrendben

Felhasznált Irodalom

- China Maritime Report No. 15: The New Chinese Marine Corps: A "Strategic Dagger" in a Cross-Strait Invasion
  - https://digital-commons.usnwc.edu/cmsi-maritime-reports/15/
- An Introduction to China's High-Mobility Combined Arms Battalion Concept
  - https://www.benning.army.mil/infantry/magazine/issues/2020/Fall/pdf/5_Arostegui-HIMOB.pdf
- Training Command Implementing Force Design 2030 through "The Game of Inches"
  - https://mca-marines.org/wp-content/uploads/Training-Command.pdf
- The PLA Marines – Li Faxin

Köszönöm a figyelmet!

Kérdések?

Kugler Péter: A Kínával kapcsolatos narratíva és infodémia, az új hidegháború kapujában

Korreferátum

Kutatásomban a mostanában a médiában egyre gyakrabban előforduló, mégis a hivatalos nemzetközi kommunikációban került új hidegháborúval, mint a nemzetközi kapcsolatok komplex jelenségével foglalkozom. E téma mind aktualitása, mind a napjainktól a következő években a világra gyakorolt hatásában kiemelkedő jelentőségű.

A hidegháború egy minden szintet átható, komplex és hosszú ideig elhúzódó konfliktus volt, melynek végén megismétlődésével senki nem számolt, hasonlóan az I. világháború utáni túlzott optimizmushoz, hogy még egy ennyire kiterjedt háború nem fog megismétlődni.

A közösségi média, illetve az interneten található tartalmak elemzésével objektívabb kép nyerhető arról, hogy az erkölcsi-ideológiai-politikai megosztottság hogyan változik, illetve az aktuális nagyhatalmi narratívák mennyire hatásosan befolyásolják az embereket. A Covid-19 járvány egyedülálló az eddigi járványok közül abban, hogy a pandémián túl a globális közösségnek még egy álhírekkel, manipulációval és szándékolt zavarkeltési hullámmal is meg kell(ett) küzdenie, ami az internet lehetőségeit kihasználva soha nem látott sebességgel terjedt. A pandémia az új variánsok megjelenése okán koránt sem tekinthető befejezettnek, de már

most látszik, hogy hatásai közép- és hosszútávon is meghatározóak lesznek.

Kínát, mint feltörekvő nagyhatalmat, illetve az USA „kihívóját" vizsgálom. A nemzetközi térben betöltött szerepének és kommunikációjának változásával együtt igyekszem mérhetővé tenni nemzetközi megítélésének változását, illetve célom összevetni a nemzetközi szakirodalomban megtalálható kutatások eredményeivel.

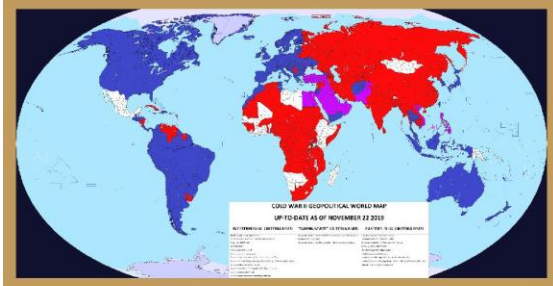
Végül kitekintek az általam legfontosabbnak gondolt két nyitott kérdésre: a járvány utáni világrend változása, mennyire fog a demokráciák és az autokratikus típusú vezetésű államok mostani egyensúlya megváltozni; a 2022. január 1-jén hatályba lépett Regional Comprehensive Economic Partnership (RCEP), mint Kína központú szabadkereskedelmi övezet lehetséges kihatásaira.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-1-I-NKE-67 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.


A Kínával kapcsolatos narratíva és infodémia, az új hidegháború kapujában
PUSKÁS TIVADAR
Kugler Péter
2022.01.20.
Témavezető:
Dr. Bányász Péter
Az Innovációs és Technológiai Minisztérium ÚNKP-21-1-I-NKE-67 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.


Áttekintés
• Az új hidegháború
• Pandémia és infodémia
• Hipotézisek
• Kutatási módszer
• Kitekintés
• Felhasznált irodalom

Forrás: QualityInspection.org



Készítette: ChrisY-DA

Az új hidegháború

- A hidegháború teljes jelenségének tudományos feldolgozása részlegesen történt csak meg
- Már benne vagyunk, vagy csak sodródunk egy új hidegháború felé?
- Mi a különbség az új hidegháború eszköz- és szövetségi rendszerében?
- Magyarország pozíciója

Pandémia és infodémia

- A pandémia kezdete, és visszásságok
- Az egészségügyi kérdés kiterjedése: gazdasági, politikai, és emberjogi kérdésekre
- Infodémia: információ + epidémia
- Narratívák és változásaik:
  pandémiás intézkedések, maszkviselés, álhírek, oltások, átoltottság, oltóanyag elfogadás

Hipotézisek

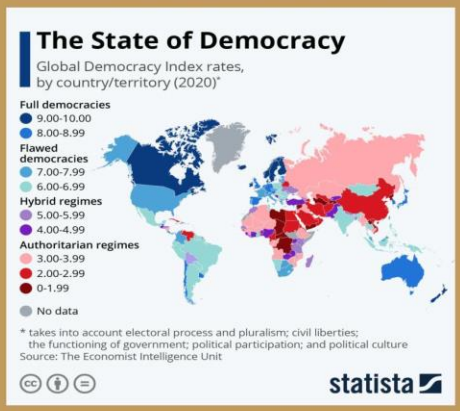
1. A Kínától segélyt/segítséget kapó országoknál, javult-e Kína megítélése a közösségi média üzeneteinek alapján?
2. Kína politikai ellenfeleinek országaiban romlott-e Kína megítélése?
3. Kína járványkezelésének nemzetközi megítélése hogyan változott?

Kutatási módszer

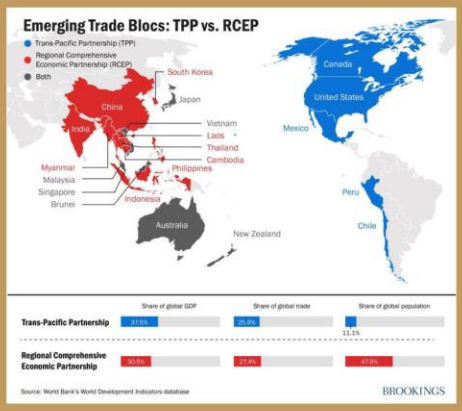
- Adatforrás: senti one
- WHO interaktív idővonala alapján fordulópontok kiválasztása
- Kulcsszó: China
- Irreleváns rekordok eltávolítása 
- Az aktuális időszak szentimentjeinek összesítése
- Fenntartások: botok, adatmennyiség, scope

Kitekintés

Demokratikus és autoriter rendszerek



Regional Comprehensive Economic Partnership (RCEP)



Felhasznált irodalom

- Azzam Mourad, Ali Srour, Haidar Harmanani, Cathia Jenainati, és Mohamad Arafeh. „Critical Impact of Social Networks Infodemic on Defeating Coronavirus COVID-19 Pandemic: Twitter-Based Study and Research Directions”. *IEEE Transactions on Network and Service Management* 17, sz. 4 (é. n.): 2145–55. https://doi.org/10.1109/TNSM.2020.3031034.
- Huimin Chen, Zeyu Zhu, Fanchao Qi, Yining Ye, Zhiyuan Liu, és Maosong Sun. „Country Image in COVID-19 Pandemic: A Case Study of China”. *IEEE Transactions on Big Data* 7, sz. 1 (2021. március 1.): 81–92. https://doi.org/10.1109/TBDATA.2020.3023459.
- Laura M. Muñoz, Maria Fernanda Ramirez, és Jorge E. Camargo. „A Data-Driven Method for Measuring the Negative Impact of Sentiment Towards China in the Context of COVID-19”. In *Applied Informatics*, 210–21, é. n. http://dx.doi.org/10.1007/978-3-030-61702-8_15.
- Lina Gong. „Humanitarian diplomacy as an instrument for China's image-building”. *Asian Journal of Comparative Politics* 6, sz. 3 (2021. szeptember 1.): 238–52. https://doi.org/10.1177/20578911211019257.
- Kusai Sándor Zoltán. „Az új hidegháború kérdéséről”. *Külügyi Szemle*, sz. 20 (2021): 3–21. https://doi.org/10.47707%2FKulugyi_Szemle.2021.2.1.
- Yan Leng, Yujia Zhai, Shaojing Sun, Yifei Wu, Jordan Selzer, Sharon Strover, Hezhao Zhang, Anfan Chen, és Ying Ding. „Misinformation During the COVID-19 Outbreak in China: Cultural, Social and Political Entanglements”. *IEEE Transactions on Big Data* 7, sz. 1 (2021. március 1.): 69–80. https://doi.org/10.1109/TBDATA.2021.3055758.
- Yung-Yung Chang. „The Post-Pandemic World: between Constitutionalized and Authoritarian Orders – China's Narrative-Power Play in the Pandemic Era”. *Journal of Chinese Political Science*, sz. 26 (2020. december 1.): 27–65. https://doi.org/10.1007/s11366-020-09695-3.


Köszönöm a figyelmet!
Az Innovációs és Technológiai Minisztérium ÚNKP-21-1-I-NKE-67 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Epresi Ádám: A Biden-adminisztráció Tajvan-politikája

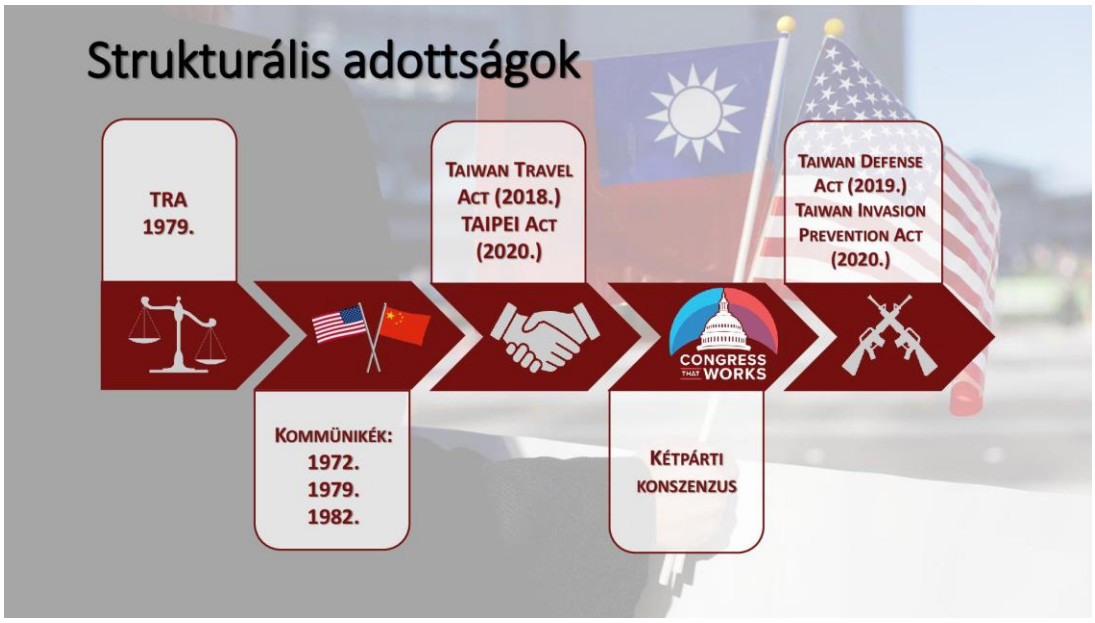
Korreferátum

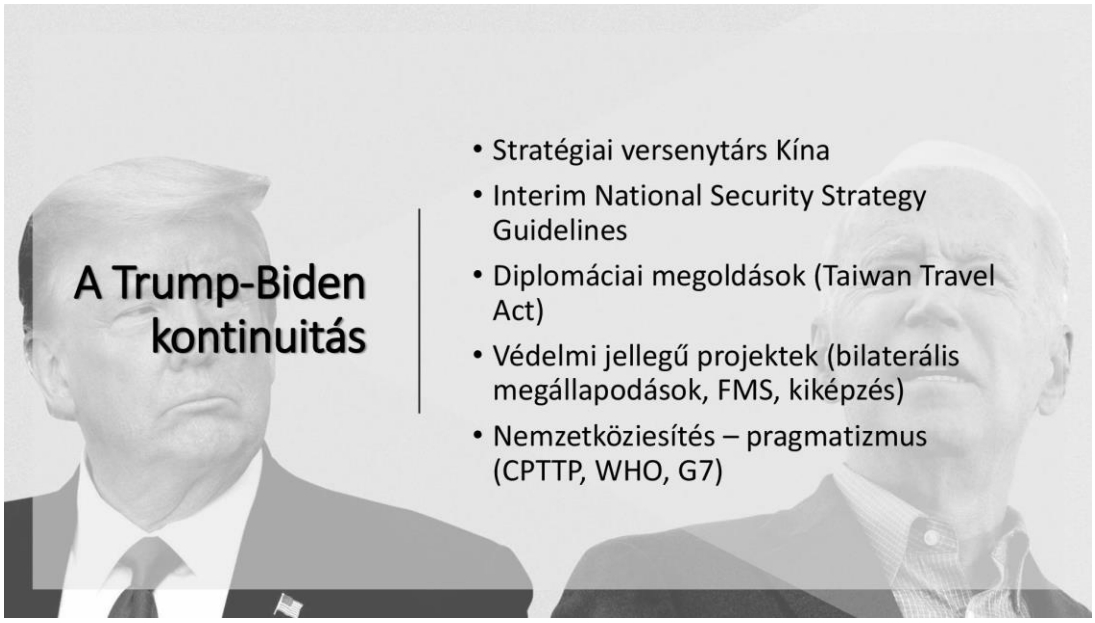
Tajvan az egyik legmilitarizáltabb és – potenciálisan – legforróbb térségben helyezkedik el, melyet nemzetközi jogi státusza tovább fokoz. Az Egyesült Államokhoz fűződő, egykor oly erős viszonya az 1970-es évek óta változott meg gyökeresen, ami a mai kapcsolatukat is determinálja. A gazdasági és politikai partnerséget azonban nem hivatalos csatornákon kénytelenek folytatni, és az egyre növekvő kínai fenyegetés, jelesül a fegyveres erőszak alkalmazásának kilátásba helyezése, kényszerpályára sodorhatja a feleket együttműködés tekintetében.

Előadásommal az egy éve hivatalban lévő Biden-adminisztráció Tajvan-politikájának általános ismertetésére vállalkozom. Szándékomban áll felvázolni, hogy milyen alapvető strukturális elemek gyakorolnak alapvető hatást az Egyesült Államok ezirányú politikájára. Számba veszem, hogy az új adminisztráció milyen módszereket, irányvonalakat vall magáénak közösen a trumpi külpolitikai apparátus által kijelöltekkel. Elemzésemben a diplomáciai és védelmi jellegű kapcsolatokon túl a Tajvan felé mutatott stratégiai magatartás, a stratégiai kétértelműség dilemmáját is bemutatom.


A Biden-adminisztráció Tajvan-politikája
Készítette: Epresi Ádám


Az előadás tartalma
• Strukturális adottságok – kapcsolatok
• A trumpi örökség továbbvitele
• Minőségi váltások
• Összegzés


Strukturális adottságok
TRA
1979.
Kommünikék:
1972.
1979.
1982.
Taiwan Travel Act (2018.)
TAIPEI Act
(2020.)
CONGRESS THAT WORKS
Kétpárti konszenzus
Taiwan Defense Act (2019.)
Taiwan Invasion Prevention Act
(2020.)


A Trump-Biden kontinuitás
• Stratégiai versenytárs Kína
• Interim National Security Strategy Guidelines
• Diplomáciai megoldások (Taiwan Travel Act)
• Védelmi jellegű projektek (bilaterális megállapodások, FMS, kiképzés)
• Nemzetköziesítés – pragmatizmus (CPTTP, WHO, G7)

Minőségi váltások

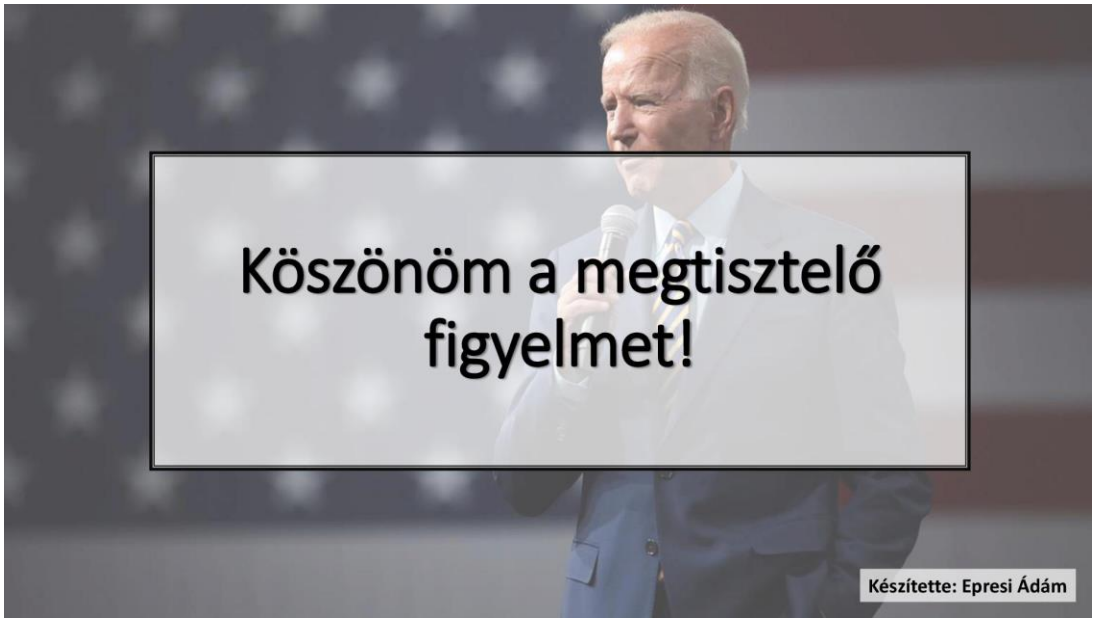
- Hagyományos szövetségi rendszer újjászervezése
- Diplomáciai megoldások (Biden beiktatása, palaui amerikai nagykövet, Summit for Democracy 2021)
- Stratégiai kétértelműség kérdése – kell-e váltás?
- *„… the smartest and effective way for us to help deter aggressive actions by (China) across the Taiwan Strait will be to stay with a policy that's been in place.” (Burns)*

Összegzés

- Magas szintű diplomácia és pragmatizmus keveréke
- Kétpárti konszenzus
- Tajvan-politika folytonossága
- Stratégiai kétértelműség
- Egyensúlyozás szükséges Kína és Tajvan viszonylatában

Felhasznált irodalom:

- Clarke, Michael – Sussex, Matthew: Why 'Strategic Ambiguity' Trumps 'Strategic Clarity' on Taiwan. https://rusi.org/explore-our-research/publications/commentary/why-strategic-ambiguity-trumps-strategic-clarity-taiwan [2022.01.16.]
- Everington, Keoni (2021), White House Says It Does Not Support Taiwan Independence, in: *Taiwan News*, www.taiwannews.com.tw/en/news/4242061 [2022.01.17.]
- Grossman, Derek: Biden Administration Shows Unwavering Support for Taiwan. https://www.rand.org/blog/2021/10/biden-administration-shows-unwavering-support-for-taiwan.html [2022.01.16.]
- Háda Béla: Joe Biden Ázsia-politikájának kiindulópontjai (SVKI Elemzések 2021/7) [2022.01.16.]
- Ishihara Tadahiro (2021) US-Taiwan Relations during the Tsai Ing-wen Administration and Prospects After the COVID-19 Pandemic, Asia-Pacific Review, 28:1, 118-141. [2022.01.17.]
- Kuehn, David: Managing the Status Quo: Continuity and Change in the United States' Taiwan Policy. Number 6, 2021. https://www.giga-hamburg.de/en/publications/giga-focus/managing-status-quo-continuity-change-united-states-taiwan-policy [2022.01.16.]
- Kwei-Bo Huang: The U.S. and Unresolved Cross-Strait Relations: From Trump to Biden In: Earl A. Carr Jr. (szerk.): From Trump to Biden and Beyond. Reimagining US–China Relations. Palgrave Macmillan, 2021. [2022.01.18.]
- Lawrence, Susan V.: Political and Security Issues (Congressonal Research Service) https://sgp.fas.org/crs/row/IF10275.pdf [2022.01.17.]
- Mazza, Michael: The Biden Administration's Diplomatic Moves Signal Strong Support for Taiwan. in: *Global Taiwan Brief*, 6, 7, 2021. pp. 13-15. https://globaltaiwan.org/wp-content/uploads/2021/04/GTB-PDF-6.7-.pdf [2022.01.16.]
- Nathan, Andrew J. (2021), Biden's China Policy: Old Wine in New Bottles?, In: *China Report*, online first 9 October, https://doi.org/10.1177/00094455211047069. [2022.01.17.]
- Taiwan: A front line in the new cold war? pp. 141-151. (2021) Asia, Strategic Survey, 121:1, 125-184 [2022.01.16.]



Bellus Bálint: A műholdromboló fegyverek napjainkban

Korreferátum

Napjainkban az űrhatalmak jelentős energiát fordítanak műholdromboló technológiák fejlesztésére, mivel egy fegyveres konfliktusban kiemelkedő jelentőségű lehet az ellenség űrbe telepített kommunikációs, navigációs és egyéb rendszereinek megsemmisítése. Előadásom célja, hogy bemutassa a műholdrombolás jelenségét, különösképpen a jelenleg ismert műholdrombolási megoldásokat és azok alkalmazásának körülményeit és tényezőit. A műholdrombolás gondolata már az űrverseny kezdetén megfogalmazódott a szuperhatalmakban. Napjainkban az űrhatalmak műholdromboló rakétákat és harci műholdakat fejlesztenek céljaik elérésére, de megjelennek szokatlan megoldások is. Véleményem szerint az űrfegyverkezés egyre jelentősebb a nagyhatalmi konfliktusokban, és ezen belül a műholdrombolás lehetősége kiemelt jelentőséggel bír.

Előadás felépítése

- Bevezetés
- A ,,korszak" kezdete
- A képességgel rendelkező országok
- Műholdromboló megoldások
- Magyar érintettség
- Összegzés

Bevezetés

- Műholdak- műholdrendszerek fontossága
- Rakétavédelem

A korszak kezdete

- 1960-as évek
- Űrverseny

A képességgel rendelkező országok

- USA (1959)
- Oroszország (1968)
- Kína (2007)
- India (2019)

Műholdromboló megoldások

Műholdromboló rakéta

- Indítás
  - Földről
  - Repülőről
- Pusztítás
  - Robbanótöltettel
  - Kinetikus energiával

Harci műhold

- Pusztítás
  - Lövedékkel
  - Lézerrel
  - Mikrohullámú fegyverrel

Szokatlan megoldások

- Robotkarral rendelkező műhold
- Fúvókában ,,rejtőző" fegyver

Magyar érintettség

- Magyarország Űrstratégiája (2021-től)

Összegzés

- Műholdrombló fegyverek fejlesztése/tesztelés napjainkban aktívan zajlik
- A világűr egyre jelentősebb hadszíntér

Baji Raik Martin: A 3D nyomtatott lőfegyverek nemzetbiztonsági kockázatai

Korreferátum

Előadásom célja elsősorban rámutatni az additív gyártás újgenerációs technológiája által létrehozott számos nemzetbiztonsági kockázatra, azon belül is az otthon gyártható 3D nyomtatott lőfegyverekre. Prezentációmban levezetem ezen illegális fegyverek egyszerű gyártási folyamatát, valamint kitérek a technológia forradalmi hatására az improvizált lőfegyverek világában; kiemelve decentralizált voltának jelentőségét a civil, valamint a katonai szektorban egyaránt. Részletesen kitérek a lőfegyvernyomtatás tevékenysége köré alakult sokszínű közösségre, valamint egyes kulcsfontosságú, szervezett csoportokra. Előadásom végén továbbá bemutatom a jelenleg fellelhető 3D nyomtatott lőfegyverek, valamint az elkészítésükhöz kulcsfontosságú fájlok legfőbb gyengepontjait, hiányosságait.

Célom az ezen lőfegyverek elérhetősége által létrehozott új nemzetbiztonsági kihívásokra való figyelemfelhívás, valamint az additív gyártás technikájának bemutatása, mint a decentralizált gyártástechnológia jövője.

Előadás felépítése

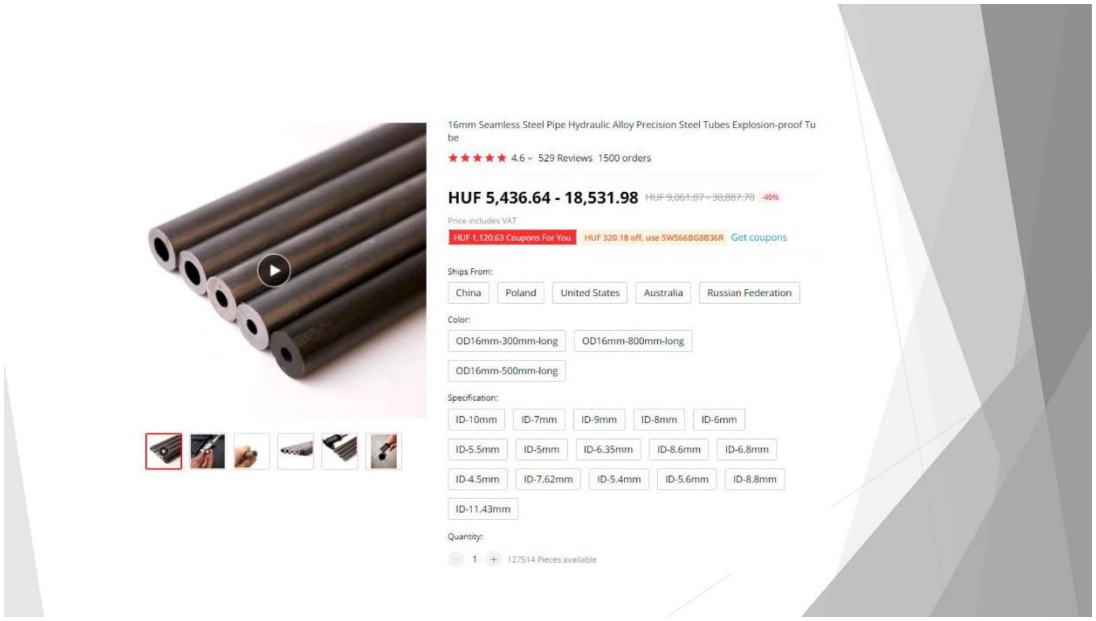
- Bevezetés: az additív gyártás, avagy 3D nyomtatás jellemzése
- A 3D nyomtatott lőfegyverek megjelenése, egyszerű múltja
- A „Deterrence Dispensed”, valamint más közösségek szerepe az improvizált fegyverek világában
- A forradalmi FGC-9
- 3D nyomtatott lőfegyverek a világban, a téma aktualitása
- Különböző nyomtatott lőfegyverek, továbbá az előttük álló akadályok bemutatása
- Összegzés


Bevezetés a 3D nyomtatásba
A 3D nyomtatás, ellentétben a különböző forgácsolási, lézervágási technikákkal ellentétben nem elvesz egy adott anyagból, hanem egy vízszintes munkalapra épít.
Ezt CAD-fájlok, valamint PLA, ABS műanyag, vagy fa, fém tekercsek felhasználásával teszi.
A különböző közösségileg elkészített CAD-fájlok elérhetőek számos portálon.
A technológia teljesen decentralizált, valamint számottevő technikai tudást nem igényel.


A 3D nyomtatott lőfegyverek megjelenése, egyszerű múltja
A legelső 3D nyomtatással készült lőfegyver 2013-ban jelent meg, „Liberator” néven.
Tervezői, valamint a fájlok terjesztői a „Defense Distributed” cégen belül végezték munkájukat, szervezetten, a nyilvánosság előtt.
A „Liberator” kezdetleges, valamint majdnem teljesen hatástalan volt, azonban sikerült a 3D nyomtatott lőfegyver koncepcióját a köztudatba juttatnia.

Az FGC-9(mm)

- Az súlyzáras FGC-9 2020 októberi megjelenése fordulópontot hozott az improvizált fegyverek történetében.
- A kifejezetten laikus embereknek tervezett fegyver otthon elkészíthető, csupán egy 3D nyomtató, valamint néhány külföldről rendelt alkatrész szükséges hozzá.
- A karabély 90%-ban 3D nyomtatással készült, a szükséges fém alkatrészei (például a fegyvercső) pedig könnyen elkészíthetőek a CAD fájlokhoz mellékelt 200 oldalas útmutatóval, amelyben a cső ECM huzagolásának elkészítésétől a lőszer újratöltéséig mindent kifejtenek, a legkisebb részletig.
- Más improvizált fegyverekkel ellentétben a lőfegyver legyártásához nem szükséges sem előzőleges szaktudás, sem felszerelt műhely.
- A lőfegyver teljesen követhetetlen. Otthoni elkészítéséből eredően, valamint szériaszám hiányában láthatatlan a hatóságok számára.


