



EIVOK 11. Szakmai Fórum



KÖZÖSSÉGI HÁLÓZATOK ÉS KOCKÁZATAI

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



2019.10.03.
Budapest

A közösségi média

- „Internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom”
- Paradigmaváltás a tartalomelőállításban



Ngai et.al. Konceptuális keret

- Az első szint a közösségi médiával kapcsolatos elméletek, modelleket jelöli:
 - a magatartáselméletek (pl. személyiségjegyek, TAM modell);
 - a szociális tanuláselméletek (pl. társadalmi tőke, társadalmi identitás);
 - a tömegkommunikációs elméletek (példáraszociális kapcsolatok, használati- juttatási modell).

Ngai et.al. Konceptuális keret

- A második szint az a platformokat jelöli:
 - tartalommegosztó oldalak (pl. YouTube, Picasa);
 - közösségi könyvjelző oldalakat (pl. Pinterest);
 - blogokat, mikroblogokat (pl. Blogger.com, Twitter);
 - virtuális/ online közösségeket (pl. Lonely Planet, Yahoo Answer);
 - közösségi hálózatokat (pl. Facebook, LinkedIn);
 - virtuális világokat (pl. Second Life).

Ngai et.al. Konceptuális keret

- A harmadik szint az egyes alkalmazási területeket fedile, ami az előző szintek integrációjából valósul meg:
 - a marketing;
 - a tudásmegosztás;
 - az ügyfélkapcsolat menedzsment;
 - az együttműködésre vonatkozó tevékenységek;
 - a szervezeti kommunikáció;
 - az oktatás és képzés;
 - és az egyebek.

KIBERFENYEGETETTSÉGEK ÉS A KÖZÖSSÉGI MÉDIA



KÖZÖSSÉGI MÉDIA, MINT HADSZÍNTÉR



OPSEC és INFOSEC a SM-ban

CAREFUL ABOUT THAT FRIEND REQUEST!

*They might be working for
the enemy!*



PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

THINK BEFORE YOU POST!

Somebody could be watching!



PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!



- Home
- Add-Ons
- Domains & IP's
- Facebook**
- Favorites
- Intelligence
- Legal Cases & Ethics
- Photo Upload & Search Sites
- Privacy
- Social Networking

Useful Facebook Links

Much of the following was heavily inspired by and put together with assistance from Michael Bazzell (www.inteltechniques.com), Henk van Ess (graph.tips), Bob Brasich (www.netbootcamp.org) and Paul Myers (www.researchclinic.net) who we are indebted to and are all worth checking out.

Facebook Law Enforcement Guide can be found [Here](#)



Facebook User Number	GO	(Places Visited)
Facebook User Number	GO	(Recent Places Visited)
Facebook User Number	GO	(Places Checked-In)
Facebook User Number	GO	(Places Liked)
Facebook User Number	GO	(Pages Liked)
Facebook User Number	GO	(Photos By User)
Facebook User Number	GO	(Photos Liked)
Facebook User Number	GO	(Photos Of -Tagged)
Facebook User Number	GO	(Photo Comments)
Facebook User Number	GO	(Apps Used)
Facebook User Number	GO	(Videos)
Facebook User Number	GO	(Videos Of User)
Facebook User Number	GO	(Videos By User)
Facebook User Number	GO	(Videos Liked)
Facebook User Number	GO	(Video Comments)
Facebook User Number	GO	(Future Event Invitations)
Facebook User Number	Year	GO (Events Invited)
Facebook User Number	Year	GO (Events Attended)
Facebook User Number	GO	(Posts by User)
Facebook User Number	Year	GO (Posts by Year)
Facebook User Number	GO	(Posts Tagged)
Facebook User Number	GO	(Posts Liked)
Facebook User Number	GO	(Employers)
Facebook User Number	GO	(Groups)
Facebook User Number	GO	(Co-Workers)
Facebook User Number	GO	(Friends)
Facebook User Number	GO	(Followers)
Facebook User Number	GO	(Relatives)
Facebook User Number	GO	(Friends' Likes)

Find your Facebook ID

To find your Facebook personal numeric ID for fb:admins, social plugins, and more, enter your **Facebook personal profile URL** below:

`https://www.facebook.com/YourProfileName`

Find numeric ID →

What's my personal profile URL?

