ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

MÉSZÁROS ALEXANDRA ÁGNES

Ipari kémkedés vizsgálata a védelmi iparban működő innovatív kis- és középvállalkozások körében

Témavezető: Dr. Kelemen-Erdős Anikó

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. 02. 01.

Tartalomjegyzék

1 Summary

Industrial espionage is not a new problem; however, as a result of globalization, the development of technology, and changing geopolitical circumstances, it has become one of the most critical issues for the defense industry.

In the post-Cold War era, Europe's defense industry underwent a transformation, resulting in SMEs becoming engaged in R&D activities and joining the defense innovation ecosystem. Despite employing advanced information security systems, defense SMEs face a serious threat of industrial espionage, given the current geopolitical and economic conditions. Consequently, the decision-makers bear significant responsibility for protecting critical business information.

The dissertation examines the industrial espionage that threatens innovative SMEs operating in the European defense industry, employing a multidisciplinary socio-technical approach focusing on the human factor. This research aims to identify measures that can effectively mitigate this threat. To accomplish this objective, this study examines the elements causing an increase in the frequency of industrial espionage, the role of the human factor, and the opportunities for reducing the identified information security risk. The results evolved from empirical data collected through in-depth interviews, applying grounded theory methodology (n=42). The advantage of this methodology is that results were not drawn from previously formulated literature and regulations; instead, the defined theory was built upon the thoughts of individuals with practical experience gathered during fieldwork. Therefore, the results can be effectively applied in real-world situations as they bridge the gap between the theoretical framework and practical application.

The purpose of this dissertation is not to define a universally effective information security system, as the diverse environmental variables affecting SMEs make such a system unfeasible. Instead, it aims to establish a framework that helps decision-makers identify specific characteristics of different situations, enabling them to apply the most suitable measures in a given scenario. Empirical results from this study suggest that the risk of industrial espionage can be addressed on three levels: managing external environmental threats, implementing a comprehensive information security policy, and mitigating threats posed by the human factor. Based on these factors, recommendations are provided for developing company-specific information security systems.

2 A kutatás előzményei

A védelmi ipar minden nemzet számára stratégiai jelentőségű. Az állampolgárok biztonságának védelme mellett számtalan társadalmi, politikai és gazdasági területen rendelkezik kiemelt szereppel. Azonban az ipar azon tulajdonsága, amely a jelen doktori értekezés szempontjából igazán releváns, hogy a tudásintenzív ágazatra jellemző aktív kutatás és fejlesztés során számtalan technológiai innovációval látja el a védelmi erőket, továbbá a teljes társadalmat. A hidegháború utáni időszakban a védelmi ipar átalakulása lehetőséget biztosított a kis- és középvállalkozások (továbbiakban kkv) számára, hogy tevékenységet folytassanak az ágazatban, amelyek azóta kiemelkedő teljesítményt nyújtanak az innovációk fejlesztése területén [2, 3, 4, 5, 6]. Az innovációs tevékenység folytatásának legértékesebb eleme – a tudást előállító ember mellett – a kritikus információ, melynek védelme kulcsfontosságú feladat, azonban jelen gazdasági és geopolitikai körülmények között a legkorszerűbb információvédelmi rendszerek alkalmazása mellett is kiemelten fenyegeti a védelmi iparban működő kkv-ket az ipari kémkedés.

Az értekezés az európai védelmi ipar területén tevékenységet folytató, innovatív kkv-k szempontjából vizsgálja az ipari kémkedés fenyegetését, szociotechnikai megközelítést alkalmazva, a humán faktort középpontba helyezve. A kutatás eredményei empirikus, a mélyinterjúk során gyűjtött adatokból fejlődtek (n=42), amelynek előnye, hogy nemcsak a korábban megfogalmazott szakirodalomból és jogszabályokból vontam le a következtetéseket, hanem a terepmunka során gyűjtött, gyakorlati tapasztalattal rendelkező személyek gondolatai szolgáltak túlnyomórészben az elméleti munka alapjául.

Korábban Magyarországon a védelmi ipar, továbbá az ehhez szükséges szakirányú oktatás néhány kivétellel gyakorlatilag megszűnt. Azonban olyan kezdeményezések hatására, mint a 2016-ban elfogadott, a magyar ipar fejlesztéséről szóló Irinyi Terv, a szintén 2016-ban meghirdetett Zrínyi Honvédelmi és Haderőfejlesztési Program, vagy a 2023-ban induló hadiipari mérnök mesterképzés az Óbudai Egyetemen lehetőséget teremtenek, hogy a nagy tőkebefektetők mellett a hazai kkv-k is csatlakozhassanak a védelmi innovációs ökoszisztémához. A **védelmi innovációs ökoszisztéma** egy olyan környezet, mely szereplői együttműködnek a nemzetbiztonsági kérdésekkel kapcsolatos kutatás, fejlesztés és innovációs (továbbiakban KFI) tevékenységekben a védelmi képességek fejlesztésének céljából, mely kooperációk lehetővé teszik a gyors és hatékony reakciót a folyamatosan változó fenyegetésekre. Ezen környezetnek fontos szereplőik a kkv-k, melyek versenyképes működéséhez szükséges megismerniük a biztonságukat fenyegető minden szervezeti külső és

belső környezeti változót. Mivel az ehhez szükséges források nem elérhetők, nem nyilvánosak, hiányosak vagy esetenként szándékosan félrevezetők, ezek kutatása új módszertani megközelítést igényel. A védelmi kkv-k védelme, továbbá a fenyegetésekre és azok elhárítására történő felkészítése a sikeres működésük miatt elengedhetetlen, ezért az értekezésben kutatott téma nagy jelentőséggel bír.

