Az információs rendszerek megsértésének esetei, motivációi és szabályozási perspektívái

VARGA ÁRPÁD
NEMZETI MÉDIA- ÉS HÍRKÖZLÉSI HATÓSÁG
ELTE ÁLLAM- ÉS JOGTUDOMÁNYI KAR

A hazai informatikai bűnözés

Kibertérhez kapcsolódó bűnözés

- Online csalás
- Zaklatás
- Cyberbullying
- Gyermekpornográfia készítése, terjesztése stb.

Kibertér függő bűnözés

- Behatolás sérülékenység feltárásával/kihasználásával
- Weboldal tartalmának felülírása (web defacement)
- Informatikai rendszerek irányításának átvétele, adatmentés
- Kártékony szoftverek készítése és alkalmazása
- Szolgáltatásmegtagadással járó támadások (Dos, DDoS)

Marleen Weulen Kranenbarg: Cyber-offenders versus traditional offenders: An empirical comparison. Netherlands, Vrije Universiteit, 2018. (Doctoral dissertation)

Jogszabályi környezet (Btk. 423,424)

- Megsértés
- Kijátszás

- Belépés
- Jogosultsága kereteit túllépve vagy megsértve bent maradás

- Akadályozás
- Adat megváltoztatása, törlése, hozzáférhetetlenné tétele

Jelentős számú információs rendszert érint

Közérdekű üzem ellen

Mikor jogszerű vagy jogosulatlan a behatolás?

A rendszer tulajdonosa által engedélyezett

Szerződéses viszony áll fenn

A rendszer nem rendelkezik védelemmel (open access)

