ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

HABILITÁCIÓS TÉZISFÜZET

DR. KOLLÁR CSABA (TUDOMÁNYOS FŐMUNKATÁRS)

A digitális kor társadalmi vetületeinek és gazdasági hatásainak vizsgálata az ember-robot interakció, az információbiztonság és az információbiztonság-tudatosság fejlesztésének fókuszában

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2022. október hónap 15. nap

TARTALOMJEGYZÉK

I. A KUTATÁS ELŐZMÉNYEI

A kommunikációval, a médiával és az elektronikával 1989 óta, velük párhuzamosan a biztonsággal 1991 óta, az informatikával pedig 1996 óta foglalkozom kisebb-nagyobb megszakításokkal. Az elmúlt évtizedekben figyelemmel kísértem azokat a műszaki, informatikai, technikai, illetve társadalmi és szervezeti változásokat, melyek egymásra hatva alakították ki és hozták létre jelenkorunkat, a digitális kort.

Szak- és diplomadolgozataim egy részénél, valamint doktori disszertációmban – mely a fogyasztói csoportkultúrát vizsgálta az információs társadalomban – is hangsúlyosan foglalkoztam azzal a kérdéssel, hogy a technikai eszközök (kiemelten az infokommunikációs eszközök) és azok használata milyen mértékben és irányba alakítják a társadalom fejlődését. Akkor, 2007-ben a következőket állapítottam meg:

(1) Az információs társadalomhoz való tartozás alapja az, hogy az egyén rendelkezzen és használja is az infokommunikációs eszközöket. Amennyiben ezt nem teszi meg (mert erre nincs lehetősége, vagy mert nem ismeri az eszköz és a rajta futó alkalmazások működését), akkor nem tud hozzáférni a digitális tartalmakhoz és javakhoz, s így egyre inkább nő a szakadék közötte és az eszközhasználók között. E folyamat a **digitális esélyegyenlőtlenség**hez vezet, melynek egyértelmű nyertesi az infokommunikációs eszközhasználók.

(2) Az infokommunikációs eszközök használata alapjaiban változtatja meg az egyén médiafogyasztási szokásait és a világról alkotott képét. Mivel a média, mint a negyedik hatalmi ág már az információs

társadalom előtti időkben is nagy hatással bírt a társadalmi gondolkodásmódra és az értékrend alakulására, ez a hatás az infokommunikációs eszközök megjelenésével és elterjedésével, valamint az eszközök által közvetített (média)tartalmak fogyasztási idejének a növekedésével még dominánsabban jelenik meg. A társadalom polgárainak többsége gyakorlatilag **azt hiszi el, amit az interneten lát**.

(3) Az infokommunikációs társadalom polgára számára már nem az információ megszerzése okoz gondot, hanem az, hogy hogyan, milyen módszerekkel tudja minél gyorsabban kiválasztani és/vagy kiszűrni a nagyon erős médiazaj és információs zaj közepette a számára megfelelő adatokat, információkat, s ezekből hogyan tud (ha egyáltalán tud) konkluzív jelleggel tudást, mégpedig releváns tudást képezni, és így megfelelően megalapozott döntést hozni. Ez újfajta viselkedésre sarkallja (3), illetve a médiatartalom-előállítók is újfajta módszereket kell, hogy használjanak a vele folytatott kommunikációban (4), amelyek együttesen a médiatartalmak és az online szolgáltatások **személyre szabhatóság**ában jelennek meg.

(4) A vezetékes és vezeték nélküli infokommunikációs eszközökkel a hálózatba „kötött” ember annak érdekében, hogy optimalizálja, kényelmesebbé és hatékonyabbá tegye az életét, szükségszerűen kilép a hagyományos világban gyakran anonim, szürke tömegmasszaszerű létéből, s „arcot ad” online tevékenységeinek, vagyis nem csak használja az online elérhető tartalmakat és erőforrásokat, hanem azok többségénél **regisztrál**.

(5) A regisztráció során rögzített statikus adatok, illetve az online erőforrás használata során keletkező dinamikus (időfüggő) adatok elemzésre révén az erőforrások marketingesei egyfelől a személy adott platformon tanúsított aktivitásait meglehetősen alaposan képesek elemezni, s így perszonalizált, személyre szabott tartalmakat és szolgáltatásokat tudnak az adott felhasználó számára kínálni. Másfelől az egyén aktivitásai folyamatosan összehasonlíthatók más egyének aktivitásaival, így megvalósítva a klasszikus klaszterizációnál sokkal hatékonyabb módszert, a **dinamikus klaszterizáció**t.

A doktori disszertációmban ismertetett kutatási eredményeimet így tudom összegezni:
Az infokommunikációs eszközökön futó tartalmak fogyasztási és az alkalmazások használati idejének drasztikus növekedésével párhuzamosan növekszik a média egyénre gyakorolt hatása (**médiaszocializáció**), a regisztráció révén csökken, illetve sok esetben **megszűnik a privát szféra**, a szervezetek az egyénről sok, s mennyiségében **folyamatosan növekvő adat**tal rendelkeznek. Ezek a folyamatok összességében nem csak az egyénről, hanem a szervezetekről, illetve általánosságban a környezetünkből származó/szóló adatok és a belőlük képzett információk és tudásjavak felértékelődéséhez vezetnek, ami elvezet minket az adatokra alapozott **digitális kor**ba.

Az elmúlt másfél évtizedben a digitális kor társadalmi vetületeivel és gazdasági hatásaival foglalkoztam, s tudományos érdeklődésem

fókuszába az információbiztonság emberi oldala, a biztonságtudatosság fejlesztése, az ember-robot interakció humán aspektusa, a mesterséges intelligencia, illetve a mesterséges intelligencia bizonyos léptékeire épülő fejlesztések és megoldások (domotika rendszerek, okosvárosok, társadalmi értékelő rendszerek) kerültek. Tézisfüzetem hipotéziseinél, azok tárgyalásánál, majd konkluzív jelleggel téziseim megfogalmazásánál is elsősorban az ezeken a területeken elért eredményeimet kívánom bemutatni.

II. ÚJ TUDOMÁNYOS EREDMÉNYEK

Első témakör. Az emberek munkáját cyber őrangyalok/titkárnők segítik, „akik" megszervezik a találkozókat, könnyebbé és kényelmesebbé teszik az életet, illetve a közeli jövőben a munkacsoport (virtuális) tagjaként aktív szerepet vállalnak a különböző munkafolyamatok hatékony végzésében. Bizonytalanná válik a kommunikációs folyamatban részt vevő szereplők azonossága, mivel egyre inkább elmosódik az ember-gép közötti különbség. Ha a fizikai életünket sivárnak érezzük, számtalan, digitális élményt nyújtó, 3D-s világban tehetjük érdekessé és élvezetessé. A korábban említett „always on" világméretű elterjedése révén elmosódik a határ a nyilvános és az intim/privát szféra között (pl.: ha valaki látja, hogy a Facebookon éjszaka még posztolok, bátran ír egy privát üzenetet nekem). Az ember egyre furcsább érzéseket kezd el táplálni a digitális családtagja iránt. Ha a családtag android, tehát emberszerű robot, akkor könnyen megkedveli, s egyfajta családtagként tekint rá. Az „emberi"

kapcsolatokban egyre inkább csökken az igény az ember-ember kapcsolatra, különösen, hogy egyre több esetben nem is lehet tudni, hogy a „vonal” másik végén emberrel, vagy géppel kommunikálunk-e (ezzel a témával még bővebben foglalkozom később). A kultúra előtt a megsokszorozott világok (virtuális világok) révén végtelen lehetőségek állnak, különösen a digitális művészi értékek előállítása, e folyamat interaktívvá tétele, megosztása, feldolgozása, stb. területén. A szocializációban ugyancsak elképzelhetetlen távlatok nyílnak meg. Kérdéses, hogy a gyermekek fejlődésére milyen hatást gyakorolnak az őket nevelő/szocializáló, velük a szüleiknél is többet foglalkozó androidok. A digitális szocializáció másik fontos kérdése, hogy a bejelentkezésünk után minket folyamatosan monitorozó alkalmazások mennyire akarnak/tudnak a számunkra egy kedves, hízelgő, de hamis világot nyújtani a személyünkre szabott tartalmak révén.

Második témakör. A munka világában úgyszintén radikális változások várhatóak, illetve már most is vannak. Az embernél okosabb/intelligensebb (gépi intelligencia) gépek megjelenése révén már nem az ember irányítja/vezérli a gépet, hanem fordítva. A gép jobb és átgondoltabb döntéseket tud hozni, mint az ember, s ami algoritmizálható, abban messze felülmúlja már most az android (robot) az embert. Újragondolva merül fel a klasszikus kérdés: mi dolgunk van a (digitális) világban ezek után. Számtalan szakma tűnik el végérvényesen, hogy átadja helyét a rendszerint informatikához köthető új szakmáknak, szakterületeknek. A szakmák oktatása is merőben megváltozik. Az oktatás helyett/mellett sokkal

inkább a tudásszervezés lép előtérbe. Minden szükséges információ megtalálható a hálón, a kérdés az, hogy hogyan lehet ezekből nem feltétlenül emberi segítséggel meg- illetve összeszervezni egy (új) szakma korszerű, s viszonylag gyorsan elsajátítható ismeretanyagát. A tanulás (igaz, nem a hagyományos módon) egy valóban élethosszig tartó folyamat lesz azok számára, akik piacképesek kívánnak maradni a munkaerőpiacon. A média gyakorlatilag konvergálódik 2020 környékére. A tartalmak minden platformon megjelennek, egymást erősíthetik, kiegészíthetik. A képernyőmérettől (telefon, tablet, laptop, monitor, TV) függetlenül olvashatjuk, nézhetjük, hallgathatjuk valós időben a tartalmakat, bár az már most megfigyelhető, hogy a képernyő mérete lesz az, amelyik alapján bizonyos médiafogyasztási szokások kialakulnak. A társadalmi folyamatok egyik érdekes és újszerű vetülete a digitális állampolgárság megjelenése, s ezzel kapcsolatban a fizikai országhatárok kérdése. A digitális állampolgárság több szinten, s az egyes szinteken számos funkcióban valósítható meg. A legegyszerűbb az állampolgári ügyek elektronikus intézése. Erre már számos példa látható Magyarországon is, igaz a megoldások egy részénél még a papír alapú, s kézzel aláírt dokumentumok beszkennelése, majd e-mailben, vagy webes felületen történő beküldése a gyakorlat. Egy másik megoldás, amikor a többféle okmányt (pl.: személyi igazolvány, lakcímkártya, TAJ-kártya, adókártya, jogosítvány) egy bankkártya méretű, digitális adatokat is tartalmazó okmánnyal váltanak ki. A kérdés, hogy a rendszer képes-e valamennyi okiratot ebbe az egybe integrálni, vagy csak a meghatározott körbe tartozó okmányokat. Egy harmadik – s jelenleg a legmodernebbnek számító – megoldás a