Az európai védelmi ipar transzformációja lehetővé tette a magánszektort képviselő kkv-k megjelenését a piacon [2, 42, 43], melyek szerepe és száma várhatóan növekedni fog a jövőben [44]. 2022-ben az Európai Unió területén több mint 2500 kkv [45], közvetlenül 463 ezer főt foglalkoztat a védelmi ipar területén [46]. Ezek a vállalkozások kiemelkedő innovációs képességekkel rendelkeznek [2, 3, 5, 47, 48, 49], amelyet nagyrészben belső kutatással és fejlesztéssel támogatnak [50]. Az európai védelmi iparnak célkitűzése, hogy képes legyen teljes mértékben a kkv-kból származó innovációkra támaszkodni [45]. Ennek eléréséhez az Európai Védelmi Alap 2022-ben 832 millió eurót [51], 2023-ban 1,2 milliárd eurót biztosított a védelmi célú KFI tevékenységekre [52]. A rohamosan fejlődő technológia jelentős hatást gyakorol a védelmi iparra, következésképpen a katonai összeütközések módszerei-, és eljárásai is változnak [53], amely megköveteli a helyi vállalkozásoktól az új technológiák fejlesztését. Mivel a nagy védelmi vállalatok nem érdekeltek a szűk piacok, vagy személyre szabott igények kiszolgálásában [43, 54], a kkv-k versenyképesen működhetnek, ha a tevékenységüket réspiacokra, továbbá személyre szabott védelmi eszközök fejlesztésére összpontosítják [6, 48, 55, 56].

A 2022. februárban kirobbant orosz-ukrán fegyveres konfliktus hatására Európa-szerte megindult a hadiipar fejlesztése, melynek következményeként a védelmi iparban előállított kritikus információ értéke ugrásszerűen növekedett, és vált keresetté az ágazat szereplői között, mely szintén fontossá teszi a tudományos probléma kutatását.

Jelen értekezésben az **ipari kémkedés** olyan szervezetek vagy kormányok által szervezett etikátlan vagy illegális információgyűjtési tevékenységet foglal magában, ami egy másik, a védelmi ipar területén működő vállalkozás KFI tevékenységéből származó, továbbá a termék előállításához és a piac ellátáshoz szükséges információ megszerzésére irányul, jelentős stratégiai és gazdasági hátrányt okozva a tudást előállító szervezetnek, és a megszerzett kritikus információt a kémkedést szervező entitás a saját előnyére fordíthatja. Az értekezésben a kémkedés tárgya elsősorban a védelmi innovációk fejlesztéséhez, előállításához és értékesítéséhez szükséges **kritikus információ**, ami minden olyan üzleti titok, amelynek az

eltulajdonítása az azt előállító vállalkozástól egy másik entitás előnyét szolgálja, miközben kárt okoz a tudást jogosan birtokló szervezetnek.

Az európai védelmi ipar területén tevékenységet folytató kkv-k ipari kémkedés elleni védekezéshez való viszonyát kvalitatív kutatás során ilyen mélységben korábban még nem vizsgálták. Bár számos megoldás található a rendelkezésre álló szakirodalomban a komplex fenyegetés megközelítésére, azonban a problémát még nem sikerült hatékonyan kezelni, ami szintén indokolja a kérdés kutatását.

Az információbiztonsági fenyegetés szervezeti szintű menedzseléséről számos elméleti aspektusú tudományos publikáció érhető el, mindazonáltal az ipari kémkedés elleni hatékony védekezés empirikus szemléletet igényel. Jelen kutatás során törekszem arra, hogy a gyakorlati alkalmazhatóságot integráljam az elméleti megközelítésbe. Ennek a perspektívának az újdonságtartalma, hogy az eredményeket a gyakorlatban hasznosítva hatékonyabban lehet védekezni az ipari kémkedés külső és belső fenyegetésével szemben egyaránt.

3 Célkitűzések

Az értekezésben célom olyan empirikus adatokon alapuló, gyakorlatban alkalmazható eredményeket megfogalmazása, melyek támogatják a védelmi vállalkozások vezetőit az ipari kémkedés elleni küzdelemben. A kontingenciaelméleti megközelítést alkalmazva nem törekszem egy univerzális, minden helyzetben jól működő információvédelmi rendszert definiálni, mivel minden vállalkozásra más külső és belső tényezők hatnak ugyanabban az időben, így ez nem megvalósítható. Azonban célom a döntéshozók számára egy olyan eszközrendszert meghatározni, melynek segítségével képesek a különböző helyzetek sajátosságait beazonosítani, és ezen szituációkban a legmegfelelőbb eszközöket alkalmazni.

A kutatás tervezése során a következő **célkitűzéseket (C**) fogalmaztam meg:

C1: A kutatás során célom az elméleti megközelítés és a gyakorlati alkalmazhatóság közötti szakadék áthidalása az ipari kémkedés megelőzésének és észlelésének területén.

C2: Célkitűzésem, hogy multidiszciplináris megközelítést alkalmazva feltárjam azon külső és belső kontingenciaváltozókat, amelyek azonosíthatók az ipari kémkedés gyakoriságának növekedése mögött.