Your Facebook personal profile URL is the the URL you get to when you click on your name in the upper left of the Facebook home page. It **should look** something like this:

- `https://www.facebook.com/JohnDoe`
- `https://m.facebook.com/sally.struthers`
- `https://www.facebook.com/profile.php?id=24353623`

Your personal profile **does not** look anything like these examples:

- `https://www.facebook.com`
 - `Sally Struthers`
-

mSIS LE: for law enforcement and public authorities

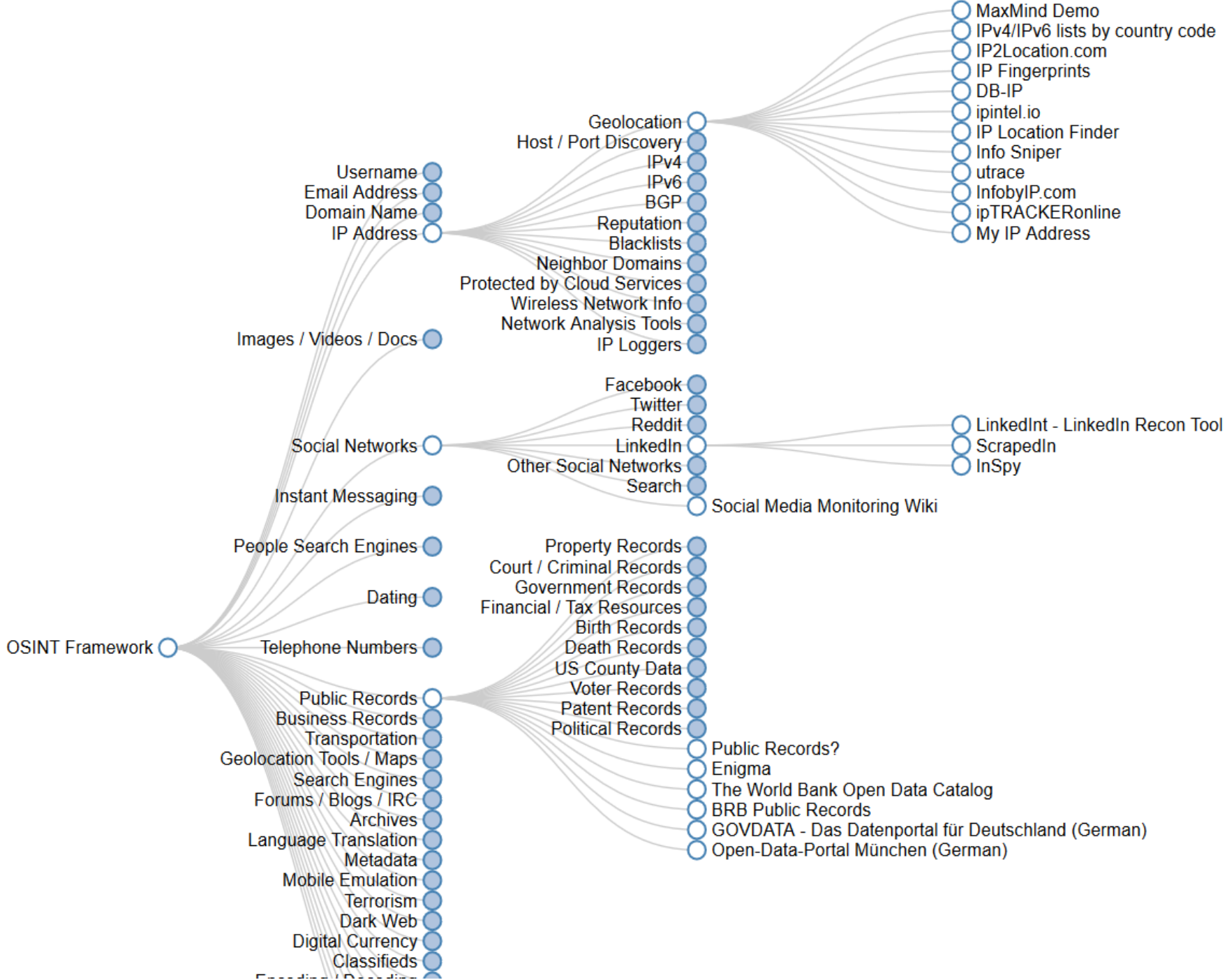
A premium solution designed specifically for, and supplied only to law enforcement

- LED / GDPR compliant
- Secure access control
- Advanced Search Tools
- Social Media Advanced Tools
- Evidence logged and hashed
- Expedited evidence management
- Exportable Audit Log
- Import & hash documents from any source
- Decision Log
- Deployment Log
- Unused material management
- Intelligence Grading (NIM 5x5x5, NIM 3x5x2, US Army & NATO)
- Editable Research Report in PDF, which is hashed
- Evidence Sheet in MS Word format, which is hashed
- Secure Case Bundle
- Disclosure feature
- Access proprietary databases



ORDER NOW

£400 +VAT
licence/year



KLE a SM-ban

- Elsősorban az általuk mindennap használt infokommunikációs eszközök védelméhez kapcsolódik.