lettországi példa. Lettország amellett, hogy már több éve bevezette az egyokmányos rendszert a közigazgatás területén, elindította a digitális állampolgárság programját is. Nem túl jelentős díj ellenében fizikai lakóhelytől függetlenül bárki Lettország digitális állampolgára lehet, s többet között így az ott lakókkal azonos feltételek mellett hozhat létre vállalkozást, illetve rá is ugyan azok az adószabályok vonatkoznak. A gazdasági életet a felhő alapú szolgáltatások, a big data analitika (nagyon sok adat elemzése, a mobil szolgáltatások és alkalmazások, a közösségi média dominanciája, a kiterjesztett és kevert valóságok, az IoT (dolgok internete), a robotok és a mesterséges intelligencia alapjaiban változtatják meg. Minden adat, így az üzleti, beszállítói, kereskedelmi, pénzügyi, valamint a fogyasztással kapcsolatos adatok a felhőbe költöznek (Cloud). Az adatok „felhősödése" mellett lehetőség van (Analitika – big data analytics) azok szofisztikált elemzésére, s az elemzés révén a fogyasztó teljes fogyasztói magatartásának a megrajzolására. A hatalmas mennyiségű adatot rövid időn belül feldolgozni képes szerverek és az azokon futó alkalmazások segítségével közel 100%-os mintavétel érhető el, közel 0%-os hiba mellett. Jelenkorunkban külön és hangsúlyosan érdemes szólni az adatok és információk védelméről és biztonságáról. Az adatok kora ugyanis magával hozza az adatok felértékelődését, s így gazdasági értékké válását. Olyan fogalmakkal találkozhatunk, mit adatvagyon, adatvédelem, adatleltár. A korábbi, akár csínytevésnek is minősíthető hackertámadások (pl.: kormányzati weboldalra meztelen női fotót, vagy trágár szöveget tesznek fel, megszerzik egy szervezet e-mailes

címlistáját, majd a címzetteknek hamis információkat küldenek) fajtái és indítékai is jelentősen megváltoztak.

Harmadik témakör. A leginkább Kevin Mitnick által fémjelzett (bár tézisfüzetemben több hasonló hackert is megnevezek) social engineering típusú támadások az ember alapvető pszichológiai jellemzőit veszik alapul, s a leggyengébb láncszem, az ember oldaláról közelítenek például az adatok illetéktelen megszerzéséhez, manipulálásához, törléséhez, a személyiség-klónozáshoz. A vállalat gazdasági és kommunikációs érdeke az, hogy ezeket a támadásokat is kivédje, munkavállalóit felkészítse az ilyen támadások felismerésére, a biztonságtudatosabb viselkedésre. Rendelkezésre állnak és a gyakorlatban is igazolták hasznosságukat olyan kommunikációs modellek (tézisfüzetemben Hymes modelljével foglalkozom), aminél a social engineering típusú támadások, illetve auditok hatékonyan elemezhetőek, s jobban lehet fókuszálni a személyközi kommunikáció információbiztonsági fókuszú fejlesztésére is.

A fentiek alapján téziseim a következő három területre vonatkoznak:

1. Az ember és a technikai környezet egymásra hatása az ember-robot interakció humán aspektusának vizsgálatán keresztül.
2. A digitális kor változásai és hatása a szervezetek életében, különösen az információbiztonság területén.
3. A kommunikációs modellek alkalmazhatósága az információbiztonság-tudatosság felmérésében és fejlesztésében.

Módszertani bevezetés

Tudományos pályafutásom során a hipotéziseim vizsgálatára egyaránt alkalmaztam kvalitatív, kvantitatív és egyéb technikákat (pl.: hálózatelemzés, játékelmélet), a természettudományos-műszaki mérés, kísérlettervezés és –kiértékelés módszereit, valamint különböző modelleket is. Az általános kutatásmódszertan, illetve több módszertan átfogó megismerésében többek között Earl Babbie, Éltető Ödön, Meszéna György, Naresh K. Malhotra, Paul A. Scipione, Tomcsányi Pál és Ziermann Margit, a kvalitatív technikákban Horváth Dóra, Klaus Krippendorff, Langer Katalin, Mitev Ariel, Roy Langmaid, Wendy Gondon, a műszaki, természettudományos területen pedig Aradi Petra, Czmerk András, Csermely Péter, Deák András, Finszter Ferenc, Gergely Pál, Halmai Attila, Harnos Andrea, Harold B. Maynard, Kemény Sándor, Koltay Tibor, Kunovszki Péter, Lakné Komka Kinga, M. Csizmadia Béla, Németh Zoltán, Reiczigel Jenő, Solymosi Norbert, Tóth János és Wenzelné Gerőfy Klára munkái segítettek. Az emberi társas- és csoportos kapcsolatok, valamint a döntéshozatal területén Forgó Ferenc, Ja I. Hurgin, Málik József Zoltán, Mérő László, Mészáros József, Molnár Sándor, Szép Jenő és Szidarovszky Ferenc, míg a kapcsolatok hálózati feltérképezésében Barabási Albert-László, Bódi-Schubert Anikó, Dobos Imre, Gelei Andrea, Mérei Ferenc, Szvetelszky Zsuzsanna művei voltak számomra az iránymutatók. A manipulációval, social engineeringgel, kommunikációs hadviseléssel kapcsolatos témáim kutatásának módszertani alapját többek között Em Griffin, Horányi Özséb és Szokolszky Ágnes írott, szerkesztett gondolatai jelentették. Egyéb módszertan tekintetében a következő szerzők

munkáit ismertem meg: Cseh-Szombathy László, Ferge Zsuzsa, Héra Gábor, Kindler József, Klein Sándor, Ligeti György, Moksony Ferenc, Nováky Erzsébet, Papp Ottó és Tibay György.

A kutatásmódszertannal foglalkozó szakirodalmak sorát én is szerettem volna gazdagítani néhány gondolatommal, így született meg szerzőtársaimmal közösen a Fogyasztói magatartás és várható trendek, különös tekintettel az e-banking-re című könyvfejezet, illetve egyszerzős munkaként a Reklám- és reklámszöveg kutatás című jegyzetem, A munkahelyi kiégés (burnout szindróma) elméleti megközelítése, kutatási irányai és közgazdaságtudományi aspektusa, valamint A szakértővé válás, illetve a szakértők kiválasztásának és megkérdezésének módszertani kihívásai című tanulmányom, valamint a 100%-os mintavétellel foglalkozó, A digitális marketing lehetőségei a kereskedelmi egységek gyakorlatában, és ennek pszichológiai aspektusai című könyvfejezetem, melyeket tézisfüzetem VI. fejezetében sorolok fel.

A következőkben az említett területeket (1) az adott kutatás előzményei, (2) a témaválasztás indoklása, (3) a kutatási célkitűzések és a téma körülhatárolása, (4) az alkalmazott kutatási módszerek ismertetése, (5) a következtetések, (6) a tézisek, illetve (7) az eredmények alkalmazási lehetőségei alpontok alapján ismertetem.

1. *Az ember és a technikai környezet egymásra hatása az ember-robot interakció humán aspektusának vizsgálatán keresztül.*

(1) Az adott kutatás előzményei

Megannyi filmben és könyvben olyan robotok voltak a főszereplők, amelyek kedvelhetők, szerethetők voltak, esetleg a néző a robot szerepével még azonosulni is tudott. A sci-fi (tudományos-fantasztikus), mint műfaj nagy hatást gyakorolt és gyakorol azokra a későbbi tudósokra és fejlesztőkre, akik gyermekkori film- és könyvélményeik alapján a fizikai világban is realizálni szeretnék a képernyőn látott, könyvben olvasott robotokról szóló elképzeléseket. A jövőkutatás, a minél nagyobb beválási valószínűségű predikciók fontosak a technikai fejlődés szempontjából, s talán a robotok és a mesterséges intelligencia az a terület, aminél a legnagyobb valószínűséggel lehet azt állítani, hogy ami a filmeken és a könyvekben bemutatásra kerül, az a jövőben valóság is lesz. Magam is sokat foglalkozom a tudományos-fantasztikus irodalom realizálódásával, s úgy gondolom, hogy az ember és a technikai környezet bemutatása a további témák ismertetésénél is jó alapot nyújthat.

Több előzetes kutatásomban foglalkoztam a jelenleg élő generációk (veteránok, babyboom, X, Y, Z, alfa) munkaerőpiaci helyzetével, illetve azzal, hogy a digitális eszközök (különösen a számítástechnikai eszközök és az internet) az adott generáció melyik életszakaszában jelentek meg. Megállapítottam, hogy mivel a fiatalabb generációk életében (a Z és az alfa generációknál) az internet, illetve a mobilinternet már születésüktől fogja jelen van, ezért szocializációjukban az előző generációkhoz képest

lényegesen komolyabb szerepet töltenek be az internethez kapcsolódó – elsősorban – mobil kommunikációs eszközök (okostelefon, tablet, egyéb okoseszközök), valamint az ezeken futó alkalmazások.