C3: Célom annak feltérképezése, hogy milyen motivációk, körülmények és támogató tényezők ismerhetők fel a vállalkozás belső érintettjei által elkövetett ipari kémkedési esetek mögött.

C4: Célkitűzésem megismerni, hogy az innovatív védelmi vállalkozásoknak, valamint azok érintettjeinek, milyen a percepciója az ipari- és gazdasági kémkedés jelentette kockázat kapcsán, illetve milyen módszereket és eszközöket alkalmaznak az ipari kémkedés fenyegetésének csökkentésére.

C5: A dinamikusan változó környezeti kontingenciatényezők mellett a kutatómunkám célja előretekinteni, hogy a jelenben alkalmazott ipari kémkedési módszerek fejlődéséből következtetve milyen természetű jövőbeni információbiztonsági fenyegetésekre szükséges felkészülni az innovatív védelmi vállalkozásoknak.

A grounded theory módszertan követelményeinek megfelelően nem fogalmazhatok meg hipotéziseket, így előhipotézisek, úgynevezett **propozíciók (P)** definiálása mellett döntöttem. A kutatás során olyan eredményekhez sikerült jutnom, melyek megalapozták az értekezésben a tézisek megfogalmazását.

P1: A belső szervezeti és külső környezeti kontingenciaváltozók folyamatos megfigyelése, elemzése és értelmezése keretrendszert nyújthat az ipari kémkedés kockázatának csökkentéséhez az innovatív védelmi kis- és középvállalkozásoknál.

P2: Meghatározhatók az innovatív védelmi kis- és középvállalkozásoknál olyan intézkedések, melyekkel a vállalkozás érintettjei által elkövetett ipari kémkedés kockázata mérsékelhető.

P3: Az innovatív védelmi kis- és középvállalkozások döntéshozói az információs technológiai szempontokat helyezik előtérbe az információbiztonsági rendszer kialakítása során, mely közben a holisztikus megközelítésű szociotechnikai szempontok a háttérbe szorulnak.

P4: Az ipari kémkedés elkövetésére alkalmas technológiák fejlődésével az innovatív védelmi kis- és középvállalkozásoknak olyan információbiztonsági fenyegetésekkel kell a közeljövőben szembenézni, melyek megkövetelik az alkalmazott információvédelmi intézkedések teljeskörű átalakítását.

Az eredményekből arra a következtetésre jutottam, hogy az ipari kémkedés kockázatát három különböző szinten szükséges kezelni, melyek a külső környezeti fenyegetés kezelése, az átfogó információbiztonsági politika és a belső érintettek jelentette fenyegetés menedzselése.

4 Vizsgálati módszerek

Jelen kutatás folyamán az adatgyűjtés szakértői mélyinterjúk során valósult meg, a gyűjtött adatok elemzése **grounded theory** (megalapozott elmélet) módszertannal történt. A grounded theory egy széles körben elismert, tudományosan megalapozott, szisztematikus adatelemzési módszertan [80, 89, 90, 91], melynek az alkalmazása során az elmélet empirikus adatokból fejlődik ki [92]. Az értekezésben alkalmazott konstruktivista megközelítés **abduktív**, mert logikai következtetéseket von le a megfigyelt jelenségről; **induktív**, mivel az elméletet a gyűjtött adatokból vezeti le; ugyanakkor **deduktív**, mert az elmélet fejlődése során az eredményeket összeveti a szakirodalommal [87, 91].

Kvalitatív kutatás során a definiált eredmények megítélésének legfontosabb kritériuma a **megbízhatóság** [95, 96, 97], amely a következetességből, az átvihetőségből, a hitelességből, és a megerősíthetőségből tevődik össze [97, 98, 99]. Az eredmények megbízhatóságának biztosítása érdekében jelen kutatás figyelembe veszi ezen szempontokat.

Az értekezésben **kontingenciaelméleti** megközelítésből vizsgáltam a védelmi ipar területén tevékenységet folytató innovatív kkv-ket fenyegető ipari kémkedés külső és belső kockázatait. Az elmélet a szervezeti viselkedést abból a szempontból vizsgálja, hogy a kontingenciatényezők hogyan befolyásolják a vállalkozás kialakítását és működését [124], melynek alapján a szervezetek teljesítménye nagy mértékben függ a külső körülmények és az előre nem jelezhető események alakulásától. Következtetésképpen nincs egy meghatározott stratégia, amit minden vállalkozás követ, hanem folyamatosan alkalmazkodniuk szükséges a külső dinamikusan változó környezethez. A megközelítés szerint azon vállalkozásoknak van a legnagyobb esélyük a sikeres működésre, amelyek rugalmasan és gyorsan képesek reagálni a külső lehetőségekre és fenyegetésekre. Az értekezésben újszerű megközelítést alkalmaztam és az ipari kémkedést a védelmi innovatív kkv-re ható kontingenciaváltozók közé kategorizáltam.

A mélyinterjúkon a védelmi iparban folytatott KFI tevékenységek területén szerzett több éves – egyes alanyok esetén több évtizedes – tapasztalattal rendelkező személyek vettek részt. 42 mélyinterjú készült, az alanyok kilenc európai országot képviseltek, melyeket az 1. táblázat szemléltet.