16mm Seamless Steel Pipe Hydraulic Alloy Precision Steel Tubes Explosion-proof Tu be
4.6 529 Reviews 1500 orders
HUF 5,436.64 - 18,531.98
Price includes VAT
HUF 1,120.63 Coupons For You
HUF 320.18 off, use SW566BG8B36R
Get coupons
Ships From:
China
Poland
United States
Australia
Russian Federation
Color:
OD16mm-300mm-long
OD16mm-800mm-long
OD16mm-500mm-long
Specification:
ID-10mm
ID-7mm
ID-9mm
ID-8mm
ID-6mm
ID-5.5mm
ID-5mm
ID-6.35mm
ID-8.6mm
ID-6.8mm
ID-4.5mm
ID-7.62mm
ID-5.4mm
ID-5.6mm
ID-8.8mm
ID-11.43mm
Quantity:
1
127514 Pieces available


3D lőfegyvergyártás a világban
A téma aktualitása
2021 júniusában, az ANOM „honeypot” applikáció segítségével a finn hatóságoknak sikerült lefoglalniuk hat 3D nyomtatott fegyverek gyártására használt nyomtatót, valamint 2 már összeszerelt FGC-9-et és alkatrészeiket.
A gyár valószínűleg a szervezett bűnözés egyik kulcsfontosságú fegyverutánpótlója volt.


3D lőfegyvergyártás a világban
A téma aktualitása
NSW Police Force
Hasonlóan a finn hatóságok akciójához, 2021 júniusában az ausztrál rendőrség is lefoglalt 3 FGC-9 karabélyt a New South Wales-i térségben.


3D lőfegyvergyártás a világban
A téma aktualitása
3D nyomtatott lőfegyvereket alkalmaz továbbá több felkelő csoport Myanmar területén, mivel azok kezelésének, valamint gyártásának egyszerűsége lehetővé teszik a gyorsabb kiképzést, valamint a decentralizált utánpótlást.


Más 3D nyomtatással létrehozott lőfegyverek
A „Deterrence Dispensed” az FGC-9 mellett más, részlegesen nyomtatott lőfegyverek létrehozására is terjeszt fájlokat.
3D nyomtatott tokozataik az USA-ban lehetővé teszik nagyobb kaliberű, forgó-tolózáras lőfegyverek hatóságoktól teljesen rejtett előállítását.

A 3D nyomtatott lőfegyverek gyengepontjai

- Lőszerutánpótlás, az útmutatók ellenére.
- Megmásítható CAD-fájlok
- Hatékony hüvelykivetés
- Teljes megbízhatóság

Összegzés

- a 3D nyomtatás rosszindulatú használata jelentős kihívással állítja szembe minden állam védelmét, kilátásban lévő átfogó megoldás nélkül. Az interneten lévő anyagok „törölhetetlen" jellege eszközeink, és stratégiánk átfogó fejlesztésére késztetnek bennünket, Hazánk örökös szolgálatában.

Forrásaim

- https://www.extremetech.com/extreme/133514-the-worlds-first-3d-printed-gun (Letöltés dátuma: 2022.01.17)
- https://en.wikipedia.org/wiki/Liberator_(gun) (Letöltés dátuma: 2022.01.16)
- https://en.wikipedia.org/wiki/FGC-9 (Letöltés dátuma: 2022.01.17)
- https://www.thesun.co.uk/news/14799456/britain-flooded-3d-guns-found-web/ (Letöltés dátuma: 2022.01.18)
- https://armamentresearch.com/3d-printed-firearms-factory-in-finland-raided/ (Letöltés dátuma: 2022.01.17)
- https://www.youtube.com/watch?v=d0q1cHAWQh8 (Letöltés dátuma: 2022.01.16)
- https://observers.france24.com/en/asia-pacific/20220114-3d-printed-weapons-myanmar-rebels (Letöltés dátuma: 2022.01.15)
- https://all3dp.com/1/3d-printed-gun-firearm-weapon-parts/ (Letöltés dátuma: 2022.01.17)
- Aliexpress (Letöltés dátuma: 2022.01.18)

Kárpáti Zalán: Nukleáris erők és a XXI. század

Korreferátum

Előadásom célja felvázolni a jelenleg atomfegyverekkel rendelkező országok nukleáris képességeinek és doktrínáinak felvázolása és kontextusba helyezése. A klasszikus atomnagyhatalmak, mint az USA és Oroszország mellett bemutatásra kerülnek a regionális nukleáris hatalmak is, megmagyarázva a nagyhatalmaktól és egymástól való eltéréseiket is. Szóba kerül az USA és a fölény-katasztrófapolitika-elmélet, Oroszország és az „eszkaláció a deeszkaláció érdekében", valamint a regionális atomhatalmak esetében a „katalizátor", a „biztos megtorlás" és az „aszimmetrikus eszkaláció" doktrínái. Ezen módszerek megismerése értékes tudást jelent a jelenlegi „második atomkorban".

AZ ELŐADÁS FELÉPÍTÉSE

- Második atomkor
- Az USA és a fölény-katasztrófapolitika-elmélet
- Oroszország és az „eszkaláció a deeszkalációért"
- Egyesült Királyság
- Regionális atomhatalmak módszerei, doktrínái
- Katalizáló arzenál
- Biztosított megtorlás
- Aszimmetrikus eszkaláció
- Összegzés

MÁSODIK ATOMKOR

- Növekvő nemzetközi feszültség
- Nagyszámú, feltörekvő szereplő
- A leszerelés vágyálma

USA

- Fölény-felsőbbrendűségi-elmélet (M. Kroening)
- Biztosított másodikcsapás-képességen túli kapacitás
- Politikai nyomásgyakorlás
- Nukleáris ernyő

Table 10.2. United States nuclear forces, January 2021

All figures are approximate and some are based on assessments by the authors. Totals for strategic and non-strategic forces are rounded to the nearest 5 warheads.

Type	Designation	No. of launchers	Year first deployed	Range (km)[a]	Warheads x yield	No. of warheads[b]
Strategic nuclear forces						3 570
Aircraft (bombers)		*107/66*[c]				*846*[d]
B-52H	Stratofortress	87/46	1961	16 000	20 x ALCMs 5–150 kt[e]	528[f]
B-2A	Spirit	20/20	1994	11 000	16 x B61-7, -11, B83-1 bombs[g]	*320*
Land-based missiles (ICBMs)		*400*				*800*[h]
LGM-30G	Minuteman III					
	Mk12A	200	1979	13 000	1–3 x W78 335 kt	600[i]
	Mk21 SERV	200	2006	13 000	1 x W87 300 kt	200[j]
Sea-based missiles (SLBMs)		*14/280*[k]				*1 920*[l]
UGM-133A	Trident II (D5/D5LE)					
	Mk4	..	1992	>12 000	1–8 x W76-0 100 kt	..[m]
	Mk4A	..	2008	>12 000	1–8 x W76-1 90 kt	1 511
	Mk4A	..	2019	>12 000	1 x W76-2 8 kt	25[n]
	Mk5	..	1990	>12 000	1–8 x W88 455 kt	384
Non-strategic nuclear forces						230[o]
F-15E	Strike Eagle	..	1988	3 840	5 x B61-3, -4[p]	80
F-16C/D	Falcon	..	1987	3 200[q]	2 x B61-3, -4	70
F-16MLU	Falcon (NATO)	..	1985	3 200	2 x B61-3, -4	40
PA-200	Tornado (NATO)	..	1983	2 400	2 x B61-3, -4	40
Total stockpile						3 800[r]
Deployed warheads						1 800[s]
Reserve warheads						2 000
Retired warheads awaiting dismantlement[t]						1 750
Total inventory						5 550[u]

OROSZORSZÁG

- Szovjetunió összeomlása, hagyományos képességek gyengülése
- Eszkaláció Deeszkaláció
- Homályos doktrína

Table 10.3. Russian nuclear forces, January 2021

All figures are approximate and are estimates based on assessments by the authors. Totals for strategic and non-strategic forces are rounded to the nearest 5 warheads.

Type/ Russian designation (NATO designation)	No. of launchers	Year first deployed	Range (km)[a]	Warheads x yield	No. of warheads[b]
Strategic nuclear forces					2 885[c]
Aircraft (bombers)	68/50[d]				580[d]
Tu-95MS/M (Bear-H)[e]	58/20	1981	6 500–10 500	6–16 x 200 kt AS-15A or AS-23B ALCMs	448
Tu-160/M (Blackjack)	13/11	1987	10 500–13 200	12 x 200 kt AS-15B or AS-23B ALCMs, bombs	132
Land-based missiles (ICBMs)	*310*				*1 186*[f]
RS-20V (SS-18 Satan)	46	1992	11 000–16 000	10 x 500–800 kt	460
RS-18 (SS-19 Stiletto)	..	1980	10 000	6 x 400 kt	..[g]
Avangard (SS-19 Mod 4)[e]	4	2019	10 000	1 x HGV [400 kt]	4
RS-12M Topol (SS-25 Sickle)	27	1985	10 500	1 x 800 kt	27
RS-12M2 Topol-M (SS-27 Mod 1/silo)	60	1997	10 500	1 x 800 kt	60
RS-12M1 Topol-M (SS-27 Mod 1/mobile)	18	2006	10 500	1 x [800 kt]	18
RS-24 Yars (SS-27 Mod 2/mobile)	135	2010	10 500	4 x [100 kt]	540
RS-24 Yars (SS-27 Mod 2/silo)	20	2014	10 500	4 x [100 kt]	80
RS-28 Sarmat (SS-X-29)	..	[2021]	>10 000	MIRV [..kt]	..
Sea-based missiles (SLBMs)	*11/176*[h]				*816*[i]
RSM-50 Volna (SS-N-18 M1 Stingray)	1/16	1978	6 500	3 x 50 kt	48
RSM-54 Sineva (SS-N-23 M1)	6/96	1986/ 2007	9 000	4 x 100 kt	384
RSM-56 Bulava (SS-N-32)	4/64	2014	>8 050	6 x [100 kt]	384
Non-strategic nuclear forces					1 010[j]
Air, coastal and missile defence	886				387
S-300/400 (SA-20/21)	60	1986	30	1 x 10 kt	48
	750[m]	1992/ 2007	..	1 x low kt	280
3M-55 Yakhont (SS-N-26)	60	[2014]	>400	1 x [.. kt]	25
SSC-1B (Sepal)	8	1973	500	1 x 350 kt	4
Air force weapons[k]	*260*				*500*
Tu-22M3 (Backfire-C)	60	1974	..	3 x ASMs, bombs	300
Su-24M/M2 (Fencer-D)	70	1974	..	2 x bombs	70[l]
Su-34 (Fullback)	120	2006	..	2 x bombs	120[l]
Su-57 (Felon)	..	[2020]	..	[bombs, ASM?]	..
MiG-31K (Foxhound)	10	2018	..	1 x ALBM	10

Type/ Russian designation (NATO designation)	No. of launchers	Year first deployed	Range (km)[a]	Warheads x yield	No. of warheads[b]
Army weapons	*164*				90
Iskander-M (SS-26 Stone)	144	2005	350[n]	[1 x 10–100 kt]	70[n]
OM729 (SSC-8)	20	2016	2 350	1 x [..kt]	20
Navy weapons	..				835
Submarine/surface ships/naval aircraft	..	Land-attack cruise missiles, sea-launched cruise missiles, anti-submarine weapons, surface-to-air missiles, depth bombs, torpedoes[o]			
Total stockpile					4 095
Deployed warheads					1 625[p]
Reserve warheads					2 470[q]
Retired warheads awaiting dismantlement					1 760
Total inventory					6 285

EGYESÜLT KIRÁLYSÁG

- „Szándékos kétértelműség"
- Integráció a NATO nukleáris védőernyőbe
- Folyamatos csökkentés

Table 10.4. British nuclear forces, January 2021

All figures are approximate and some are based on assessments by the authors.

Type/designation	No. of launchers	Year first deployed	Range (km)	Warheads x yield	No. of warheads
Sea-based missiles (SLBMs)	*4/64*[a]				*120*
Trident II D5	48[b]	1994	>10 000[c]	1–8 x 100 kt[d]	120
Total operationally available warheads					120[e]
Other stored warheads					105[f]
Total inventory					225[g]

REGIONÁLIS ATOMHATALMAK LEHETŐSÉGEI (V. NARANG)

- Katalizáló arzenál
- Biztosított megtorlás
- Aszimmetrikus eszkaláció

KATALIZÁLÓ ARZENÁL

- Kezdetleges képességek a harmadik fél bevonásához
- Néhány robbanófej összeszerelése
- Kezelése nem nyilvános
- Homályos képességek és bevethetőség

- Izrael (1967-1990)
- Dél-Afrika (1979-1991)
- Pakisztán (1986-1997)

BIZTOSÍTOTT MEGTORLÁS

- Nukleáris megtorlás komoly kár elszenvedése után
- Túlélőképes másodikcsapás-képesség
- Szoros politikai kontroll
- Egyértelmű képességek, homályos bevethetőség

- Kínai Népköztársaság (1964-)
- India (1974-)
- Izrael (1991-)

Table 10.6. Chinese nuclear forces, January 2021

All figures are approximate and some are based on assessments by the authors.

Type/Chinese designation (US designation)	No. of launchers	Year first deployed	Range (km)[a]	Warheads x yield[b]	No. of warheads[c]
Aircraft	*20*[d]				*20*
H-6K (B-6)	20	2009	3 100	1 x bomb	20
H-6N (B-6N)	–	[2022]	..	1 x ALBM	–
H-20 (B-20)	–	[2020s]	..	..	–
Land-based missiles[e]	*244*				*204*
DF-4 (CSS-3)	6[f]	1980	5 500	1 x 2.3 Mt	6[f]
DF-5A (CSS-4 Mod 1)	10	1981	>12 000	1 x 4–5 Mt	10
DF-5B (CSS-4 Mod 2)	10	2015	12 000	5 x 200–300 kt MIRV	50
DF-5C (CSS-4 Mod 3)	–	..	..	MIRV	–
DF-21A/E (CSS-5 Mod 2/6)[g]	40	1996/2017	2 100	1 x 200–300 kt	40
DF-26 (CSS-18)	100	2015	>4 000	1 x 200–300 kt	20
DF-31 (CSS-10 Mod 1)	6	2006	>7 000	1 x 200–300 kt	6
DF-31A/AG (CSS-10 Mod 2)	72	2007/2018	>11 200	1 x 200–300 kt	72
DF-41 (CSS-20)	–	[2021][f]	>12 000	3 x 200–300 kt MIRV	–
Sea-based missiles (SLBMs)	*4/48*[f]				*48*[f]
JL-2 (CSS-N-14)	48	2015	>7 000	1 x 200–300 kt	48
Total stockpile	**312**				**272**
Other stored warheads[h]					[78]
Total inventory	**312**				**[350]**[h]

ASZIMMETRIKUS ESZKALÁCIÓ

- Elsőcsapás-doktrína, elsődlegesen ellenséges hagyományos erők ellen
- Elsőcsapás-képességek
- Eszközök és irányítás integrálva a haderőbe
- Egyértelmű képességek és bevethetőség

- Franciaország (1960-)
- Pakisztán (1998-)
- Észak-Korea (2016-)

Table 10.8. Pakistani nuclear forces, January 2021

All figures are approximate and some are based on assessments by the authors.

Type/designation	No. of launchers	Year first deployed	Range (km)[a]	Warheads x yield[b]	No. of warheads[c]
Aircraft[d]	*36*				*36*
Mirage III/V	36	1998	2 100	1 x 5–12 kt bomb or Rahd ALCM (in development)[e]	36
Land-based missiles	*118*[f]				*118*
Abdali (Hatf-2)	10	2015	200	1 x 5–12 kt	10
Ghaznavi (Hatf-3)	16	2004	300	1 x 5–12 kt	16
Shaheen-I (Hatf-4)	16	2003	750	1 x 5–12 kt	16
Shaheen-IA (Hatf-4)[g]	..	..	900	1 x 5–12 kt	..
Shaheen-II (Hatf-6)	16	2014	2 000	1 x 10–40 kt	16
Shaheen-III (Hatf-..)[h]	..	[2023]	2 750	1 x 10–40 kt	..
Ghauri (Hatf-5)	24	2003	1 250	1 x 10–40 kt	24
Nasr (Hatf-9)	24	2013	70	1 x 5–12 kt	24
Ababeel (Hatf-..)	..	..	2 200	MIRV or MRV	..[i]
Babur GLCM (Hatf-7)	12	2014	350[j]	1 x 5–12 kt	12
Babur-2 GLCM (Hatf-..)	..	..[k]	700	1 x 5–12 kt	..
Sea-based missiles					
Babur-3 SLCM (Hatf-..)	..	..[l]	450	1 x 5–12 kt	..
Total stockpile	**154**				**154**
Other stored warheads[m]					11
Total inventory	**154**				**165**[m]

ÖSSZEGZÉS

- Hidegháborús modellek elavultsága
- Többpólusú világrend, többszereplős elrettentés
- Küszöbállamok

KÖSZÖNÖM A MEGTISZTELŐ FIGYELMET!

FORRÁSOK

- Korda, Matt; Kristensen, Hans M.: North Korean nuclear weapons, 2021, Bulletin of the Atomic Scientists, 77:4, 222-236
- Kroenig, Matthew: The Logic of American Nuclear Strategy: Why Strategic Superiority Matters, Oxford University Press, 2018
- Narang, Vipin: Nuclear Strategy in the Modern Era: Regional Powers and International Conflict, Princeton University Press, 2014
- Woolf, Amy F.: Russia's Nuclear Weapons: Doctrine, Forces, and Modernization, Congressional Research Service https://sgp.fas.org/crs/nuke/R45861.pdf (Letöltve: 2022. 01. 12.)
- World nuclear forces in SIPRI Yearbook 2021, Oxford University Press, 333-412

Fülöp Bence: Armageddon hadművelet

Korreferátum

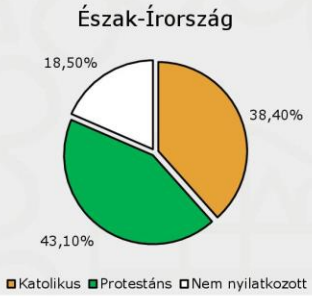
A „Zavargások” (angolul: The Troubles) három évtizedes és több, mint háromezer-ötszáz áldozatot követelő időszaka az Ír-sziget meghatározó periódusa volt, ami a mai napig kiemelkedően fontos befolyásoló szereppel bír Írország és Észak-Írország politikájában és kultúrájában. Előadásomban a hazánkban kevésbé ismert konfliktus egy érdekes haditervét mutatom be, ami az „Armageddon” fedőnevű hadijáték keretében született, de sosem valósult meg. A vallási és részben etnikai alapú konfliktusban a római katolikusokat patronáló déli fél az 1969 augusztusában lezajló bogside-i csata után készítette el saját tervezetét, amelyben jelentős szerepet kaptak volna az olyan nem tisztán katonai célpontok elleni elterelő fellépések, mint a gazdasági és kulturális létesítmények elfoglalása, valamint az Ír Hadsereg gerillaakciói két katolikus többségű városban, mivel egy konvencionális invázió lehetősége egyből elvetésre került a brit haderő ereje és képességei végett. Az előzmények és a tervezet ismertetése után megállapítom egy 1969-es hipotetikus végrehajtás feltételezett hosszú- és rövidtávú következményeit mindegyik félre levetítve. Végezetül a konfliktus aktuális vonatkozásairól is szót ejtek zárógondolatként.

Előadás felépítése

1. Előzmények
2. Tervezés
3. Hipotetikus lefolyás
4. Erőviszonyok
5. Hipotetikus következmények
6. Záró gondolatok

A „Zavargások” Írországa

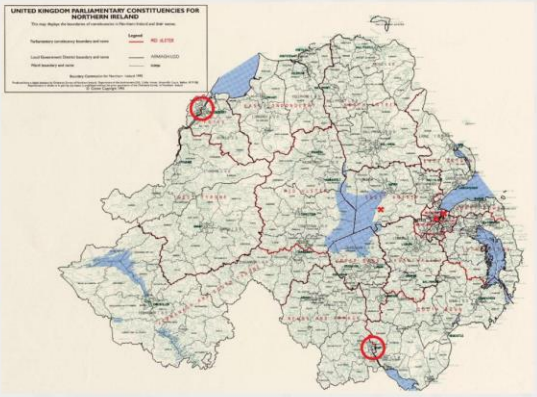
- 1916 – húsvéti felkelés
- 1919-21 – angol-ír háború
- 1922-23 – ír polgárháború
- 1949 – Írország teljes függetlensége
- ’60-as évek polgárjogi mozgalmai
- 1969 augusztusa – bogside-i csata
- Lynch beszéde



Tervezés

- John Lynch beszéde
  - John Taylor belügyi kisminiszter reakciója
- Augusztus 30 - Sean MacEoin vkf. Parancsot kap
- *Planning Board on Northern Ireland Operations*

Operation Armageddon



Erőviszonyok

- Déli fél
  - 2 136 fő harckész
    - 12 ezer helyett
  - Logisztikai hiányosságok

- Északi fél
  - 3 000 jól képzett katona
  - RUC
  - +380 ezer + RN + RAF
  - NATO

ARMY

Hipotetikus következmények

- Brit ellenintézkedések
- Vallási ellentétek és a konfliktus súlyosbodása
  - ~~*Alacsony intenzitási konfliktus*~~
- Diplomáciai és gazdasági elszigetelődés
  - EGK
  - ENSZ

Záró gondolatok

- 1998 – nagypénteki egyezmény
  - A „Zavargások” vége
- 2007 – Paisley-McGuiness kormány
- Brexit

Források

1. Donnacha Ó Beacháin: The Destiny of the Soldiers: Fianna Fáil, Irish Republicanism and the IRA, 1926-1973. Dublin, Gill & MacMillan, 2010.
2. David McKittrick, David McVea: Making Sense of the Trouble: The Story of the Conflict in Northern Ireland. Amsterdam, New Amsterdam Book, 2002.
3. The Irish Times, 2009. augusztus 31., 13. o.
4. John Burns: "Irish army plotted Belfast guerrilla war". The Sunday Times, 2009.
5. The Sunday Times (Irish edition), 2009. aug. 30, 4. o.
6. CAIN Web Service, Ulster University

Lux Benjámin: Kárpátalja geopolitikája a XX. század első felében

Korreferátum

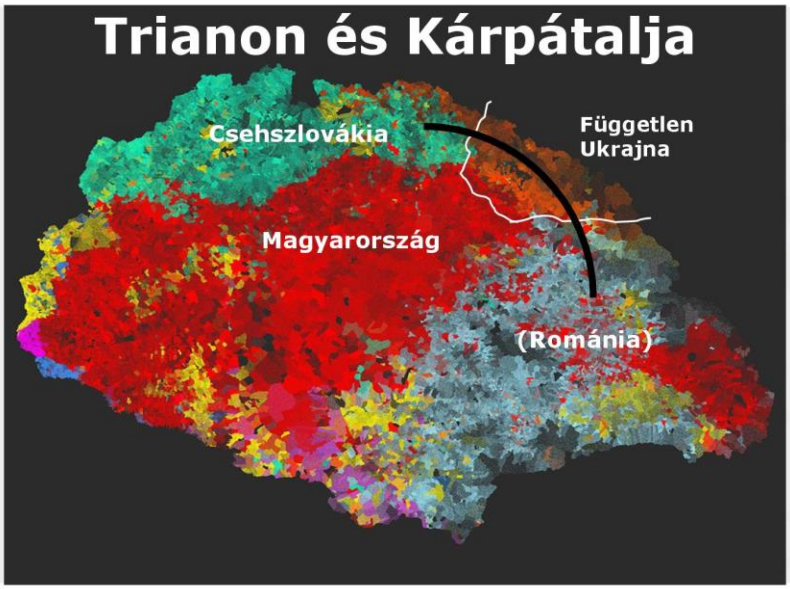
A világsajtóban napi szinten olvashatunk az Ukrajna és Oroszország között egyre inkább elmérgesedő szembenállásról. Hazánknak ez a konfliktus nem csupán azért érdemel kiemelt figyelmet, mivel egy velünk szomszédos országról van szó, hanem az ott található magyar kisebbség okán is. A trianoni béke során elszakított területek közül minden kétséget kizárólag Kárpátalja és a Kárpátalján élő magyarság járta be a „legszínesebb" utat a 20. században: a régió 1920-tól Csehszlovákia, 1939 és 45 között újfent Magyarország, ezt követően pedig a Szovjetunió részét képezte, egészen annak 1991-es bukásáig. Kárpátalja ennek a közel 70 éves periódusnak a legintenzívebb szakaszát egyértelműen az 1938 és 45 közötti időszakban élte át, melynek során nem kevesebb, mint 6 állam próbálta a terület hovatartozását valamilyen módon befolyásolni.

Előadásom célja bemutatni az 1920-as, 30-as és 40-es években Kárpátalja térségéért folytatott geopolitikai harcot, melynek során tökéletesen kikristályosodik a nagyhatalmi érdekek primátusa. Az első világháborút követően a francia befolyás, valamint a kisantant igényei határozták meg a terület sorsát, amely 1938-ban került ismét a hatalmi játszmák célkeresztjébe. Birtoklása mind a náci Németország, mind a Szovjetunió számára fontos mérföldkövet jelentett volna közép-európai pozíciójuk megerősítésében és

stratégiai céljaik elérésében, (melynek okán mindkét oldal igényt tartott a területre). Ennek ellenére pont Kárpátalja magyar kézre kerülése jelentette a német-szovjet közeledés, majd a Molotov-Ribbentrop paktum létrejöttének egyik alapját. A térség emellett kiemelt szerepet játszott a lengyel csapatok nyugatra való menekítésében, és a magyar-lengyel kapcsolatok újbóli felvirágzásában. Végül pedig a 2. világháborút követően a régió révén Szovjet-Oroszország a történelme során először vehetett birtokba területet a Kárpátokon belül.

Előadás felépítése

1. A 3+1 „kérő”
2. A ruszinok
3. A magyar álláspont 1938 előtt
4. Németország
5. Lengyelország
6. Fordulópont
7. Szovjetunió
8. Árpád-vonal
9. Összegzés

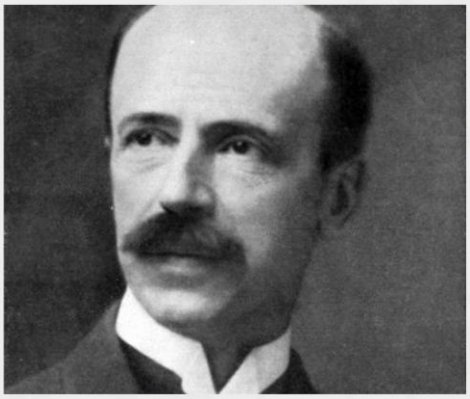


A ruszin-ok

- 1910
- Keleti szláv nép
- 500e + 500e
- Népszavazás (USA)
- **?ruszin = ukrán?**

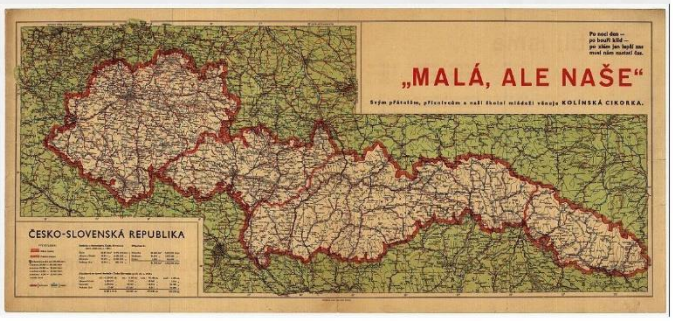
A bethleni konszolidáció és Kárpátalja

- Revízió
- Bethlen – pánszlávizmus
- Népszavazás!

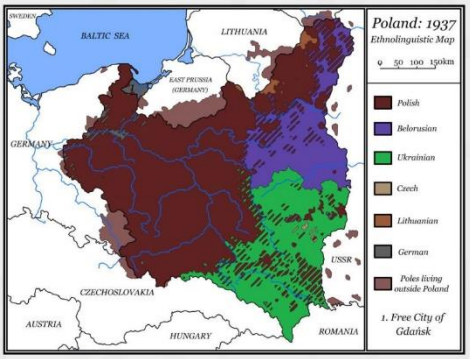


Németország és Kárpátalja

- 1938. augusztus 22. – Kiel
- Müncheni-egyezmény – I. bécsi döntés
- Autonómia
- Etnikai határ!
- **Ukrán Piemont**



Lengyelország érdeke



Hitler ukrán Piemont ⟷ Sztálin multietnikumú birodalma

A fordulópont

- ***Franciák felmondják a szovjetekkel kötött közös 1935-ös kölcsönös segítségnyújtási szerződést!***

- Németország lemond Kárpátaljáról!