(2) A témaválasztás indoklása

Számos olyan fejlesztésnek vagyunk a szemtanúi (pl.: EveR, DER2, Saya, Sophia, Jangjang), amelyiknél az elsődleges cél olyan robotok megalkotása, amelyek alapvetően az emberre minél jobban hasonlító androidok, humanoidok. Ez igaz többek között antropometriai jellemzőikre, mimikájukra, gesztusaikra, hangjukra. Jelen témám az ember érzékszervei (esetünkben látás, hallás, tapintás) útján érzékelhető, hagyományos és kiterjesztett/virtuális külvilágban jelen levő, embernek tűnő robotmegjelenésekkel és megnyilvánulásokkal foglalkozik. A (közel)jövőben egyre több területen jelenik meg a mesterséges intelligencia és a humanoid robotok, ami alapjaiban változtatja meg az ember kapcsolatát a (technikai) környezethez. Úgy gondolom, hogy ennek vizsgálata fontos feladat a műszaki-informatikai terület vonatkozásában is.

(3) A kutatási célkitűzések és a téma körülhatárolása

Kommunikációs aspektusból elsősorban azt vizsgálom, hogy milyen lehet, mitől függhet az ember-robot kapcsolat, kialakulhatnak-e emberi érzelmek, ezek, illetve a kapcsolat elmélyülhet-e. Témám ismertetésekor részint teoretikus, részint empirikus források, ez utóbbinál saját kutatás segítségével vizsgálom, illetve határolom körül a témát.

(4) Az alkalmazott kutatási módszerek ismertetése

Témám ismertetésekor alapvetően négy kutatási módszert használok:

1. Dokumentumelemzés
2. Fókuszcsoportos megkérdezés
3. Fókuszcsoportos szakértői megkérdezés
4. Nagymintás, online kérdőíves kutatás

Szeretném megjegyezni, hogy a szakértői fókuszcsoportos kutatást Ványa Lászlóval közösen végeztem az alábbi munkamegosztás szerint:

- Kutatási koncepció megfogalmazása (K. Cs.)
- Kutatási koncepció véglegesítése (V. L.)
- Fókuszcsoportban részt vevő személyek kiválasztása (V. L.)
- Fókuszcsoportos beszélgetés megtervezése (K. Cs. + V. L.)
- Fókuszcsoportos beszélgetés megvalósítása (K. Cs. + V. L.)
- Eredmények kiértékelése (K. Cs.)
- Eredmények alapján tanulmány elkészítése (K. Cs. + V. L.)

(5) Következtetések

1. A Bergeri axiomák (bizonytalanságcsökkenés elmélete) átírhatóak és alkalmazhatóak az ember-robot interakcióra is.
2. Az ember részéről a robot (gép) iránt táplált szimpátia viszonylag egzakt módon vizsgálható.
3. A jövőben megjelenő robotok már képesek lehetnek arra, hogy az emberekben mélyebb érzelmeket váltsanak ki, az emberek ragaszkodjanak hozzájuk, társuknak tekintsék őket/azokat.

4. Az ember-robot interakciót nem lehet csak pesszimista, elutasító, illetve csak optimista, maximálisan elfogadó és támogató nézőpontból szemlélni.
5. A robotok folyamatosan jelennek meg a társadalmi élet különböző színterein, így a munkában, a magánéletben, a nyilvános helyeken, a hivatalokban, a honvédelemben.
6. A társadalom tagjai ugyan még általánosságban a robot kifejezést használják valamennyi robotra, de a megjelenésük, az autonómiájuk szintje, a mesterséges intelligenciájuk, a tanulási és környezeti adaptációs képességük és készségük miatt rövid időn belül szükség lesz a fogalom fragmentálódására, ahogy az már megtörtént pl. a robot/dron különválasztásakor.
7. A különböző országok és kultúrák emberről és értékről alkotott fogalmai tovább differenciálják a robotokról alkotott képet, akárcsak a polgári és katonai vélekedés a témáról, illetve a különböző generációk robotértelmezései.
8. A jövő katonai vezetőinek foglalkoznia kell a katona-robot interakcióval, mivel akár békeidőben, akár háborúban a robot – autonómiája szintjétől függően – egyre markánsabb kiszolgáló, támogató, döntéselőkészítő és -végrehajtó szerepet fog kapni.
9. Az ember-robot interakciók elemzése és fejlesztése során újra kell gondolni akár a polgári, akár a katonai életben a műveleti, a munka-, a környezet- az informatikai és az információbiztonság fogalmát és a fogalmak tartalmi összetevőit.

10. Az ember-robot interakciók területi diverzitásának és a kapcsolat elmélyülésének következtében egyre komolyabb veszélyei lehetnek a társadalom tagjai számára a robotok és a mesterséges intelligencia működését befolyásoló informatikai támadásoknak.

(6) Tézisek

1. Az ember-robot interakciók révén elmélyül és érzelmekkel is gazdagodik a kapcsolat.
2. Az ember-robot interakciók biztonságos informatikai hátterének a megteremtése az alapja annak, hogy a kapcsolatban a robot (mesterséges intelligencia) az elvárt módon viselkedjen és kommunikáljon az emberrel.

(7) Az eredmények alkalmazási lehetőségei

Az ember-robot interakció humán oldalának jobb megismerése segíthet abban, hogy a jövő katonái eredményesebben tudjanak együttműködni a nem emberi (értsd: robot, bot, mesterséges intelligencia) partnerekkel annak érdekében, hogy hatékonyabban legyenek képesek megoldani a honvédelemből eredő közvetlen és közvetett (képzés, szállítás, stb.) feladatokat.

2. *A digitális kor változásai és hatása a szervezetek életében, különösen az információbiztonság területén.*

(1) Az adott kutatás előzményei

A biztonság (Security és safety) fogalmának vizsgálatánál megállapítottam, hogy a fogalom nem csak felértékelődik, de komplexebb jelentést is kap jelenkorunkban. Meglátásom szerint meg lehet különböztetni többek között (1) az interneten található személyes adatokkal történő visszaélést, a felhasználó eszközének feltörését és (2) vírussal való megfertőzését és/vagy (3) a rajta található adatok ellopását, (4) a weboldalak feltörését, (5) elérhetetlenné tételét, (6) a rajta található tartalmak illetéktelen módosítását, (7) az adatbázisok feltörését és onnan az adatok ellopását, (8) a társadalomra veszélyes tartalmak megjelenítését (pedofília, terrorista üzenetek), (9) bűnszervezetek és terrorakciók online irányítását és szervezését, (10) a bizalmas adatok visszaélésével történő zsarolást, (11) a szervereket és hálózati eszközöket ért fizikai támadást, (12) pénzmosást, társadalomra veszélyes csoportok pénzügyi támogatását. Ezek a veszélyek a társadalom és a munkaszervezetek valamennyi tagját, illetve a munkaszervezeteket és azok kommunikációs platformjait egyaránt érintik.

A hagyományos kor analóg információközlése és a digitális kor digitális/digitalizált információközlése között számos különbség található. Miközben az információs társadalom korát, vagy más névvel az adatok korát megelőző időszakokban a mediatizált, tehát valamely médium által közvetített információnál a jel alapvetően folytonos függvénye az

időnek, vagy más ismérvnek, addig a digitális jel a diszkrét jelnek bináris számokkal kódolt megjelenési formája. Analóg jelhordozónak/tárolónak tekintjük például a magnókazettát, a VHS-kazettát, digitálisnak a pendrive-ot, az SD-kártyát, a merevlemezt, az okostelefon, illetve a tablet háttértárát, a felhőt (cloud).

A kutatás előzményeként a teoretikus források, valamint szekunder kutatási jelentések alapján megállapítottam, hogy lényeges eltérések mutatkoznak a hagyományos/analóg, illetve digitális formában jelen levő információk előállítási, megismertetési/bemutatási és sokszorosítási költségei és időkerete között is. A digitális korra vonatkozó közgazdasági elméletek másfajta nézőpontból születtek meg Shapiro és Varian (2000) az információ előállítási költségével kapcsolatban azon a véleményen vannak, hogy az előállítási költséget alapvetően az „első példány költsége" határozza meg. Meglátásuk szerint „az állandó költségek magasak, de a sokszorosítás változó költségei alacsonyak. Minél többet termelünk, annál alacsonyabb az átlagos termelési költség."

A digitális korban, vagy más névvel az adatok korában a materializálódott javakkal szemben a szimbolikus javak felértékelődését figyeltem meg, értve ezalatt az adatokat, az információkat, s az ezekből képzett tudást. A javak felértékelődésének a velejárója egy változóban levő tulajdonosi szemléletmód: szükség van olyan erőforrások bevonására, amelyek lehetővé teszik az adatok/információk tárolását, védelmét (ezt tekinthetjük a rendszer hardverelemeinek), s szükség van olyan megoldásokra (a rendszer szoftverelemei), amelyek hatékonyan képesek a

védelem szoftveres és humán folyamatait – beleértve az információbiztonság-tudatosság fejlesztését is – megfelelő szinten biztosítani.
Témám feldolgozásának megkezdése előtt a hiteles, szakmai hírforrásokra támaszkodva megállapítottam, hogy a személyes és a szervezeti adatok és az azokat tároló eszközök illetéktelen kezekbe kerülése (pl.: adatlopás, személyiséglopás), az adatok/webhely tartalmának megváltoztatása (deface), az adatbázisok elleni támadások (SQL injection), az adatok közötti kapcsolatok illetéktelen személyek által történő elemzése (pl.: big data analitika), a webhelyek elérhetetlenné tétele (DoS és DDoS támadás), az adatokat tartalmazó könyvtárakhoz történő hozzáférést blokkoló zsarolóvírusok (ransomware), a kémprogramok (spyware) – hogy csak a fontosabb veszélyeket említsem – olyan tényezők egy szervezet életében, amelyek nagyon komoly anyagi kárt is jelenthetnek.

(2) A témaválasztás indoklása

Véleményem szerint a technika fejlődése, a különböző technikai eszközök, berendezések, megoldások megjelenése a munkahelyeken a digitális kort megelőző korokban is újabb és újabb kihívások elé állította a munkavégző embert. A digitális kor azonban sokkal dinamikusabban produkálja ezeket a kihívásokat. A munkavégző ember technikai megoldásokhoz való adaptációs képessége és az adaptációs idő drasztikus lecsökkenése, a munkafolyamatok automatizálása, a szervezeteket segítő/működtető szoftverek (mesterséges intelligencia, tanulógépek) egyre markánsabb megjelenése és az ezektől való függés egyaránt erősíti a rendszerek információbiztonsági működésének fontosságát.