Interjú	Ország	Szektor/profil	Az alany pozíciója
I. szakasz (2022. I.-II. negyedév)			
1.	Anglia	Repülőipar	Fejlesztőmérnök
2.	Anglia	Repülőipar	Fejlesztőmérnök
3.	Ausztria	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
4.	Ausztria	Gépalkatrész gyártás	Vezérigazgató
5.	Bulgária	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
6.	Bulgária	Védelmi felszerelés nagykereskedő	Tulajdonos/Vezérigazgató
7.	Csehország	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
8.	Csehország	Védelmi felszerelés KFI és gyártás	Fejlesztőmérnök
9.	Horvátország	Fémalkatrész gyártás	Vezérigazgató
10.	Horvátország	Fémalkatrész gyártás	Értékesítési igazgató
11.	Lengyelország	Fémalkatrész gyártás	Fejlesztőmérnök
12.	Lengyelország	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
13.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Információbiztonsági szakértő
14.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Vezérigazgató
15.	Magyarország	Repülőipar – alkatrész KFI	Információbiztonsági szakértő
16.	Magyarország	Védelmi felszerelés KFI és gyártás	Tulajdonos/vezérigazgató
17.	Magyarország	Védelmi felszerelés KFI és gyártás	Információbiztonsági szakértő
18.	Magyarország	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
19.	Magyarország	Katonai jármű KFI és gyártás	Fejlesztőmérnök
20.	Németország	Katonai jármű KFI és gyártás	Fejlesztőmérnök
21.	Németország	Katonai jármű KFI és gyártás	Információbiztonsági szakértő
22.	Németország	Védelmi felszerelés KFI és gyártás	Fejlesztőmérnök
23.	Németország	Védelmi felszerelés KFI és gyártás	Fejlesztőmérnök
24.	Németország	Optika	Értékesítési igazgató
25.	Szerbia	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
26.	Szerbia	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
27.	Szerbia	Optika	Információbiztonsági szakértő
II. szakasz (2022. III. negyedév)			
28.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Vezérigazgató
29.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Információbiztonsági szakértő
30.	Magyarország	Repülőipar – alkatrész KFI	Információbiztonsági szakértő
31.	Magyarország	Űripar – alkatrész KFI	Vezérigazgató
32.	Magyarország	Űripar – alkatrész KFI	Információbiztonsági szakértő
33.	Magyarország	Katonai jármű – alkatrész KFI	Vezérigazgató
34.	Magyarország	Katonai jármű – alkatrész KFI	Információbiztonsági szakértő
35.	Magyarország	Védelmi felszerelés KFI és gyártás	Tulajdonos/vezérigazgató
36.	Magyarország	Rakétaelhárító rendszer	Tulajdonos/vezérigazgató
III. szakasz (2023. I. negyedév)			
37.	Anglia	IT – hardverfejlesztés	Fejlesztőmérnök
38.	Anglia	Űripar – alkatrész KFI	Tulajdonos
39.	Németország	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
40.	Magyarország	Védelmi felszerelés KFI és gyártás	Tulajdonos
41.	Magyarország	IT – szoftverfejlesztés	Fejlesztőmérnök
42.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Információbiztonsági szakértő

1. táblázat: Az interjúalanyok jellemzői

Forrás: saját szerkesztés (n=42)

5 Új tudományos eredmények

Tézis 1.

A kutatásaim eredményei alapján állítom, hogy a védelmi iparban tevékenységet folytató innovatív kis- és középvállalkozásoknak a kritikus információ hatékony védelméhez minden olyan külső környezeti változót folyamatosan monitorozni és elemezni szükséges, melyek közvetlenül vagy közvetve hatást gyakorolnak a tevékenység folytatására. Bármely külső kontingenciatényező, mely olyan hirtelen jelentkező információigényt válthat ki az ágazat valamelyik szereplőjéből, amelyet nem képes vagy hajlandó a rendelkezésre álló erőforrásokkal kielégíteni, ipari kémkedést idézhet elő. A környezet folyamatos elemzése nem csak információbiztonsági szempontból támogatja a vállalkozást, hanem lehetőséget biztosít azon katalizáló faktorok észlelésére, melyek hatására megszülethet az innovatív ötlet.

Kapcsolódó publikációk: **P2** (MTA besorolás szerint B), **P5** (Q3), **P6** (MTA besorolás szerint A), **P7**, **P8.**

Tézis 2.

A mélyinterjúk során gyűjtött adatok alapján állítom, hogy a védelmi iparban tevékenységet folytató innovatív kis- és középvállalkozásoknak az információvédelmi rendszer kialakítása során minden, a vállalkozás zavartalan működéséhez nélkülözhetetlen belső folyamatot, továbbá az azokat támogató humán tényezőt, információt, berendezést és eszközt vizsgálni és szinkronizálni szükséges. Az ipari kémkedés kockázatának hatékony mérséklése csak szociotechnikai szemlélettel kialakított, vállalatspecifikus rendszerrel lehetséges.

Kapcsolódó publikációk: **P1** (Q2), **P3**, **P4**, **P6** (MTA besorolás szerint A).

Tézis 3.

Kutatásaim igazolják, hogy az ipari kémkedés szempontjából az innovatív védelmi kis- és középvállalkozások számára a legkritikusabb tényező a humán faktor, mely megnyilvánulhat szándékosan elkövetett esetek, és véletlen hibákból eredő incidensek formájában, mert bennfentes ismeretei és a rendszerhez való hozzáférése miatt jelentős kárt képes okozni szervezetnek.