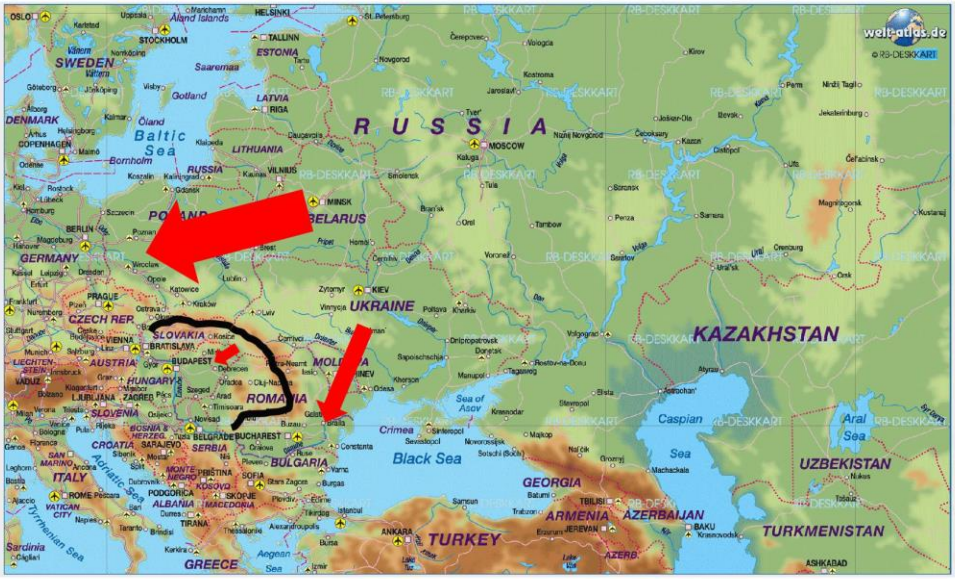
Szovjetunió

Miért?

- Ukrán nacionalisták
- Kárpát-medencébe jutás
- *Ősi anyaföld – Történelmi ok!*

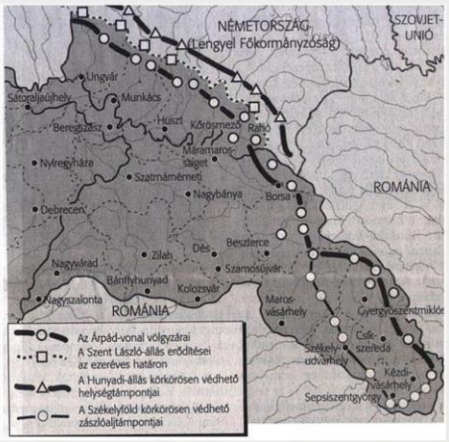
Hogyan?

- Diplomáciai utalások – Jugoszlávia
- Nyelvi eszközök – Kárpát-Ukrajna
- Beneš ajánlata



Az Árpád-vonal

- Komolyan veszik a célzásokat
- Sztójay – Magyarország vége
- Kárpátok vonalának védése



Összegzés

- Összekötő/elválasztó szerep
- (Nagy)hatalmi játszótér
- Autonómia - ruszin fogyás
- Csehszlovákok -> Szovjet bejutása a Kárpát-medencébe

Felhasznált szakirodalom

- Horváth, T. (2000). *AZ ÁRPÁD -VONAL SZAKMAI SZEMMEL (1940 -1944).* [online] Available at: https://folyoirat.ludovika.hu/index.php/mkk/article/download/3237/2483 [Accessed 20 Nov. 2021].
- Ignác Romsics (2019). *Bethlen István politikai életrajz.* Budapest] Helikon.
- Kuprii, T., Tymish, L. and Panasiuk, L. (2019). Subcarpathian Ruthenia in conditions of pre-war international crisis of 1938 and territorial encroachments of neighboring states (on regional press materials). *Skhid*, 0(6(164)), pp.75–82.
- Pastor, P. (2019). Hungarian And Soviet Efforts To Possess Ruthenia, 1938–1945. *The Historian*, 81(3), pp.398–425.
- Vološin, A. (1935). Carpathian Ruthenia. *The Slavonic and East European Review*, [online] 13(38), pp.372–378. Available at: https://www.jstor.org/stable/4203006 [Accessed 18 Jan. 2022].


PUSKÁS TIVADAR
NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
KÖSZÖNÖM A FIGYELMET!
VÁROM SZÍVES KÉRDÉSEIKET!
uni-nke.hu
ÚJ TÍPUSÚ KIHÍVÁSOK A BIZTONSÁGBAN – 2022.01.20.

Kiss András László: "Aki bújt, aki nem", avagy a digitális terepmintákról

Korreferátum

Az előadás központi témája a digitális terepminták és azok működési elvének a bemutatása. Kutatásomhoz számos tanulmányt, illetve saját kutatómunkát is felhasználtam. Az előadásnak nem célja meghatározni, hogy melyik terepminta a leghatékonyabb, csupán betekintést adni a digitális terepminták világába és a hatékony működésük mibenlétébe. A kutatásom fókuszában a digitális terepminták, és az alaklélektan szakmai felhasználása áll. Az előadás során számos képpel próbálom majd érzékeltetni, illetve a hallgató számára minél befogadhatóbbá tenni ezt a rendkívül komplex, illetve szerteágazó témát, illetőleg végezetül bemutatok egy teljesen magyar eredetű digitális terepmintát.


Az előadás felépítése
• A kezdetek
• MARPAT
• A digitális minták és a fraktálok
• Alaklélektan
• CONPAT

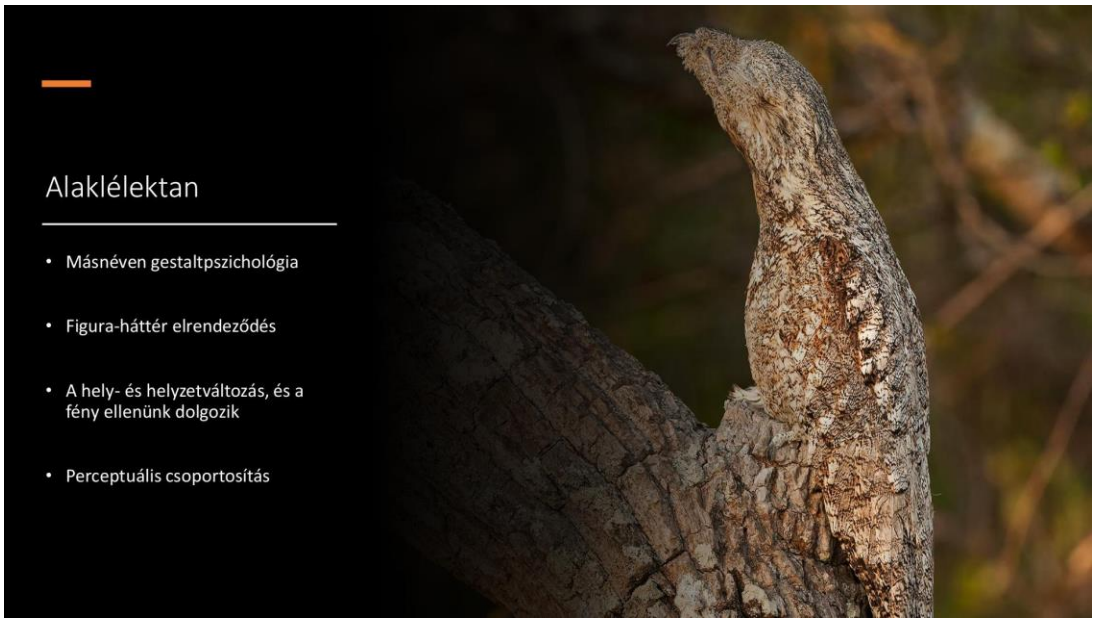

A kezdetek
• 19. századi reformok a katonai egyenruhák közt
• A Nagy Háború, és az álcák
• A khaki hódítása
• Technikai fejlődés, digitalizálódás

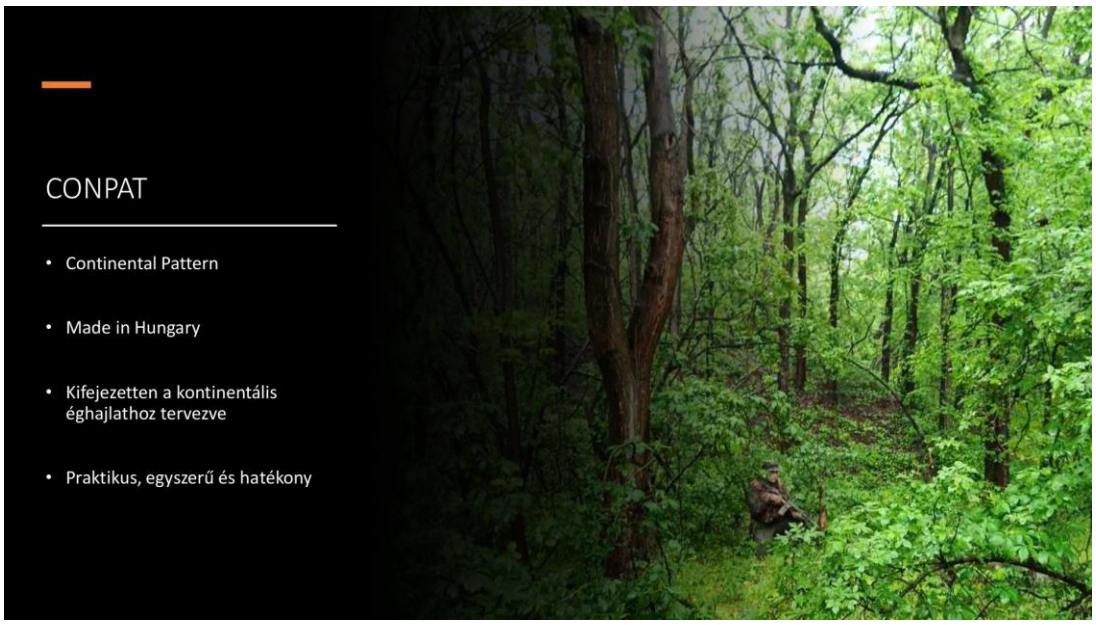
MARPAT

- 2001.
- Timothy R. O'Neill
- Számos variáció
- A digitális minták elterjedése

A digitális minták és a fraktálok

- Cél: A sziluett megtörése
- Digitalizálás, képpontosítás
- Fraktálok létrehozása
  - Nem differenciálhatók
- Tökéletes minta nem létezik


Alaklélektan
• Másnéven gestaltpszichológia
• Figura-háttér elrendeződés
• A hely- és helyzetváltozás, és a fény ellenünk dolgozik
• Perceptuális csoportosítás


CONPAT
• Continental Pattern
• Made in Hungary
• Kifejezetten a kontinentális éghajlathoz tervezve
• Praktikus, egyszerű és hatékony

Végezetül

Források

- http://www.pencottcamo.com/gallery/
- [1] Laszlo Talas, Roland J. Baddeley and Innes C. Cuthill: Cultural evolution of military camouflage /2017./ https://royalsocietypublishing.org/doi/10.1098/rstb.2016.0351 Letöltés dátuma: 2021.10.24.
- M Friškovec, H Gabrijelčič – Fibres & Textiles in Eastern Europe, /2010./ http://www.fibtex.lodz.pl/2010/4/68.pdfLetöltés dátuma: 2021.10.24.
- Robin J. Wharton: BARRIERS TO IMPLEMENTING A SINGLE JOINT COMBATCAMOUFLAGEUNIFORM/2017./Letöltés dátuma: 2021.10.29. https://apps.dtic.mil/sti/pdfs/AD1053502.pdf
- Saját kutatómunka
- Great Potoo. Photo: Thomas Marent

Korcsik Kristóf: A magyar-csehszlovák lakosságcsere és hatásai napjainkban

Korreferátum

Kutatásom célja a magyar-csehszlovák lakosságcsere és a reszlovakizáció történetének, valamint ezen két esemény a szlovákiai magyar kisebbségre gyakorolt, mai napig velünk élő hatásainak bemutatása. A kutatás során először megvizsgáltam a lakosságcsere és a reszlovakizáció történéseit és folyamatait, mely során külön figyelmet szenteltem a történtek nagyhatalmi összefüggéseinek feltárására, majd a szlovákiai magyarság mai napi helyzetét vizsgáltam legfőképpen a kisebbségi nyelvhasználat szlovákiai jogi szabályozásán keresztül, megkülönböztetett figyelemmel keresve a napjainkban tapasztalható folyamatok kapcsolódási pontjait a lakosságcserével és a reszlovakizációval. A kutatás során egyértelműen kimutathatóvá vált, hogy az imént említett két történelmi esemény jelentősen hozzájárult a felvidéki magyarság lélekszámának számottevő csökkenéséhez, egyrészt a lakosságcsere keretein belül és azon kívül végrehajtott áttelepítésekkel, másrészt a szlovákiai magyarság ellen irányított, és gyakran erőszakos asszimilációs törekvésekkel. Ugyancsak jelentős hatás, hogy a Szlovákia területén élő kisebbségek nyelvhasználati, kulturális és egyéb jogaikat mai napig nem élhetik meg teljesen, hiszen a lakosságcsere alapját adó kisebbségellenes gondolkodásmód a szlovák politikai elit köreiben manapság is megtalálható, jóllehet korlátozottabb mértékben, mint a második

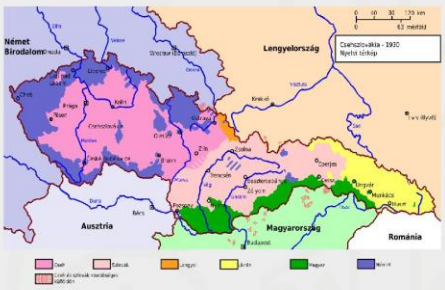
világháborút követő időszakban. A kutatás segítséget nyújthat a mai szlovákiai kisebbségi folyamatok megértéséhez a történelmi „alapok”, indíttatások leírásán keresztül, hiszen a történelem, mint oly sokszor korábban, most is egyfajta megalapozójaként szolgált a jelenkori történéseknek.

Előadás felépítése

1. Előzmények
2. Beneš moszkvai tárgyalásai
3. A magyarok jogfosztásának megkezdése
4. A felvidéki magyarok deportálása
5. A prágai tárgyalások
6. A lakosságcsere szünetelése, majd újraindulása
7. Az áttelepítettek száma
8. Reszlovakizáció
9. A lakosságcsere és a reszlovakizáció etnikai következményei
10. A szlovákiai magyarság helyzete napjainkban
11. Mai napig tartó hatások

Előzmények

- Csehszlovákia fennállása:
  - 1918-1939
  - 1945-1992
- 1938 és 1939 között következik be a felbomlás
  - Oka: magyar és német kisebbségek → állam területi épségét és szuverenitását fenyegetik
- Majd 100 éve fennálló probléma



Beneš moszkvai tárgyalásai

- 1942-43 folyamán szövetséges hozzájárulás a németek kitelepítéséhez
- Beneš felismeri a szovjetek szerepét a térségben
- Magyarok kitelepítésének ötlete: 1943 decembere, Moszkva
  - szovjet-csehszlovák barátsági tárgyalások
  - 3 hivatalos tárgyalás: December 14, 16, 18
  - Záróokmány aláírásának javaslata

A magyarok jogfosztásának megkezdése

- 1945. február 16 után: SZNT 4/1945 sz. rendelet
  - a német, a magyar és a szlovák árulók 50 holdnál nagyobb birtokainak elkobzása
- Sorozatos atrocitások, fokozatos jogfosztás
  - Magyar nemzetiségű köz- és magánalkalmazottak elbocsátása
  - Magyarok részvételének megtiltása a helyi községi tanácsokban
  - Magyarok fokozatos táborokba gyűjtése, embertelen állapotok
- 45' tavaszától a hazai sajtó értesítése→ Ideiglenes Nemzeti Kormány részéről több mint 184 jegyzék a Szövetséges Ellenőrző Bizottságnak

A felvidéki magyarok deportálása

- A potsdami konferencia elutasítja az egyoldalú kitelepítést→ csalódottság
- Kényszerítő eszköz: magyarok deportálása cseh területekre
  - Hivatalos indok: németek kitelepítése következtében előállt munkaerőhiány
- Hivatkozási alap: Általános munkakötelezettségről rendelkező 88/1945. számú elnöki dekrétum
  - 16-55 év közötti férfiak és 18-45 év közötti nők
- 2 hullám, az első humánusabb
  - Első hullám: 1945. október 25-december 4

A prágai tárgyalások

- 1945. december 3-6
- Szervezett lakosságcsere ötlete csehszlovák részről
- Magyar fél az önkéntes lakosságcserét támogatja
- Eredménytelen tárgyalások
- Nyilvánvalóvá válik, hogy a szövetséges nagyhatalmak nem szólnak bele az ügybe
- Újabb tárgyalások Prágában 1946 elején
  - Eredmény: magyar-csehszlovák lakosságcsere egyezmény megkötése, 1946. február 27

A lakosságcsere szünetelése, majd újraindulása

- Újabb ellentétek 1946 nyarán keletkeztek
- Magyar diplomácia eléri a nagyhatalmak távolmaradását
- Csehszlovák részről válaszként újra megindulnak a deportálások
  - Erőszakosabb, kegyetlenebb
- A deportálás ismét eléri célját→ tárgyalások újraindulása 1947 elején
- Eredmény: lakosságcsere újbóli megindításáról döntés 1947. március 24-én
- A csere egészen 1948 decemberéig tartott

Az áttelepítettek száma

- Áttelepülni kívánkozó szlovákok száma **1947 február**jában: több mint **95 ezer** fő
  - Ténylegesen áttelepült **73 273** fő (59 774 lakosságcsere keretein belül, 13 449 azon kívül)
- Kitelepítendő magyarok kiválasztása: Szlovák Telepítési Hivatal
  - **Vagyoni, politikai, területi és etnikai kritériumok**
  - Cél: magyar etnikum három vagy négy részre való feldarabolása
  - Legnagyobb figyelem: Pozsony és Ipolyság közötti terület
- Csehszlovákia összesen **181 512** felvidéki magyart szeretett volna áttelepíteni (31,7%)
  - Valójában **89 660** főt telepítettek át (55 487 kényszerből, 34 173 önként)
  - Lakosságcsere leginkább a Garam mentén teljesítette küldetését

Reszlovakizáció

- Alapfeltevés: magyarság nagy része elmagyarosodott vagy elmagyarosított szlovák
- Gyakorlati megvalósítás 1946 tavaszán kezdődik meg
- 1946. június 17-e és július 1-je között zajlik a kampány
- Eredménye minden várakozást felülmúl
- Gyakorlatilag az egész országra kiterjedt
- Összesen **352 038** személy kérte szlovákká minősítését (342 942 magyarlakta járásokból, 9906 az összes többi járásból)
- Határidőn kívül beérkezett kérvények száma több mint 60 ezer

Reszlovakizáció 2.

- 1930-ban csehszlovák állampolgársággal rendelkezők 62%-a eleget tesz a felhívásnak
- **Oka: üldöztetések alóli mentesülés reménye**
- Különbség mutatkozik a városokban, szórványban és vegyes etnikumú területeken élő magyarok és a zárt magyar etnikai területeken élő magyarok között
- Kétnyelvű, kettős identitású népesség nagy része reszlovakizált
  - 1921. és 1930. évi csehszlovák, és 1941. évi magyar népszámlálás különbségei

A lakosságcsere és a reszlovakizáció etnikai következményei

- felvidéki magyarság 15%-a kerül áttelepítésre
- Sikerült megbontani a magyar etnikai terület egységét
  - Ezek térsége vegyes lakosságúvá válik
- Számos új szlovák nyelvsziget jött létre

A szlovákiai magyarság helyzete napjainkban

- Főként szlovákok lakta régiókban gyakran a magyarul tudó emberek sem beszélnek már magyarul
- Magyarlakta területeken:
  - Nagymértékű asszimiláció
  - Hivatalos szóbeli és írásbeli kommunikáció szlovák nyelven zajlik
- A magyarok száma csökken
  - 1991: 568 000
  - 2011: 458 000
  - Okai: természetes fogyás; asszimiláció

A szlovákiai magyarság helyzete napjainkban 2.

- Magyar nemzetiségi alapon szerveződő pártok eredményessége nem igazán tér el Észak- és Dél-Szlovákiában
- 2011: kisebbségi nyelvtörvény módosítás
  - Szankciók a jogok be nem tartása esetére
  - Pozitív elmozdulás
  - Viszont nem oldja meg a kisebbségek nyelvhasználatával kapcsolatos problémákat

Mai napig tartó hatások

- Beneš-dekrétumok kérdése
- Nyelvhasználat kérdése

Felhasznált szakirodalom

- Tóth Ágnes: Telepítések Magyarországon 1945-1948 között. Bács-Kiskun Megyei Önkormányzat Levéltára, Kecskemét, 1993.
- Fülöp Mihály: Az elfelejtett béke. Tanulmánykötet a párizsi magyar békeszerződés életbelépésének 70. évfordulójára. Dialóg Campus Kiadó, Budapest, 2018.
- Szalai Gábor (2021). A csehszlovák-magyar lakosságcsere egyes külpolitikai összefüggései. Közép-Európai Közlemények, 13(4), 207-230, http://www.analecta.hu/index.php/vikekkek/article/view/33469.
- Varga Csilla (2017): A szlovákiai kisebbségek helyzete napjainkban, In. Regio, 25(1), 188-194.
- Popély Árpád (2002): Lakosságcsere és reszlovakizáció, In.Demográfia, 45(4), 468-491.
- Vadkerty Katalin (2007): A kitelepítéstől a reszlovakizációig. Trilógia a cseh-szlovákiai magyarság 1945-1948 közötti történetéről. Pozsony: Kalligram Könyvkiadó.

PUSKÁS TIVADAR

NEMZETI KÖZSZOLGÁLATI EGYETEM LUDOVIKA

KÖSZÖNÖM A FIGYELMET!

VÁROM SZÍVES KÉRDÉSEIKET!

uni-nke.hu

ÚJ TÍPUSÚ KIHÍVÁSOK A BIZTONSÁGBAN – 2022.01.20.

Vattai Eszter: Az infokommunikációs technológiák térhódítása, és annak hatása napjainkra

Korreferátum

Jelen előadásom az infokommunikációs technológiákat taglalja, és ossza fel a hidegháborúktól napjainkig. A kérdéskör mentén így egyik oldalról a nemzeti, illetve szövetségesi rendszerhez kapcsolódó technikai eszközök előnybe részesítése (és így a nagyobb vélt biztonság), másrészről a megállíthatatlanul globalizálódó infokommunikációs környezet előnyeinek és lehetőségeinek kihasználása áll szembe.

Bemutatómban, az infokommunikációs technológiák és a biztonság összefüggéseit kívánom bemutatni, hiszen amellett, hogy a korszerű eszközök számos módon jobbá teszik életünket, számos veszélyt is hordozhatnak. Gondoljunk csak az adataink védelmére, vagy akár például nem kellően biztonságos technológiák alkalmazására. Kiegészülve kronologikus felosztásban olvashatjuk a főbb nemzetbiztonságot is érintő technológiai botrányokat.

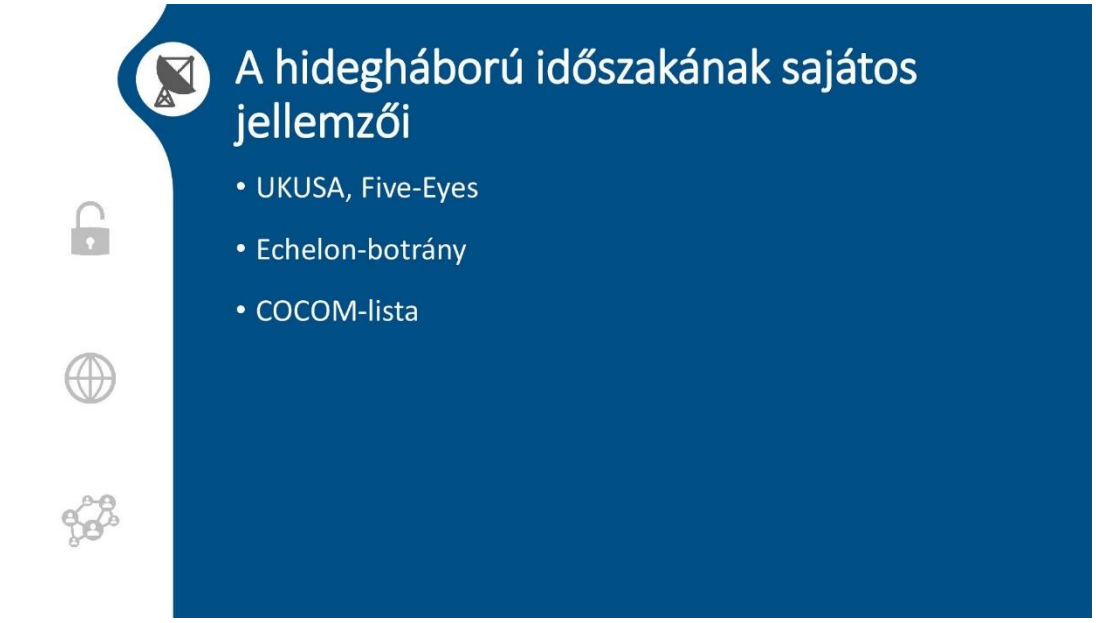
Véleményem szerint, ezek a botrányok és kezdetleges kommunikációs eszközök voltak az alappillérei a jelen társadalmunknak és technológiai eszközeinknek. Ezért is volt fontos ennek bemutatása, hogy megismerjük az alapot, ahonnan indult ez a tömérdek információ- és adathalmaz. Az első kommunikációs afférokból is látszott, hogy minden, aminek látható nyoma van, előbb-utóbb nem marad titok az emberiség számára, nevezzük ezt „technológiai lábnyomnak”. Kezdetben inkább nagyobb tehetősebb

körökben jelent meg, majd folyamatosan fejlődött és ért el a mindennapi emberhez, ezzel együtt a kiszolgáltatottság veszélye az internet felé folyamatosan nőtt.

A jelenben, ha egy képet megosztunk, ha egy posztot kiírunk, vagy elfogadjuk azokat a bizonyos „cookie" beállításokat, minden mozdulatunk és érdeklődési körünk lekövethető. Bizonyos szabályzók már léteznek erre, de mindig figyelnünk kell adatink biztonságára és arra is, hogy ne szippantson be minket a közösségi média világa. Realizálnunk kell a tényt, hogy „sose lehetünk egyedül", hiszen a technológia fejlődése megteremtette azt a szituációt, hogy bárhol és bárki lekövethető és lehallgatható legyen, legyenek példák erre a munkában bemutatott esetek.

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 és a nemzetközi színtéren látható folyamatokat vázoltam.


Az infokommunikációs technológiák térhódítása, és annak hatása napjainkra
Hidegháború
Kémbotrányok
Nemzetközi esetek
Közösségi hálók veszélye
Készítette: Vattai Eszter


A hidegháború időszakának sajátos jellemzői
• UKUSA, Five-Eyes
• Echelon-botrány
• COCOM-lista

UKUSA, Five Eyes

- SIGINT kapcsolatok
- BRUSA/UKUSA megállapodás UK-val, USA-val, majd Ausztrália, Kanada, Új-Zéland
- Céljuk, az emberek lehallgatása törvényesen, az együttműködések segítségével

Echelon-botrány

- Duncan Campbell újságírótól származik
- Cheshire települését vették észre
- Képesek voltak lehallgatni a rádió és telefonvonalakat, elolvasni a fax és e-mail forgalmazásokat
- Üzemeltetője az NSA

Kémbotrányok, technológiai incidensek

- U-2 incidens és néhány jelentősebb eseménye
- Profumo-ügy
- Watergate-botrány
- Toshiba botrány
- Crypto AG-botrány
- Wiki-leaks
- Edward Snowden
- Cambridge Analytica botrány

Wiki-leaks

- 2006-ban alapította Julian Assange
- Célja csökkenteni az országon belüli korrupciót
- „Collateral Murder” videó, háborús naplók
- Bradley Manning közlegény
- Az oldal még most is működik és szivárogtat ki információkat

Edward Snowden

- Infrastruktúra elemzőként dolgozott az NSA-nél
- Félrevezetés az amerikaiak által
- 2013-as interjúja robbantotta ki a botrány
- Létezik-e magánszféra?