(3) A kutatási célkitűzések és a téma körülhatárolása

Jelen téma kutatásának a célja az, hogy dokumentumelemzés módszerével feldolgozza a téma releváns szakirodalmát (teoretikus megközelítés), majd egy fókuszcsoportos, valamint két, nagymintás, online kutatás bemutatásával megadja a téma magyarországi vonatkozású empirikus vetületét is.

(4) Az alkalmazott kutatási módszerek ismertetése

Témám ismertetésekor alapvetően három kutatási módszert használok:

1. dokumentumelemzés
2. fókuszcsoportos megkérdezés
3. két nagymintás, online kérdőíves kutatás

Szeretném megjegyezni, hogy az első nagymintás kutatásban, melynek témája a digitális munkahely információbiztonsági aspektusa volt, Poór Józseffel közösen az alábbi munkamegosztás szerint végeztük el a feladatot:

- Kutatási koncepció kidolgozása (K. Cs.)
- Kutatási koncepció véglegesítése (K. Cs. + P. J.)
- Kérdőív kérdéseinek összeállítása (K. Cs.)
- Kérdőív programozása (K. Cs.)
- Eredmények kiértékelése (K. Cs.)
- Eredmények alapján tanulmány elkészítése (K. Cs. + P. J.)

Ebben a kutatásunkban két hipotézist vizsgáltunk:

1. A vállalati vezetők jelentős része nagyon alulinformált az információbiztonság új kihívásainak tekintetében.
2. Miközben a vállalat nagy ellenőrzést gyakorol a tulajdonában és/vagy fennhatósága alatt levő, irodákban, munkahelyeken található eszközökre (pl.: asztali számítógép), illetve magára ezekre a fizikai helyekre is, addig a hordozható eszközök tekintetében sokkal lazábban jár el, különösen, ha azok a munkavállaló tulajdonában vannak.

Másik online kutatásunkban az önkormányzati vezető tisztségviselő információbiztonság-tudatosságát vizsgáltam Vinogradov Szergejjel közösen az alábbi munkamegosztás szerint:

- Kutatási koncepció kidolgozása (K. Cs.)
- Kutatási koncepció véglegesítése (K. Cs.)
- Kérdőív kérdéseinek összeállítása (K. Cs.)
- Kérdőív programozása (K. Cs.)
- Eredmények kiértékelése SPSS-sel (V. Sz.)
- Eredmények alapján tanulmány elkészítése (K. Cs. + V. Sz.)

Ebben a kutatásunkban három hipotézist vizsgáltunk:

1. A városi és a községi önkormányzatok között jelentős különbségek állnak fenn az információvédelemmel kapcsolatos szabályozási gyakorlatban.
2. A városi és a községi önkormányzatok információvédelmi infrastruktúrája eltérő.

3. A városi és a községi önkormányzatok tisztségviselőinek eltérő információbiztonság-tudatosságuk van.

(5) Következtetések

1. A digitális korban a munka(végzés) nem feltétlenül kötődik a szervezet fizikai helyéhez. Ez azt jelenti, hogy az információbiztonsággal kapcsolatos elvárások sorában meg kell jelennie a szervezet fizikai helyén kívüli helyszíneken tanúsított biztonságos munkavégzésre vonatkozó elvárásoknak is.
2. Célszerű olyan informatikai és biztonságos (digitális) munkakörnyezetet kialakítani, amelyben a munkavállaló jól és kényelmesen érzi magát, s rendelkezésére állnak mindazok az erőforrások, amelyek révén munkáját hatékonyan tudja elvégezni.
3. Ha nem jelent jelentős kockázatot a vállalat számára a munkavállaló megjelenése az online platformokon, s aktivitása különösen a közösségi médiában, akkor biztonság-tudatosságának a fejlesztése eredményesebb a megjelenés tiltásához képest.
4. A tudásalapú vállalati működés egyik alapja az adat és az információ, a másik a folyamatosan új ismeretekkel gazdagodó munkavállaló. Ez utóbbinál a szervezetnek érdemes biztosítani az összes olyan platformot és tudásfelületet, ami hozzájárul a munkavállaló szakmai fejlődéséhez.
5. A szervezetek digitális átállása, majd a folyamat tovább gondozása időigényes tevékenység. Mivel nem minden munkavállaló sorolható a korai elfogadók és innovátorok közé, ezért a szervezetnek

türelemmel kell viseltetnie az idősebb, kevésbé proaktív munkavállalók irányába, különösen, hogy a munkavállaló számára idegen munkakörnyezetben való munkavégzés növeli az információbiztonsági kockázatot.

6. A digitális munkahely kiterjed a beszállítókra, vásárlókra, ügyfelekre, partnerekre egyaránt. Az adatok és információk védelme – bár más-más fókuszból – valamennyi érintett közös érdeke, ezt érdemes bennük tudatosítani.
7. A munkakapcsolatok csak akkor működnek, ha a munkavállalók nem élik meg azokat másképp a hagyományos és a digitális világban.
8. A digitális korban működő vállalatok valamennyi alkalmazottja és vezetője számára az információbiztonságnak olyan fókusznak kell lennie, amelyik megkerülhetetlen valamennyi munka- és kommunikációs folyamatban. Ez azt jelenti, hogy a biztonsági fókusznak a szervezeti filozófiában és a szervezeti alapértékek között is meg kell jelennie.
9. Ugyan az információbiztonság területén jelenleg a szabályzatokon, szabályzókon, előírásokon, rendeken, rendeleteken, szankcionáláson van a hangsúly, a jövőt illetően azonban a biztonságtudatosság erősítése, kompetencia (képesség, jártasság, készség) szintű elsajátítása/használata és az ilyen irányú elköteleződés kialakítása kap majd nagyobb fókuszt.
10. Az információbiztonsággal és -tudatossággal foglalkoznia kell valamennyi szervezetnek, ha minimalizálni akarja az informatikai és

információbiztonsági káresemények számát és hatását a vállalati nyereségre.

(6) Tézisek

1. Mivel a szervezeti vezetők jelentős része alulinformált az információbiztonság új kihívásainak tekintetében, ezért szükség van biztonságtudatosságuk fejlesztésére.
2. Miközben a vállalat nagy ellenőrzést gyakorol a tulajdonában és/vagy fennhatósága alatt levő, irodákban, munkahelyeken található eszközökre (pl.: asztali számítógép), illetve magára ezekre a fizikai helyekre is, addig a hordozható eszközök tekintetében sokkal lazábban jár el, különösen, ha azok a munkavállaló tulajdonában vannak.
3. A városi és a községi önkormányzatok között jelentős különbségek állnak fenn az információvédelemmel kapcsolatos szabályozási gyakorlatban, információvédelmi infrastruktúrája eltérő.
4. A városi és a községi önkormányzatok tisztségviselőinek nincs markánsan különböző információbiztonság-tudatosságuk.

(7) Az eredmények alkalmazási lehetőségei

A második téma jelentőségét abban látom, hogy az általam feldolgozott szakirodalom, valamint a tézisfüzetemhez kapcsoló válogatott publikációim révén bemutatott kutatások alapján egy átfogó képet kaptam arról, hogy – elsősorban – Magyarországon a szervezetek (profitorientált, önkormányzati) vezetői milyen információbiztonság-tudatossággal rendelkeznek, hogyan vélekednek az általuk képviselt szervezet digitális

átállásáról, milyen információbiztonsági kihívásokkal találkozhatnak munkájuk során. A harmadik és a negyedik téma ismertetésekor konkrét módszereket mutatok be, melyek jelen témám eredményeinek ismeretében hatékony megoldást jelenthetnek a problémák (egy részének) orvoslására.

3. A kommunikációs modellek alkalmazhatósága az információbiztonság-tudatosság felmérésében és fejlesztésében.

(1) Az adott kutatás előzményei

Harmadik témám bemutatásánál a kutatási előzmények között tudom megnevezni a második témám ismertetése során tett megállapításaimat. Több kutatásomról szóló eredményeim és az azokból készített tanulmányaim alapján megállapítottam, hogy amíg az informatikai és számítástechnikai rendszerek és eszközök (pl.: végpontok) fejlesztésével, működtetésével, üzemeltetetésével, karbantartásával, használatával kapcsolatban az ember nem kerülhető ki, addig rendszerint az ember válik a rendszer leggyengébb láncszemévé. Az egyre szimbiotikusabb ember-gép (technikai környezet – 1. téma) kapcsolat, s e kapcsolat mennyiségi (időbeni) és minőségi (kapcsolat elmélyülése, érzelmek megjelenése) változása szükségszerűvé teszi a technikai-műszaki területen az eddiginél is markánsabb humán aspektusú vizsgálódást. Az embernek vannak olyan szociológiai, szociálpszichológiai és pszichológiai jellemzői, amelyek általánosságban igazak a (nyugati) társadalmakban élők többségére. Ilyen a társaság iránti igény, a valahová tartozás fontossága, a helyzetek

emocionális és morális kezelése, a közlés (kommunikáció) kényszere, énünk (személyiségünk) reprezentálása, megmutatása, a lelki és mentális védtelenség a szélhámosokkal, csalókkal szemben. A digitális kor előtt is foglalkoztak a manipulációval (ahogy arról még írok jelen témám részletes feldolgozásánál), a (kegyes és egyéb) hazugságokkal tudományos (pl.: Nordau Miksa (1913): Konvencionális hazugságok modern kultúréletünkben) és szépirodalmi megközelítésből (pl.: Thomas Mann (1954): Bekenntnisse des Hochstaplers Felix Krull – Egy szélhámos vallomásai) egyaránt.