CNO a SM-ban

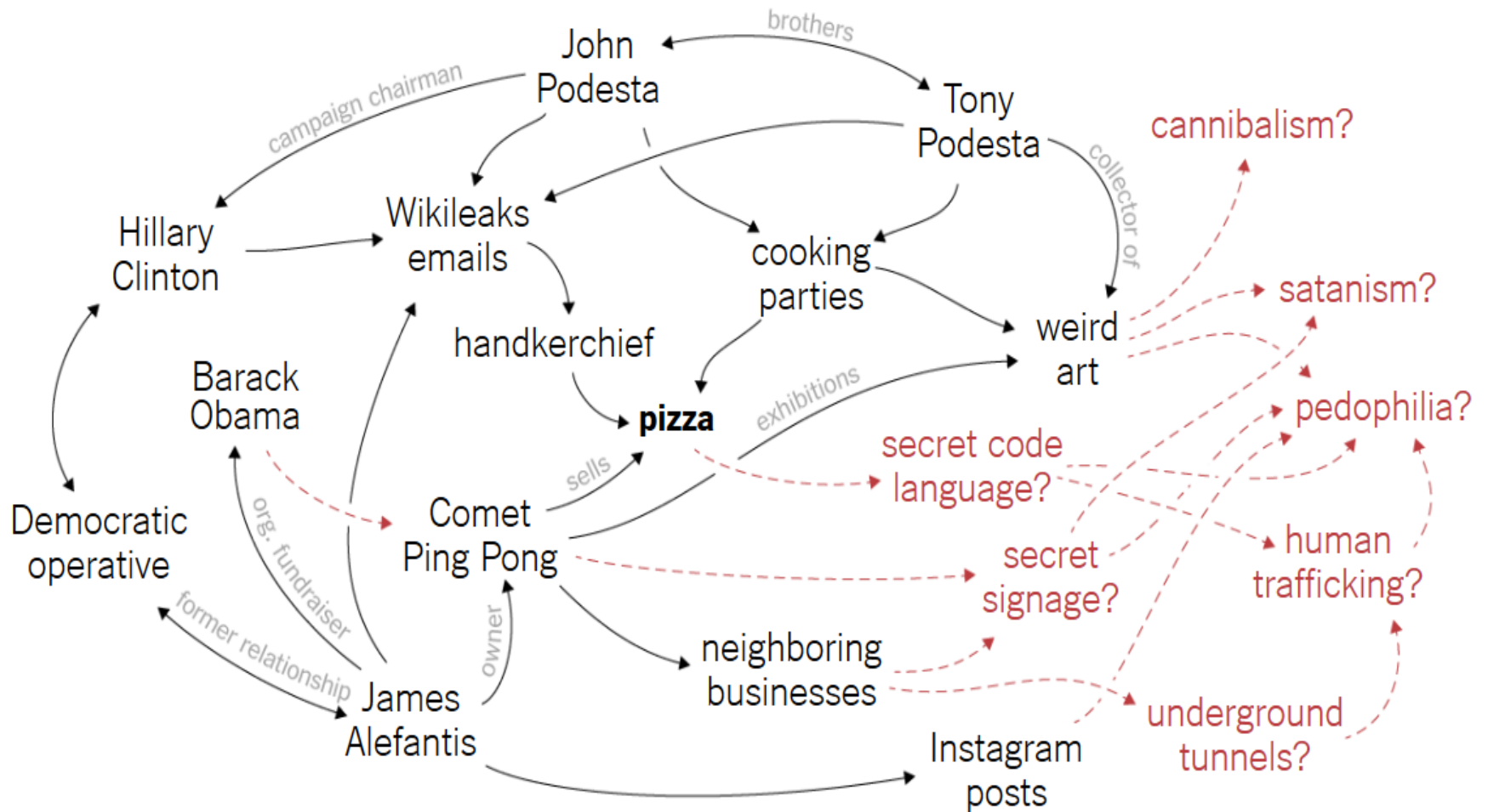
"Rayban Sunglasses Sale - Save 90% Payment Currency \$ € €
Latest Styles & Fast Shipping - Buy Now!"
<https://www.facebook.com/media/set/?set=a.1477134742572880.1073741828.100008291044264&type=1>
765483



A háború a politika folytatása, más eszközökkel



A szereplők



(deep)fake news

C:\Windows\system32\cmd.exe - C:\Users\Wlwe30\AppData\Local\Temp\lt.exe122020240720175740701516002407430 - C:\fake\model\Gf\

Loss: 0.0131192 0.0284258
Loss: 0.0133844 0.0297791
Loss: 0.0134255 0.0276863
Loss: 0.0141915 0.0294043
Loss: 0.0137763 0.0287212
Loss: 0.0137484 0.0266243
Loss: 0.0144165 0.0302228
Loss: 0.0140602 0.0293561
Loss: 0.0139947 0.0243249
Loss: 0.0142748 0.0277912
Loss: 0.0135723 0.0252593
Loss: 0.0138054 0.0273463
Loss: 0.0139144 0.0263917
Loss: 0.0139326 0.0282852
Loss: 0.0137718 0.028179
Loss: 0.013718 0.0267709
Loss: 0.0135604 0.0242651
Loss: 0.0131127 0.0265873
Loss: 0.0138906 0.0269189
Loss: 0.0135601 0.0249349
Loss: 0.0147892 0.0271665
Loss: 0.0142162 0.0300568
Loss: 0.0133938 0.0279701
Loss: 0.0142279 0.0283884
Loss: 0.0147165 0.0307378
Loss: 0.0134466 0.0280544
Loss: 0.013884 0.0288009
Loss: 0.0132272 0.0257779
Loss: 0.0138434 0.0271418

Training Preview



The image displays a terminal window on the left showing a list of 20 loss values, each consisting of two numbers separated by a space. On the right, a window titled 'Training Preview' shows a 10x10 grid of 100 generated face images. These images appear to be synthetic, showing a variety of facial features and expressions, likely generated by a deep learning model. The background of the slide features a faint, stylized floral pattern.