Cambridge Analytica botrány

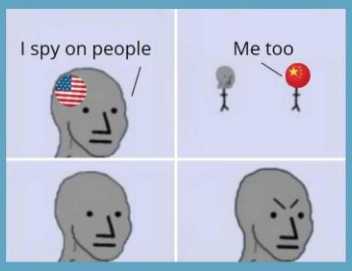
- 50 millió ember adatai kerülhettek illetéktelenekhez, későbbi ellenőrzések után kiderült, ez a szám a 87 milliót is elérte
- „thisisyourdigitallife” app
- Aleksandr Kogan-hoz fűződik
- Több politikai hatása is volt

A nemzetközi színtéren látható esetek

- USA-Kína technológiai konfliktusa
- High-tech cégek konfliktusa a nagyhatalmakkal

USA-Kína technológiai konfliktusa

- Donald Trump korlátozta bizonyos állami szféráknak, hogy olyan cégekkel szerződjenek, akik kollaboráltak a Huawei-el
- Kína ezután beperli az USA-t és kereskedelmi vitába keverednek
- Az USA 2021. májusban tovább szigorítja a korlátozásokat
- Honor az új Huawei



High-tech cégek konfliktusa a nagyhatalmakkal

- 2020. második felében tárgyalások zajlottak a négy legnagyobb high-tech céggel
- David Cicilline kongresszusi képviselő szerint; romboló, káros módszerekkel gyakorolták hatalmukat
- A tech-cégek képviselői tagadják az állítást
- Nem valószínű, hogy a kongresszus új jogszabályokat alkosson ennek megoldására

Közösségi hálók veszélye a 21. században

- Mentális és fizikai egészség károsodása
- Dezinformáció
- Algoritmusok hatása a gondolkodásunkra, tetteinkre

Dezinformáció

- Melyek a dezinformációt segítő tényezők?
- Post-truth politika, álhírek gyors terjedése
- Átalakult hírfogyasztási szokások, túlzott információmennyiség, algoritmusok

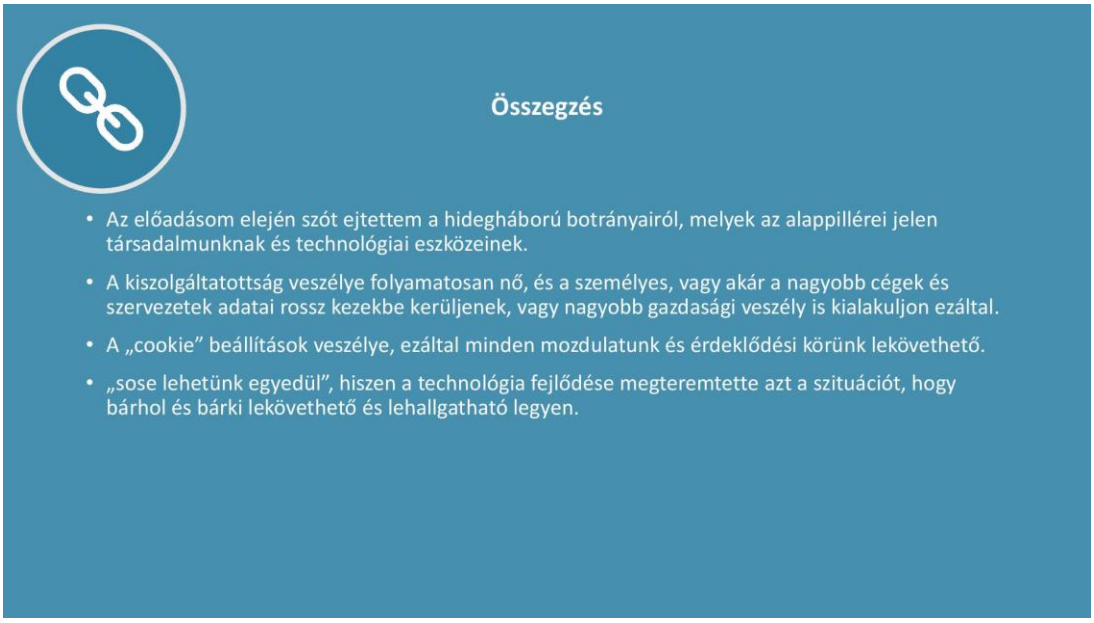
Algoritmusok hatása a gondolkodásunkra, tetteinkre

- Mi alapján működnek az algoritmusok?
- „Filter bubble”-intellektuális elkülönítés a felhasználó által kedvelt és nem kedvelt tartalmai között

algorithm
noun

Word used by programmers when they do not want to explain what they did.


Az infokommunikációs technológiák térhódítása, és annak hatása napjainkra
Összegzés
Felhasznált irodalmak,
Készítette: Vattai Eszter


Összegzés
• Az előadásom elején szót ejtettem a hidegháború botrányairól, melyek az alappillérei jelen társadalmunknak és technológiai eszközeinek.
• A kiszolgáltatottság veszélye folyamatosan nő, és a személyes, vagy akár a nagyobb cégek és szervezetek adatai rossz kezekbe kerüljenek, vagy nagyobb gazdasági veszély is kialakuljon ezáltal.
• A „cookie" beállítások veszélye, ezáltal minden mozdulatunk és érdeklődési körünk lekövethető.
• „sose lehetünk egyedül", hiszen a technológia fejlődése megteremtette azt a szituációt, hogy bárhol és bárki lekövethető és lehallgatható legyen.

Internetes források

- https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc; letöltve: 2020.10.18.; fordította: szerző
- https://www.nsa.gov/news-features/declassified-documents/ukusa/ ; letöltve: 2020.10.16.; fordította: szerző
- https://hvg.hu/tudomany/20180317_cambridge_analytica_adatgyujtes_facebook; letöltve: 2021.03.15.
- https://theconversation.com/post-truth-politics-and-why-the-antidote-isnt-simply-fact-checking-and-truth-87364; Post-truth politics and why the antidote isn't simply 'fact-checking' and truth: John Keane letöltve: 2021.04.10.; fordította: szerző
- https://www.bbc.com/news/business-48441814; Huawei: US blacklist will harm billions of consumers, 29 May 2019 letöltve: 2020.10.01.; fordította: szerző
- https://www.bbc.com/news/business-53583941; Apple, Amazon, Facebook, Google face claims of 'harmful' power, 30 July 2020 letöltve: 2021.04.15.; fordította: szerző
- https://www.technologyreview.com/2010/12/09/120156/everything-you-need-to-know-about-wikileaks/; Everything You Need to Know About Wikileaks, Two experts lay out the facts surrounding the controversy: Jonathan Zittrain, Molly Sauter, december 9, 2010; letöltve: 2021.03.15.; fordította: szerző
- https://www.theguardian.com/world/video/2014/jul/17/edward-snowden-video-interview; letöltve: 2021.03.15.
- https://www.thelivingmoon.com/45jack_files/03files/ECHELON_Menwith_Hill.html; 2020.10.17.; fordította: szerző

Nyomtatott források, ábrák jegyzéke

- Papp Kristóf Csaba: A Cambridge Analytica-botárny tanulságai; KNBSZ: Szakmai Szemle, XVIII. évfolyam 1. szám 2020. március; 145.-158. oldal; letöltve: 2021.04.22.
- Lélektani műveletek a közösségi médiában: Bányász Péter, Dobos László, Palla Gergely, Polner Péter, (14. oldal); Dialóg Campus, Budapest, 2019

- https://hu.stt-kharisma.org/article/1335320/; letöltve: 2021.05.14. (1.ábra)
- https://www.pixtastock.com/illustration/75323234; letöltve: 2021.05.14. (2.ábra)
- https://asiatimes.com/2020/02/china-takes-a-stab-at-one-of-the-five-eyes/; letöltve: 2021.05.14. (3.ábra)
- A rádiótechnika évkönyve – 2002: Horváth Lajos: A világ legnagyobb fülei... (4.,5. ábra)
- https://hu.wikipedia.org/wiki/WikiLeaks; letöltve: 2021.05.14. (6. ábra)
- http://www.evault.com.my/edward-joseph-snowden; letöltve: 2021.05.14. (7.ábra)
- https://www.inc.com/alyssa-satara/if-you-dont-fully-understand-cambridge-analytica-scandal-read-this-simplified-version.html; letöltve: 2021.05.14. (8. ábra)
- https://www.boredpanda.com/huawei-google-memes/?utm_source=google&utm_medium=organic&utm_campaign=organic; letöltve: 2021.05.15. (9.ábra)
- https://www.bbc.com/news/business-53583941; letöltve: 2021.05.15. (10.ábra)
- https://knowledge.wharton.upenn.edu/article/rothschild-project-ratio/; letöltve: 2021.05.15. (11. ábra)
- https://www.pinterest.co.uk/pin/73042825179196258/; letöltve: 2021.05.15. (12.ábra)


Az infokommunikációs technológiák térhódítása, és annak hatása napjainkra
Köszönöm a megtisztelő figyelmet!
Készítette: Vattai Eszter
Elérhetőség:
Email: vattaieszter2001@gmail.com
Mobil: +36/30-4899246

Baglyos Sándor: IT biztonsági auditálás

Korreferátum

Napjainkban az informatikai szolgáltatások olyan mértékben befolyásolják a különböző szervezetek működését, hogy hatékony ellenőrzés, kontroll nélkül a biztonságos üzemelés nem képzelhető el. Az informatikai megoldások által elérhető kényelemnek azonban ára van. A felhasználók kiszolgáltatottabbak a különböző típusú szándékos és nem szándékos informatikai károkozásokkal szemben. Az informatikai eszközök használata komoly kockázatokat hordoz magában, bizalmas adatok elvesztése, illetéktelenekhez kerülése komoly anyagi és erkölcsi károkat okozhat. Ellentétben a hagyományos, papír - alapú iratkezelés áttekinthető szabályrendszerével, az elektronikus megvalósítás során új követelmények fogalmazódnak meg. Kialakult egyfajta függőség az informatikai rendszerekkel szemben, és ez a tény megnövelte az információ- és informatikai biztonság, ezzel együtt az ellenőrzés szerepét. A biztonság meglétét a szervezetek számára igazolja a nemzetközileg is elfogadott auditok elkészítése és azokon történő megfelelése. Az informatikai auditor dolgozhat egy szervezeten belül, ahol feladata az ellenőrzés alapjainak megismertetése az IT ellenőrzés és biztonság területén dolgozókkal, illetve a vezetőkkel, majd egy közös fogalomrendszer kialakítása a feladat megoldásához. Az informatikai rendszerek üzemeltetése, a gyors fejlődés és az újabbnál újabb kiberbiztonsági fenyegetések mellett nehéz a megfelelő intézkedéseket megfogalmazni és azokat alkalmazni. Ezt

segíti az üzletmenet-folytonossági terv (Business Continuity Plan, BCP) az adott szervezet működési folyamatainak zavartalan fenntartásához szükséges feladatok összessége, amely számba veszi az egyes folyamatok lehetséges fenyegetettségeit, a fenyegetettségek bekövetkezési valószínűségét és a folyamat kieséséből származó esetleges károkat. A fentieken alapuló kockázatelemzés eredményeképpen határozza meg a szervezet funkcionalitásának fenntartásához szükséges eljárásokat. A versenyképesség fenntartása és az üzleti környezetben való túlélés megköveteli ezeknek a tényezőknek a lehető legjobb alkalmazását.

Előadás felépítése

- Téma aktualitása
- Tudományos probléma
- Kutatási célkitűzések
- Hipotézisek
- Kutatási módszerek
- Auditálás megjelenése
- Információ biztonsági auditálás
- A belső ellenőrzések átalakulása a Covid-19 alatt
- Home office távmunka biztonság munkáltatói oldalról
- Biztonságtudatosság fejlesztése

Téma aktualitása

[1]

Informatikai kockázatok
- Bizalmas adatok elvesztése
- Illetéktelenekhez kerülése

Anyagi és erkölcsi károk

Tudományos probléma

[2]

Nélkülözhetetlen informatikai rendszerek

Sérülékenység
Kockázat
Ellenőrzések szükségessége

Kutatási célkitűzés

Magyarországi intézmények információbiztonsági tudatosságának érettségi fejlesztése

Hipotézisek

H1. Azok az **intézmények**, amelyek rendelkeztek **üzletmenet-folytonossági tervvel**, könnyebben megbirkóztak a **COVID-19** járvány **nehézségeivel**.

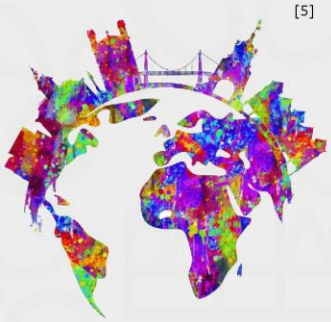
H2. A **COVID-19** járvány első hullámát **követően** a szervezetek **megalkották** a hiányzó üzletmenet-folytonossággal kapcsolatos **terveiket**. A jövőben **több energiát** fektetnek a saját üzletmenet-folytonossági tervük elkészítésére.

H3. Minél nagyobb egy **szervezet**, annál **kifinomultabb** az **érettségi modellje**.

Kutatási módszerek

[4]

[5]



Auditálás megjelenése

[6]

Audit jelentése „vizsgálat”

Rendszer, folyamat, termék

Lehet teljeskörű vagy részleges

Információ biztonsági auditálás

[7]

- Belső és külső audit
- Materiális és immateriális értékek
- Külső audit elfogulatlan + Ellenőrzi a belső auditot
- Törvényi kötelezettségek, belső szabályozás

A belső ellenőrzések átalakulása a Covid-19 alatt

[8]

A belső ellenőrzések átalakulása a Covid-19 alatt

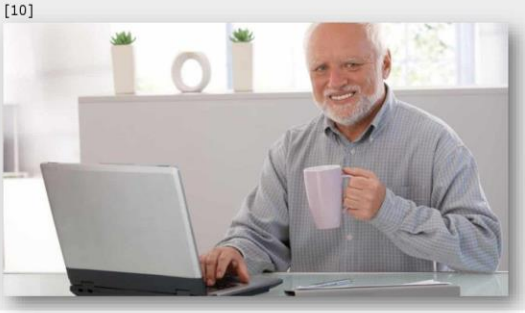
- A kockázati szakértők átirányítása a koronavírus prioritásához
- Új végrehajtási modellek és értékteremtési módok létrehozása
- Proaktív kommunikáció a vezetőség és az auditbizottság között
- A rövid távú többletkapacitást felhasználni olyan tevékenységekre, amelyek stratégiai szinten segítik a szervezet működését

Home office biztonsága munkáltatói oldalról

[9]

Biztonságtudatosság fejlesztése

[10]



- E-mail csatolmányok
- Linkek
- Kártékony kódok
- Ismeretlen külső eszközök
- Belépési azonosítók

Összegzés

[11]

- Hiányosságok feltérképezése
- IT struktúra működési problémákra való felhívás
- Jelenlegi IT struktúra fejlesztési tanácsadás
- Kollégák fejlődési lehetőségeinek elősegítése

Felhasznált irodalom

1) https://cmp.smu.edu.sg/sites/cmp.smu.edu.sg/files/perspectives/Digitalisation.jpg

2) https://media.istockphoto.com/photos/technician-with-a-laptop-computer-and-black-male-engineer-colleague-picture-id1131198259?b=1&k=20&m=1131198259&s=170667a&w=0&h=CfO71_GjHJPYJ-da3wuXRlRkuVErkARJb6024udByKU=

3) https://www.medicalnews.md/wp-content/uploads/2020/08/sh_vector_dominos_1680080773_REV.jpg

4) https://cdn.guidingtech.com/imager/assets/2020/10/1304530/edit-google-forms_05be6e9b9d53d1d1680b6ab56f4753b7_4d470f76dc99e18ad75087b1b8410ea9.png?1602482887

5) https://www.altec-inc.com/wp-content/uploads/2019/04/Audit.png

6) https://www.utoronto.ca/sites/default/files/GettyImages-1180387443.jpg

7) https://safety4sea.com/wp-content/uploads/2020/04/COVID19_Infographics_mrt20_0211.jpg

8) https://www.peoplemanagement.co.uk/Images/secure-stamp-graphic_tcm27-92122.jpg

9) https://assets2.theenglishfarm.com/sites/default/files/styles/featured_image/public/harold_2.jpg?itok=NGsRc1Co

10) https://scontent-vie1-1.xx.fbcdn.net/v/t1.6435-9/72211376_3582199385130944_9044006918309281792_n.jpg?_nc_cat=102&ccb=1-5&_nc_sid=09cbfe&_nc_ohc=QgeuFAgFuHcAX8MK22N&_nc_ht=scontent-vie1-1.xx&oh=30cdb762fa1bc2019ca1a4fb154b5a31&oe=616DE5CC

11) https://www.thestatesman.org/wp-content/uploads/2020/09/Email-Malware-Attack.jpg

12) https://signal.avg.com/hs-fs/hubfs/Blog_Content/Avg/Signal/AVG%20Signal%20Images/What%20is%20Malware%20(Signal)%20-%20refresh/Malware-spreading.png?width=1320&name=Malware-spreading.png

13) https://www.eagleedge.com.au/wp-content/uploads/2021/03/3-Ways-a-Risk-Audit-Will-Help-Your-Business-Prepare-for-the-Unknown-copy.webp

KÖSZÖNÖM A FIGYELMET!

KÉRDÉS?

uni-nke.hu

Kiss Márton: Az emlékezetpolitika, mint a biztonsági kihívás a 21. századi Európában

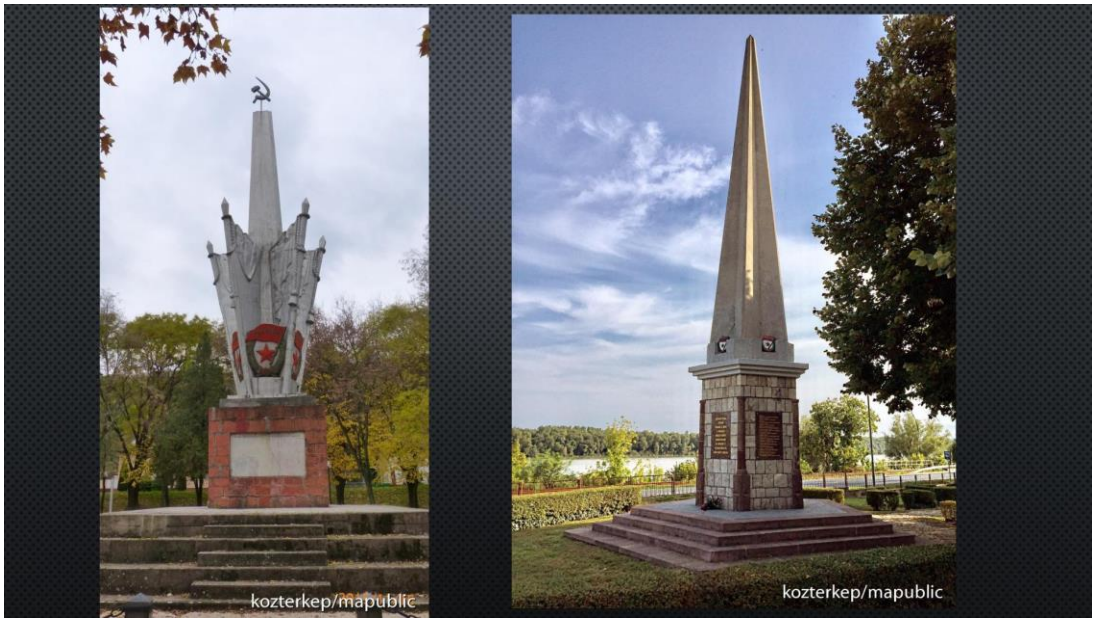
Korreferátum

Az emlékezetpolitika értelmezését számos tudományág megtette az idők folyamán. Az egyéni és csoportos identitás vizsgálatakor fontos szerepet szánnak a múlt eseményeinek értelmezésére. A kutatók egyenes arányosságot feltételeznek az identitás erőssége a különböző emlékezetek mélysége között. Biztonságpolitikai szempontból az emlékezet kérdése egyszerre jelenhet meg integráló erőként és a széthúzás példájaként. Samuel Huntington jól utalt arra, hogy a 21. században a különböző civilizációk határán újfajta konfliktusok törhetnek ki – ilyen lehet az európai emlékezetpolitikák összeütközése is.

Előadásomban két ilyen struktúrát kívánok bemutatni, melyek alapvetően egymással szemben határozzák meg magukat. Az egyik az Európai Unió közös emlékezetpolitikája a 21. században, melynek célja a különböző államok egységének erősítése, egyben az intézménybe vetett bizalom növelése volt. Ebben fontos szerepet szántak a nácizmus és a „sztálini diktatúra” áldozatainak közös emlékezetének, mint egymást kiegyenlítő faktoroknak. A traumatizált 20. század emlékezete az orosz emlékezetpolitikában is szerepet játszik. Különleges kérdést jelent az orosz állam szovjet múlthoz kötődő viszonya, valamint a tapasztalatok külkapcsolatokban történő felhasználása. Tipikus példa erre

Vladimir Putyin 2021-es beszéde, melyben a háború emlékezetét vetette össze az aktuális politikai klímával.

A különböző dokumentumok összevetésével kívánom bemutatni, hogy az emlékezetpolitika milyen módon van hatással a relatív biztonságérzetre és mikortól válik a külpolitika motorjává.

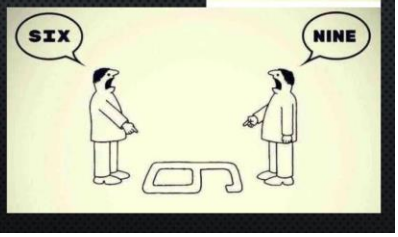

kozterkep/mapublic
kozterkep/mapublic

EMLÉKEZET ÉS BIZTONSÁG

- EGYÉNI ÉS KOLLEKTÍV EMLÉKEZET (HALBWACHS)
- PIERRE NORA: EMLÉKEZETI HELYEK (LIEUX DE MÉMOIRE)
- AZ ERŐS IDENTITÁS POZITÍV HATÁSSAL VAN A BIZTONSÁGRA
- TRAUMATÁRSADALMAK:
  - NÁCIZMUS <-> SZTÁLINISTA DIKTATÚRA
- HUNTINGTON CIVILIZÁCIÓS ELMÉLETE
- KÉT EMLÉKEZETPOLITIKAI PÉLDA
  - EURÓPAI UNIÓ
  - OROSZORSZÁG

AZ EMLÉKEZETPOLITIKA, MINT „SOFT POWER”

- AZ EMLÉKEZETPOLITIKA TIPIKUSAN A „PUHA ERŐ" (SOFT POWER) ESZKÖZÖK KÖZÉ SOROLANDÓ
- TÖBB SZINTEN IS ÉRTELMEZHETŐK
  - ÁLLAMI SZFÉRA
  - SZUPRANACIONÁLIS SZERVEZETEK ESETÉBEN (EURÓPAI UNIÓ)
  - ÁLLAMOK KÖZÖTTI KAPCSOLATOKNÁL (EU <-> OROSZORSZÁG VISZONYLATA)
- HATÁSÁT NÉZVE TEKINTHETJÜK:
  - ERŐSÍTŐ (INTEGRÁLÁS)
  - GYENGÍTŐ (DEZINTEGRÁLÁS)
- TIPIKUS PÉLDA A HIDEGHÁBORÚBAN TAPASZTALT „KÉT VILÁG" TÉTELE
- HUNTINGTON CIVILIZÁCIÓS ELMÉLETE SZERINT
  - A HÁBORÚK A CIVILIZÁCIÓS HATÁROKON TÖRTÉNNEK

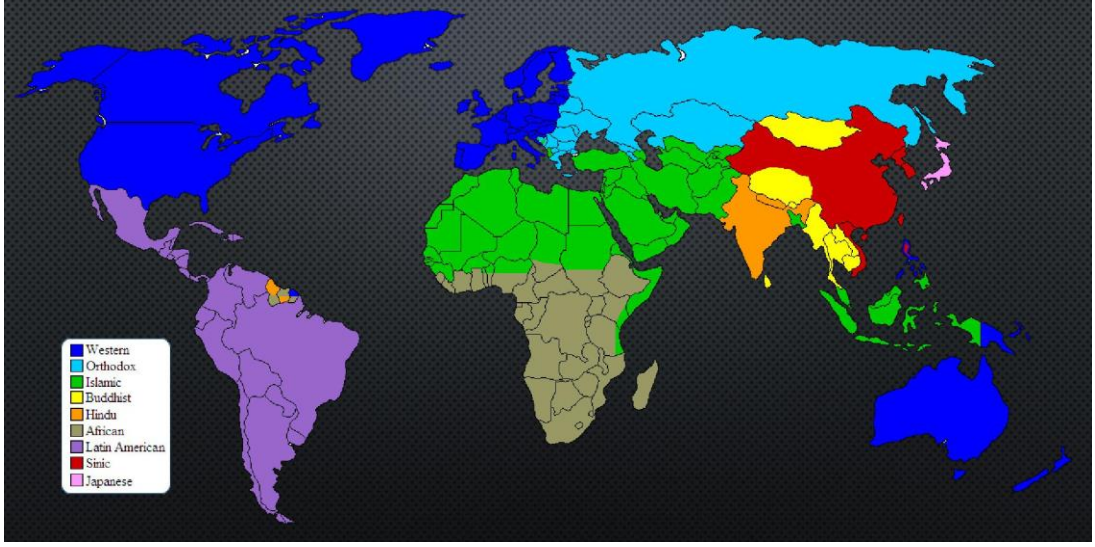


KÉT VILÁG (1945) ÉS A HIDEGHÁBORÚ

- EURÓPA FELOSZTÁSA TÖBB SZINTEN
  - POLITIKAI ÉRTELEMBEN: JALTA (1945)
  - GAZDASÁGILAG: MARSHALL-TERV(1947) – KGST (1949)
  - KATONAI: NATO (1949) – VARSÓI SZERZŐDÉS(1955)
  - „INTELLEKTUÁLIS": 1945 -

Map showing the way Europe was divided into rival alliances during the Cold War

HUNTINGTON ELMÉLETI MEGKÖZELÍTÉSE



AZ EURÓPAI UNIÓ EMLÉKEZETPOLITIKÁJA (2015)

- **MARKUS J. PRUTSCH**: EUROPEAN HISTORICAL MEMORY: POLICIES, CHALLENGES AND PERSPECTIVES (BRUSSELS, 2015)
- NÁCIZMUS ÉS A SZTÁLINISTA TERROR CSELEKEDETEIT EGY SZINTRE (EQUAL LEVEL) KELL HOZNI
- TRANSZEURÓPAI KONTEXTUSBAN ÉRTELMEZETT TÖRTÉNELEM ÉS TAPASZTALATOK ÖSSZESSÉGE
- „EURÓPAI ÖRÖKSÉG" ALAPJA – KÉT HÁBORÚ A 20. SZÁZADBAN ÉS AZOK KÖVETKEZMÉNYEI
- ÖRÖKSÉGVÉDELEM ÉS FENNTARTÁS A FELADAT

AZ OROSZ ÁLLAM EMLÉKEZETPOLITIKÁJA

- VLADIMIR PUTYIN NYILATKOZATA A 2. VILÁGHÁBORÚ TAPASZTALATAIRÓL
  - A 21. SZÁZADI EURÓPAI ÁLLAMOK ELFELEJTETTÉK MÜNCHEN TAPASZTALATAIT (1938)
  - A NÉPSZÖVETSÉG NEM TETTE A DOLGÁT
  - LENGYEL- ÉS NYUGATELLENES MEGFOGALMAZÁSOK
  - HIVATKOZIK AZ EURÓPAI PARLAMENT EGYIK DOKUMENTUMÁRA, MELY SZTÁLINT FELELŐSSÉ TESZI A HÁBORÚ KIROBBANTÁSÁRA – PUTYIN EZT VITATJA

ÖSSZEFOGLALÁS

- AZ EMLÉKEZETPOLITIKA A 21. SZÁZADBAN ÚJ ERŐRE KAPOTT, MINT „SOFT POWER"
- AZ EGYÉNI ÉS KÖZÖSSÉGI EMLÉKEZET HATÁSSAL VAN A STABILITÁSRA
- HUNTINGTON ÓTA TUDJUK, HOGY A CIVILIZÁCIÓS HATÁROKON AZ EMLÉKEZET FONTOS TÉNYEZŐ LEHET
- AZ „EURÓPA-PROJEKT" RÉSZTVEVŐI KÖZÖS EMLÉKEZETPOLITIKÁT KÍVÁNTAK ÉPÍTENI, HOGY EZZEL ERŐSÍTHESSÉK A KOHÉZIÓT
- OROSZORSZÁGBAN VLADIMIR PUTYIN A MÁSODIK VILÁGHÁBORÚ EMLÉKEZETÉT A KÜLPOLITIKÁJÁNAK MEGHATÁROZÓ ELEMÉVÉ TETTE


KÖSZÖNÖM A MEGTISZTELŐ FIGYELMET!
EU 2016
IS
STEFAN MARES

Dr. Magyar Sándor: Az elektronikus információs rendszerek (EIR) fejlődése a kibertérben

Korreferátum

Napjainkban egyre intenzívebben növekszik a függőség az elektronikus információs rendszerektől (a továbbiakban: EIR). Az EIR-ek tekintetében a rendszerszemléletű gondolkodás, a technikai eszközök biztosítása, a képzett személyzet megléte ugyanolyan hangsúlyos, egyiket sem célszerű alul pozícionálni.

A kibertér már a legmagasabb szintű szabályozói körben jelen van Magyarországon. A stratégiák rámutatnak az információtechnológia rohamos fejlődésére, a fenyegetések növekvő számának és hatásának kockázataira is.