Engedély és szerződés nélkül

A szerződés kereteinek megsértésével, vagy a jogosultság kereteit túllépve

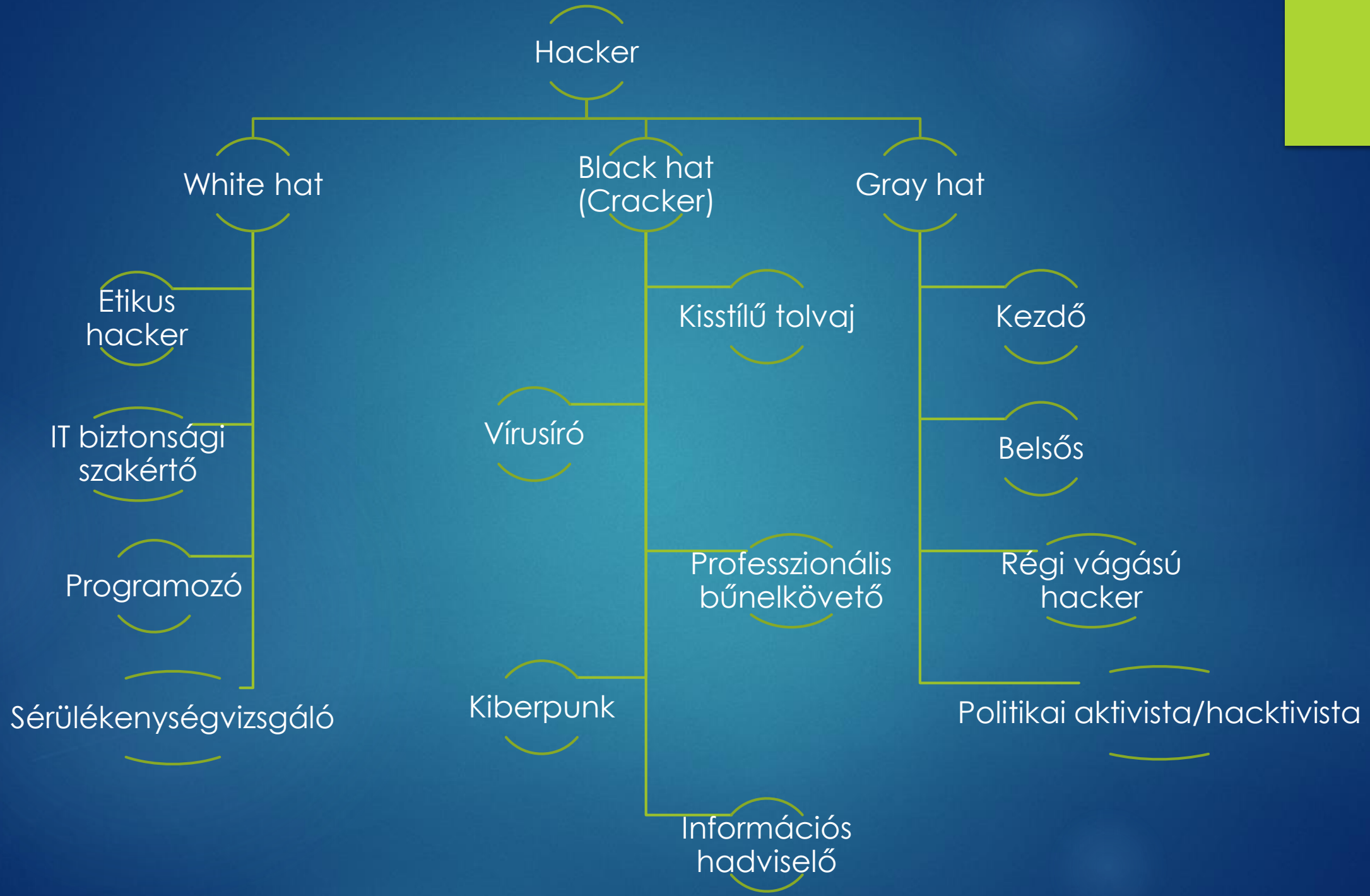
Önszorgalomból

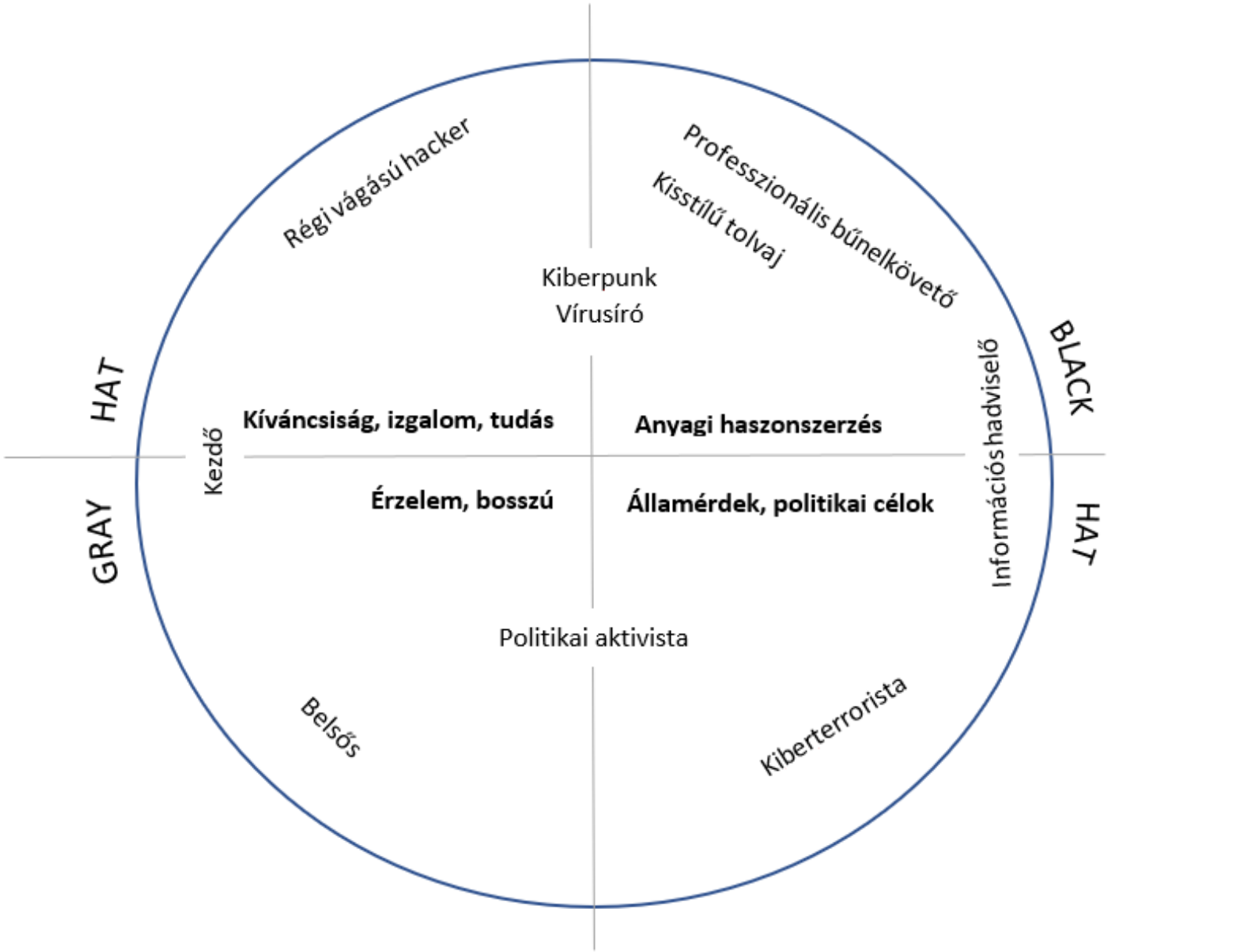
Kártékony céllal

Az etikus hacking feltételei:

David-Olivier Jaquet-Chiffelle and Michele Loi: Ethical and Unethical Hacking, In: The Ethics of Cybersecurity i.m. 179–204.

A behatolást végzők kriminológiai csoportosítása és fogalmai





Az informatikai bűnözés motivációs hálója

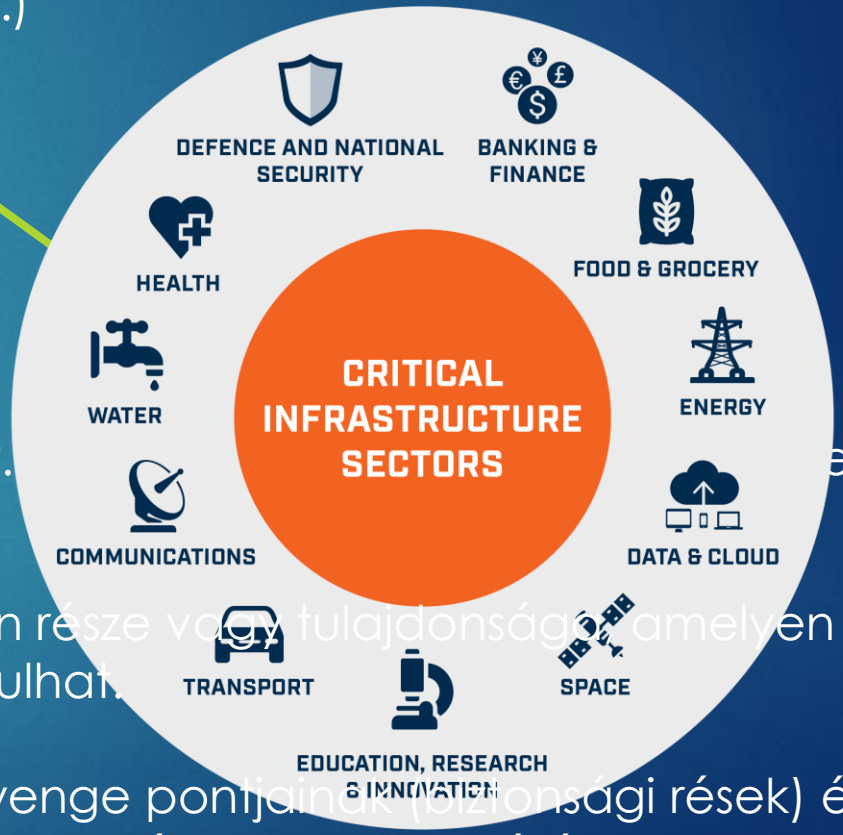