A Facebook szerepe a választásokban



KIBERBŰNÖZÉS ÉS KÖZÖSSÉGI MÉDIA



Malwarek

"Rayban Sunglasses Sale - Save 90% Payment Currency \$ € €
Latest Styles & Fast Shipping - Buy Now!"
<https://www.facebook.com/media/set/?set=a.1477134742572880.1073741828.100006291044264&type=1>
765483



Gyermekek szexuális kizsákmányolása



SOCIAL ENGINEERING



Emily Williams

- Aamir Lakhani és Joseph Muniz
- Facebook, LinkedIn
- „egy meg nem nevezett, a kiberbiztonság területén érdekelt amerikai kormányügynökség”



Online kommunikáció



Kibertér és a terrorizmus összefonódása



DAWN NEWS

GZ Productions - 04 settembre 2013

Notizie e riviste

Installa



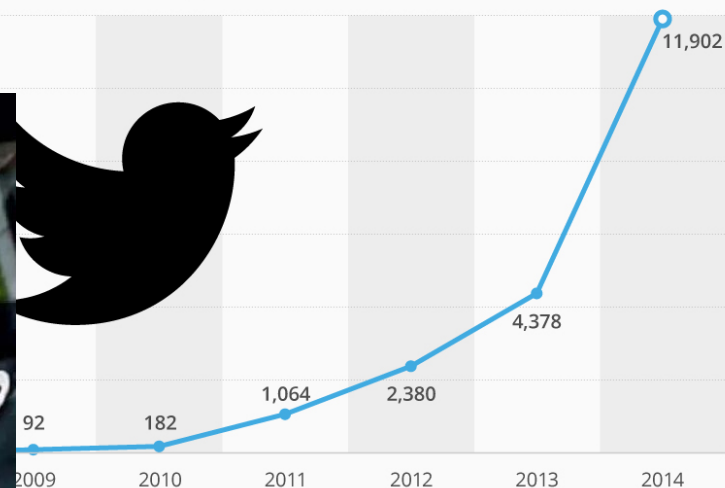
Aggiungi alla lista desideri

L'app è compatibile con tutti i tuoi dispositivi

★★★★☆ (71)