Kapcsolódó publikációk: **P1**(Q2), **P3**, **P4.**

Tézis 4.

Empirikus kutatásommal bizonyítom, hogy az ipari kémkedés elleni védekezésben meghatározó a döntéshozók figyelmének felhívása a fenyegetés okaira, természetére, globális trendjeire és a lehetséges következményekre, mert hiányos ismereteik következményeként olyan megelőzési és észlelési szempontokat hagyhatnak figyelmen kívül, melyek sebezhetővé teszik a vállalkozást a vizsgált probléma szempontjából.

Kapcsolódó publikációk: **P1** (Q2), **P2** (MTA besorolás szerint B), **P3**, **P4**.

Tézis 5.

Az ipari kémkedés elkövetésére használt eszközök és módszerek bár folyamatosan fejlődnek, azonban az internet és az okoseszközök elterjedése óta nem jelentek meg olyan diszruptív innovációk a területen, amelyek alapjaiban formálnák át a védekezési rendszereket, csak a már régóta alkalmazott technológiák vállnak célzottabbá és hatékonyabbá. Azonban a napjainkban jellemző dinamikus technológiai fejlődés mellett bármikor megjelenhet egy olyan diszruptív innováció, amellyel szembeni védekezésre nincsenek felkészülve az értekezés írásának időpontjában alkalmazott információvédelmi rendszerek, ami szintén alátámasztja az 1. tézist.

Kapcsolódó publikációk: **P5** (Q3).

6 Az eredmények hasznosítási lehetősége

6.1 Az eredmények elméleti hasznosíthatósága

Jelen kvalitatív kutatás eredményei a védelmi iparban működő innovatív kkv-ket fenyegető ipari kémkedés attribútumait, és a probléma elleni védekezési lehetőségeket vizsgálva gazdagítja a témában rendelkezésre álló szakirodalmat empirikus adatokon alapuló elmélettel. Az ipari kémkedés egy viszonylag új és nehezen kutatható tudományos terület, amely az esetszámok növekedése és negatív következményei ellenére kevés tudományos figyelmet kap [12, 13, 39, 70, 71, 72, 73], így a jelen doktori értekezésben definiált eredmények hozzájárulnak a tudományos probléma elméleti hiányosságainak mérsékléséhez.

A kutatás során az 1960-as években definiált kontingenciaelméleti megközelítésből vizsgáltam a védelmi ipar területén tevékenységet folytató innovatív kkv-ket fenyegető ipari kémkedés külső és belső kockázatait, mely során arra a következtetésre jutottam, hogy a módszer a napjaink dinamikusan változó környezetében is aktuális és releváns megközelítés. Az értekezés azon külső és belső kontingenciatényezőkkel egészíti ki a tudományos problémát vizsgáló szakirodalmat, melyek globális szinten hozzájárulnak az ipari kémkedéshez fűződő esetszámok növekedéséhez (Tézis 1., 2.).

Bár a kutatás a védelmi ipar területén működő kkv-k körében folyt, azonban az esetszámok növekedéséért felelős azonosított gazdasági és geopolitikai külső kontingenciatényezők más európai innovatív iparágakra is vonatkoztathatók, melyek csak közvetve kapcsolódnak a védelmi iparhoz (például autóipar vagy gyógyszeripar), így gazdagítva a szakirodalmat.

Az értekezésben részletesen bemutatom a védelmi ipar stratégiai szerepét és az ipari kémkedés komplex problémakörét szekunder adatokra támaszkodva, korábbi primer eredményeimmel kiegészítve, egy összefoglaló elemzést biztosítva a témákban érdekelt kutatóknak.

A korábbi kutatások az ipari kémkedés összetett kérdéskörét főként a technológiai [17, 33], jogi [17, 34, 35], és a külső tényezők szempontjából vizsgálják [36], kevés tudományos figyelmet fordítva a belső fenyegetésre [25, 33, 37, 38, 205]. Azonban az értekezésben definiált elmélet magában foglalja a belső érintettek által elkövetett szándékos és véletlen incidensek mögött azonosított tényezőket is (Tézis 3.).

A kutatás eredményei hozzájárulnak a menedzsment tudományok fejlesztéséhez a gazdasági és ipari kémkedés kockázatának csökkentésére alkalmazható, empirikus adatokon alapuló gyakorlatok definiálásával (Tézis 4.), továbbá az ipari kémkedés elkövetésére alkalmas

eszközök és módszerek közeljövőben várható természetének bemutatásával (Tézis 5.), alapot biztosítva a kutatóknak a téma mélyebb kifejtésére. Bár a digitalizáció szempontjából elérhetők tudományos publikációk a jövőbeni információbiztonsági fenyegetésekről [137, 138, 240], azonban ezen megközelítések mellett jelen értekezés társadalmi és pszichológiai szempontból is érinti az ipari kémkedés várható körülményeit, amely szintén kevésbé kutatott terület.

Jelen kutatás során az empirikus adatok elemzése kvalitatív grounded theory módszertannal történt. A metodológia bemutatása közben kiemelt figyelmet fordítottam a kutatás megbízhatósági kritériumának szakirodalomelemzés alapján történő összefoglalására és ismertetésére, amely keretrendszert nyújt a kvalitatív elemzést végző kutatóknak a definiált eredményeik megbízhatóságának alátámasztásában.