Az EIR-ek fejlesztése során különösen nagy figyelmet kell fordítani a feltörekvő és felforgató technológiák területére. Ezen területre vonatkozó kutatási irányoknak folyamatosan meg kell jelenniük a nemzetközi trendek aktuális fejlesztési irányaiban. Ezen belül kiemelésre került a mesterséges intelligencia és a kvantumszámítástechnika területe is. Példaként került említésre, hogy amennyiben a kvantumszámítástechnika elérhetővé válik, a jelentősen megnövekedett számítási kapacitás miatt a jelenlegi aszimmetrikus kulcsú titkosítással rendelkező rendszerek (VPN-ek, webszerverek – böngészők közötti kommunikációk, kriptovaluták stb.) már nem lesznek megfelelően védettek.

Az átfogó stratégiai gondolkodásra is szükség van a rendszerek teljes életciklusa során. A kutatás-fejlesztés esetében továbbra is szükséges a megfelelő kapacitások folyamatos biztosítása.

Az elektronikus rendszerek szerepkörei tekintetében a feladatok elhatárolása kiemelt, ha bármely terület (üzemeltető, fejlesztő, eseménykezelő, sérülékenység vizsgáló, hatósági személy stb.) nem kapja meg a megfelelő támogatottságot, akkor az negatív hatással lehet a többi érintett számára is.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Az elektronikus információs rendszerek (EIR) fejlődése a kibertérben

Magyar Sándor ezredes (PhD), egyetemi adjunktus

A kibertér már mindenütt, még a legmagasabb szintű szabályzókban is Magyarországon

- *1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról*
- *1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról*
- *1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról*
- *2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről*
- *…*

A kibertér is fejlődik, folyamatosan változik

- *Intenzív növekedés.*
- *Nagyfokú függőség.*
- *Ellenálló képesség.*
- *Hálózatelmélet.*
- Felforgató technológiák.
- *Előre menekülés a technológiák területén.*

Fejlődés irányainak lefedése nem kerülhető ki.

- 5G Koalíció
- Mesterséges Intelligencia Koalíció
- Drón Koalíció
- Kvantuminformatika Nemzeti Laboratórium
- Autonóm Rendszerek Nemzeti Laboratórium
- Biztonsági Technológiák Nemzeti Laboratórium
- Infokommunikációs és Információtechnológiai Nemzeti Laboratórium
- …

Átfogó módon kell gondolkodni

- Látni kell a fejlődést fő irányait.
- Meg kell érteni az információs technológia fejlődésének hatását.
- Követés vagy lemaradás.
- Kutatás, fejlesztés, innováció.
- Nem csak a technológián van hangsúly, hanem a humán faktoron is.

Költségvetés oldalán is biztosított a fejlődés a szervezetekben?

- Az egyszeri beruházásoknál is ~20% évenkénti követési költség tervezése a következő évtől:
  - hardver amortizációra;
  - szoftver követésre;
  - képzésre.
- **Döntési pont** a költségcsökkentés és a képességvesztés mérlegelése.

Rendszerszemléletű gondolkodás

Szükséges technikai eszközök biztosítása (HW, SW).
Képzett személyzet.
Rendelkezésre álló idő.
…
…
…
PreDeCo.

Feladatok elhatárolása

- Különböző:
  - szerepkörök;
  - gondolkodás;
  - megértettség, érdekérvényesítés.

Felhasznált irodalom

- Kovács László: Kiberbiztonság és -stratégia. Dialóg Campus, Budapest, 2018.
- Szendy István: A katonai stratégia. Hadtudomány, 2019/1–2., 18–34.
- Maggie Gray, Amy Ertan Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment NATO CCDCOE
- Sarandis Mitropoulos, Christos Douligeris Why and how informatics and applied computing can still create structural changes and competitive advantage.
- 1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján) A hálózati és információs rendszerek biztonságára vonatkozó Stratégia
- 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról
- 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról
- 1456/2021. (VII. 13.) Korm. határozat Magyarország kutatási, fejlesztési és innovációs stratégiájának (2021–2030) elfogadásáról.
- Babics Emil, Farkas Lóránt, Imre Sándor, Kovács Benedek, Németh Edina, Szabó Áron, Kvantumkommunikáció 2030 kerekasztal beszélgetés, INFOKOM 2021 konferencia.

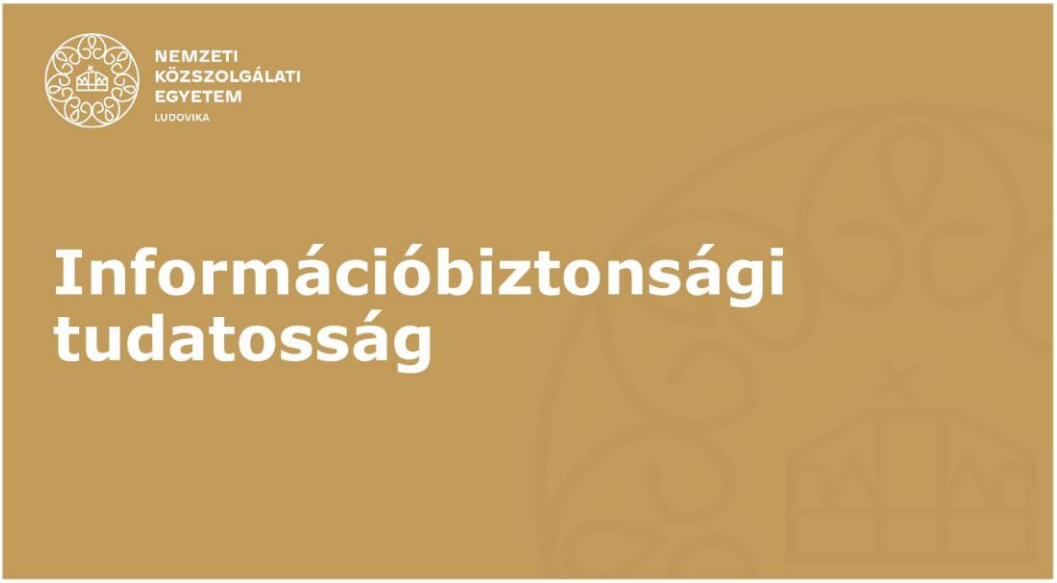
NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA

Köszönöm szépen a figyelmet!

Dr. Kerti András: Információbiztonsági tudatosság

Korreferátum

Közhely, de igaz egy információs rendszerben leggyengébb láncszem az ember. Ha eltekintünk a rosszindulatú károkozásoktól, a legtöbb problémát a rendszerek, a rendszerekben meglévő kockázatok ismeretének a hiánya okozza. Ez a tudatlanság nem feltétlenül a képzettség hiányából adódnak, sokkal inkább a gyors változás következtében az ismeretek elavulásából. Egy szervezet számára alapvető érdek, hogy az információs rendszereit biztonságosan üzemeltesse, és ehhez a munkatársai tudását naprakészen tartsa. Természetesen a különböző szerepkörű munkavállalók számára más és más képzés szükséges. Akkor járunk el hatékonyan, ha ezeket a képzéseket, tudatosításokat nem ad-hoc, hanem az információbiztonsági irányítási rendszerben, egy információbiztonsági tudatosítási tervben rögzítjük. Hogyan célszerű megtervezni, megszervezni ezt az információbiztonsági tudatosítási tervet, erről szól az előadásom.



Tudatosság- tudatosítás

- Tudatosság- tudatosítás
- A tudatosítás nem képzés. A tudatosságot bemutató előadások célja egyszerűen a biztonságra való figyelem összpontosítása. A figyelemfelkeltő előadások célja, hogy az egyének felismerjék az informatikai biztonsággal kapcsolatos aggályokat és ennek megfelelően reagáljanak. (Tacepaok)

Tudatosság

- A szervezet felügyelete alatt munkát végző személyeknek tudatában kell lenniük a következőknek:
  - a) az információbiztonsági politika;
  - b) hozzájárulásuk az információbiztonság-irányítási rendszer eredményességéhez, beleértve az információbiztonsági teljesítmény növekedésének előnyeit; és
  - c) az információbiztonság-irányítási rendszer követelményeinek való meg nem felelés következményei.

  MSZ ISO/IEC 27001 7.3

Képzés, oktatás

- A képzés arra törekszik, hogy releváns és szükséges biztonsági készségeket és kompetenciákat nyerjen.
- Az oktatás integrálja a különféle funkcionális specialitások összes biztonsági készségét és kompetenciáját egy közös tudásanyagba. . .

A tudatossági és képzési program kialakítása

- Három általános megközelítést:
  - Központosított stratégia és végrehajtás;
  - Központosított stratégia, elosztott megvalósítás;
  - Elosztott stratégia és megvalósítás.
- A tudatosság és a képzési program tevékenységének felügyeletére átfogott és létrehozott modell a következőktől függ:
  - A szervezet mérete és földrajzi eloszlása;
  - Meghatározott szervezeti szerepek és felelősségek; és
  - Költségvetési előirányzatok és hatóság.

Az információbiztonsági tudatosság kialakításának folyamata

- Tervezés megkezdése előtt:
  - Szerepek és felelősségek kiosztása
- Stratégia kialakítása
- Tervek kialakítása
- Oktatások, képzések gyakorlások végrehajtása
- A tudatosság monitorozása
- Stratégia és a tervek pontosítása

Tudatossági stratégia

- Célja: rögzíteni
  - Kinek (célcsoport)
  - Milyen gyakran (ismétlődés)
  - Milyen témában, témakörben
  - Milyen formában

Oktatunk, tartunk képzést

- Formája, írott vagy mátrix
- Tartalmaz(hatj)a: az éves oktatásra szánt költséget is.

Minta egy képzési mátrixra

IT Security Training Matrix - *System Administrator*

Training Areas	Functional Specialities						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulations				1D ✓			
2. Security Program							
2.1. Planning							
2.2. Management				2.2D ✓			
3. System Life Cycle Security							
3.1 Initiation				3.2D ✓			
3.2. Development				3.3D ✓			
3.3. Test and Evaluation				3.4D ✓			
3.4. Implementation			3.4C ✓	3.4D ✓			
3.5. Operations	3.5A ✓		3.5C ✓	3.5D ✓			
3.6. Termination				3.6D ✓			
4. Other							

Tudatossági terv

- Célja: a stratégia alapján aktuálissá vált információbiztonsági tudatosítási folyamatok végrehajtása
- Tartalma lehet:
  - Ki
  - Mikor, (idő és időtartam)
  - Kinek, kiknek,
  - Milyen formában
  - Miről tart képzést
  - A szükséges erőforrások
- Jóváhagyás?

Tervezés folyamata

- Szükségletfelmérés elvégzése
  - A speciális képzési igények szempontjából legalább a következő szerepekkel kell foglalkozni:
    - Ügyvezetés
    - Biztonsági személyzet
    - Rendszertulajdonosok, rendszergazdák és informatikai támogató személyzet
    - Felhasználók

Tervezés folyamata
A „mércék kitűzése”

- A bonyolultságnak arányosnak kell lennie annak a személynek a szerepével, aki részt vesz a tanulási erőfeszítésekben. Az anyagot két fontos kritérium alapján kell kidolgozni:
  - a célszemély szervezeten belüli pozíciója és
  - az adott pozícióhoz szükséges biztonsági készségek ismerete.

Tervezés folyamata
Tudatossági témák kiválasztása

- Jelentős számú témát lehet megemlíteni és röviden megvitatni bármely képzési formában
- A témák a következők lehetnek:
  - Jelszó használata és kezelése
  - Vírusok, férgek, trójai falovak és más rosszindulatú kódok elleni védelem
  - Információbiztonsági politika - a meg nem felelés következményei
  - Ismeretlen e-mail / mellékletek

Tervezés folyamata
Tudatossági témák kiválasztása 2

- A témák a következők lehetnek:
  - Webhasználat
  - a felhasználói tevékenység figyelemmel kísérése
  - Spam
  - Adatok biztonsági mentése és tárolása
  - Incidens kezelés
  - Vállszörfözés
  - Változások a rendszer környezetében - növekszik a rendszerek és az adatok kockázata

Tervezés folyamata
Tudatossági témák kiválasztása 3

- A témák a következők lehetnek:
  - Készlet- és vagyonátadás (pl. A média fertőtlenítése)
  - Személyes használat
  - Hordozható eszközök biztonsági problémái
  - „Bizalmas” információk továbbítása az interneten
  - Laptop biztonság utazás közben
  - Támogatott / engedélyezett szoftverek a szervezeti rendszereken - a konfigurációkezelés része
  - Belépés-ellenőrzési kérdések

Tervezés folyamata
Tudatossági témák kiválasztása 4

- A témák a következők lehetnek:
  - Egyéni elszámoltathatóság
  - Látogatók ellenőrzése
  - A titoktartási aggályoktól függő információk védelme - rendszerekben, archiválva, biztonsági másolaton, nyomtatott formában és megsemmisítésig
  - E-mail kezelés- csatolt fájlok és egyéb szabályok.

Tervezés folyamata
A képzés formája

- Előadás
- Gyakorlás
- Oktató film
- Tanfolyam
- Csapatmunka
- Csapatépítés
- Agymenés ☺

A tervezés folyamata
A „tananyag” forrása

- Tanulmányok, tankönyvek
- Tanácsadó cégek
- Internetes és online újságok
- Konferenciák
- Saját incidensek! (GDPR)
- Fontos kérdés: Ki tartja a képzést

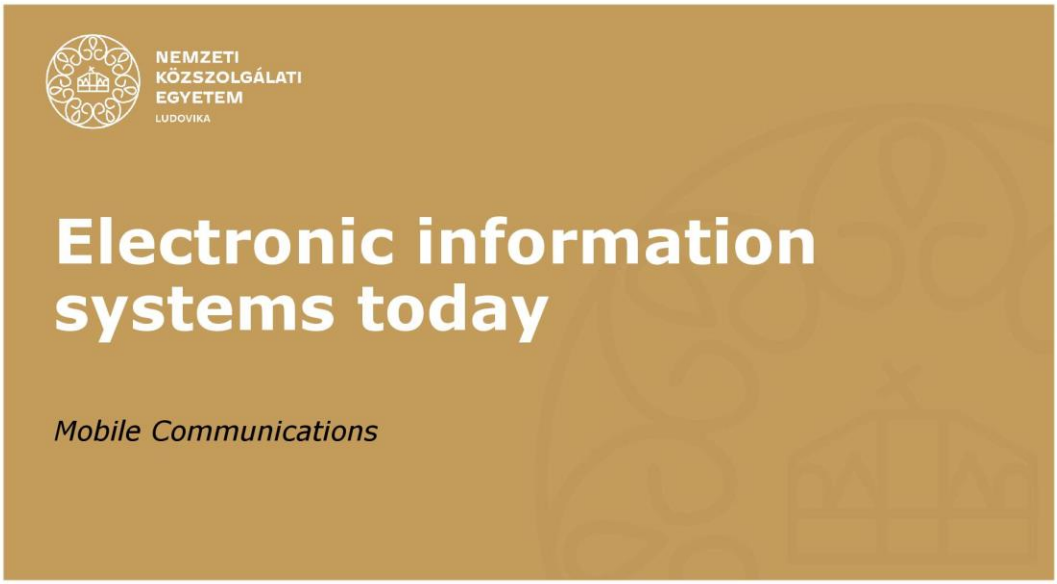
KÖSZÖNÖM A FIGYELMET!

uni-nke.hu

Dr. Farkas Tibor: Electronic information systems today: mobile communications

Korreferátum

The evolution of mobile telecommunications systems is unstoppable. The desire for wireless freedom continues unabated, and there is a need for wireless telecommunications to be able to handle the high volumes of data traffic. This high data traffic is coming from both residential and industrial users, and 5G technology can provide the answer. Several European countries are committed to digitalization and are therefore using all possible means to support and promote the development of a digital society and economy. Governments see 5G as an opportunity that has become a key economic and social issue. This presentation summarizes the general mobile telecommunications needs.

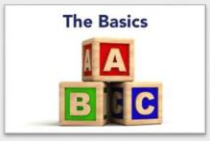


MAJ Tibor FARKAS
associate professor

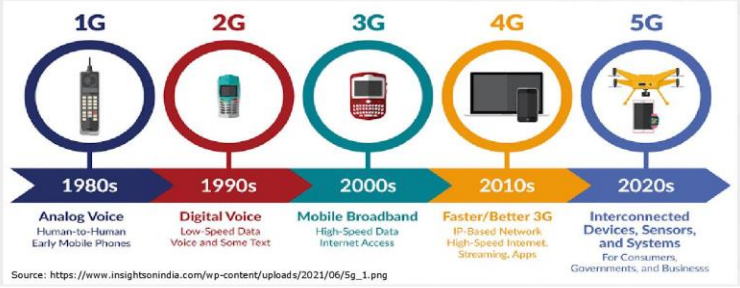
Ludovika-UPS
Faculty of Military Sciences and Officer Training
CIS Department

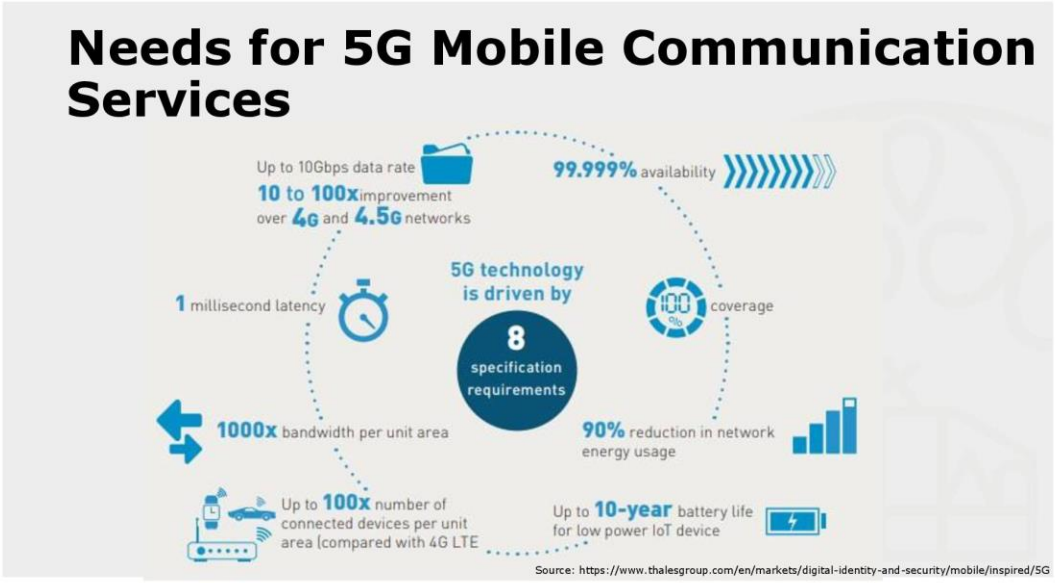
farkas.tibor@uni-nke.hu
+36-1/432-9000 (29-289)

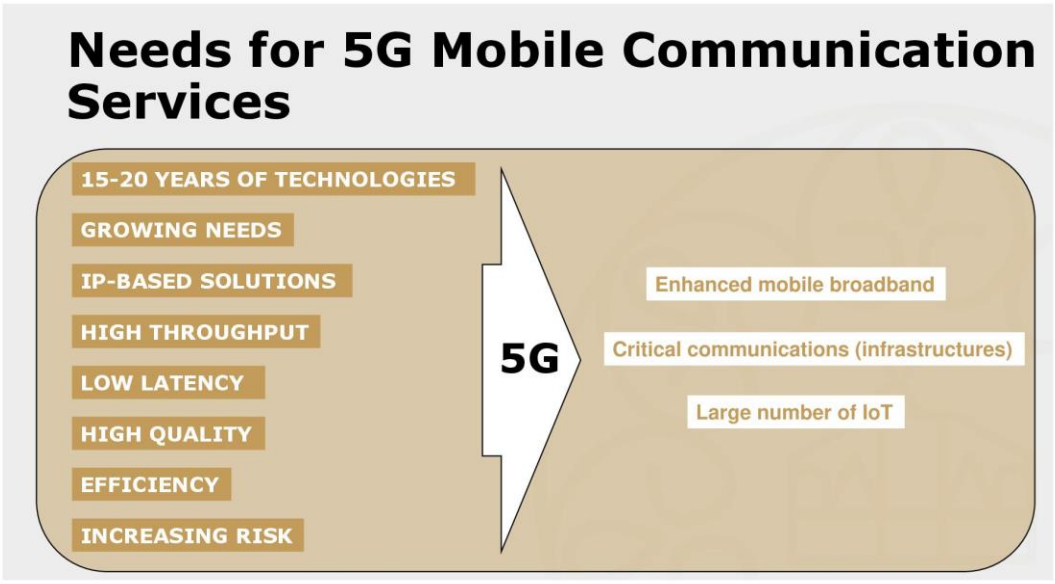
Mobile communication



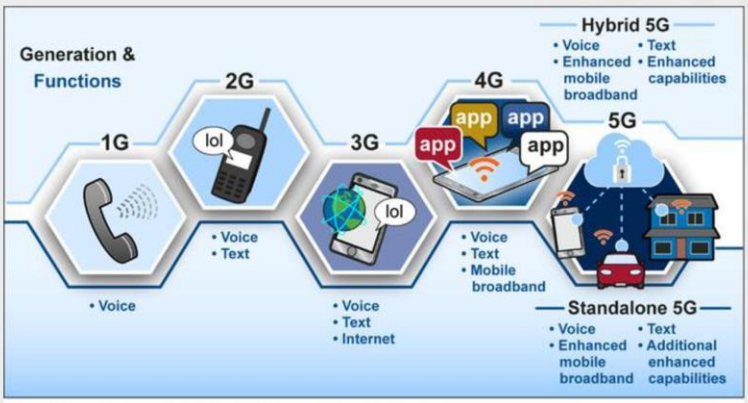
Basically, the mobile communication is the exchange of voice and data using a communication facility at the same time without any physical link.




Needs for 5G Mobile Communication Services
Up to 10Gbps data rate
10 to 100x improvement over 4G and 4.5G networks
99.999% availability
1 millisecond latency
5G technology is driven by
8 specification requirements
coverage
1000x bandwidth per unit area
90% reduction in network energy usage
Up to 100x number of connected devices per unit area (compared with 4G LTE
Up to 10-year battery life for low power IoT device
Source: https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G


Needs for 5G Mobile Communication Services
15-20 YEARS OF TECHNOLOGIES
GROWING NEEDS
IP-BASED SOLUTIONS
HIGH THROUGHPUT
LOW LATENCY
HIGH QUALITY
EFFICIENCY
INCREASING RISK
5G
Enhanced mobile broadband
Critical communications (infrastructures)
Large number of IoT

For what!



Threats/Security

- end-user tools threats
  - Laptop, **smartphone**
- threats to operating systems
- datas on smartphones
- continuous threat
  - Phcsical
  - General Cyber Security
  - Network and wi-fi
  - Application

Solutions for Security

- Primary authentication
- Credential Storage
- Secondary authentication
- Inter-operator Security
- Privacy
- Service based auth.
- CU-DU interface
- Key hierarchy
- Mobility

operating systems
central network and service infrastructure
human side by user and operator

Conclusion

- End-user equipments
- Operation Sytem
- Applications
- Firmware/Hardware
- End-user
- ISP
- MDM/UEM
- Security requirements


TIME FOR QUESTIONS
12
1
2
3
4

Dr. László Gábor: Infodémia

Korreferátum

A 2020 tavaszán kitört COVID-19 világjárvány az érdeklődés középpontjába emelete az internetes tevékenységek hatásait, kockázatait is. A pandémia kezelésében kiemelt figyelmet kell kapnia a hiteles, gyors, pontos információszolgáltatásnak. A digitális és a fizikai környezetben azonban a túl sok, vagy éppen a hamis, félrevezető információk miatt a pandémiával kapcsolatos információáramlás is sok esetben „fertőzött". Az internet, a közösségi média segít betölteni az információs űrt, de fel is erősíti az információs túlterheltséget, valamint a káros üzenetek hatását. A közösségi médiának köszönhetően az információk, köztük a dezinformációk vagy az álhírek is gyorsan terjednek. Az előadás bemutatja az infodémia jelenségével kapcsolatos fogalmi keretrendszert, hatásokat, valamint az információkezelés és a tudásgazdálkodás területén felmerült biztonsági kihívásokat, kockázatokat.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Infodémia

Dr. László Gábor

Új típusú kihívások a biztonságban
Budapest, 2022. január 21.

Információs túlterheltség

Andrea Piacquadio fotója a Pexels oldaláról

Infoxication

Az internet fejlődésével kapcsolatos jelenség, amely arra utal, hogy a világhálón található végtelen mennyiségű adat és tartalom miatt nehéz vagy lehetetlen döntést hozni vagy tájékozódni egy adott témában.

→ Információs túlterheltség

Forrás: https://www.zorraquino.com/en/dictionary/internet/what-is-infoxication.html

Infodémia

Forrás: WHO/Sam Bradd, https://www.who.int/health-topics/infodemic

Álhírek a mainstream médiában

S. Hermann & F. Richter képe a Pixabay -en.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu

Dr. Bányász Péter: A COVID-al kapcsolatos érzelmek vizsgálata Magyarországon

Korreferátum

A 2019. év végén megjelent új típusú koronavírus számost szempontból állította kihívások elé a társadalmakat és a kormányzatokat. Az előadó úgy véli, az egyik legnagyobb fenyegetést az álhírek jelentik, amelyek a koronavírussal kapcsolatban új szintre léptek. Ennek oka, hogy az áltudományos hírek egyre nagyobb mértékű elfogadottsága nem csupán a sikeres járványkezelést akadályozzák, de hosszú távon a demokratikus intézményekbe vetett közbizalom erodálásával a nyugati típusú demokráciák súlyos válságához vezethetnek. Előadásomban a koronavírus oltásokkal kapcsolatos érzelmeket vizsgálom magyar internetezők körében 2020. január 1. és 2021. november 25. közötti intervallumban két aspektusból: (1) általánosságban az oltással kapcsolatos attitűdöt, (2) a COVID-al kapcsolatos álhírek megítélését.


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL
Új Nemzeti Kiválóság Program
INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM
A COVID-al kapcsolatos érzelmek vizsgálata Magyarországon
Új típusú kihívások a biztonságban konferencia
2022. január 21.
Dr. Bányász Péter
Az Innovációs és Technológiai Minisztérium ÚNKP-21-2-II-NKE-142 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült.


Nem is oly' rég...
Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine
Fazze offered money to YouTubers and bloggers to falsely claim jab was responsible for hundreds of deaths
NEWS
Biden orders spy agencies to review whether COVID-19 came from Wuhan lab
By Steven Nelson
May 26, 2021 | 1:54pm | Updated

Nem is oly' rég...