ISIS Is Expanding Its Reach On Twitter

Pro-ISIS Twitter accounts created by year



Brookings Institute

Forbes statista



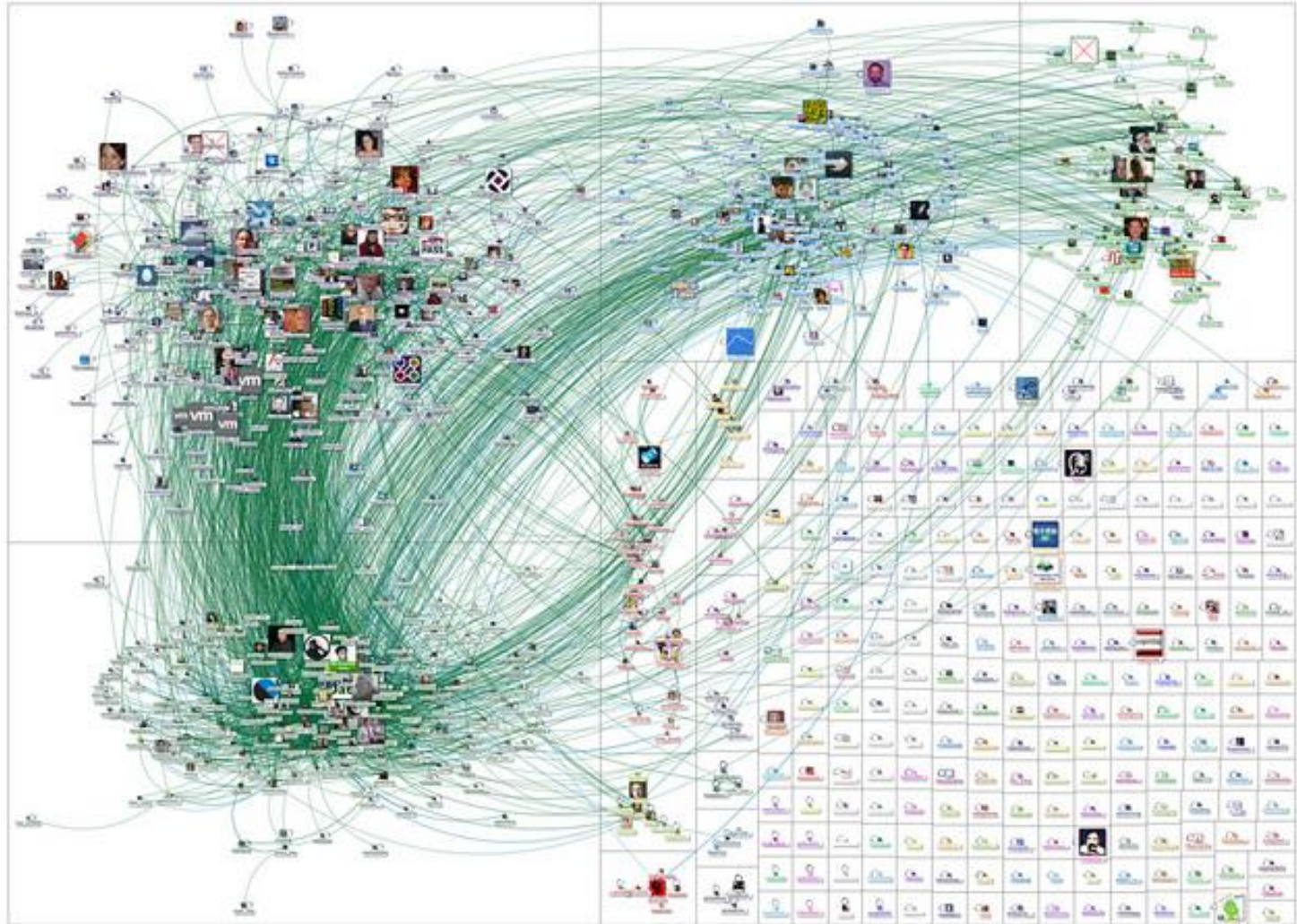
Darknet

- MIT LÁTNÁK A KÍVÁNCSI SZEMEK AZ ONLINE KOMMUNIKÁCIÓNKBÓL?
- CRIME AS A SERVICE



Internet of Things, Big Data, Clouds

Social media network connections among Twitter users



KÖZÖSSÉGI MÉDIA ÉS HACKTIVIZMUS





Garry Kasparov ✓
@Kasparov63

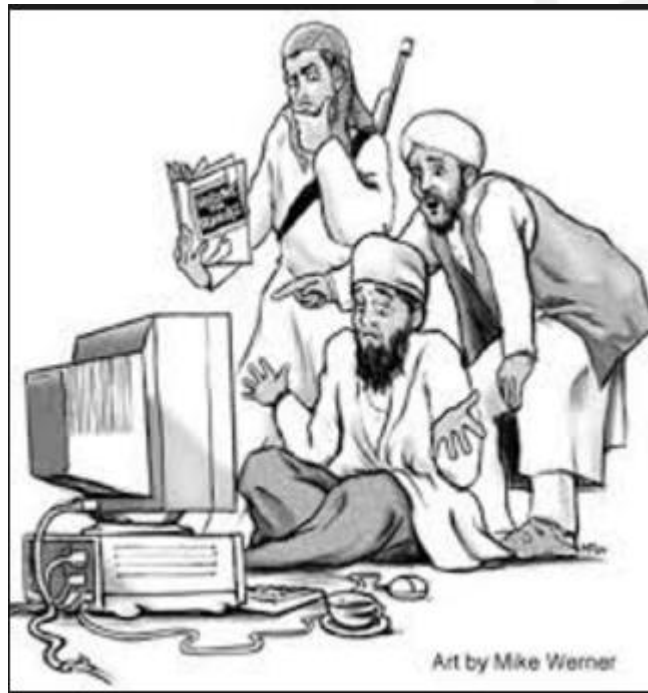
 **Follow**

Anyone can edit Wikipedia, but only the KGB can edit Wikileaks.