Az értekezésben összegyűjtött kutatási limitációk szintén gazdagítják az elméletet, felhívva a kutatók figyelmét azon nehézségekre, melyeket figyelembe szükséges venni a téma tudományos megközelítésű vizsgálata során.

6.2 Az eredmények gyakorlati hasznosíthatósága

Az értekezés eredményei betekintést nyújtanak a védelmi ipart fenyegető ipari kémkedés komplex jelenségébe, így hasznos információkkal szolgál az innovatív vállalkozások vezetőinek. Ennek keretében fontosnak érzem, hogy a definiált elmélet a tudományos körök mellett azon döntéshozók számára is elérhető legyen, akiknek a mindennapi üzleti gyakorlatára lehet jelentős hatással (Tézis 4.). A célom olyan empirikus – kiemelkedő ágazati ismeretekkel rendelkező interjúalanyok tapasztalatain alapuló – eredmények feltárása volt, melyek a gyakorlatban alkalmazva hatékonyabb információbiztonsági intézkedések tervezését és végrehajtását teszik lehetővé.

A kutatás fókusza kiterjedt a vállalkozásokat fenyegető külső és belső kontingenciatényezőkre egyaránt, ezáltal keretrendszert nyújt azon változók azonosításához, amelyekkel szemben védeni szükséges a kritikus információt (Tézis 1 –2.). A globális esetszámok növekedését okozó gazdasági és geopolitikai faktorok feltárása a gyakorlati alkalmazás során segít a döntéshozóknak felismerni azon környezeti eseményeket, melyek folyamatos megfigyelésével képesek csökkenteni az ipari kémkedés kockázatát. Az azonosított elmélet alapot biztosít a hatékony információbiztonsági rendszer kialakításához, a belső érintettekhez fűződő fenyegetés kezeléséhez, továbbá az információbiztonsági politika definiálásához.

Az értekezésben bemutatott, információs technológiai rendszer fejlesztésének szempontjait ismertető eredmények gyakorlati jelentősége, hogy felhívja a döntéshozók figyelmét a belső

érintettek információs technológiai ismereteinek hiányosságaira, továbbá a véletlen elkövetett hibák csökkentésére alkalmas, könnyen kezelhető és felhasználóbarát rendszer kialakításának fontosságára (Tézis 4.). Az információvédelmi rendszer kialakítása során a kkv-knél gazdasági szempontokat is figyelembe kell venni, mivel ezek bevezetése és üzemeltetése financiális terhet jelenthet. Az értekezésben bemutatott rendszer megvalósítása során azonban lehetőségük van a vezetőknek a rendelkezésükre álló erőforrások alapján meghatározni azokat a módszereket és eszközöket, melyek a költséghatékonyság mellett is megfelelő mértékben csökkentik az ipari kémkedés kockázatát (Tézis 5.).

A kvalitatív kutatás megbízhatóságának kritériuma az átvihetőség, mely fontos a gyakorlati felhasználás szempontjából, mivel a döntéshozók sok esetben csak egy vagy néhány kutatásból származó eredményre támaszkodhatnak, amelyek empirikus alkalmazása eltérhet a kutatási környezettől. Az átvihetőség kritériumának való megfelelést biztosítja, hogy az adatgyűjtés kilenc európai országban a védelmi ipar számos területén történt.

Az értekezés alapján definiálható azon területek listája, melyeket kiemelten ajánlott magyarázni a belső érintettek képzése során, így összeállítható egy olyan hatékony oktatási program, mely segíthet az alkalmazottak felkészítésében az ipari kémkedés veszélyeire és a megelőzési módszerekre (Tézis 3.).

Az eredmények szintén támogathatják az állami és iparági szabályozó szervezeteket a hatékonyabb intézkedések kidolgozásában az ipari kémkedés kezelésére.

A kutatás során gyűjtött adatokból következtethető, hogy a vállalkozások döntéshozói tisztában vannak az ipari kémkedés kockázatával, mert alkalmaznak a megelőzésére és észlelésére alkalmas eszközöket, azonban a használt rendszerek hiányosságaiból feltételezhető, hogy nem gondolják úgy, hogy ők is valóban áldozatul eshetnek. Ennélfogva fontos a vezetők tudatosságának növelése és figyelmük felhívása az ipari kémkedési incidensek gyakoriságára és káros következményeire (Tézis 4.). A definiált elmélet támogatja a fenyegetés természetének megértését, így segítve az üzleti kockázatok hatékonyabb értékelését és a döntéshozást az információbiztonság javítása érdekében.

7 Irodalmi hivatkozások listája

[1] WIMMER, B.: Business Espionage: Risks, Threats, and Countermeasures; Oxford, Elsevier 2015.

[2] CHIN, W.: Technology, War And the State: Past, Present and Future; International Affairs 95. 4. (2019) pp. 765–783. DOI: https://doi.org/10.1093/ia/iiz106

[3] TAKSÁS B.: Trinity of Defense Industry; Economics and Management 2019. 1. (2019) pp. 70–86.

[4] CHEUNG, T. M.: A Conceptual Framework of Defence Innovation; Journal of Strategic Studies 44. 6. (2021) pp. 775–801.
DOI: https://doi.org/10.1080/01402390.2021.1939689

[5] DOMBROWSKI, P. – GHOLZ, E.: Identifying Disruptive Innovation: Innovation Theory and the Defense Industry; Innovations: Technology, Governance, Globalization 4. 2. (2009) pp. 101–117.