(2) A témaválasztás indoklása

A social engineering típusú támadások részint informatikai, részint humán aspektusúak. Ez utóbbinál a támadó célja az, hogy a gyanútlan áldozattal rövid idő alatt olyan kommunikációs keretet alakítson ki, melyben a diskurzust irányítva el tudja érni a célját, ami többek között lehet a számára, illetve megbízója számára fontos féltitkos, illetve titkos információk megszerzése, illetéktelen belépés lezárt és/vagy védett irodai részekbe, bejutás (felső)vezetők irodai szobájába. A téma aktualitását az adja, hogy miközben az informatikai rendszerek műszaki/informatikai biztonsága egyre jobbnak mondható, addig a rendszereket használó és üzemeltető humán erőforrás, vagyis a munkavégző ember biztonságtudatosságában komoly hiányosságok mutatkoznak, amik nem csak a saját munkájára, hanem a szervezetre is veszélyt jelenthetnek. Jelen témám feldolgozásakor az elméleti alapok ismertetése után négy esettanulmányon keresztül mutatom be a verbális, a nonverbális, s bizonyos

szituációkban a metakommunikatív szemiotikai csapdákat, s e csapdákból felépített komplex manipulációs folyamatokat, elsősorban Dell Hymes SPEAKING modellje alapján.

Az információs társadalomban, illetve e fogalmat fokozatosan leváltó digitális korban, vagy más névvel az adatok korában az ezt megelőző korokhoz képest másfajta értékek kerültek a fókuszba. A hálózatba kapcsolt vezetékes és vezeték nélküli kommunikációs eszközök (asztali számítógépek, szerverek, okostelefonok, laptopok, tabletek, stb.) révén – feltételezve az aktív info-kommunikációs kapcsolatot az egyén készüléke és a hálózat között – az emberek aktivitásának egyre nagyobb része valósul meg a digitális világban, a kibertérben. Az olyan tevékenységek mellett, mint a kommunikáció, vagy a munka, a számunkra értékes adatok és információk tárházai is a kibertérbe költöztek, s e folyamat nem csak az egyénekre, hanem a szervezetekre is jellemző. Az adatok, az információk felértékelődésével párhuzamosan újfajta egyéni és szervezett bűnözési formák jelentek meg. Az elkövetők számára az értéket nem, vagy elsősorban nem maga az eltulajdonított tárgy jelenti, hanem az informatikai adathordozón levő adatok, információk, adatbázisok, illetve a bűnesetek egy részében nem is tárgyakat, hanem csak adatokat és információkat lopnak el az elkövetők, vagy megbízóik kívánságainak megfelelően manipulálják, átírják, vagy törlik az adatbázisok, a publikusan, illetve csak a belső hálózatból elérhető weblapok tartalmát, stb. Hiba lenne azt állítani, hogy ezek a feladatok kivétel nélkül komoly informatikai/programozói tudást igényelnek, annál is inkább, mivel a bűnszervezetekben elkövetett tevékenységek jelentős részénél megfigyelhető a

munkamegosztás. Az egy területre (pl.: adathalászat, nyomeltakarítás, szerverek feltörése) szakosodott szakemberek között megjelennek azok a bűnelkövetők, akik elsősorban már nem a kódolással, kódfejtéssel foglalkoznak, hanem a kommunikációs, pszichológiai, szociálpszichológiai modellek és általánosságban az emberi viselkedés magas fokú ismerői, s feladatuk az, hogy a komplex informatikai védelemmel rendelkező szervezetek legsebezhetőbb pontját, rendszerint az azt üzemeltető, fenntartó, fejlesztő, használó (munkavégző) embert vegyék célba, s olyan helyzeteket teremtsenek, ahol a célszemély(ek) az általuk elvárt módon viselkedjen. Magyar nyelven is megjelent Mitnick életével foglalkozó két könyv (Mitnick, Simon, 2003, 2006), amelyben a főszereplő-szerző külön fejezetben foglalkozik a megtévesztés művészetével, a social engineeringgel. A szerzők megfogalmazása szerint „a támadó az emberi természet legnemesebb tulajdonságát használja ki: azt a természetes törekvésünket, hogy segítőkészek, udvariasak, pozitívak legyünk, csapatjátékosként viselkedjünk, illetve azt a vágyunkat, hogy elvégezzük a munkánkat”.

(3) A kutatási célkitűzések és a téma körülhatárolása

Kutatási célom annak teoretikus és empirikus vizsgálata, hogy az információbiztonság-tudatossággal kapcsolatos auditok során egy 1974-ben publikált modell alkalmas-e arra – szükség esetén némi átdolgozást és átértelmezést követően – hogy az audit eredményeit (különösen a social engineering típusú audit esetében) feldolgozva hatékonyan rámutasson a munkavégző ember sebezhetőségére. Azért tartom fontosnak egy modell

– kutatásom szemponjtából Hymes SPEAKING modellje – használatát, mert a megfelelő modell kiválasztása és alkalmazása olyan többletinformációkkal gazdagíthatja az információbiztonsággal foglalkozó szakembereket, amelyeket egyébként nem tudnának megszerezni.

(4) Az alkalmazott kutatási módszerek ismertetése

Témám ismertetésekor alapvetően két kutatási módszert használok:

1. dokumentumelemzés
2. Hymes SPEAKING modelljének segítségével négy esettanulmány feldolgozása

(5) Következtetések

Úgy gondolom, hogy a négy esettanulmány rámutatott azokra a pszichológiai és kommunikációs csapdákra, melyekbe miden munkavállaló beleeshet. Ezek a csapdák nem csak a vizsgált üzleti, hanem a magánéletben is megtalálhatóak. Vannak olyan emberek, akik különösebb előképzettség nélkül is eredményesen képesek manipulálni a környezetükben élőket. A social engineerek erre a „szakmára” rendszerint tudatosan készülnek, s ha rendelkeznek is egy bizonyos manipulatív eszközkészlettel, szakmai ismereteiket folyamatosan fejlesztik. Jelen korunk programozói és hálózati ismeretekkel rendelkező hackereihez hasonlóan a humán alapú támadásokkal (vagy azzal is) foglalkozó social engineerek is egyre ritkábban dolgoznak szórakozásból, a háttérben szervezeti és kormányzati megrendelők állnak. A vállalatok informatikai sebezhetősége egyre komolyabb kihívást jelent valamennyi szervezet számára. Ennek része,

hogy a social engineer tudással rendelkező auditorok a vállalatoknál ad hoc jelleggel különböző teszttámadásokat hajtanak végre, s a tapasztalatok alapján a biztonsági előírásokra, képzésre, a tudatosság fejlesztésére vonatkozó ajánlásokat fogalmaznak meg, illetve programokat indítanak el. Meggyőződésem, hogy ebben a folyamatban Hymes SPEAKING modelljének használata többletinformációval gazdagítja az információbiztonsági eseteket/incidenseket elemző szakembereket. Mivel tanulmányom elméleti, illetve az esettanulmányokat bemutató részeiben leírtam már azokat a fontosabb ismereteket, amelyek révén a modellben elemeztem a humán alapú social engineering támadásokat, így azokat nem kívánom még egyszer megismételni.

(6) Tézisek

1. A személyközi kommunikáció során azonosítható szereprelációk segíthetnek az információbiztonság-tudatosság fejlesztésében.
2. A személyközi kommunikációs helyzetekben az ember viselkedésének a megismerése fontos tényező a személyre, munkacsoportra, munkaszervezetre szabott információbiztonsági programok megalkotásakor.
3. A kommunikációs modellek közül Dell Hymes SPEAKING modellje alkalmas a humán típusú social engineering támadások elemzésére.

(7) Az eredmények alkalmazási lehetőségei

Megállapítottam, hogy a modell lehetővé tette, hogy a social engineering típusú támadások és azok folyamata nyolc szempont szerint vizsgálható,

s a levont következtetések az információbiztonsággal foglalkozó szakemberek számára – még ha a modellt nem is ismerték – informatív jelleggel bírnak. Ennek érdekében a négy esettanulmányt cikkem kéziratának leadása előtt odaadtam több olyan szakembernek, akik a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakán, illetve az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában tanulnak. Az esetleírásokat, a feldolgozási rendszert megértették, s úgy ítélték meg a modellt, hogy az akár a jelenlegi, akár egy néhány további szemponttal kiegészített változatában (pl.: anyagi veszteség mértéke, a használt eszközök markánsabb informatikai típusú leírása, biztonsági kockázat-besorolás) alkalmas a további elemzésre, s iparágtól/ágazattól függetlenül az adott szervezet információbiztonsági programjának az elkészítéséhez, illetve a fejlesztéséhez kellő alapot szolgáltat. Úgy gondolom, hogy a megbízhatóság dimenziójában is megállja a helyét a modell. Hymes kritériumai szerint akár az esettanulmányokban bemutatott, akár más social engineering típusú támadások is elemezhetőek, értékelhetőek a segítségével. Amennyiben rendelkezésre állnak a hang- és videofelvételek, akkor a teszttámadások jól dokumentálhatóak.

III. A KUTATÁS ÉS AZ EREDMÉNYEK HATÁSA, VISSZHANGJA

Felkérés a témában konferenciaelőadásra (válogatás):

- Kollár Csaba (2017): A katona-robot interakció fejlődési irányai a következő évtizedekben, 1-40 pp. A XXI. SZÁZADI TECHNOLÓGIA KIHÍVÁSAI ÉS LEHETŐSÉGEI A HON- ÉS RENDVÉDELEM TERÜLETÉN című konferencián elhangzott előadás prezentációja, Időpont: 2017. Április 27., Helyszín: Belügyminisztérium Nemzetközi Oktatási Központja, Budapest.
- Kollár Csaba (2017): Az ember-robot interakció múltja, jelene és jövője a tudomány és a fikció szemszögéből (I. rész), 1-39 pp. A NKE HHK Elektronikai Hadviselés Tanszék és a Magyar Hadtudományi Társaság Elektronikai, Informatikai és Robotikai Szakosztály által szervezett szakmai napon elhangzott előadás prezentációjának első része, Időpont: 2017. május 16., Helyszín: Nemzeti Közszolgálati Egyetem Zrínyi Miklós Laktanya és Egyetemi Campus, Budapest.
- Kollár Csaba (2016): Szerethetők-e a robotok: Az ember-robot interakció humán oldala, 1-45 pp. ROBOTHADVISELÉS 2016 TUDOMÁNYOS KONFERENCIÁN elhangzott előadás prezentációja, Időpont: 2016. november 24., Helyszín: Nemzeti Közszolgálati Egyetem Zrínyi Miklós Laktanya és Egyetemi Campus, Budapest.
- Kollár Csaba (2017): A személyközi diskurzus, mint elemzésre alkalmas forrás az információbiztonság területén, 1-16 pp. A III. Forráskutatás, forráskiadás, tudománytörténet konferencián elhangzott

előadás prezentációja, Időpont: 2017. november 16–17., Helyszín: ELTE BTK Budapest.