11:51 PM - 8 Oct 2016

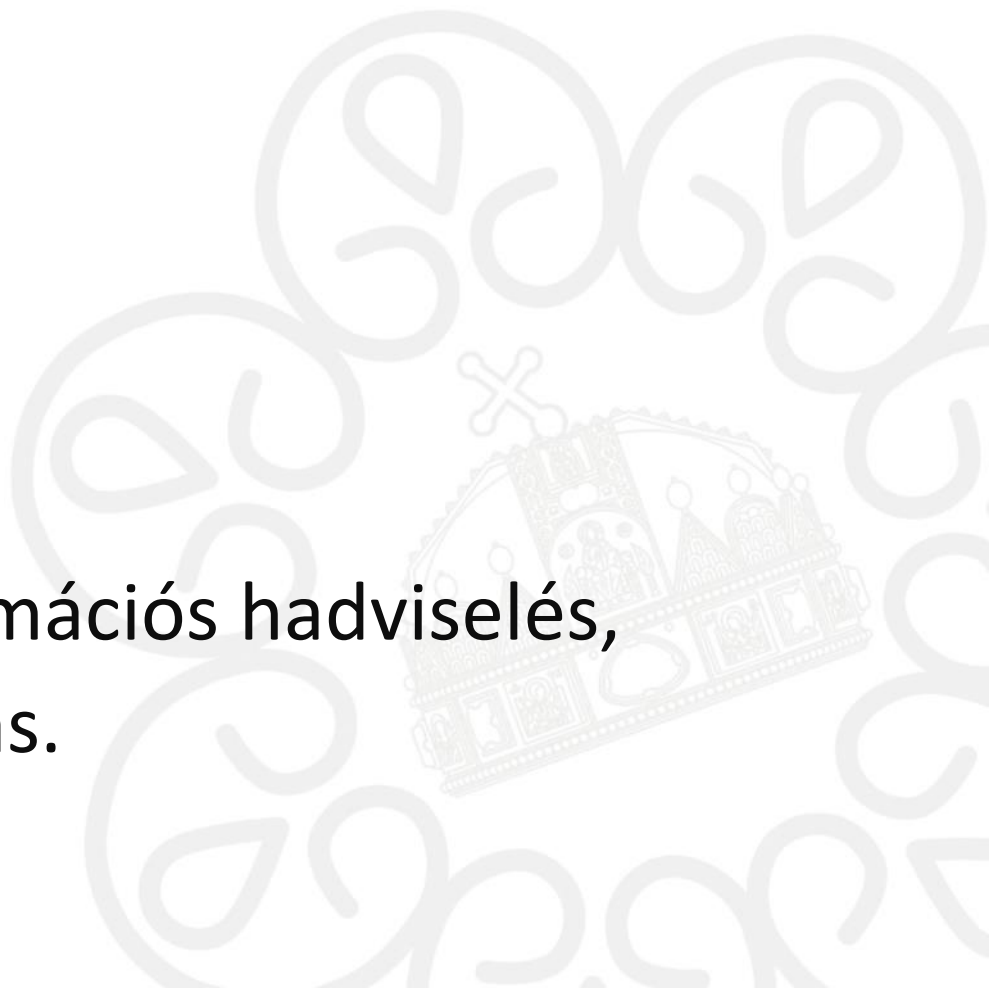
  1,927  2,795

KÖZÖSSÉGI MÉDIA ÉS KIBERTERRORIZMUS



Nincsenek még kiberterroristák, de...

- információgyűjtés,
- social engineering,
- kapcsolattartás,
- propaganda,
- új tagok toborzása,
- támogatók szerzése,
- pszichológiai és információs hadviselés,
- komplex kibertámadás.



KÖZÖSSÉGI MÉDIA ÉS KIBERKÉMKEDÉS



- Szereplők sokasága;
- magánszféra a digitális világban;
- Snowden.



Közösségi média a szervezetekben

- TTT?
- Eltérés a generációk között
- Biztonságtudatosság szintje
- Számos lehetőség a szervezetek esetében
- Munkaidő vs. Szabadidő
- BYOD



Aktív közösségi média jelenlét

SWOT	Pozitív oldal	Negatív oldal
Belső tényezők	Erősségek • Információk nyilvánosságra hozatalának ellenőrzött formája • Egységes arculat • Közvetlen és nyílt kommunikációs csatorna a társadalom felé	Gyengeségek • Információbiztonsági-tudatosság alacsony szintje • A közösségi média használatát érintő megfelelő kontrollok hiánya
Külső tényezők	Lehetőségek • Társadalmi megítélés javítása • Félrevezető információk és álhírek hatásainak csökkentése • A társadalmi feszültség és pánik megelőzése	Fenyegetések • Kritikus információk kiszivárgása • Műveleti biztonság sérülése • Szervezet társadalmi megítélésének romlása

Jogi paradoxonok

- Mtv
 - „**a munkavállaló a munkaviszony fennállása alatt** - kivéve, ha erre jogszabály feljogosítja - **nem tanúsíthat olyan magatartást, amellyel munkáltatója jogos gazdasági érdekeit veszélyeztetné. A munkavállaló munkaidején kívül sem tanúsíthat olyan magatartást, amely - különösen a munkavállaló munkakörének jellege, a munkáltató szervezetében elfoglalt helye alapján - közvetlenül és ténylegesen alkalmas munkáltatója jó hírnevének, jogos gazdasági érdekének vagy a munkaviszony céljának veszélyeztetésére.** A munkavállaló magatartása a 9. § (2) bekezdésében foglaltak szerint **korlátozható.** A korlátozásról a munkavállalót írásban előzetesen tájékoztatni kell.”
 - „**a munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti.** A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló **magánélete nem ellenőrizhető.** A munkáltató előzetesen **tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról,** amelyek a munkavállaló ellenőrzésére szolgálnak.”