[6] MÉSZÁROS A. Á. – TÓTH I. M. – CSISZÁRIK-KOCSIR Á.: A védelmi ipar lokális gazdaságra gyakorolt hatásának kvalitatív vizsgálata; Vállalkozásfejlesztés a XXI. században 2022. 2. (2022) pp. 193–206.

[7] EURÓPAI BIZOTTSÁG: Felhasználói útmutató a kkv-k fogalommeghatározásához, 2020.
https://ec.europa.eu/docsroom/documents/42921/attachments/1/translations/hu/renditions/native (letöltve: 2023. 12. 20.).

[8] GHERGHINA, Ș. C. – BOTEZATU, M. A. – HOSSZU, A. – SIMIONESCU, L. N.: Small and Medium-Sized Enterprises (SMEs): The Engine of Economic Growth through Investments and Innovation; Sustainability 12. 1. (2020) p.: 347.
DOI: https://doi.org/10.3390/su12010347

[9] TAKSÁS B.: Hadiipari kutatások jelentősége; Hadmérnök 12. 3. (2017) pp. 167–174.

[10] T. CSIKI T.: Kísérlet a védelmi ipar fejlesztésére Magyarországon?. In: TÁLAS P. – CSIKI T. /szerk./: Magyar biztonságpolitika 1989–2014. Tanulmányok. Nemzeti Közszolgálati Egyetem, Stratégiai Védelmi Kutatóközpont. 2014., pp. 127–141. ISBN 978-615-5305-50-4

[11] HAIG Z.: Információbiztonság; Nemzeti Közszolgálati Egyetem 2017.
URI: http://hdl.handle.net/20.500.12944/100142

[12] SØILEN, S. K.: Economic and Industrial Espionage at the Start of the 21st Century - Status Quaestionis; Journal of Intelligence Studies in Business 6. 3. (2016) pp. 51–64.
DOI: https://doi.org/10.37380/jisib.v6i3.196

[13] BUTTON, M.: Editorial: Economic and industrial espionage; Security Journal 33. (2020) pp. 1–5. DOI: https://doi.org/10.1057/s41284-019-00195-5

[14] THORLEUCHTER, D. – VAN DEN POEL, D.: Protecting Research and Technology from Espionage; Expert Systems with Applications 40. 9. (2013) pp. 3432–3440. DOI: https://doi.org/10.1016/j.eswa.2012.12.051

[15] SUTHERLAND, I. – JONES, A.: Industrial Espionage from Residual Data: Risks and Countermeasures; Australian Digital Forensic Conference 12. 1. (2008) pp. 167– 172. DOI: https://doi.org/10.4225/75/57b2771540cc2

[16] HÄRTING, R. C. – BÜHLER, L. – WINTER, K. – GUGEL, A.: The Threat of Industrial Espionage for SME in the Age of Digitalization; Procedia Computer Science 207. (2022) pp. 2940–2949.
DOI: https://doi.org/10.1016/j.procs.2022.09.352

[17] LYAN, I. – FRENKEL, M.: Industrial Espionage Revisited: Host Country–Foreign Multinational Corporation Legal Disputes and the Postcolonial Imagery; Organization 29. 1. (2020) pp. 30–50.
DOI: https://doi.org/10.1177/1350508420928517

[18] TRIM, P. R.: Counteracting Industrial Espionage through Counterintelligence: The Case for a Corporate Intelligence Unit and Collaboration with Government Agencies; Security Journal 15. (2002) pp. 7–24.
DOI: https://doi.org/10.1057/palgrave.sj.8340001

[19] SINHA, S.: Understanding Industrial Espionage for Greater Technological and Economic Security; IEEE Potentials 31. 3. (2012) pp. 37– 41.
DOI: https://doi.org/10.1109/MPOT.2012.2187118

[20] NASHERI, H.: Economic Espionage and Industrial Spying: Dimensions of Economic Espionage and the Criminalization of Trade Secret Theft; Cambridge, Cambridge University Press 2004., pp. 1– 29.
DOI: https://doi.org/10.1017/CBO9780511610288.002

[21] WAGNER, R. E.: Bailouts and the Potential for Distortion of Federal Criminal Law: Industrial Espionage and Beyond; Tulane Law Review 86. 5. (2012) pp. 1017– 1055.

[22] NYESTE P.: A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén; Felderítő Szemle 12.1. (2013) pp. 100–119. ISSN: 1588-242X

[23] SCHUBERT B.: Az ipari kémkedés megjelenése a magyar büntetőjogban – a Huawei-ügy tükrében, 2019.
https://arsboni.hu/ipari-kemkedes-a-huawei-ugy-tukreben/ (letöltve: 2023. 12. 20.)

[24] 2018. évi LIV. törvény az üzleti titok védelméről

[25] BARRACHINA, A. – TAUMAN, Y. – URBANO, A.: Entry with two Correlated Signals: the Case of Industrial Espionage and its Positive Competitive Effects;

International Journal of Game Theory 50. (2021) pp. 241–278.
DOI: https://doi.org/10.1007/s00182-020-00748-8

[26] ROTHKE, B.: Corporate Espionage and What Can Be Done to Prevent It; Information Systems Security 10. 5. (2001) pp. 1– 7, 2001.
DOI: https://doi.org/10.1201/1086/43315.10.5.20011101/31716.3

[27] SCHUMPETER, J. A.: Business Cycles: A Theoretical, Historical, And Statistical Analysis of the Capitalist Process; New York, McGraw Hill Book Co 1939.