A tesztelés iránya szerint eltérő szabályok és védelmi szint:

Létfontosságú rendszerek sérülékenységvizsgálata

2013. évi L. törvény (Ibtv.)

Közszolgálati szervek

2012. elemek



Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.

Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.

Szabályozási kérdések

Nemzeti Kibervédelmi Intézet vizsgálata (Ibtv. – jogszabály engedélye)

Szerződéses sérülékenységvizsgálat (sértetti beleegyezés)

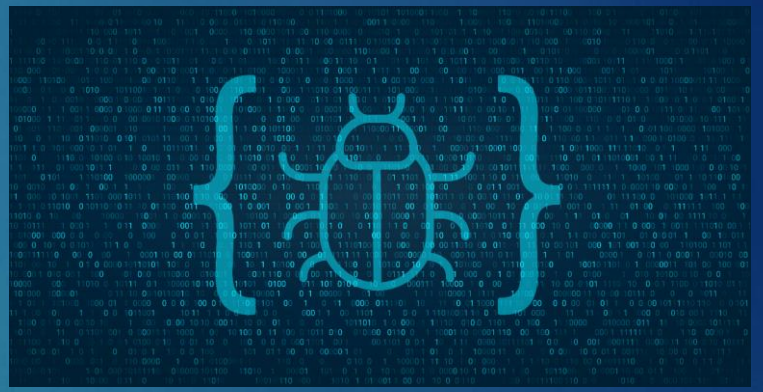
Minden más esetben:

Materiális jogellenesség

Társadalomra veszélyesség (biztonsági esemény)

Lehetséges megoldások

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



ENISA – CVD Policy ajánlás

- Támogatja a nemzeti CVD irányelvek kialakítását (2022)

Egy olyan keretrendszer, amelyben a biztonsági kutatók számára lehetővé teszik és bátorítják az IKT-termékek és -szolgáltatások kutatását bizonyos szabályok betartásával.

Feltéve, ha minden talált sebezhetőséget jelentenek a nemzeti hatóságoknak vagy a termék forgalmazójának.

A nemzeti CVD-politika segít növelni a kiberbiztonság és az átláthatóság általános szintjét a bevezető országban. Segít a bizalom kiépítésében és növeli az IKT-szolgáltatásokba és –termékekbe vetett bizalmat.

- NIS2 – European Vulnerability Database

CVD irányelvek Európában

- Rendelkezik CVD irányelvvel: Hollandia, Franciaország, Belgium, és Litvánia
- Implementáció folyamatban: Dánia, Németország, Lettország és Portugália
- A NIS 2 részeként kívánja bevezetni: Olaszország és Ausztria

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

CENTRE FOR
CYBER SECURITY
BELGIUM

Litvánia

- 2021 június – Law on Cyber Security

- A kommunikáció integritása, és a rendszer működése nem sérülhet
- A sérülékenység felfedezését követően a folyamat azonnali felfüggesztésre kerül
- A keresést követő 24 órán belül jelentés az NCSC-nek, a Védelmi minisztériumnak, vagy a CSE-nek
- A koordinátor kihagyásával is lehet a szoftver gyártója felé jelzést tenni
- Az adatok ellenőrzésének, mentésének, rögzítésének, elemzésének, tárolásának, másolásának, törlésének, megsértésének, módosításának tilalma
- A belépés során nem történhet jelszópróbálgatás, illegálisan, vagy social engineering által megszerzett jelszavak nem használhatók
- Sérülékenység jelentést a fenti szervek kaphatnak, nincs nyilvánosságra hozatal
- Szoftverek esetén jelzést tehet az NCSC, de nem kötelezhet