Azonban

- NAIH
 - a jelentkező **előzetes tájékoztatása** a közösségi oldalainak vizsgálatáról;
 - **kizárólag a nyilvánosan elérhető adatokat** ismerheti meg a munkáltató, a korlátozottan nyilvános adatokat nem nézheti meg. Korlátozottan nyilvános adat például, ha az érintett egy zárt csoport tagja, és ebben a zárt csoportban oszt meg tartalmat. A munkáltató ilyen esetben nem kérhet meg senkit, aki ennek a zárt csoportnak a tagja, hogy számára információkat osszon meg az érintett tevékenységéről;
 - a munkáltató **csak azokat a nyilvános adatokat vizsgálhatja, amelyek a pályázattal, a munkakör betöltésével kapcsolatosak.** Ebbe a körbe azonban nem tartozhat bele a magánélettel, párkapcsolattal, vallással összefüggő adatok megismerése.

Sajátosságok

- Hivatásos egyének esetében Hjt, Hszt, különböző utasítások (pl. 11/2015. (VII. 10.) ORFK utasítás)
- Korlátozások
- Technológiai fejlődést nem tudja követni a jogszabály
- PET

Lehetőségek hivatali használatra

- Szervezet pozitív percepcionálása,
- Kapcsolattartás ügyfelekkel,
- Tájékoztatás,
- Kríziskommunikáció,
- E-kognokrácia,
- Belső kommunikációs csatorna,
- E-learning munkatársaknak
-



Azonban...!

- Közösségi hálózatok használatának általános kockázatai:
 - alacsony privacy-érzékenységű környezet,
 - nem felügyelhető ismeretlen helyen lévő szerveren tárolt adat,
 - nem kívánt információmegosztást eredményező alapértelmezett beállítások,
 - metaadatok,
 - mások által közzétett információk alapján tehető következtetések,
 - nehezen átlátható/befolyásolható jogosultsági rendszer (pl. oldalak esetében),
 - vonzó támadási célpont, social engineering, identity theft

...

- Közösségi hálózatok használatának adatvédelmi jogi kérdései
 - fiók vs jogi személyazonosság,
 - szerzői jogvédelem,
 - korlátozott információs önrendelkezés,
 - akár eltérő jogrendszer szerinti tágra nyitott EULA-k

...

- Közösségi hálózatok vegyes célú használatának kockázatai
 - hivatali és magáncélú felhasználása egyazon fióknak,
 - téves információtovábbítás/-kezelés,
 - magánfiók kompromittálódása a hivatali fiókot is kompromittálhatja,
 - nagyobb social engineering támadási felület

Használjuk-e a hivatalban?

- átfogó kockázatelemzést kell készíteni
 - használhatók saját vagy a NEIH által javasolt módszertanok, de azok kiválasztását mindenképp hozzá kell igazítani a szervezet célkitűzéseire és lehetőségeire
 - közösségi média állandóan változik, a modellnek követnie kell
 - Ahhoz, hogy fel tudjuk mérni a lehetséges kockázatokat elsőként fel kell mérnünk, hogy a védendő vagyonelemek közül melyek azok, amiket érinthetik a közösségi hálózatok irányából származó fenyegetések
 - milyen jellegű információkat érinthet

Fenyegetések

Fenyegetési kategória	Fenyegetés	Fenyegetés leírása
Technikai és eszközalapú fenyegetések	Sérülékenységek kihasználása	Szoftveres sérülékenységek kihasználása, melyek lehetővé teszik az eszközök feltörését és az érzékeny adatokhoz való illetéktelen hozzáférést
A szervezet megítélését érintő fenyegetések	A szervezet közösségi média oldalainak eltérítése	A támadók valamilyen módszert felhasználva illetéktelen hozzáférést szereznek a szervezet közösségi média profiljaihoz, ahol olyan információkat tehetnek közzé, amik rombolják a társadalmi megítélést. Emellett a szervezet megítélését rombolhatják az ál-csoportok nevében közzétett félrevezető információk, amik a gyanútlan felhasználókat megtéveszthetik és pánikot kelthetnek.
	A szervezetet érintő hamis vagy rosszindulatú információk közzététele	A szervezetet lejárató információk nyilvánosságra hozása a közösségi hálózatokon. Ezek gyakran valamilyen szervezett dezinformációs vagy propagandahadjárat részeként kerülnek végrehajtásra