Módszertan

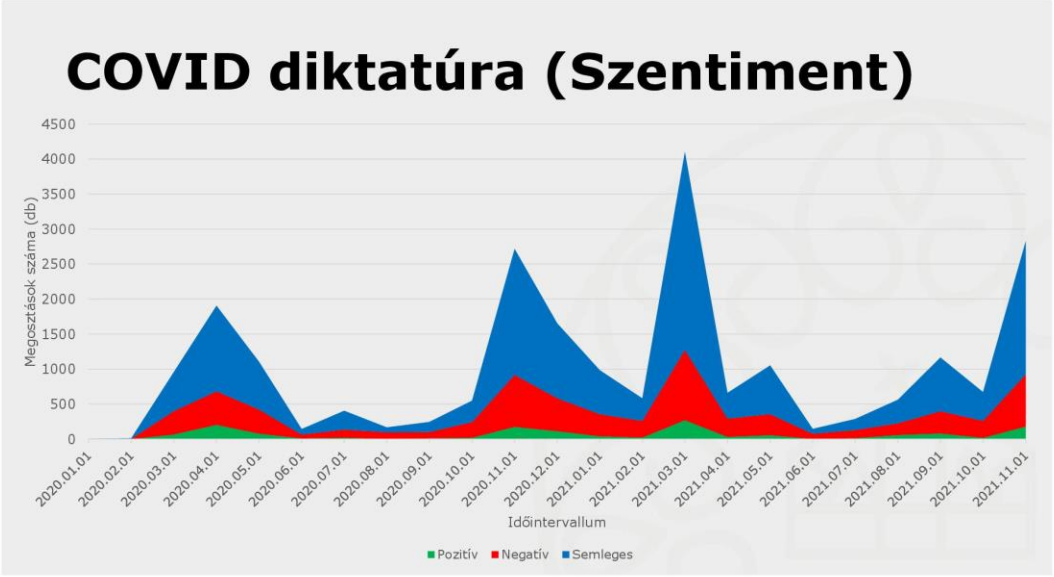
- Kulcsszó- és szentiment analízis („semleges")
- 2020. január 1.-2021. november 25.
- Magyar nyelven különböző kulcsszavak
- OSINT és ennek módszertani korlátai
- Megosztás vs elérés

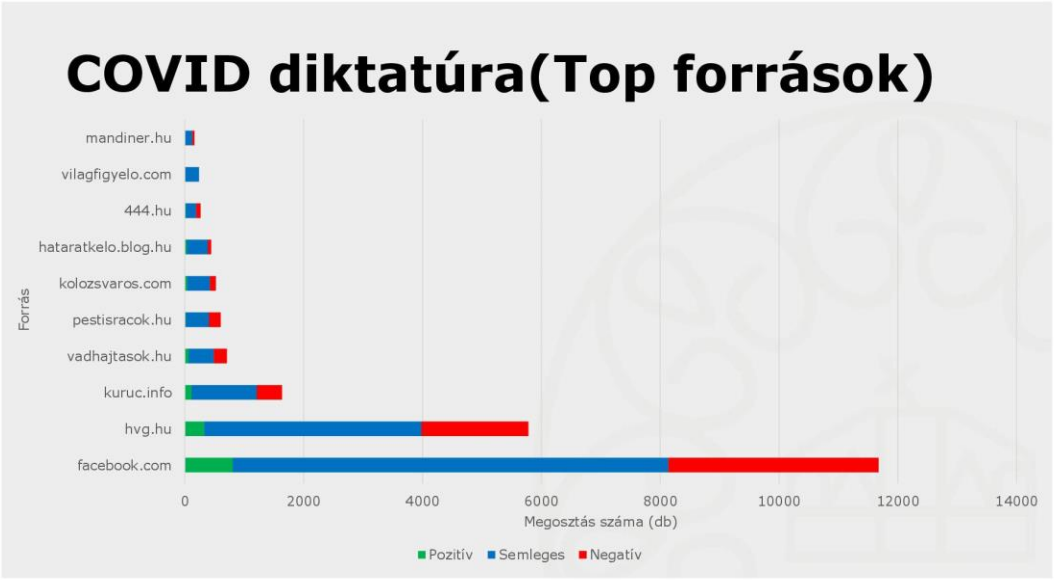
Néhány álhír téma

	Megosztás (darab)			
	Összes	Elérés	Pozitív	Negatív
COVID és biológiai fegyver	4 017	~3 millió	191	530
COVID és 5G	23 112	~25 millió	1 290	3 374
COVID és chip	4 171	~6 millió	417	702
COVID és Bill Gates	28 006	~35 millió	1 655	4 460

Néhány oltással kapcsolatos téma

	Megosztás (darab)			
	Összes	Elérés	Pozitív	Negatív
COVID és oltás	535 490	~2,7 milliárd	30 249	83 944
COVID és kötelező oltás	18 518	~34 millió	965	2 886
COVID és vakcina	542 730	~3,5 milliárd	32 446	83 153
COVID és diktatúra	24 247	~53 millió	1 454	6 746


COVID diktatúra (Szentiment)
Megosztások száma (db)
4500
4000
3500
3000
2500
2000
1500
1000
500
0
2020.01.01
2020.02.01
2020.03.01
2020.04.01
2020.05.01
2020.06.01
2020.07.01
2020.08.01
2020.09.01
2020.10.01
2020.11.01
2020.12.01
2021.01.01
2021.02.01
2021.03.01
2021.04.01
2021.05.01
2021.06.01
2021.07.01
2021.08.01
2021.09.01
2021.10.01
2021.11.01
Időintervallum
Pozitív
Negatív
Semleges


COVID diktatúra(Top források)
Forrás
mandiner.hu
vilagfigyelo.com
444.hu
hataratkelo.blog.hu
kolozsvaros.com
pestisracok.hu
vadhajtasok.hu
kuruc.info
hvg.hu
facebook.com
0
2000
4000
6000
8000
10000
12000
14000
Megosztás száma (db)
Pozitív
Semleges
Negatív

COVID diktatúra(Top források)

- Top forrás: Facebook, összesen 11 673 említés
- A témában a leggyakrabban posztoló top 30 szerző közül 27-en Facebookon a legaktívabbak.
- A Facebookos oldalak impaktját sokféleképpen vizsgálhatjuk:
  - bejegyzésre érkezett likeok száma (ez esetben Dúró Dóra a top influencer 9 555 like-al, amit 13, a témában írt bejegyzésére kapott),
  - egy másik szempont lehet a bejegyzés tovább osztásának a száma (ez esetben a Hihetetlen Magazin, aminek a témában írt 71 bejegyzését összesen 4 254 alkalommal osztották tovább).

Felhasznált irodalom

- Bíró-Nagy, A. – Szászi, Á. (2021): *Lélekben a járványon túl – A magyar társadalom a koronavírus-járvány negyedik hullámában*. Budapest: Friedrich-Ebert-Stiftung – Policy Solutions
- Crawford, J. R. – Henry, J. D. (2004): The Positive and Negative Affect Schedule (PANAS): Construct Validity, Measurement Properties and Normative Data in a Large Non-Clinical Sample. *The British Journal of Clinical Psychology*, 43, 3, 245–65, https://doi.org/10.1348/0144665031752934
- Hua, J. – Shaw, R. (2020): Corona Virus (COVID-19) "Infodemic" and Emerging Issues through a Data Lens: The Case of China. *International Journal of Environmental Research and Public Health,* 17, 7, 2309, https://doi.org/10.3390/ijerph17072309
- Romer, D. – Jamieson, K. L. (2021): Patterns of Media Use, Strength of Belief in COVID-19 Conspiracy Theories, and the Prevention of COVID-19 From March to July 2020 in the United States: Survey Study. *Journal of Medical Internet Research,* 23, 4, e25215, https://doi.org/10.2196/25215.
- Ullah, I. - Khan, K. S. - Tahir, M. J. - Ahmed, A. – Harapan, H. (2021): „Myths and Conspiracy Theories on Vaccines and COVID-19: Potential Effect on Global Vaccine Refusals. *Vacunas,* 22, 2, 93–97, https://doi.org/10.1016/j.vacun.2021.01.001

Felhasznált irodalom

- HVG. „Tech: Nem létező svájci tudóst idézett a kínai média a koronavírus eredetvitájáról" Utolsó hozzáférés 2021. augusztus 31. https://hvg.hu/tudomany/20210811_Svajc_Kina_covid_fake_news.
- Henley, Jon. „Influencers Say Russia-Linked PR Agency Asked Them to Disparage Pfizer Vaccine". Utolsó hozzáférés: 2021. augusztus 20. http://www.theguardian.com/media/2021/may/25/influencers-say-russia-linked-pr-agency-asked-them-to-disparage-pfizer-vaccine.
- Klepper, David. „Facebook Bans Firm behind Pfizer, AstraZeneca Smear Campaign". Utolsó hozzáférés: 2021. augusztus 20. https://apnews.com/article/technology-europe-business-health-coronavirus-pandemic-2f2fe7911b4657ede152d5c21531d6b0.
- Kovács László és Krasznay Csaba. „»Mert övék a hatalom«: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során". *Nemzet és Biztonság* 10. 3. szám, (2017) 3–15.
- Koronavírus tájékoztató oldal. „Magyarországra érkezett vakcinák típusa és mennyisége". Utolsó hozzáférés: 2021. augusztus 17. https://koronavirus.gov.hu/cikkek/magyarorszagra-erkezett-vakcinak-tipusa-es-mennyisege-8.
- Marton Péter. *Covid-19 - Az egészségtelen politikák ragálya*. Budapest: Noran Libro Kft. 2019.
- Mathieu, Edouard, Hannah Ritchie, Esteban Ortiz-Ospina, Max Roser, Joe Hasell, Cameron Appel, Charlie Giattino és Lucas Rodés-Guirao. „A Global Database of COVID-19 Vaccinations". *Nature Human Behaviour* 5. no 7. (2021) 947–53. https://doi.org/10.1038/s41562-021-01122-8.
- Reichert, Corinne. „5G Coronavirus Conspiracy Theory Leads to 77 Mobile Towers Burned in UK, Report Says". Utolsó hozzáférés 2021. augusztus 11. https://www.cnet.com/health/5g-coronavirus-conspiracy-theory-sees-77-mobile-towers-burned-report-says/.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

Új Nemzeti Kiválóság Program

INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM

Köszönjük a megtisztelő figyelmet!

KÉRDÉS?

Dr. Bányász Péter
banyasz.peter@uni-nke.hu

Szűcs Attila: Biztonsági kihívások a mesterséges intelligencia katonai alkalmazásában

Korreferátum

A Mesterséges Intelligencia (MI) alkalmazásának a döntéselőkészítésben, akár vállalati, akár katonai döntéshozatali mechanizmusban, megvannak a maga biztonsági kockázatai.

A MI sokkal nagyobb adatbázisokban dolgozik (Big Data), mint amit egy ember átlátni képes. Ha abban előfordul hibás, vagy szándékos dezinformálási céllal torzított adat, akkor az a feldolgozás során, ha azt csak az MI végzi, szinte kiszűrhetetlen.

A másik igen fontos tényező az idő. A MI sokkal gyorsabban végez el elemzéseket, döntési folyamatokat, mint az ember. A döntési helyzetben lévő számára ez követhetetlen. Egy katonai vezető számára a szembenálló fél fölött fölényt jelentheti az időtényező. A felkínált lehetőség elfogadása szinte automatikusnak tekinthető. Ez egyszersmind a felelősség relativizálását is jelenti, hiszen csak követnünk kell a MI által javasoltakat.

Kulcstényező lehet, hogy a már meglévő alkalmazásokat mennyire fenttartások nélkül veszi át a katonai döntéshozatal. Így a korábban elkészített alkalmazásokban rejlő esetleges hibákat is átvesszük. Olyanokat, melyek esetleg az eredeti alkotó, alkalmazó esetén nem kerültek napvilágra.

Az általános kihívásokról

- A MI sokkal nagyobb adatbázisokban dolgozik (Big Data), mint amit egy ember átlátni képes. Így ha abba előfordul hibás adat, vagy szándékosan torzítottadat, akkor az a feldolgozás során nehezen szűrhető.
- A MI sokkal gyorsabban futtat le egy művelet sort, mint azt egy operátor akárcsak értelmezni tudná. A folyamat részlépéseit nem tudja és nem is feladata lekövetni.
- A program modulok felhasználása már korábban is felvetette azt a kérdést, hogy aki a saját programjába beemel egy korábban más által létrehozott elemet, az az abban rejlő esetleges hibát ill. rejtett kódot is beépíti.

Általános következtetés

- A sebesség és összetettség eredményeképpen ha azt is mondjuk, hogy a MI csupán a döntéselőkészítésben játszik szerepet, valójában ezt az „előkészített döntést” akár véglegesnek is tekinthetjük. A többi önmegnyugtatás.

Kihívások a katonai döntéshozatalban

- Az idő szorításában.
  Vajon melyik lesz az a parancsnok, aki akárcsak megkérdőjelezi a MI által tett javaslatot?
- Bonyolultságban.
  Amikor ott villog a piros gomb, és a döntéshozónak fogalma sem lesz arról, hogy a mi alapján választott célpontot.
- Rendszerkommunikációban.
  A különböző MI alkalmazások kommunikálnak egymással anélkül, hogy ez az operátor előtt nyilvánvaló lenne, olyan sebességgel ami emberi léptékkel amúgy is követhetetlen. Ha kap is arról értesítést, hogy a döntési alternatíva felállítása során mely rendszerek vettek részt, az annak részleteit nem fogja tartalmazni.

Következtetés a katonai döntéshozatalban

- A reakcióidő a katonai döntéshozatalban kulcstényező. Akár a légvédelemben, akár az ellenséges haditechnikai eszközök detektálása és eliminálása során. Ezért valószínűtlen, hogy a MI által adott válasz helyett bárki mást választana.
- Az MI használata egyszersmind a felelőség kérdését is relatívizálja. Csak úgy mint az általános, a MI döntéshozatali előkészítést támogató funkciója során itt is elmondható Dr. Gerő Péter szavaival, hogy: aki a „Nagy szent és érthetetlen" szerint cselekszik azt aligha vonják felelőségre még ha hibázik is. Aki viszont ezt kétségbe vonva hibázik azt biztosan.

Köszönöm a figyelmet.

Kérdések?

Dr. Tóth András: Hálózatba kapcsolat harctéri eszközök (IoBT)

Korreferátum

A hálózatba kapcsolt eszközök egyre szélesebb körben elterjedése elérte a katonai műveleteket. A mindennapjainkban IoT-ként (Internet of Things) ismert eszközök komoly potenciált jelenethetnek egy-egy katonai műveletben, amennyiben azokat megfelelően használjuk fel. A polgári élettel ellentétben az itt használható eszközök köre lényegesen szűkebb, ám ezek a hálózatba kapcsolt harctéri eszközök nagymértékben megkönnyíthatik az információszerzést, ezzel hozzájárulva az információs fölény megszerzéséhez. A műveleti helyzetké közel valós idejű követésének lehetőségével a döntéshozatali folyamatok is lényegesen lecsökkenthetők.

Azonban komoly figyelmet kell fordítnunk a biztonság kérdésére ezeknek az eszközöknek alkalmazása során. A szerző által végzett kutatás ezekre a potenciális veszélyforrásokra fókuszál, alapvető célja volt meghatározni azokat a lehetéses támadsi vektorokat, amelyek az egyes alkalmazási rétegeket érintheti, továbbá azok hatását az adatok védelmére.


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
PUSKÁS TIVADAR
Hálózatba kapcsolat harctéri eszközök (IoBT)
Dr. Tóth András
Új típusú kihívások a biztonságban
2022. január 21.
„Az MTA Bolyai János Kutatási Ösztöndíj, valamint Innovációs és Technológiai Minisztérium ÚNKP-21-5-NKE-149 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült."


Tartalom
I Kutatási célok, kérdések, témaválasztás
II Módszertan
III Fogalmi meghatározások
IV Biztosági kihívások
V Következtetések

I. Kutatási célok, kérdések

RQ1 Hogyan valósítható meg a harctéri érzékelő- és fegyverrendszerek hálózatba kapcsolása?

RQ2 Milyen biztonsági kockázatokat jelent az IoBT alkalmazása?

II. Módszertan

- Releváns tudományos publikációk meghatározása hálózatelméleti módszerekkel, ezek összehasonlító elemzése;
- Releváns szakmai jelentések elemzése.

III./1 Fogalmi meghatározások

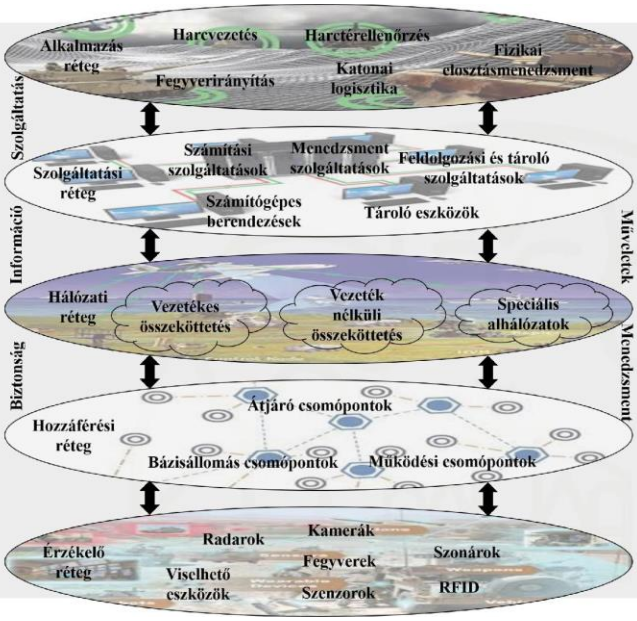
Internet of Things (IoT)

Olyan hálózatba kapcsolt eszközök, melyek egymással kétirányú kommunikációt folytatnak, és a működés közben keletkező adatokat, információkat képesek más berendezésekre eljuttatni, továbbá valamilyen technológia (adatbázisok, fájlmegosztás, felhőalapú rendszerek) segítségével megosztani.

Hálózatba kapcsolat harctéri eszközök (IoBT)

Olyan hálózatba kapcsolt harctéri eszközök, melyek egymással kétirányú kommunikációt folytatnak, és a működés közben keletkező harctéri adatokat, információkat, műveleti helyzetképet képesek más berendezésekre eljuttatni, továbbá valamilyen technológia (adatbázisok, fájlmegosztás, felhőalapú rendszerek) segítségével közel valós időben megosztani, a döntésmeghozatal támogatása érdekében.

III./2 Fogalmi meghatározások



IV/1. Biztonsági kihívások

Réteg	Lehetséges támadási vektor	Adatvédelmi aggályok
Alkalmazás / Szolgáltatási réteg	Rosszindulatú vírus / féreg / trójai faló, kémprogramok	- Ki fér hozzá az IoBT-eszközök és rendszerek által gyűjtött adatokhoz és információkhoz? - Hogyan használhatók fel a rendszerben tárolt és kezelt adatok?
	Rosszindulatú szkriptek	
	Szolgáltatásmegtagadás (DoS)	
	Szoftver sebezhetőségek	
	Kódbefecskendezés	
	Puffer túlcsordulás	
	Érzékeny adatokhoz való illetéktelen hozzáférés/manipulálás	
	Adatszivárgás	

IV/2. Biztonsági kihívások

Réteg	Lehetséges támadási vektor	Adatvédelmi aggályok
Hálózati réteg	DoS-támadások	- Biztonságos vagy nem biztonságos hálózatokon keresztül továbbítják az adatokat? - Megbízhatóak-e a vezeték nélküli hálózatok és a felhőszolgáltatások, mennyire könnyen válhatnak támadás célpontjává?
	Spoofing támadások	
	Csomagreplikációs támadások	
	Sinkhole-támadások	
	Routing információkkal kapcsolatos támadások	
	Féreglyuk-támadások	
	RFID jogosulatlan hozzáférés	
	Szimatolós támadások	
	Forgalomelemző támadások	

IV/3. Biztonsági kihívások

Réteg	Lehetséges támadási vektor	Adatvédelmi aggályok
Hozzáférési / Szenzor réteg	Csomópontok elfogása / manipulálása / fizikai sérülést okozó támadások	- Az eszközök a műveleteket nagymértékben befolyásoló érzékeny adatokat gyűjtenek és tárolnak, mint például a helymeghatározás, a mozgási útvonalak, az egészségi állapot.
	Fizikai támadások / szabotázs	
	DoS támadások	
	Csomópontok zavarása	
	Social Engineering	
	Rosszindulatú kódinjekciós támadások	
	Rosszindulatú csomópontok injektálása	
	Lehallgatás és interferencia	
	Rádiófrekvenciás interferencia az RFID-ken	

Következtetések

- A legjobb és leggyorsabb döntések meghozatala, valamint a valós idejű műveleti helyzetkép követése érdekében elengedhetetlen a harctéri érzékelő eszközök és rendszerek hálózatba kötése;
- A IoBT esetében ugyanazok a támadási vektorok jelennek meg, mint a normál IoT elemek esetében;
- Ennek megfelelően az alapvető védelmi megoldások is hasonlóak az okos városokban alkalmazott IoT eszközökéhez, rendszerekéhez.

Felhasznált irodalom

- Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018
- Burmaoglu S., Saritas O., Yalcin H. (2019) Defense 4.0: Internet of Things in Military. Science, Technology and Innovation Studies. Springer, Cham. https://doi.org/10.1007/978-3-030-04370-4_14
- Vulic, Ivan & Prodanovic, Radomir & Ivan, Tot & Dušan, Bogićević (2020). Model for authenticating the Internet of Military Things and Internet of Battlefield
- L. Mishra, Vikash and S. Varma (2020) Internet of Things for Military Applications, *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2020, pp. 118-123, doi: 10.23919/INDIACom49435.2020.9083730.
- Zhu, Lin & Majumdar, Suryadipta & Ekenna, Chinwe (2020) An invisible warfare with the internet of battlefield things: A literature review. Human Behavior and Emerging Technologies. 3. doi:10.1002/hbe2.231.
- Lori Cameron: Internet of Things Meets the Military and Battlefield, https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

KÖSZÖNÖM A FIGYELMET!

VÁROM A KÉRDÉSEIKET!

uni-nke.hu

Kirovné Dr. Rácz Réka: A szélsőséges időjárási események okozta károk társadalmi költsége

Korreferátum

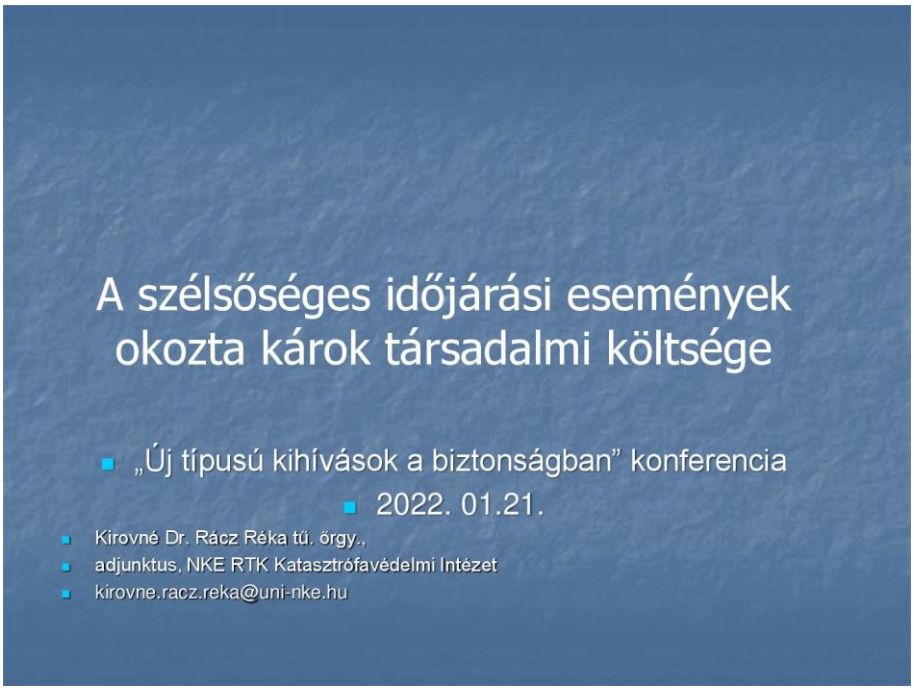
Az éghajlat változásának következményeként megjelenő szélsőséges időjárási események okozta károk, illetve azok felszámolásának költségei jelentős terhet rónak globális szinten a gazdaságra.

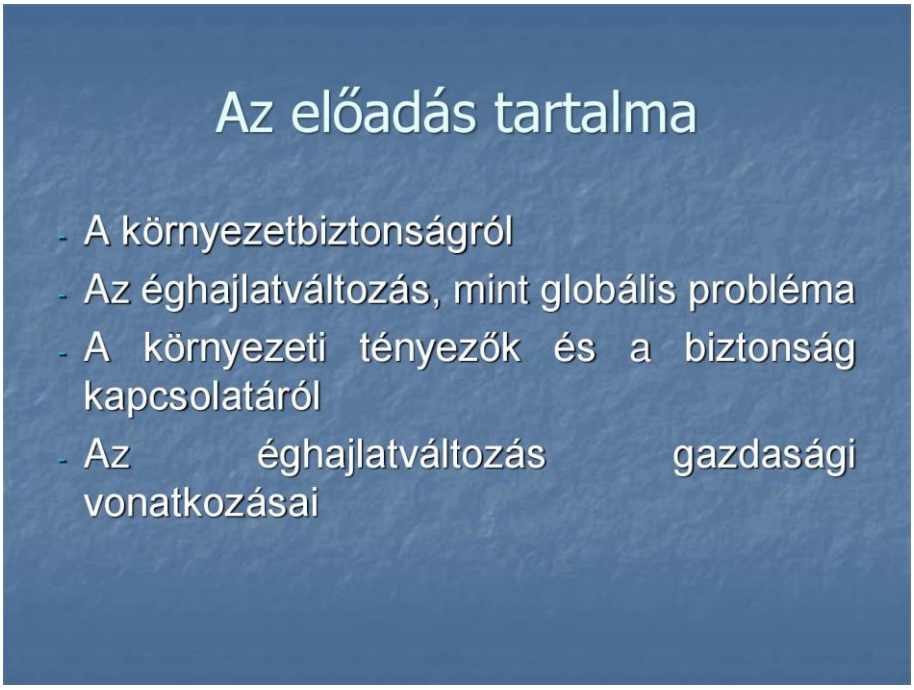
Tekintettel arra, hogy az éghajlatváltozás hatásai nem egyenletesen oszlanak el a világ tájain – és éppen a legszegényebb országok szenvedik el leginkább a negatív hatásokat – az éghajlatváltozás az egyik legkomolyabb fenyegetés a fejlődő világ számára és nagy akadálya annak, hogy visszaszorítsuk a szegénységet ezekben az országokban.

A legszegényebb fejlődő országok gazdasága erősen függ a mezőgazdaságtól, ami a gazdasági ágazatok közül a leginkább függ az éghajlattól. Hosszú távon – éghajlati, vízrajzi jellemzőik figyelembevételével – ezek a területek tapasztalják majd meg a felmelegedés leggyorsabb ütemét, így a biodiverzitás romló körülményeit, a vízkészlet csökkentést, valamint az infrastruktúra, az emberi egészség romlását.

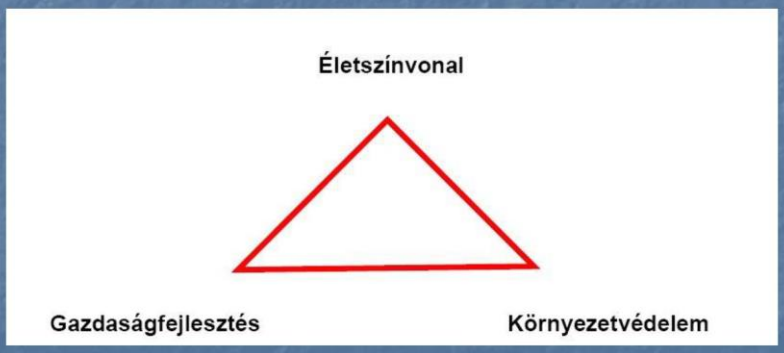
A szélsőséges időjárási események (viharok, tájfunok, hurrikánok, árvizek, szárazság, hőhullámok) okozta károk költségei globális szinten jelentősek a világ GDP-jének arányában.

Előadásomban az éghajlatváltozás negatív gazdasági hatásaira, mint egyfajta biztonsági kihívásra hívom fel a figyelmet.


A szélsőséges időjárási események okozta károk társadalmi költsége
„Új típusú kihívások a biztonságban” konferencia
2022. 01.21.
Kirovné Dr. Rácz Réka tű. őrgy.,
adjunktus, NKE RTK Katasztrófavédelmi Intézet
kirovne.racz.reka@uni-nke.hu


Az előadás tartalma
A környezetbiztonságról
Az éghajlatváltozás, mint globális probléma
A környezeti tényezők és a biztonság kapcsolatáról
Az éghajlatváltozás gazdasági vonatkozásai

Egyensúly a gazdaságfejlesztés és a környezetvédelem kérdésében



Az éghajlatváltozásról

- Fogalma: „ az éghajlati elemek magasabb vagy alacsonyabb értékek irányába történő tartós és/vagy rövidebb-hosszabb ideig fellépő, esetleg irreverzibilis változása, amelyek gyakorlati hatása érzékelhető és mérhető, sőt jelentős emberi- társadalmi következményekkel jár.”
- Ez elsősorban általános felmelegedést jelent, melyet az üvegházhatású gázok légköri koncentrációjának növekedésével hoznak összefüggésbe.

Az éghajlatváltozás gazdasági hatásai (8)

- A szélsőséges időjárási események, katasztrófák következményeinek felszámolása nagyon költséges a világ minden táján
- Az éghajlatváltozás közgazdaságtana → a károsanyag kibocsátást befektetésnek kell tekinteni
- Az éghajlatváltozás figyelmen kívül hagyása a gazdasági növekedés rovására mehet hosszútávon
- Az éghajlatváltozás nagy kihívás a fejlődő világ számára, akadálya a szegénység visszaszorításának

Katasztrófavédelmi szempont

- Előrejelzések szerint a globális csapadékmennyiség csökkenni fog, a lokális előrejelzésekben azonban sok a bizonytalanság.
- A szélsőséges időjárási események gyakorisága és intenzitása szintén növekedhet.
- Azok a társadalmi- gazdasági és ökológiai rendszerek a legsebezhetőbbek, amelyek a legérzékenyebben reagálnak az éghajlatváltozásra. Ezek többségükben a legszegényebb, legfejletlenebb országok.

Az éghajlatváltozás hatása a gazdaságra

- Az éghajlat megváltozásának következményeként megjelenő szélsőséges időjárási események okozta károk
- Az Egyesült Királyság : élen jár az éghajlatváltozás gazdasági hatásainak vizsgálatában.
- Költség-haszon elemzés: a tervezett kibocsátáscsökkentés hatása a gazdaságra.
- „Az éghajlatváltozás közgazdaságtana" című jelentés: a kibocsátáscsökkentést befektetésnek kell tekinteni, ami segít abban, hogy jövőbeni nagyon komoly gazdasági kockázatokat elkerüljünk
- Egyensúlyban kell tartani a gazdaság fejlesztését és a környezet védelmét.