- Kollár Csaba (2017): Hackerpszichológia., 1-40 pp. A Kutatók éjszakája 2017 rendezvényen elhangzott előadás prezentációja, Időpont: 2017. szeptember 29., Helyszín: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Budapest.
- Kollár Csaba (2017): A személyközi kommunikáció narratívái és diskurzusai az információbiztonság fókuszában., 1-23 pp. A SZIMBIÓZIS NAPOK 2017 – kulturális antropológiai fesztivál Narratíva és emlékezet szekcióban elhangzott előadás prezentációja, Időpont: 2017. május 12-13., Helyszín: Auróra, Budapest.

Tantárgyak oktatása, illetve új tantárgyak bevezetése az Óbudai Egyetemen:

- Adat és információvédelem
- Infokommunikációs rendszerek
- Információbiztonság alapjai
- Információbiztonság IT-gyakorlata
- A mesterséges intelligencia a biztonságtechnikában
- A mesterséges intelligencia a műszaki életben

Tantárgyak oktatása az Óbudai Egyetem 2023. szeptemberében induló kibermérnök képzésén:

- Adatvédelem, adatbiztonság
- Információbiztonság humán aspektusai

- Információbiztonság követelményei a közszférában

Tantárgyak oktatása a Biztonságtudományi Doktori Iskolában:

- Az ember-robot interakció biztonsági aspektusa
- A domotika rendszer biztonsága
- A mesterséges intelligencia felhasználási lehetőségei a biztonságtechnikában

Tantárgyak oktatása a Katonai Műszaki Doktori Iskolában:

- Kutatási adatok feldolgozása, publikálása
- Az információbiztonság humán oldala

Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karon a Mesterséges Intelligencia Műhely elindítása és vezetése.

Az Óbudai Egyetem által gesztorált, nemzetközi, „HEDY – Élet a MI-korban” ERAMUS+ partnerségi projekt (KA220-HED 0C8D3623) szakmai vezetése.

IV. IRODALMI HIVATKOZÁSOK LISTÁJA

- Argall, Brenna D. – Billard, Aude G. (2010): A survey of Tactile Human-Robot Interactions. Robotics and Autonomous Systems. Volume 58, Issue 10, 31 October 2010, 1159-1176 pp.

- Aronson, Elliot (2011): The Social Animal (11. kiadás). New York: Worth Publishers, 431 p.
- Barabasi Albert László (2014): Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life. New York: Basic Books, 304 p.
- Bartels, Andreas –Zeki, Semir (2000): The Neural Correlates of Romantic Love. Neuroreport, 11, 3829-3834 pp.
- Bauer, Andrea – Wollherr, Dirk – Buss, Martin (2008): Human-Robot Collaboration: a Survey. International Journal of Humanoid Robotics 5(1), 47-66 pp.
- Bereczkei Tamás (2016): Machiavellizmus. A megtévesztés pszichológiája. Budapest: Typotex, 268 p.
- Berek Lajos – Berek Tamás – Berek László (2016): Személy- és vagyonbiztonság. Budapest: Óbudai Egyetem, 318 p.
- Berg, Oscar (2013): The 6 Pillars of The Digital Workplace, http://www.oscarberg.net/2013/09/the-6-pillars-of-digital-workplace.html, letöltve: 2022.09.20.
- Breazeal, Cynthia L. (2002): Designing sociable robots. London: MIT Press, 273 p.
- Breazeal, Cynthia L. (2003): Toward sociable robots. Robotics and Autonomous Systems. Volume 42, Issues 3–4, 2003 március, 167–175 pp.
- Buss, David M. (2000). The Dangerous Passion: Why Jealousy is Necessary as Love and Sex. New York: Free Press, 272 p.

- Buss, David M. (2003): The Evolution Of Desire: Strategies of Human Mating. New York: Basic Books, 368 p.
- Carbaugh, Donald (1989): Fifty terms for talk: A cross-cultural study. International and Intercultural Communication Annual, 1989/13, 93–120 pp.
- Carter, Steven – Sokol, Julia (2004): Men Who Can't Love: How to Recognize a Commitment phobic Man Before he Breaks Your Heart. New York: Penguin Putnam, Inc. 299 p.
- Choi, Charles Q. (2008): Not Tonight, Dear, I Have to Reboot. Scientific American, 2008 március. https://www.scientificamerican.com/article/not-tonight-dear-i-have-to-reboot/ letöltési ideje: 2022. 09. 20.
- Chris Farmer: What is PDCA? előadás, 2014. január
- Creswell, John W. (2007): Qualitative inquiry and research design: Choosing among five approaches. Thousand Oaks: Sage, 472 p.
- Damasio, Antonio (2000): The Feeling of What Happens: Body and Emotion in the Making of Consciousness. New York: Mariner Books, 386 p.
- Dautenhahn, Kerstin (1998): The art of designing socially intelligent agents – science, fiction, and the human in the loop. Applied Artificial Intelligence. Volume 12, 1998, Issue 7-8, 573–617 pp.
- Dautenhahn, Kerstin (2007): Socially intelligent robots: dimensions of human-robot interaction. Philosophical Transaction of the Royal Society, Volume 362, issue 1480, 679–704 pp.

- Deming, Edwards W. (1986) : Out of the Crisis. MIT Center for Advanced Engineering Study Cambridge: MIT Press, 524 p.
- DiSalvo, Carl F. –Gemperle, Francine –Forlizzi, Jodi – Kiesler, Sara (2002): All Robots Are Not Created Equal: The Design and Perception of Humanoid Robot Heads. Proceedings of the 4th conference on Designing interactive systems: processes, practices, methods, and techniques. 2002. június, London, 321-326 pp.
- Dooley, Larry M. (2002): Case Study Research and Theory Building. Advances in Developing Human Resources, 2002 4: 335, 126-142 pp.
- Dreyfus, Suelette – Assange, Julian (1997): Underground. Sydney: Red Book, 329 p.
- Duffy, Brian R. (2003): Anthropomorphism and the social robot. Robotics and Autonomous Systems 42 (2003), 177–190 pp.
- Duranti, Alessandro (1985): Sociocultural Dimensions of Discourse. In: Teun A., Van Dijk (szerk): Handbook of Discourse Analysis. London: Academic Press Limited 193-230 pp.
- Dyson, Esther (2004): 2.0. verzió. Életünk a digitális korban, Budapest: HVG Kiadó, 352 p.
- Fisher, Helen E. (1998). Lust, Attraction, and Attachment in Mammalian Reproduction. Human Nature, vol. 91, 23-52 pp.
- Fong, Terrence – Nourbakhsha, Illah – Dautenhahnc, Kerstin (2003): A survey of socially interactive robots. Robotics and Autonomous Systems. Volume 42, Issues 3–4, 2003 március, 143–166 pp.

- Gall, Meredith W. – Borg, Walter R. – Gall, Joyce P. (2007): Educational Research: An Introduction, 8th Edition. Cambridge: Pearson, 704 p.
- Ghosh, Santanu (2011): Top seven social media threats http://www.computerweekly.com/tip/Top-seven-social-media-threats, letöltve: 2022. 09. 20.
- Goodrich, Michael A. – Schultz, Alan C. (2007): Human-Robot Interaction: A Survey. Foundations and Trends in Human–Computer Interaction. Vol. 1, No. 3 (2007) 203–275 pp.
- Griffin, Em (2001): Bevezetés a kommunikációelméletbe. Budapest: Harmat. 535 p.
- Haig Zsolt – Várhegyi István (2005): Hadviselés az információs hadszíntéren. Budapest: Zrínyi Kiadó, 286 p.
- Hakim, Catherine (1998). Developing a Sociology for the Twenty-first Century: Preference Theory. British Journal of Sociology, 49, 137-143 pp.
- Hankiss Ágnes (1978): A bizalom anatómiája. Budapest: Magvető Kiadó, 172 p.
- Hinds-Addow, Simone (2014): Love with robots will be as normal as love with other humans. http://www.psychology.nottingham.ac.uk/staff/ddc/c8cxpa/further/Dissertation_examples/Hinds-Addow_14.pdf letöltési ideje: 2022. 09. 20.
- Hogan, Kevin (2008): A meggyőzés tudománya. Budapest: Danvantara Kiadó, 212 p.

- Horányi Özséb (szerk.) (2007): A kommunikáció mint participáció. Budapest: Typotex Kiadó, 332 p.
- Hováth Dóra – Mitev Ariel (2015): Alternatív kvalitatív kutatási kézikönyv. Budapest: Alinea Kiadó, 394 p.
- Hymes, Dell (1972): Models of the Interaction of Language and Social Life, In Gumperz, John – Hymes, Dell (szerk): Directions in Sociolinguistics: The Ethnography of Communication, New York: Holts Rinehart & Winston, 35-71 pp.
- Hymes, Dell (1974): Foundations in Sociolinguistics: An Ethnographic Approach. Philadelphia: University of Pennsylvania Press, 247p.
- Izsa Jenő (2009): Nemzetbiztonsági alapismeretek. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 196 p.
- Jóri András – Soós Andrea Klára (2016): Adatvédelmi jog. Magyar és európai szabályozás. Budapest: HVG Orac, 372 p.
- Kahn, Jr Peter H. – Ruckert, Jolina H. – Kanda, Takayuki – Ishiguro, Hiroshi – Reichert, Aimee L. – Gary, Heather E. – Shen, Solace (2010): Psychological Intimacy with Robots? Using Interaction Patterns to Uncover Depth of Relation. Proceedings of the 5th ACM/IEEE International Conference on Human-Robot Interaction, 123–124 pp.
- Kehal, Harbhajan S. – Singh, Varinder P. (2004): Digital Economy: Impact, Influences and Challenges. London: Idea Group Publishing, 289 p.