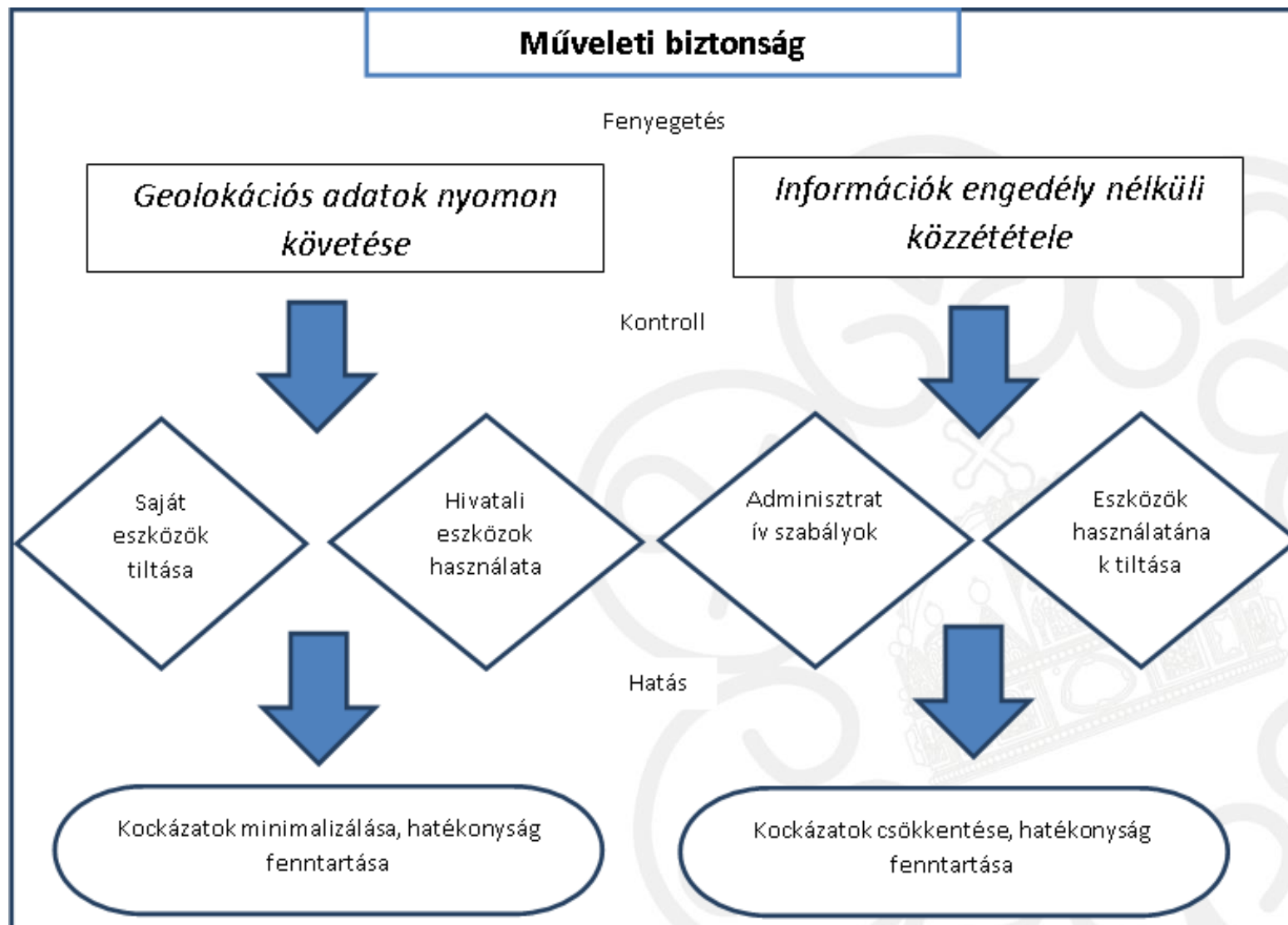
Fenyegetések

Fenyegetési kategória	Fenyegetés	Fenyegetés leírása
A munkavállalókat érintő fenyegetések	Social engineering támadások	A közösségi médián keresztül a támadók könnyen kapcsolatba tudnak lépni a munkavállalóval, a hiszékenységet kihasználva pedig különböző támadások valósíthatók meg. Ezek segítségével illetéktelen hozzáférést szereznek a munkavállalók közösségi média profiljaihoz, ahol érzékeny információkhoz férhetnek hozzá. Kiemelt figyelmet kell fordítani a különböző online levelezőkliensekre, melyek gyakran össze vannak kötve a közösségi média profilokkal.
	OSINT-alapú információgyűjtés	A szervezetre vonatkozó információk összegyűjtése, az egyre bővülő OSINT módszerekkel. A közösségi média jól használható a munkavállalók kilétének megállapítására és a rájuk, valamint a szervezetre vonatkozó információk összegyűjtésére
	A szervezetet érintő információk szándékos kiszivárogtatása	A munkavállaló által hozzáférhető érzékeny belső információk tudatos kiszivárogtatása a közösségi médiában, ami rombolhatja a szervezet jó hírnevét és társadalmi megítélését

Fenyegetések

Fenyegetési kategória	Fenyegetés	Fenyegetés leírása
A műveleti biztonságot érintő fenyegetések	Bejegyzések, képek és videók engedély nélküli közzétele a közösségi médiában	Az állomány tagjai előzetes engedély nélkül tesznek közzé információkat egy művelet végrehajtása során, mellyel veszélyeztetik a műveleti biztonságot
	Geolokációs adatok nyomon követése	A bekapcsolt eszközökön futó közösségi média alkalmazások által gyűjtött geolokációs adatok nyomon követése. Mindez jelentősen kihathat a műveleti biztonságra

A műveleti biztonságot érintő kockázatok kezelése



KÖSZÖNÖM A MEGTISZTELŐ FIGYELMET!

- Kérdés?
- Banyasz.peter@uni-nke.hu