Az éghajlatváltozás hatása a gazdaságra

- Az éghajlatváltozás hatásai nem egyenletesen oszlanak el a világ tájain. A legszegényebb országok szenvedik el a leghamarabb és leginkább a negatív hatásokat, ezért nagy akadály a fejlődő világ számára az éghajlatváltozás.
- A legszegényebb fejlődő országok gazdasága erősen függ a mezőgazdaságtól, ami a gazdasági ágazatok közül leginkább függ az éghajlattól.
- Nincs megfelelő egészségügyi ellátásuk→ a szélsőséges időjárás, extrém hőmérsékleti értékek megnövelik a betegségek, elhalálozások arányát.

Az éghajlatváltozás hatása a gazdaságra

- A szélsőséges időjárás (viharok, tájfunok, hurrikánok, árvizek, szárazság, hőhullámok) költségei elérhetik a világ GDP-jének 0,5-1%-át és ez az arány tovább fog nőni.
- Biztosítók szerepe a károk megtérítésére, a betegségek biztosítására megváltozik.

Köszönöm a megtisztelő figyelmet!

Dr. Horváth Zoltán: Rejtjelezést és adatrejtést megvalósító programcsomag

Korreferátum

A híradó képzés nem képzelhető el a rejtjelezés és az adatrejtés lehetőségeinek ismerete nélkül. Az ismeretanyag közlését követő tanulási folyamat hatékonysága növelhető, ha az elméleti ismeretek gyakorlati úton történő alátámasztása megvalósul.

A gyakorlati alkalmazáshoz az asztali számítógépek aritmetikai képessége csekély. Megfelelő aritmetikai háttér nélkül – csak elméleti ismeretekre alapozva – az „elfogadás, belátás” nehezen valósul meg.

Érintett területek:

- aritmetikai műveletek végzése nagy természetes számokon;
- szimmetrikus- és aszimmetrikus rejtjelezés, valamint adatrejtés gyakorlati megvalósítása;
- kulcskezelés;
- bizalmasság, hitelesség, letagadhatatlanság.

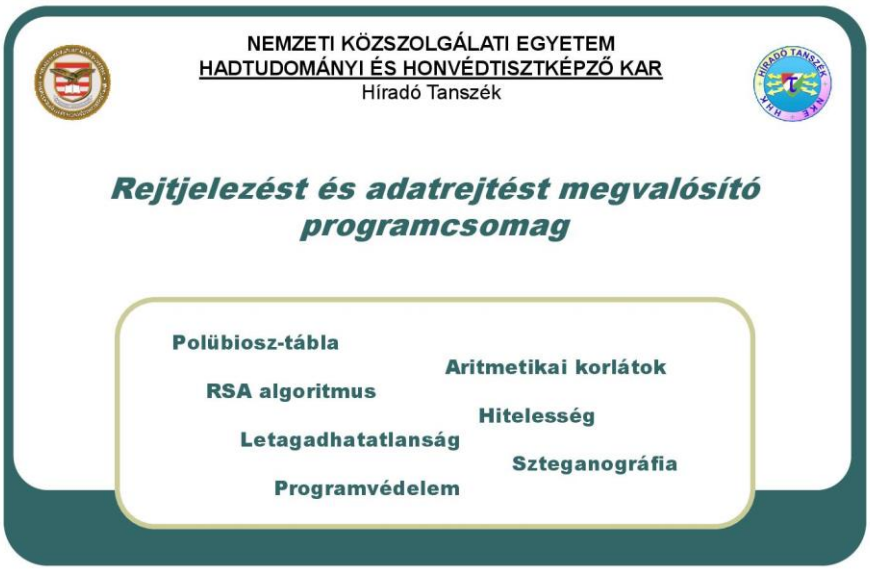
Megoldás:

Egy programcsomag, mely segítségével a hallgatók tanulmányozhatják a szimmetrikus- és aszimmetrikus rejtjelezés, valamint adatrejtés gyakorlati megvalósítását.

Ez a programcsomag a „játszva tanulás” lehetőségét nyújtja akár irányított, akár feladat-orientált alkalmazás során.

Szimmetrikus, és aszimmetrikus kódolást, valamint adatrejtést megvalósító programcsomag:

- Szimmetrikus rejtjelezés megvalósítása Polübiosz-tábla alkalmazásával;
- Speciális kripto-számológép alkalmazása;
- Aszimmetrikus rejtjelezés megvalósítása RSA-algoritmus alkalmazásával;
- Adatrejtés megvalósítása képfájlban;
- A programcsomag illetéktelen felhasználás elleni védelme.



Dr. Horváth Zoltán László
NKE HHK Híradó Tanszék
adjunktus

Bevezetés

A programcsomag célkitűzése:

A híradó képzés nem képzelhető el a rejtjelezés és az adatrejtés lehetőségeinek ismerete nélkül. Az ismeretanyag közlését követő tanulási folyamat hatékonysága növelhető, ha az elméleti ismeretek gyakorlati úton történő alátámasztása megvalósul.

A probléma:

A gyakorlati alkalmazáshoz az asztali számítógépek aritmetikai képessége csekély. Megfelelő aritmetikai háttér nélkül – csak elméleti ismeretekre alapozva – az „elfogadás, belátás" nehezen valósul meg.

Bevezetés

Érintett területek:

- aritmetikai műveletek végzése nagy természetes számokon
- szimmetrikus- és aszimmetrikus rejtjelezés, valamint adatrejtés gyakorlati megvalósítása
- kulcskezelés
- bizalmasság, hitelesség, letagadhatatlanság

Megoldás:

Egy programcsomag, mely segítségével a hallgatók tanulmányozhatják a szimmetrikus- és aszimmetrikus rejtjelezés, valamint adatrejtés gyakorlati megvalósítását.

Ez a programcsomag a „játszva tanulás" lehetőségét nyújtja akár irányított, akár feladat-orientált alkalmazás során.

A programcsomag

Szimmetrikus, és aszimmetrikus kódolást, valamint adatrejtést megvalósító programcsomag:

- Szimmetrikus rejtjelezés megvalósítása Polübiosz-tábla alkalmazásával
- Speciális kripto-számológép alkalmazása
- Aszimmetrikus rejtjelezés megvalósítása RSA-algoritmus alkalmazásával
- Adatrejtés megvalósítása képfájlban
- A programcsomag illetéktelen felhasználás elleni védelme

Szimmetrikus kódolás

Polübiosz-tábla

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

'SI' → '34 42'

	A	C	D	8	Q
B	A	B	C	D	E
F	F	G	H	I	K
9	L	M	N	O	P
1	Q	R	S	T	U
H	V	W	X	Y	Z

'SI' → 'D1 8F'

Szimmetrikus kódolás

Kibővített Polübiosz-tábla

	1	2	3	4	5	6	7	8	9	W
A	0	1	2	3	4	5	6	7	8	9
B	K	L	É	Á	?	Ó	Ü	Ö	,	Ű
C	J	H	G	F	D	S	A	I	Y	Í
D	P	Ő	Ú	M	N	B	V	C	X	:
E	O	I	U	Z	T	R	E	W	Q	.
F	/	y	g	SP	x	>	{	i	o	j
G	a	#	~	<	+	|	w	"	\	ő
H	t	'	d	ó	@	q	(	é	f	&
I	;	k	n	b	÷	DEL	[	s	CR	)
J	e	$	)	LF	§	l	í	c	-	p
K	_	ü	r	v	ú	z	TAB	%	ű	u
L	]	*	h	`	ö	=	m	á	^	...

- *Kulcs hossza:* **10 * 12**
- *Kulcs:*

'123456789W' - 'ABCDEFGHIJKL'

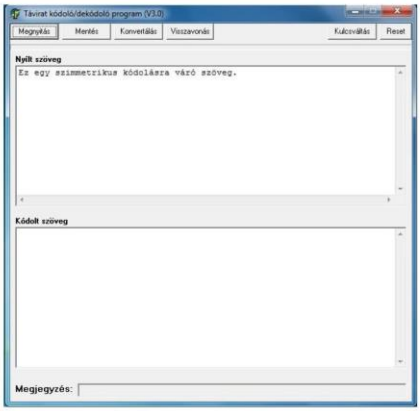
- *Üzenet:*

'Nap'

- *Kódolt üzenet:*

'5D1GW JXXXX'

Szimmetrikus kódolás



Távirat kódolása:

- **Input:**

„Távirat kódolása.”

- **Kulcs:**

123456789W –
ABCDEFGHIJKL

- **Output:**

E5L8K 4F8K3 G1H1F
4I2H4 H3F9J 6L8I8
G1EWX

Kripto-számológép, korlátok

A probléma:

Létkérdés a természetes számok ***pontos ábrázolás***a.

Miért is?

Előfordulhat, hogy többszáz számjegyet tartalmazó szám feldolgozása válik szükségessé: hatványozás, egészosztás, maradékképzés.

Például:

Számítsa ki $x := 82^{119}$ értékét:

Aritmetikai korlát

Hagyományos kalkulátort, asztali számítógépet alkalmazva az eredmény:

x = 5,544321854676070973542400878072 9e+227 (32 digit)

A pontos eredmény:

x =
554432185467607097354240087807286407466831135156589286803650522
040664691422534845106733761420641234832687474104136345777145439
768082364148623991444395487858861744062094132337697803148549625
156729172449383034620876026179609427968 (ez 228 számjegy)

Az eredmény ilyen pontos ábrázolása hagyományos úton nem valósítható meg.

Miért fontos ez:

Valamennyi számjegyre szükség van a számítások során. A lebegőpontos számábrázolás extrém méretű természetes számok esetén erre alkalmatlan.

Sztring-alapú aritmetika

Számjegyek összege:	***Számjegyek szorzata:***
$c_{n-1} = 1$	$c_{n-1} = 3$
’8’ → a = ***8***	’8’ → a = ***8***
’6’ → b = ***6***	’6’ → b = ***6***
s := a + b + c	m := a * b + c
c_n := ***s div 10 = 1***	c_n := ***m div 10 = 5***
s_n := ***s mod 10 = 5***	m_n := ***m mod 10 = 1***
s_n → ’s_n’, azaz ***’5’***	m_n → ’m_n’, azaz ***’1’***

Komplemensek képzése

Kilences-komplemens:

'A' kilences-komplemense ***'B'***, ha rendre:

$b_n = 9 - a_n$

Tizes-komplemens:

'B' := 'B' + '1'

Komplemensek képzése

9999	kilences-komplemens:	⇒	*7059*
- 2940	tizes-komplemens:	⇒	7059+1
7059		=	*7060*

$s_n = a_n + b_n + c_{n-1}$

			1 ($c_0 := 1$)
4738	4738	4738	
- 2940	+ 7060	+ 7059	
1798	11798	11798	

Kripto-számológép

Végezhető alapműveletek:

- Összeadás, szorzás, hatványozás
- Kivonás, egészosztás, maradékképzés

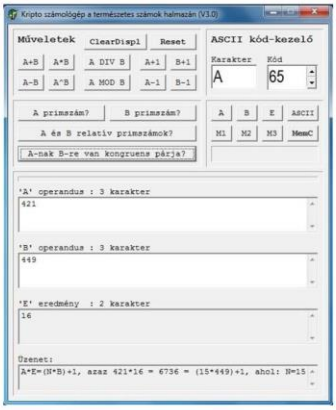
Többszáz helyiértékű számok esetén

Végezhető összetett műveletek:

- Prímek- és relatív prímek ellenőrzése
- Kongruens számpár keresése

  (A * B = C * N + 1) egyenlet megoldása

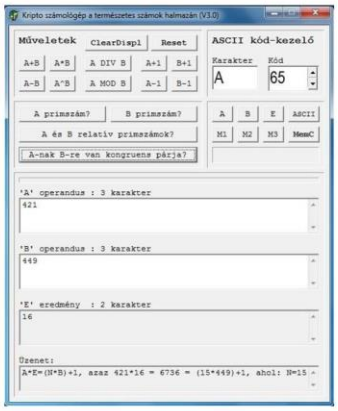
Kripto-számológép



RSA-kulcs képzése:

- **A** := **37**; és **B** := **47**
- **A** és **B** prím ?
- **A * B** → **E**
- **E** → **M1**
- **(A-1) * (B-1)** → **E**
- **E** → **B**
- **A** := **119**
- **A** és **B** relatív prim ?
- **A**-nak van kongruens párja **B**-re
- a kulcspár első szegmense:
  - **A = 119**
  - **E = 167**
- a kulcspár második szegmense:
  - **M1 = 1739**

Kripto-számológép



RSA-kódolás

- ***Input:***
  ‚D' (ASCII táblázatban a **68**. karakter)
- ***Kulcspár:***
  - **119 1739**
  - **167 1739**
- ***Kódolás:***
  $68^{119} \bmod 1739 = 1264$
- ***Dekódolás:***
  $1264^{167} \bmod 1739 = 68$
- ***Output:***
  ‚D' (ASCII táblázatban a **68**. karakter)

Aszimmetrikus kódolás (RSA)

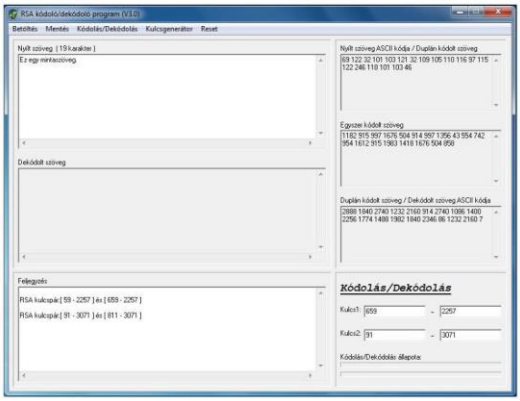
Az aszimmetrikus kódolás problémaköre:

- Privát kulcs – Publikus kulcs
- Kulcsgenerálás szabályai
- Kódolás – dekódolás folyamata

Aszimmetrikus kódolás:

- Kulcselosztás
- Hitelesség és letagadhatatlanság
- Hibrid kódolás

Aszimmetrikus kódolás (RSA)



Kulcsképzés

$P_A := 37$
$Q_A := 79$
$E_A := 127$

A kulcspár:

- 127 - 2923
- 199 - 2923

$P_B := 43$
$Q_B := 59$
$E_B := 157$

B kulcspár:

- 157 - 2537
- 481 - 2537

Szteganográfia

Adatrejtés (szteganográfia):

- A szteganográfia nem az üzenet titkosításával, hanem elrejtésével foglalkozik. Fontos, hogy az üzenet létezéséről csak a címzett tudjon.
- A digitális adatok sok lehetőséget kínálnak arra, hogy elrejtsünk valamit valamiben. Ilyenek például a médiafájlok (kép, hang, stb).
- Struktúrájuk ismeretében kialakítható egy olyan rejtett kommunikációs csatorna, mely ismerete nélkül a „mellékesen” közölt információ nem fedhető fel.
- Fontos, hogy az adatközlés során a „torzulás” ne keltsen feltűnést, maradjon észrevehetetlen.

Szteganográfia

Adatrejtés (szteganográfia) megvalósítása tömörítetlen TrueColor 24 bites BMP fájlban:

- **A fájl felépítése három jól elkülöníthető részből áll:**
  - ***Fájl fejléc*** (14 bájt), a fájlra vonatkozó alapvető adatokat tárolja
  - ***Információs fejléc*** (40 bájt), az eltárolt kép jellemzőit írja le (felbontás, színmélység, tárolás módja, stb.)
  - ***Bittérkép***, a kép tényleges tárolási helye, ahol képpontról képpontra jegyzik fel azok színkomponenseit BRG sorrendben (a program ezt a területet alkalmazza adatrejtésre)
- **Ha a bittérkép mérete: 1024×768 képpont (a képfájl mérete: 2,36 MByte):**
  - Ez 1024*768*3 ≅ **2.36 Mbit**, vagyis ≅ **295 kByte** információhordozó kapacitást jelent
  - Ez azt jelenti, hogy **a képfájl méretének kb. 12,5%-a** alkalmas rejtett információ továbbításra
  - Keretrendszer kialakítása (járulékos információk, mint pl.:**felismerés, adat-vége**, egyébként értelmezhetetlen)

Szteganográfia

Adatrejtés a legalacsonyabb helyiértékű bitek (LSB) alkalmazásával (Chr(97)=‚a' rejtése)

Jellemzők:

- méret:	**45 254** Byte
- felbontás:	**150 x 100** pixel
- színmélység:	**24 bites** BMP
- kapacitás :	**5 280** Byte

nyers kép

…	11011010	
1	01111010	0
2	00001100	0
3	11011100	0
4	01111010	0
5	00001100	0
6	11011011	1
7	01111010	0
8	00001100	0
…	11011010	

tabula rasa

	11011010	
	01111010	0
	00001100	0
	11011100	0
	01111010	0
	00001100	0
	11011010	0
	01111010	0
	00001100	0
	11011010	

adatrejtő kép

	11011010	
	01111010	0
	00001101	1
	11011101	1
	01111010	0
	00001110	0
	11011010	0
	01111010	0
	00001101	1
	11011010	

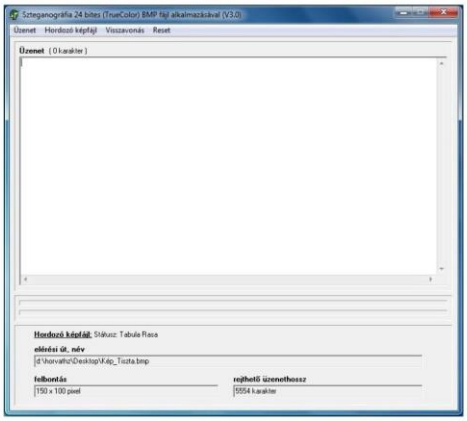
Szteganográfia



Vajon a képek közül melyik:

- a nyers
- a tisztított (tabula rasa)
- az adathordozó

Szteganográfia



Adatrejtés:

- Tisztítás
- Rejtés
- Felfedés

Programvédelem

Célkitűzés:

A programcsomag oktatási célra készült. Az illetéktelen másolatok alkalmazása - amellett hogy nem tisztességes - hamis biztonságérzetet kelthet a felhasználóban.

Az illetéktelen másolatok alkalmazási lehetőségét meg kell akadályozni.

Megoldás:

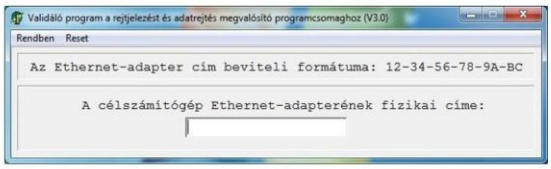
Hardverfüggő futtathatóság: A számítógépben található hálózati adapter fizikai címe (MAC-cím) alapján a számítógép azonosítható.

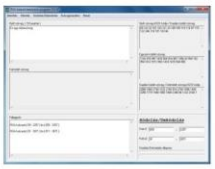
Programvédelem

Program futtatásának engedélyezése MAC-cím alapján

A hálózati adapter a *hardverkulcs*. Ha a MAC-cím értéke megegyezik a programban regisztrált értékkel, akkor futtatható a program.

Javaslat: **A validáló programot ne adjuk át másnak.**





Befejezés

Az alkalmazás előnyei:

- A „játszva tanulás”, előnye
- Az egyes eljárások gyakorlati megtapasztalása
- A kulcselosztás problémaköre, a kulcs értékének felismerése
- A hibrid kódolás hatékonysága
- Az elmélyített ismeretek alapján biztonságos kommunikációs protokollok kialakítása

Összességében egy olyan programcsomag készült, mely a megszerzett elméleti ismeretek gyakorlati alkalmazásán keresztül képes az ismeretek elmélyítésére, és a programcsomag alkalmazásán keresztül biztosítja a biztonságos kommunikáció, valamint a kommunikációs protokollok biztonságos kialakításának mélyebb megismerését.

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
Híradó Tanszék

Köszönöm a figyelmet.

Dr. Horváth Zoltán László
adjunktus

NKE HHK
Híradó tanszék
E-mail: horvath.zoltan@uni-nke.hu

Bús Nikolett Katalin: Információbiztonsági stratégia alkotás

Korreferátum

A modern IT-megoldások, új technológiák átszövik életünket és a hazai KKV-k, nagyvállalatok a működésük alapjait is ezen a platformon növekvő intenzitással alkalmazzák.

Azonban meg kell említeni, hogy a nagyvállalatok tudatosan felépített minőségbiztosítása, cégstratégiája magával, illetve magában hordozza azt az elvet, melyet a cég/társaság/vállalat a működési folyamatainak tervezése, szervezése, fenntartása és folyamatos javítása mellett valósít meg.

Véleményalkotásom az elmúlt 15 év vállalati irányítási rendszerek (minőségbiztosítás, környezetvédelem, munkabiztonság) építésében és üzemeltetésében szerzett tapasztalatom mondatja. Mind a KKV-nál, mind nagy nemzetközi cégeknél a cég tulajdonos, illetve a cégvezetés stratégiája, illetőleg kockázatvállalása dönteti el, hogy a cég milyen körülmények között működik, milyen fejlesztéseket vezet be / hajt végre. Néha tudatos kockázatvállalással élik a KKV-k napjaikat. A magyar tulajdonosi hátterű cégeknél/társaságoknál/vállalatoknál pedig erre halmozódik egy gondolat, miszerint „nálunk ez nem történhet meg”.

Előadásom szeretném bemutatni egy magyar nagyvállalat versenyképességi programjában elfoglalt helyét az Információbiztonsági stratégia alkotásnak.

Kijelenthető, hogy az elmúlt két évben új üzleti irányok fejlődtek. S már a közeljövő is nagy kihívásokat jelez. Lehet-e mindezt hagyományos módszerekkel szervezni és vezetni?

Szinte mindenki tudja, érzi, hogy nem. Csekély előrelátással is látható, hogy a versenyképességen múlik a jövő. Azon, hogy mennyire törekszünk gyorsan, rugalmasan és főleg sokkal hatékonyabban dolgozni. Úgy, hogy közben megőrizzük a Vállalat működési értékeit; az elismert magas szaktudást, elkötelezettséget, a ma már Magyarországon egyedülálló műszaki kivitelezői képességeket. S mindezt alapvető értékekre: a tisztességre és a biztonságra alapozva. Ez azonban ma már kevés. Kiegészíteném az információbiztonsággal!

Projektvezetési képességeink elismerésre méltóak, de vannak nálunk sokkal jobbak. Nem vagyunk kellően rugalmasak stratégiai céljaink kitűzésében, követésében, az irányításban. Nagyon is fejlesztendő a tehetségek felkutatása és segítése, a döntések számokkal való támogatása, a teljesítmények értékelése, ezeken felül az információbiztonság is sok problémás kérdést vet fel.

A versenyképességi program 7 területet ölelt át, melyben az alábbi területek viszonyában került megvizsgálásra az információbiztonsági alapkövetelmények:

- *Stratégiai* projekt.
- *Irányítási modell* projekt.
- *Riportok rendszere* projekt.
- *Teljesítményértékelés* projekt.
- *Projektmenedzsment* projekt.

- *Tehetségfejlesztés* projekt.
- *Adatbiztonság* projekt.

Információbiztonsági stratégia alkotás

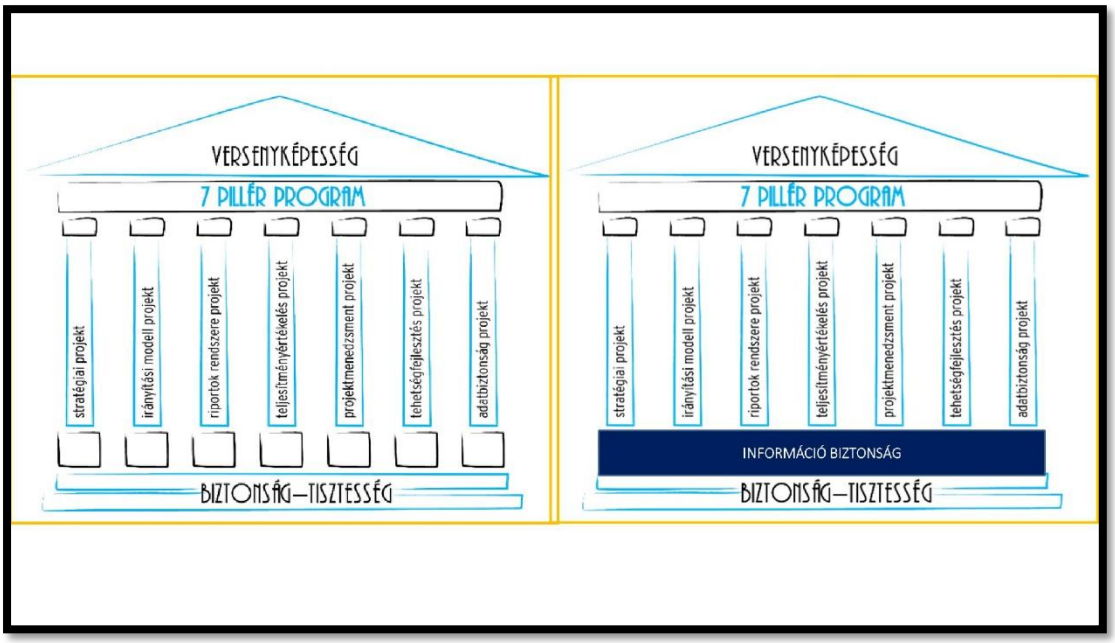
Egy magyar nagyvállalat versenyképességi programjában

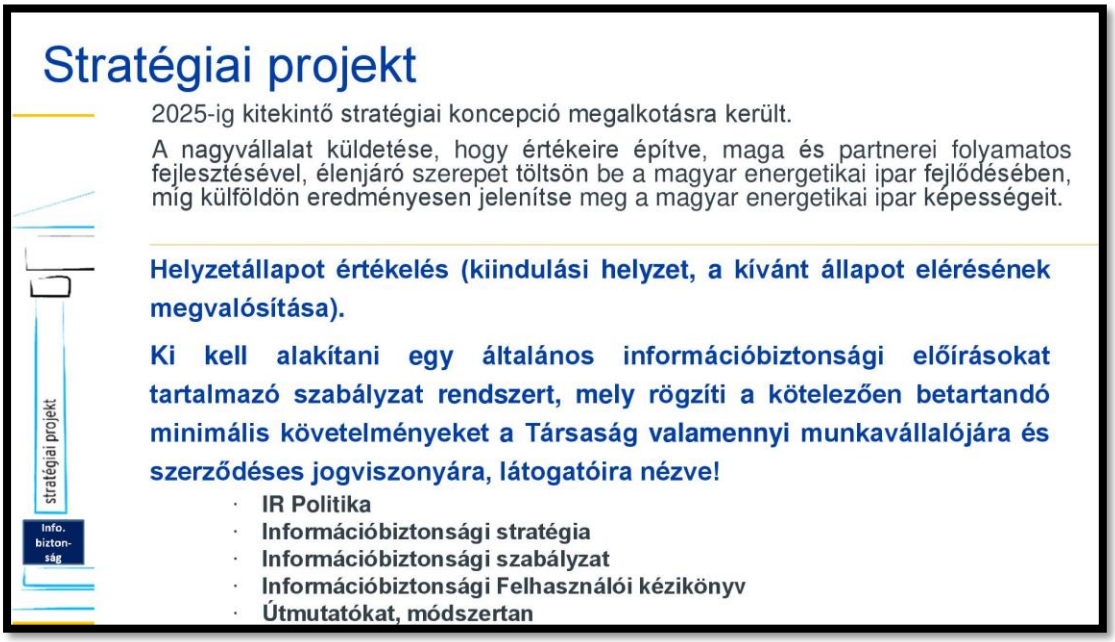
Bús Nikolett Katalin; Ph.D.doktorandusz,
Óbudai Egyetem Biztonságtudományi Doktori Iskola,
e-mail: bus.nikolett@uni-obuda.hu, ORCID: 0000-0002-3069-4512

Célkitűzésem

Kutatásom során az alábbi célokat tűztem ki:

1. A tanulmányaim felhasználásával és adaptálásával az információbiztonságot alapértékként megjelentetni egy nagyvállalat versenyképességi programjában.
2. Javaslatokat tenni a fejlesztésre.