Kétségek

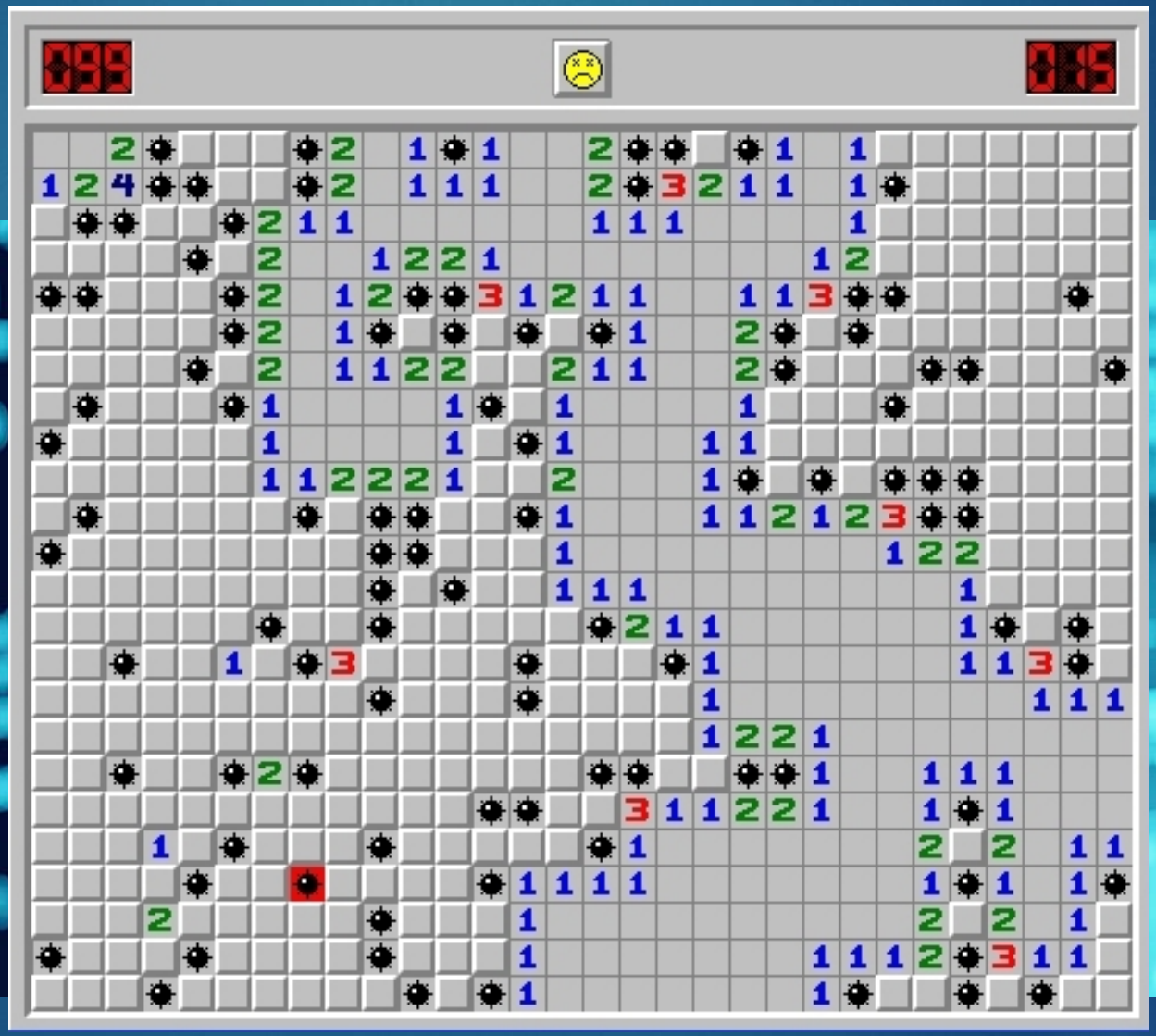
Motivációból eredő szociológiai kriminológiai problémák (neutralizáció, sodródás, differenciális asszociáció)

Büntetőjogi garanciarendszer felpuhításának kockázata (társadalomra veszélyesség, büntetőeljárási nehézségek, generális prevenció)

Adatvédelmi garanciák (adatvédelmi incidens bejelentés, személyes adatok védelme, adatbiztonsághoz való jog)

Információbiztonsági kockázatok, NIS Irányelv szerinti bejelentési gyakorlatok kérdése

ÖSSZEFOGLALVA



Felhasznált szakirodalom

- Ambrus István: Digitalizáció és büntetőjog, Wolters Kluwer, Budapest, 2021.
- David-Olivier Jaquet-Chiffelle and Michele Loi: Ethical and Unethical Hacking, In: The Ethics of Cybersecurity.
- ENISA: Coordinated Vulnerability Disclosure Policies in the EU https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu
- Krasznay Csaba, Dobos László, Palla Gergely, Pollner Péter: Információbiztonsági incidensek a közigazgatásban In: Auer, Ádám; Joó, Tamás Hálózatok a közszolgálatban. Budapest, Magyarország : Ludovika Egyetemi Kiadó (2019) 247 p. pp. 135-154. , 20 p.
- Marleen Weulen KRANENBARG: Cyber-offenders versus traditional offenders: An empirical comparison. Netherlands, Vrije Universiteit, 2018. (Doctoral dissertation)
- Mezei Kitti: Az információs rendszer vagy adat megsértése a bírói gyakorlat tükrében Kúriai Döntések: Bírósági Határozatok: A kúria lapja 70 : 4 pp. 618-625. , 8 p. (2022)
- Mezei Kitti: A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban Rendőrségi Tanulmányok 3 : 2 pp. 23-43. , 21 p. (2020)
- Sorbán, Kinga: Vírusok és zombik a büntetőjogban: Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései In Medias Res: Folyóirat a Sajtószabadságról és a Médiaszabályozásról 7:2 pp. 369-386. , 18 p. (2018)
- Szathmáry Zoltán: Etikus és nem etikus hacking - a kéretlen sérülékenységvizsgálat büntetőjogi kérdései Magyar Jog 67 : 6 pp. 340-346. , 7 p. (2020)

Köszönöm a megtisztelő figyelmet!

varga.arpad@mtmi.hu