- Klenke, Karin (2008): Qualitative Research in the Study of Leadership. Bingley: Emerald Group, 454 p.
- Knight, Heather – Satkin, Scott – Ramakrishna, Varun – Divvala, Santosh (2011): A Savvy Robot Standup Comic: Online Learning through Audience Tracking. International Conference on Tangible and Embedded Interaction, 2011. január, 187-192 pp.
- Lawrence Lessig (2004): Free culture: how big media uses technology and the law to lock down culture and control creativity. New York: The Penguin Press, 352 p.
- Lévay Gábor (2006): OSINT (Open Source Intelligence) - Nyílt információs hírszerzés. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 192 p.
- Levine, Rick – Locke, Christopher – Searls, Doc – Weinberger, David (2001): Cluetrain – a hagyományos üzletmenet végnapjai, Typotex: Budapest 219 p.
- Levy, David (2008): Love and Sex with Robots: The Evolution of Human Robot Relationships. New York: Harper. 352 p.
- Levy, Steven (2010): Hackers: Heroes of the Computer Revolution. New York: O'Reilly, 520 p.
- Libin, Alexander V. – Libin, Elena V. (2004): Robotic Psychology. Encyclopedia of Applied Psychology, Volume 3. Elsevier, 295-298 pp.
- Lippenmeier, Norbert – Wiesner Erzsébet (szerk.) (1998): Tanulmányok a szupervízió köréből. Salgótarján: Médiamix Kiadó, 153 p.

- MacDorman, Karl F. – Minato, Takashi – Shimada, Michihiro – Itakura, Shoji – Cowley, Stephen – Ishiguro, Hiroshi (2005): Assessing human likeness by eye contact in an android testbed. Proceedings of the XXVII Annual Meeting of the Cognitive Science Society. 2005. július, Stresa, 1373-1378 pp.
- Matel, Maldona (2009): "The Ethnography of communication". Bulletin of the Transilvania University of Brasov. Vol-2(51)-2009, Series IV; Philosophy and cultural Studies.
- Mayer-Schönberger, Viktor – Cukier, Kenneth (2014): BIG DATA. Forradalmi módszer, amely megváltoztatja munkánkat, gondolkodásunkat és egész életünket, Budapest: HVG Kiadó, 280 p.
- McConnell, Jane (2015): The Workplace in the Digital Age. Elektronikus prezentáció: http://www.slideshare.net/NetJMC/e2-summit2015-netjmc, letöltés: 2022. 09. 20.
- Mitnick, Kevin D. – Simon, L. William (2003): A legendás hacker. A megtévesztés művészete. Budapest: Perfact Kiadó, 348 p.
- Mitnick, Kevin D. – Simon, L. William (2006): A legendás hacker. A behatolás művészete. Budapest: Perfact Kiadó, 311 p.
- Mori, Masahiro (2012): The Uncanny Valley. http://spectrum.ieee.org/automaton/robotics/humanoids/the-uncanny-valley Letöltés ideje: 2022. 09. 20.
- Muha Lajos (szerk.) (2004): Az informatikai biztonság kézikönyve. Budapest: Verlag Dashöfer, kapcsos könyv.
- Nábrády Mária (2014): A megtévesztés művészete. Budapest: Libri, 140 p.

- Nikolaidis, Stefanos – Kuznetsov, Anton – Hsu, David – Srinivasa, Siddharta (2016): Formalizing Human-Robot Mutual Adaptation: A Bounded Memory Model. HRI'16 The Eleventh ACM/IEEE International Conference on Human Robot Interaction. Christchurch, New Zealand, 75-82 pp.
- Nomura, Tatsuya – Kanda, Takayuki – Suzuki, Tomohiro – Kato, Kennsuke (2004): Experimental Investigation into Influence of Negative Attitudes toward Robots on Human-Robot Interaction. Proceedings of the 3rd Workshop on Social Intelligence Design (SID2004), Twente, 125-135 pp.
- Nomura, Tatsuya – Kanda, Takayuki – Suzuki, Tomohiro – Kato, Kennsuke (2005): People's Assumptions about Robots: Investigation of Their Relationships with Attitudes and Emotions toward Robots. Proceedings of Robot and Human Interactive Communication, ROMAN 2005. IEEE International Workshop, 114-132 pp.
- Nomura, Tatsuya – Shintani, Takuya – Fujii, Kazuki – Hokabe, Kazumasa (2007): Experimental Investigation of relationships between anxiety, negative attitudes, and allowable distance of robots. Proceedings of the 2nd IASTED International Conference on Human Computer Interaction. ACTA Press, Chamonix, France, 13-18 pp.
- Oroszi Eszter Diána (2008): Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője. Budapest: BCE, 89 p.

- Paré, Gui (2002): Enhancing the Rigor of Qualitative Research: Application of a Case Methodology to Build Theories of IT Implementation. The Qualitative Riport, 2002, vol 7, no 4. 1-34 pp.
- Philipsen, Gerry: A beszédkódok elmélete. A kommunikáció etnográfiája. Griffin, Em (szerk 2001): Bevezetés a kommunikációelméletbe. Budapest, Harmat. 428-439 pp.
- Pilch, Irena (2008): Machiavellianism, emotional intelligence and social competence: Are Machiavellians interpersonally skilled? In.: Polish Psychological Bulletin, 2008/39/3, 158-164 pp.
- Poulsen, Kevin (2011): Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground. New York: Broadway Paperbacks, 266 p.
- Rajnai Zoltán – Nguyen Huu Phouc Dai (2015): General audit of the infrastructure, improvements in network security features, fixing potential security holes in a company. In.: Rajnai Zoltán, Nyikes Zoltán, Milan Pavlovic (szerk.): Proceedings on Applied Internet and Information Technologies. 258 p. Konferencia helye, ideje: Zrenjanin, Szerbia, 2015.10.21-2015.10.23. Zrenjanin: University of Novi Sad, Faculty of Technical Sciences, 148-151 pp.
- Rajnai Zoltán (2017): Információbiztonság tudatosság. In: Bitay Enikő (szerk.): A XXII. Fiatal Műszakiak Tudományos Ülésszak előadásai: Proceedings of the XXII-th International Scientific Conference of Young Engineers. 418 p. Konferencia helye, ideje: Kolozsvár, Románia, 2017.03.23-2017.03.24. Kolozsvár: Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 37-43 pp.

- Rashid, Faymida Y (2016, frissítve 2018-ban): Introducing the 'Treacherous 12,' the top security threats organizations face when using cloud services, in: http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html, letöltve: 2022. 09. 20.
- Ray, Manas – Biswas, Chinmay (2011): A study on Ethnography of communication: A discourse analysis with Hymes ‘speaking model’. Journal of Education and Practice, 2011/2/6, 33-40 pp.
- Rekleitis, Evangelos (szerk., 2016): Big Data Threat Landscape and Good Practice Guide https://www.enisa.europa.eu/publications/big-data-threat-landscape, letöltve: 2022. 09. 20.
- Richards, Jack Croft – Schmidt, Richard W. (2013), Dictionary of Language Teaching and Applied Linguistics, New York: Longman Publications, 814 p.
- Russell, Ryan (2005): A Háló kalózai - Hogyan lopjunk kontinenst. Budapest: Kiskapu Kiadó, 412 p.
- Schneier, Bruce (2008): Schneier on security. Indianapolis: Wiley Publishing, 336 p.
- Shapiro, Carl – Varian, Hal R. (1999, 2000): Information Rules: A Strategic Guide to the Network Economy. Boston (MA): Harward Business School Press, 368 p.
- Sheridan, Tom B. (1992): Telerobotics, Automation, and Human Supervisory Control. Cambridge: MIT Press, 415 p.
- Síklaki István (szerk 2008): Szóbeli befolyásolás I. Nyelv, gondolkodás, kultúra. Budapest: Typotex, 348 p.

- Simon, George (2009): Bárányбőrben. A nyílt agressziótól a manipulációig. Budapest: Háttér Kiadó, 340 p.
- Steinberg, Shirley – Parmar, Priya – Richard, Birgit (szerk., 2005): Contemporary Youth Culture: An International Encyclopedia. London: Greenwood, 720p.
- Sterling, Bruce (1993): The Hacker Crackdown: Law And Disorder On The Electronic Frontier Mass Market. New York: Bantam, 336 p.
- Sternberg, Robert – Gracek, Susan (1984): The Nature of Love. Journal of Personality and Social Psychology, 4(2), 312-329 pp.
- Sullins, John P. (2012): Robots, Love and Sex: The ethics of building a love machine. IEEE Transactions on Affective Computers. Vol 3. No. 4., 2012 október, 398-409 pp.
- T. Kiss Tamás (1999): A szemtől-szembeni formációk kommunikációs viszonyai. Budapest: Új mandátum, 383 p.
- Thomaz, Andrea – Hoffman, Guy – Cakmak, Maya (2016): Computational Human-Robot Interaction. Foundations and Trends in Robotics. Vol. 4: No. 2-3, 105-223 pp.
- Trivers, Robert L. (1972). Parental Investment and Sexual Selection. Sexual Selection and the Descent of Man, 136–179 pp.
- Vasvári György (2009): A társadalmi és szervezeti (vállalati) biztonsági kultúra. Budapest: Ad Librum. 100 p.
- Vida Csaba (2000): Vállalatirányítás IV. Módszerek és eszközök. Pécs: PTE, 70 p.

- Zand-Vakili, Elham –Fard Kashani, Alireza –Tabandeh, Farhad (2012): The Analysis of Speech Events and Hymes' SPEAKING. Factors in the Comedy Television Series: "FRIENDS". New Media and Mass Communication, 2012/2., 27-43 pp.