VERSENYKÉPESSÉG
7 PILLÉR PROGRAM
stratégiai projekt
irányítási modell projekt
riportok rendszere projekt
teljesítményértékelés projekt
projektmenedzsment projekt
tehetségfejlesztés projekt
adatbiztonság projekt
BIZTONSÁG–TISZTESSÉG
VERSENYKÉPESSÉG
7 PILLÉR PROGRAM
stratégiai projekt
irányítási modell projekt
riportok rendszere projekt
teljesítményértékelés projekt
projektmenedzsment projekt
tehetségfejlesztés projekt
adatbiztonság projekt
INFORMÁCIÓ BIZTONSÁG
BIZTONSÁG–TISZTESSÉG


Stratégiai projekt
2025-ig kitekintő stratégiai koncepció megalkotásra került.
A nagyvállalat küldetése, hogy értékeire építve, maga és partnerei folyamatos fejlesztésével, élenjáró szerepet töltsön be a magyar energetikai ipar fejlődésében, míg külföldön eredményesen jelenítse meg a magyar energetikai ipar képességeit.
Helyzetállapot értékelés (kiindulási helyzet, a kívánt állapot elérésének megvalósítása).
Ki kell alakítani egy általános információbiztonsági előírásokat tartalmazó szabályzat rendszert, mely rögzíti a kötelezően betartandó minimális követelményeket a Társaság valamennyi munkavállalójára és szerződéses jogviszonyára, látogatóira nézve!
· IR Politika
· Információbiztonsági stratégia
· Információbiztonsági szabályzat
· Információbiztonsági Felhasználói kézikönyv
· Útmutatókat, módszertan
stratégiai projekt
Info. bizton-ság

Irányítási modell projekt

Átláthatóvá és egyértelművé tegye a vezetői információk Vállalaton belüli áramlását: milyen információk, milyen fórumokon kerülnek tárgyalásra, továbbításra.

A projekt lefektette az értekezleti (vezetői értekezletek, projektértekezletek, tematikus értekezletek, fórumok) rendeket.

Az értekezleti típusok meghatározásánál, különös tekintettel figyelembe kell venni a résztvevők körét, az értekezleten felhasznált információk forrását, hitelességét, valamint az adott értekezlet döntéshozatali kompetenciáját.

A Társasági hierarchiában az alulról felfelé történő információáramlás lehetőségének biztosítását, amellyel elő tudjuk segíteni a munkavállalóktól az észrevételek, javaslatok a megfelelő fórumokra jussanak el (átadott információ védelme; anonimitás).

irányítási modell projekt

Info. biztonság

Riportok rendszere projekt

Átláthatóvá és egyértelművé tegye elsősorban a vezetői információk társaságunkon belüli áramlását, hozzáférését - értekezleti típusokból, mint kijövő adat egységes struktúrában megjelenését az adatok közlésére, továbbá meghatározza az elosztási jegyzéket (papír alapú riport esetén), hozzáférési szinteket (elektronikus riport esetén).

Két kérdőívet - az adattárolásra használt IT-rendszerek és fejlesztési elképzelések, másrészt a gazdasági feladatok kapacitásigényeinek felmérését szolgálták volna.

Fejlesztés irányainak kontrollja

- **harmadik fél bevonása**
- **adatok köre**
- **új elektronikus iktatórendszer (megvalósíthatósági elemzés-erőforrásigények becslése és kockázati mátrix); nem „dobozos" termék (üzemeltetési kézikönyv)**
- **az informatikai szolgáltató által üzemeltetett ügyviteli rendszerek szinergiája**
- **adatok migrálása**

VERS

7 PILL

riportok rendszere projekt

Info. biztonság

BIZTO

Teljesítményértékelés projekt

Munkavállalók eddig csak részben, eseti jelleggel kaptak formalizált elvárást és visszacsatolást a teljesítményükkel kapcsolatban. Szervezeti célok elérésében.

Kérdőíves felmérés eredménye - az egységes megítélés elmaradása.

n+1 szintű vezetőnek egy olyan követelményt támaszt, hogy jobban felügyelje, figyelje munkavállalói teljesítményét. Így abban az esetben, ha valaki nem tiszta szándék által vezérelt, úgy az n+1 szintnek, átfogó értékelés esetén, illetve magasabb pozícióban pedig 180fokos értékelési rend bevezetésével átlátható lesz a munkavállalói lelkület.

- **Egységes megítélés**
- **„eredményességi mutatók" (Key Performance Indicator) – szervezeti egység**
- **Értékelési mutatószámok – egyén, szervezeti egység**

Projektmenedzsment projekt

Projektmátrix megalkotása, mely arra tervezett, hogy kockázati alapon sorolja be a különböző projekteket kategóriákba, amelyekhez elvárásokat, eszköztárat rendel.

Szempontrendszer:Értékhatár; Egyedi/ismert tevékenység; Piac, vevőkör; Aggregált kockázat; Vállalkozási forma;

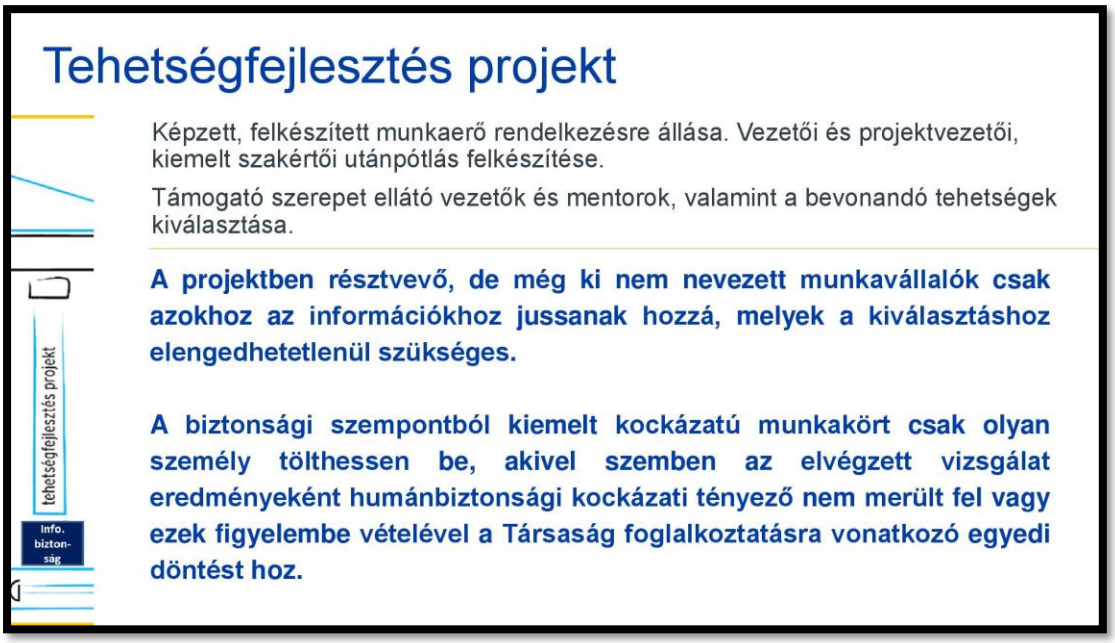
Az adminisztratív védelem:

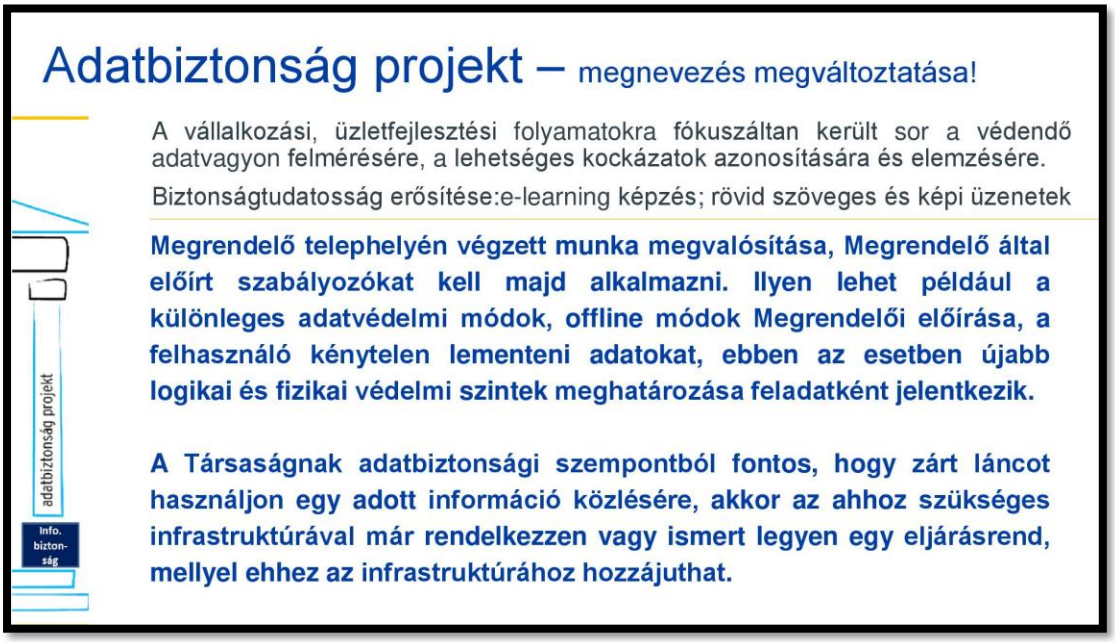
- **projekt specifikus szabályozók**
- **információáramlás**
- **‚alvállalkozói láncolat'**

A fizikai védelem

- **őrzés, védelem, elkerítések, elzárható terek kialakítása**
- **a mobil (változó), telephelyi munkahely, telepített építőipari kivitelezési helyszínek**

A logikai védelem


Tehetségfejlesztés projekt
Képzett, felkészített munkaerő rendelkezésre állása. Vezetői és projektvezetői, kiemelt szakértői utánpótlás felkészítése.
Támogató szerepet ellátó vezetők és mentorok, valamint a bevonandó tehetségek kiválasztása.
A projektben résztvevő, de még ki nem nevezett munkavállalók csak azokhoz az információkhoz jussanak hozzá, melyek a kiválasztáshoz elengedhetetlenül szükséges.
A biztonsági szempontból kiemelt kockázatú munkakört csak olyan személy tölthessen be, akivel szemben az elvégzett vizsgálat eredményeként humánbiztonsági kockázati tényező nem merült fel vagy ezek figyelembe vételével a Társaság foglalkoztatásra vonatkozó egyedi döntést hoz.
tehetségfejlesztés projekt
Info. bizton-ság


Adatbiztonság projekt – megnevezés megváltoztatása!
A vállalkozási, üzletfejlesztési folyamatokra fókuszáltan került sor a védendő adatvagyon felmérésére, a lehetséges kockázatok azonosítására és elemzésére.
Biztonságtudatosság erősítése:e-learning képzés; rövid szöveges és képi üzenetek
Megrendelő telephelyén végzett munka megvalósítása, Megrendelő által előírt szabályozókat kell majd alkalmazni. Ilyen lehet például a különleges adatvédelmi módok, offline módok Megrendelői előírása, a felhasználó kénytelen lementeni adatokat, ebben az esetben újabb logikai és fizikai védelmi szintek meghatározása feladatként jelentkezik.
A Társaságnak adatbiztonsági szempontból fontos, hogy zárt láncot használjon egy adott információ közlésére, akkor az ahhoz szükséges infrastruktúrával már rendelkezzen vagy ismert legyen egy eljárásrend, mellyel ehhez az infrastruktúrához hozzájuthat.
adatbiztonság projekt
Info. bizton-ság

Köszönöm a megtisztelő figyelmet!

Németh Attila: Drón detektálás, drón elhárítás kihívásai

Korreferátum

A drónok a mindennapi életünk részévé váltak. A hobbi célú használat mellett, a mezőgazdasági, logisztikai, mentési feladatok mellett védelmi célokra is rendszeresen használják. Az elmúlt időszakban a drónokat a harctéren túl is felhasználják fegyverként, felderítésre és üzemszerű működés megzavarására. Több alkalommal zavarták már meg a légiközlekedés rendjét, ez hazánkban is megtörtént 2019 őszén, de Svédországban 2022. január közepén, egyidejűleg, több atomenergetikai létesítmény felett azonosítottak jogszerűtlen drónokat. 2019-ben Szaúd-Arábiában konkrét támadást hajtottak végre drónokkal olajfinomítókkal szemben, jelentős károkat okozva, amely a világgazdaságra is kihatott. A drónok elterjedtsége és a felsorolt példák okán a drónok elleni védekezésre kiemelt figyelmet kell fordítani.

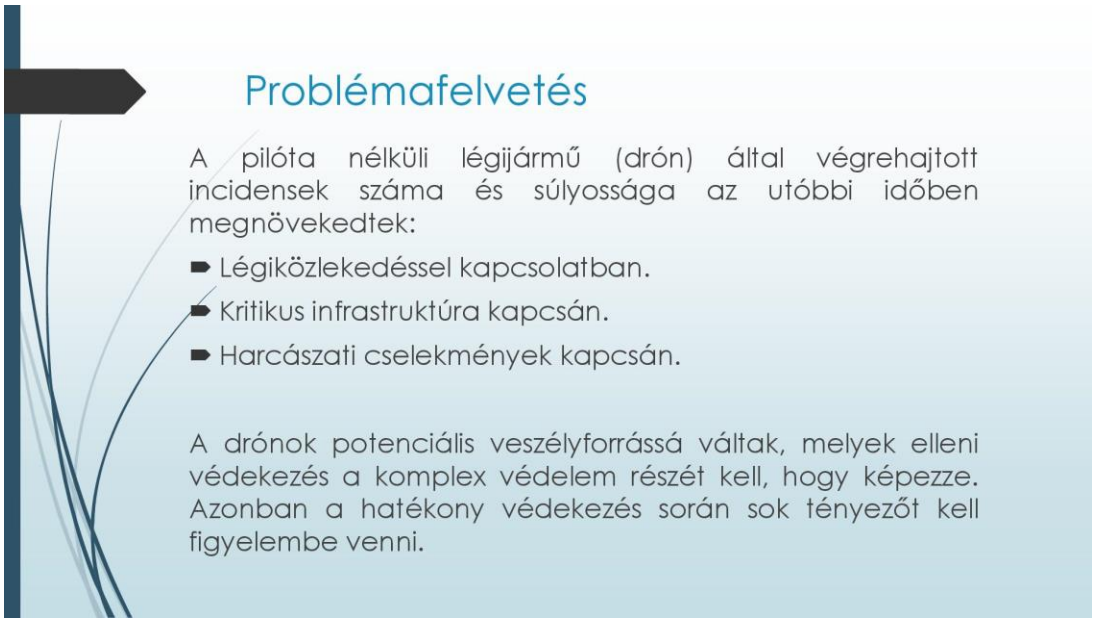
A drónok elleni védekezés első eleme a drónok detektálása, a jogos és jogosulatlan drónok azonosítása. A drónok azonosítása során nem elegendő a kereskedelmi forgalomban kapható drónok detektálását biztosítani, mivel számos lehetőség van egyedi drónvezérlés kialakítására, ezért nem elegendő az együttműködő gyártók azonosító rendszerére alapozni. Olyan detektáló rendszereket kell alkalmazni, amely a drónok valamely jellemzőjét képes azonosítani. Ezek számbavételét követően a működési elvük elemzését követően, tulajdonságaik vizsgálatával meg kell állapítani,

melyek azok a körülmények, amelyek vonatkozásában nem hatékonyak. A detektálási eszközök hiányosságait azonosítva lehetőség nyílik arra, hogy a védekezés fontos eleme úgy kerüljön kialakításra, hogy az elérhető leghatékonyabb legyen, és képes a drónok felderítésére.

A drón elhárítás előfeltétele a detektálás, ha sikerül azonosítani a jogosulatlan drónt, akkor meg kell akadályozni, hogy a védendő teret elérje. A védendő tér lehet objektum, akár kritikus infrastruktúra, közlekedési eszköz, vagy embertömeg, rendezvény, esetleg védendő személy. A drón mozgásának megakadályozása történhet fizikai megsemmisítéssel, esetleg fizikai akadállyal, vagy elektronikus rendszerbe történő beavatkozással. Az eltérő módszerek eltérő eredménnyel járnak, amelynek megválasztása során figyelembe kell venni a környezeti körülményeket, a veszély szintjét, és a védendő tér jellegét.

A rendszer kiválasztása során a drón elhárító rendszerek működési elvük elemzését követően, tulajdonságaik vizsgálatával meg kell állapítani, melyek azok a körülmények, amelyek vonatkozásában nem hatékonyak. Figyelemmel kell lenni, hogy mi történik a drónnal az elhárítást követően, milyen szinten veszélyeztet testi épséget, milyen mértékű anyagi kárt okoz. Szintén figyelembe kell venni, hogy a sikertelen elhárítási kísérlet milyen következményekkel jár a környezetre tekintettel, milyen károkat okoz. Az elhárítási eszközök hiányosságait azonosítva lehetőség nyílik arra, hogy az elhárítás eszköze úgy kerüljön kiválasztásra, hogy az elérhető leghatékonyabb legyenek.

A kihívások azonosítása, és elemzése lehetőséget teremt arra, hogy a hátrányok és előnyök figyelembe vételével kerüljön kialakításra a kockázat arányos komplex védelmi rendszer.



Áttekintés

- Drón incidensek
- Drón detektálási lehetőségek
- Drón detektálás kihívásai
- Drón elhárítási lehetőségek
- Drón elhárítás kihívásai
- Konklúzió

Drón incidensek

Légiközlekedés

Repülőterek felderítése, megbénítása

- Heathrow, Liszt Ferenc repülőtér

Repülők elleni támadás

- Saudi Airport

Kritikus infrastruktúra

Olajfinomító elleni támadás

- Szaúd-Arábia

Atomerőmű felderítése

- Svédország

Drón detektálási lehetőségek

Passzív módon

Rádiófrekvenciás detektálás

- Vezérlő jel, video jel detektálása
- Vezérlő jel értelmezése

Optikai érzékelés

- Hőkamera
- AI támogatott mozgást azonosító kamera

Hang érékelés

- Rotor hang azonosítása

Aktív módon

Rádiólokációs detektálás

- Felületről visszaverődő elekromágneses hullám azonosítása
- AI támogatott azonosítás

Drón detektálási kihívásai

Passzív módon

Rádiófrekvenciás detektálás

- Előre programozott repülés esetén nincs kisugárzott jel, ilyenkor a navigációs rendszerek jelei alapján hajtja végre a repülést a drón
- Egyedi rádiós vezérlés esetén nehezen, vagy lassan azonosítható, a teljes sáv ellenőrzése roppant erőforrásigényes
- Legalább három állomás szükséges a helymeghatározásához
- Vezérlőjel titkosított csatornát alkalmaz, megismerése kihívást jelent

Drón detektálási kihívásai Passzív módon

Optikai érzékelés

- Időjárási körülményekre érzékeny megoldás
- Sok eszköz szűkséges a körkörös detektáláshoz
- Egy kamera csak egy mozgó tárgy azonosítására, követésére alkalmas
- Hőkamera kis távolságra hatékony, a háttér hőkibocsátás

Hangérzékelés

- Zajos, városi környezetben hatástalan
- Szeles körülmények hatékonyság csökkentő

Drón detektálási kihívásai Aktív módon

Rádiólokációs detektálás

- Városi környezetben korlátozott a hatékonysága a sok mozgó tárgy miatt
- Sok eszköz szűkséges a körkörös detektáláshoz, helymeghatározáshoz
- Madarakat összekeverheti a drónokkal
- Működtetése képzett humánerőforrást igényel


Drón elhárítási lehetőségek
Elektronikus módon
Elektormágneses zavarással
Vezérlőjel
Navigáció
Elektromágneses impulzus (EMP)
Lézer


Drón elhárítási lehetőségek
Fizikai beavatkozással
Elfogás
Madarak
Hálóvetők
Drón raj
Megsemmisítés
Lőfegyver
Rakéta

Drón elhárítás kihívásai

Elektronikus módon

- Elektormágneses zavarás kihívásai
  - Nem szabványos vezérlőjel zavarásához széles spektrumú zavarásra van szűkség
  - Szélessávú zavarás a kommunikációs rendszerek megbénulását okozza
  - Nagyteljesítményű zavarás szükséges hatékony védelemhez, sok helyszín nagy energiaigény
  - Navigációs jelek megzavarása, hamisítása kihat a légi-, víziközlekedési rendszerekre
  - Szabványos navigációs csatornák megzavarása mellett hamis navigációs jel sugárzására is szűkség van (spoofing)
  - A dróndetektáló és zavaró eszközök vezeték nélküli kapcsolatát is megzavarja, a drón védelmi rendszer működését ellehetetleníti.

Drón elhárítás kihívásai

Elektronikus módon

- Elektromágneses impulzus (EMP)
  - Az elhárítás során a impulzus irányában kilométerekkel messzebb is egészségkárosodást elektronikus eszközök meghibásodását okozhatja
  - Légi közlekedést veszélyeztetheti
  - Nagy bemeneti energiaigény telepítésnél nehézséget okoz
- Lézer
  - Körülményes célratartás
  - Az elhárítás során a impulzus irányában kilométerekkel messzebb is egészségkárosodást elektronikus eszközök meghibásodását okozhatja

Drón elhárítás kihívásai

Fizikai beavatkozással

- Madarak
  - A madár megsérül
  - Nem minden esetben motivált a madár
  - Több drón esetében nem hatékony
- Hálóvetők
  - Kis hatótávolság
  - Célzás, utántöltés nehézkes
  - A találatnál sem biztos a hatékony elfogás, háló nem megfelelően
  - Több drón esetében nem hatékony

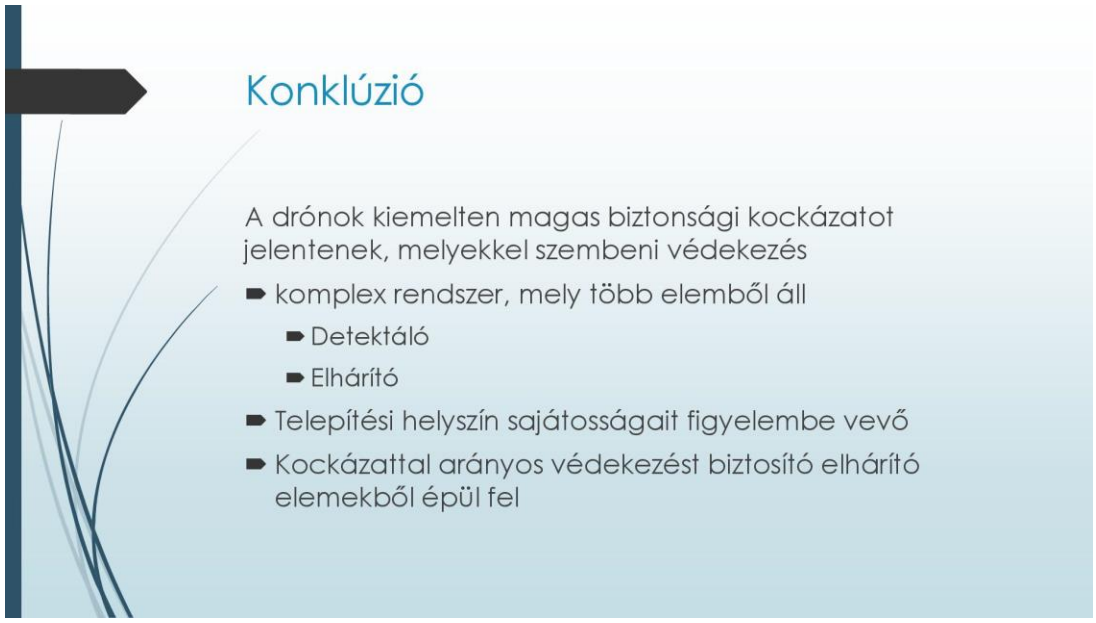
Drón elhárítás kihívásai

Fizikai beavatkozással

- Drón raj
  - Precíz irányítást és koordinációt igényel
  - Nehézkes a drónokat folyamatosan üzemkész állapotba tartani

Megsemmisítés

- Lőfegyver, Rakéta
  - Aránytalan pusztítás céltévesztés esetében
  - Precíz irányítást, célzást igényel


Konklúzió
A drónok kiemelten magas biztonsági kockázatot jelentenek, melyekkel szembeni védekezés
komplex rendszer, mely több elemből áll
Detektáló
Elhárító
Telepítési helyszín sajátosságait figyelembe vevő
Kockázattal arányos védekezést biztosító elhárító elemekből épül fel


Köszönöm a figyelmet!

Felhasznált irodalom, képek forrásai

- PÁNYA Nándor (2016): A Pilóta nélküli légi járművek vizsgálata autonómia szempontjából. Elérhető: Repüléstudományi közlemények, XXVIII. évfolyam, 81-94. oldal. Elérhető: http://www.repulestudomany.hu/folyoirat/2016_1/2016-1-08-0322_Panya_Nandor.pdf (letöltés ideje: 2021. április 2.)
- NÉMETH András (2018): UAV-k alkalmazása a közfeladatok ellátása során II., Hadmérnök XIII. évfolyam 3. szám, 73-75. oldal. Elérhető: http://real.mtak.hu/87038/1/183_06_nemeth.pdf,
- SERBAKOV Márton Tibor (2019): A terroristák drónhasználata. Elérhető: Nemzetbiztonsági Szemle 7. évfolyam 2019. év 4. szám 30–43. oldal.
- KRAJNC Zoltán (2018): Drónok, hibrid fenyegetés, terrorizmus a légtérből: a légi hadviselés privatizálása. Elérhető: Hadmérnök XIII. évfolyam 4. szám – 2018.december. Url: http://hadmernok.hu/184_29_kranjc.pdf,

Felhasznált irodalom, képek forrásai

- MANGA László (2016): Drónok és alkalmazási területeik, avagy szóba jöhetnek-e egy esetleges nukleáris baleset esetén. Elérhető: Műszaki Katonai Közlöny XXVI. évfolyam, 2016. 2. szám, 187-189. oldal.
- Shaan Shaikh, Wes Rumbaugh:The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense
- **Fotók forrásmegjelölése:**
- https://www.bbc.com/news/av/world-middle-east-49736754
- https://thearabweekly.com/houthi-drone-strike-hits-civilian-plane-saudi-airport
- https://www.bbc.com/news/world-europe-60035446

Ináncsi Mátyás: Nyílt információ kérdésköre a közösségi média vonatkozásában

Korreferátum

A közösségi média a mindennapunk részét képezi. Az alapvető működése a személyes adatainkból áll. Mi a felhasználók hozzuk létre a tartalmat, mi reagálunk mások tartalmaira. Ezen tevékenységünk során a saját személyes adatainkat tesszük publikussá és elérhetővé. Jelenleg különböző jogszabályok igyekeznek megvédeni a személyes adataink biztonságát: ilyen az európai adatvédelmi rendelet (GDPR), illetve hazai szinten az Információs önrendelkezési jogról szóló törvény igyekszik megvédeni az adatbiztonságunkat.

Előadásomban bemutatom, azt hogy a közösségi média világában mi minősül nyílt információnak. Ez nem azonos a normál köztudatba vett nyílt információ kategóriával. Itt sokkal tágabbá válik a kérdéskör, hiszen mi a személyes adatainkat tesszük nyílttá. Ez egy nagy bizalmat igénylő döntés, és felmerül a kérdés, hogy a szolgáltatók megbízhatóak e? Válaszként bemutatom a múltbeli nagyobb incidenseket: kiemelten a Cambridge Analytica, és az End-to-End titkosítási botrányt. Bemutatásra kerül, hogy ezek az incidensek tulajdonképpen hogyan helyezhetőek párhuzamba a GDPR és Információs törvény személyes adat definíciójával. Válasz kerül arra is, hogy tulajdonképpen lehet-e személyes adatot gyűjteni így? Végezetül a közösségi médiában követendő kiberhigéniás lépéseket fogalmazom meg (csak szükséges adatok

megosztása, opcionális adatok mellőzése, követhetőségünket csökkentő lépések, IoT eszközök kapcsolata).

II. Mi minősül nyílt információnak?

- A közösségi média vonatkozásában a kérdéskör tágabb:
  - Hiszen hozzájárulásunkkal teszünk fel személyes adatot publikussá azaz nyílttá:
    - Teljes nevünk
    - Aktuális képünk
    - Munkahelyünk
    - + egyéb más közösségi kontent:
      - Tartózkodási hely
      - Státusz, állapot
      - Érzelmek
      - Szentiment
- Ezen adatok feldolgozásra kerülnek, és reklám formájában eljut a „fogyasztóhoz” azaz a felhasználóhoz

III. Személyes adat jogszabályi vonatkozása

- GDPR alapján:
  - „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható
- Info törvény még tágabban kezeli:
  - személyes adat: az érintettre vonatkozó bármely információ;

IV. Lehetséges személyes adatot gyűjteni?

- GDPR szerint nem….
  - Felmerül a kérdés, hogy ez az oka a Meta (Facebook) kivonulásának?
- Info törvény szerint sem
- Technikailag nézve senki sem gyűjt személyes adatot
  - Ellenpéldának lásd:
    - Cambridge analytica, Cookie tracking incident, Vég-vég titkosítás kérdése
    - Felhasználói moderáció veszélye

V. Ön kiberhigénia közösségi média vonatkozásában

- Csakis a minimumra törekedjünk
  - Feltétlenül szükséges minden adatot megadnunk?
  - Szükséges a munkahely láthatósága? Más opcionális adatok (iskola, egyetem, érdeklődési kör)?
  - Követhetőségünk növekedésére figyelnünk kell
- IOT eszközökből eredő kihívások
  - A személyes adat köre kitágul ennek vonatkozásában


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
Köszönöm a figyelmet!
Kérdéseikre örömmel válaszolok!

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)