V. A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK

- Haig Zsolt; Kollár Csaba (2017): INFORMATION SECURITY FROM THE ASPECT OF MILITARY ICT STUDENTS: Current issues and responses with the help of document analysis and focus group survey. ECONOMICS AND MANAGEMENT 2017: 1 pp. 49-57., 9 p.
- Kárász Balázs; Kollár, Csaba (2020): Leadership Responsibilities in Information Security Awareness Development. ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE 19: 2 pp. 79-91., 13 p.
- Kollár Csaba (2016): Szerethetők-e a robotok: Az ember-robot interakció humán oldalának teoretikus aspektusa. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 26: különszám pp. 142-154., 13 p.
- Kollár Csaba (2017): SOCIAL ENGINEERING A GYAKORLATBAN: Manipulációk értelmezése a SPEAKING modellben. JELKÉP: KOMMUNIKÁCIÓ KÖZVÉLEMÉNY MÉDIA (ISSN: 0209-584X) (3), 62-77 pp.

- Kollár Csaba (2018): Az információbiztonság humán aspektusai: A biztonságtudatossági ellenőrzés során alkalmazott social engineering technikák elemzése a SPEAKING modell segítségével. BELÜGYI SZEMLE: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA (2010-) (ISSN: 2062-9494) 66: (2), 22-45 pp.
- Kollár Csaba (2022): Az ember-mesterséges intelligencia interakció kommunikációtudományi kérdései. In: Konczosné Szombathelyi Márta; Balogh Gábor; Jarjabka Ákos (szerk.) Kommunikáció - Gazdaság - Kultúra - Nyelv: 50 éve a közgazdász képzés szolgálatában. Tiszteletkötet Borgulya Istvánné részére. Pécs, Magyarország: Pécsi Tudományegyetem Közgazdaságtudományi Kar Vezetés- és Szervezéstudományi Intézet 310 p. pp. 58-69., 12 p.
- Kollár Csaba; Gombos Norbert; Vinárné Bellász Zsuzsanna (2016): Az információs gazdaság és az információbiztonság. Az információs társadalom egyik lehetséges megközelítése. ACTA ACADEMIAE BEREGSASIENSIS (ISSN: 2310-1954) 15: (1.), 225-231 pp.
- Kollár Csaba; Poór József (2016): Organisations in Digital Age – Information Security Aspects of Digital Workplaces. In: Michelberger Pál (szerk): Management, Enterprise and Benchmarking in the 21st Century III. Budapest: Keleti Károly Faculty of Business and Management, 73-82 pp.
- Kollár Csaba; Ványa László (2017): Szerethetők-e a robotok?: Az ember-robot interakció humán oldalának empirikus aspektusa. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 27: 1-2 pp. 163-177., 15 p.

- Kollár Csaba; Vinogradov Szergej (2018): A magyarországi községi és városi önkormányzatok vezető tisztségviselőinek információbiztonság-tudatossága. PRO PUBLICO BONO: MAGYAR KÖZIGAZGATÁS; A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA.

VI. TOVÁBBI TUDOMÁNYOS KÖZLEMÉNYEK

Módszertani közleményeim:

- Kollár Csaba (2004): Reklám- és reklámszöveg kutatás. Jegyzet. Budapest: Prema Consulting, 150 p.
- Kollár Csaba (2007): A digitális marketing lehetőségei a kereskedelmi egységek gyakorlatában, és ennek pszichológiai aspektusai. In.: Sikos T. Tamás (szerk.): A bevásárlóközpontok jelene és jövője. Komárom: Selye János Egyetem Kutatóintézete, 104-127 pp.
- Kollár Csaba (2014): A munkahelyi kiégés (burnout szindróma) elméleti megközelítése, kutatási irányai és közgazdaságtudományi aspektusa. FLUENTUM: NEMZETKÖZI GAZDASÁG- ÉS TÁRSADALOMTUDOMÁNYI FOLYÓIRAT, 1: (3) 1-19 pp.
- Kollár Csaba (2018): A szakértővé válás, illetve a szakértők kiválasztásának és megkérdezésének módszertani kihívásai. VEZETÉSTUDOMÁNY, 49: (2) pp. 63-75 pp.
- Mészáros Katalin; Szabóné Pataky Eszter; Iszak Noémi; Kállay Balázs; Gyöngyösy Zoltán; Kollár Csaba (2008): Fogyasztói magatartás és várható trendek, különös tekintettel az e-bankingre. In.: Herczeg

János (szerk.): Marketingkutatás módszertan: Első kötet: Elméleti alapok. Sopron: Papírmanufaktúra Kft., 182-225 pp.

Habilitációs pályázati témáimhoz szorosan kapcsolódó válogatott közleményeim:

- Heitlerné Lehoczky Mária; Kollár Csaba (2022): A mesterséges intelligencia múltja, jelene és jövője a senior és a junior szakértők szemszögéből: 1. rész BIZTONSÁGTUDOMÁNYI SZEMLE 4: 1 pp. 117-129., 13 p.
- Kollár Csaba (2015): Munkaadók és munkavállalók a digitális korban: Az intranettől a digitalizált munkahelyig. In: Futó Zoltán (szerk.): Tudomány és innováció a lokális és globális fejlődésért: nemzetközi tudományos konferencia előadásai. 311 p. Szarvas: Szent István Egyetem Egyetemi Kiadó, 157-163 pp.
- Kollár Csaba (2017): Emlékeink lenyomatainak információbiztonsága: Hogyan őrizhetőek meg és írhatóak át emlékeink a digitális korban? POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT 13: 4-6 pp. 173-183., 11 p.
- Kollár Csaba (2019): A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában. In: Rajnai, Zoltán (szerk.). Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori iskola 247 p. pp. 47-61., 15 p.
- Kollár Csaba (2019): A mesterséges intelligencia, mint komplex rendszer információbiztonsági kihívásai. In: Rajnai, Zoltán (szerk.)

Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori iskola 247 p. pp. 62-70., 9 p.

- Kollár Csaba; Poór József (2016): The leaders' awareness of information security. In: Dragica Radosav (szerk.): ENGINEERING MANAGEMENT AND COMPETITIVENESS (EMC 2016): VI International Symposium. Zrenjanin: University of Novi Sad, Faculty of Technical Sciences, 12-18 pp.

KÖSZÖNETNYILVÁNÍTÁS

Egy diplomadolgozat, egy doktori disszertáció, egy könyv – bár rendszerint csak egy, vagy könyvek esetében egy-néhány szerző jegyzi is, mégis – csapatmunka. Csapatmunka abban az értelemben, hogy a szerző titkolva, vagy korrekten lehivatkozva vesz át elképzeléseket más szerzők korábbi munkáiból, és azokat vagy szó szerint idézve, vagy átdolgozva, vagy az ott leírtakat továbbgondolva és kiegészítve építi be saját művébe, teszi saját munkássága szerves részévé. Csapatmunka abban az értelemben is, hogy az írásmű készítése közben, vagy még azt megelőzően az általunk tisztelt, szeretett és fontosnak tartott személyhez fordulunk, tanácsukat, véleményüket kérjük munkánk egészével, vagy egy részével kapcsolatban. Én is ezt tettem, s abban a szerencsés helyzetben voltam, hogy sok kiváló szakemberrel, kollégával kutathattam, publikálhattam közösen.

Elsőként az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar két professzorának, Rajnai Zoltánnak és Berek Lajosnak

tartozom köszönettel. Berek professzor úr a biztonságtudományi diszciplína biztonságtechnikai vonatkozásaival, Rajnai professzor úr az információbiztonsági vetületeivel ismertetett meg, illetve az információbiztonság-tudatosság fejlesztésének a fontosságára hívta fel a figyelmemet. Köszönettel tartozom továbbá Rajnai professzor úrnak azért is, hogy annak idején bizalmat szavazott nekem, hogy el tudtuk indítani a Biztonságtudományi Szemle című lektorált, szakmai-tudományos folyóiratot, illetve a Mesterséges Intelligencia Műhelyt. Mindkét kezdeményezés nem csak a saját, hanem a Folyóiratban publikáló, illetve a Műhelyben kutató és tevékenykedő hallgatók, doktoranduszok, kollégák szakmai fejlődését is szolgálják.

Köszönettel tartozom a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar két professzorának, Haig Zsoltnak és Ványa Lászlónak. Haig professzorral úrral az információbiztonságról, Ványa professzorral úrral pedig a robotikáról és a mesterséges intelligenciáról beszélgettünk számtalan alkalommal. Beszélgetéseinkből közös és saját kutatásokat indítottam el, melyek eredményei közös és saját tanulmányok formájában jelentek meg szakmai-tudományos folyóiratokban.

A digitális kor szervezetekre, s a szervezetek munkatársaira és vezetőire gyakorolt hatásának vizsgálatára Poór József az MTA doktora bíztatott. Több kutatásában és a belőlük született tanulmányok elkészítésében vettem részt.

Nevezett professzorok mellett közös tanulmányokat, könyvfejezeteket jegyzek többek között a következő kollégákkal is: Antalík Imrich, Bálint Brigitta, Balogh Gábor, Csehné Papp Imola, Dobay Péter, Farkas Attila,

Farkasné Kurucz Zsuzsa, Fodor Péter, Gábrielné Tőzsér Györgyi, Gombos Norbert, Heitlerné Lehoczky Mária, Horbulák Zsolt, Juhász Tímea, Kárász Balázs, Mészáros Katalin, Nemeskéri Zsolt, Palancsa Attila, Tokár-Szadai Ágnes, Vinárné Bellász Zsuzsanna, Vinogradov Szergej.
Köszönettel tartozom néhai Tomcsányi Pál akadémikusnak, aki a kutatásmódszertannal kapcsolatos kurzusain javasolta, hogy kezdjek el foglalkozni a digitális korral, illetve, hogy ismerjem meg és bátran kísérletezzek a különféle kutatási módszerekben rejlő lehetőségekkel. Hasonló hálát érzek néhai Menyhay Imre professzor irányába, aki felhívta a figyelmemet arra, hogy a technikai fejlődés és fejlesztés csak akkor érdemes támogatásra, ha abban a humán fókusz dominánsan van jelen.

Nevezettek erőfeszítéseinek köszönhető, hogy eddigi szakmai-tudományos pályafutásomról az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában katonai műszaki tudományágban jelen habilitációs pályázati anyagommal számot adhatok. Ha a számadás nem, vagy csak részint sikerült, akkor a hiányosságokért egyedül engem terhel felelősség, ha viszont sikerült, akkor ez valamennyi támogató csapattag sikere is.