[28] HEGEDŰS E. – GYARMATI J.: A haditechnikai kutatás-fejlesztés helye, szerepe és sajátosságai; Hadmérnök 17. 2. (2022) pp. 17–32.
DOI: https://doi.org/10.32567/hm.2022.2.2

[29] KELEMEN-ERDŐS A. – MÉSZÁROS A. Á.: Az ipari és gazdasági kémkedés kvalitatív vizsgálata a védelmi iparban; Felderítő Szemle 2022. 4. (2022) pp. 95–110. (1588-242X)

[30] PRIPORAS, C. V.: Competitive Intelligence Practice in Liquor Retailing: Evidence from a Longitudinal Case Analysis; International Journal of Retail & Distribution Management 47. 9. (2019) pp. 997– 1010. ISSN: 0959-0552

[31] HOMOLIAK, I. – TOFFALINI, F. – GUARNIZO, J. D.– ELOVICI, Y. – OCHOA, M.: Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures; ACM Computing Surveys 52. 2. (2020) pp. 1–40.
DOI: https://doi.org/10.1145/3303771

[32] SAXENA, N. –HAYES, E. – BERTINO, E. – OJO, P. – CHOO, K. K. R. – BURNAP, P.: Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses; Electronics 9. 9. (2020) p. 1460.
DOI: https://doi.org/10.3390/electronics9091460

[33] ASHENDEN, D.: In Their Own Words: Employee Attitudes Towards Information Security; Information and Computer Security 26. 12. (2018) pp. 327– 337.
DOI: https://doi.org/10.1108/ICS-04-2018-0042

[34] LEE, S. – LEE, J. – JUNG, J.: An Exploration of the Necessary Competencies of Professional Police Investigators for Industrial Espionage Cases in South Korea; Security Journal 33. (2020) pp. 119–138.

[35] AKOTO, W.: Cyber Economic Espionage: A Framework for Future Research. In: DEESE, D. /szerk./: A Research Agenda for International Political Economy. Edward Elgar Publishing, Cheltenham, 2022., pp. 159–170.

[36] COLWILL, C.: Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days?; Information Security Technical Report 14. 4. (2009) pp. 186– 196. DOI: https://doi.org/10.1016/j.istr.2010.04.004

[37] BEDFORD, J. – VAN DER LAAM, L.: Organizational Vulnerability to Insider Threat. In: STEPHANIDIS, C. /szerk./: HCI International 2016 – Posters' Extended

Abstracts. HCI 2016. Communications in Computer and Information Science 617. 2016., pp. 465–470. DOI: https://doi.org/10.1007/978-3-319-40548-3_77

[38] HOU, T. – WANG, V.: Industrial Aspionage –A Systematic Literature Review (SLR); Computers & Security 98. 102019 (2020) DOI: https://doi.org/10.1016/j.cose.2020.102019

[39] BRANCIK, K. – GHINITA, G.: The Optimization of Situational Awareness for Insider Threat Detection; CODASPY '11: Proceedings of the First ACM Conference on Data and Application Security and Privacy, San Antonio, TX USA, 2011., pp. 231–236. DOI: https://doi.org/10.1145/1943513.1943544

[40] CHANDAN, H. C.: Blurred Lines between Competitive Intelligence and Corporate Espionage; Corporate Espionage, Geopolitics, and Diplomacy Issues in International Business (2017). DOI: https://doi.org /10.4018/978-1-5225-1031-4.ch001

[41] ZAYTSEV, A. – MALYUK, A. – MILOSLAVSKAYA, N.: Critical Analysis in the Research Area of Insider Threats; 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), 2017., pp. 288– 296. DOI: https://doi.org /10.1109/FiCloud.2017.16

[42] MÉSZÁROS A. Á.: Innovation in the Defence Industry from the End of the Cold War to the War in Ukraine; Journal of Regional Security (2024) (Megjelenés alatt.)

[43] LESKE, A. D. C.: A Review on Denfese Innovation: From Spin-off to Spin-in; Brazilian Journal of Political Economy 38. 2. (2018) pp. 377–391. DOI: https://doi.org/10.1590/0101-31572018v38n02a09

[44] BAKOS C. A.: Modern könnyűgyalogság a jövő konfliktusaiban, háborúiban; Honvédségi Szemle - Hungarian Defende Review 146. 1. (2018) pp. 3–11.

[45] EUROPEAN COMISSION: Defence Industry and Space, 2022. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en (letöltve: 2023. 09. 23.)

[46] EUROPEAN PARLIAMENT: Fact Sheets on the European Union, 2022. https://www.europarl.europa.eu/factsheets/en/sheet/65/defence-industry (letöltve: 2023. 09. 23.)

[47] MÉSZÁROS A. Á. – TÓTH I. M. – CSISZÁRIK-KOCSIR Á.: The Impact of Investments in the Defense Industry on Local Economies; Macrotheme Review: A Multidisciplinary Journal Of Global Macro Trends 11. 1. (2023) pp. 52–61.

[48] MÉSZÁROS A. Á.: A kontingenciaelmélet alkalmazása az innovatív kis- és középvállalkozások vizsgálata során az európai védelmi iparban; Hadmérnök 18. 3. (2024) pp. 103–119. DOI: https://doi.org/10.32567/hm.2023.3.8

[49] CHEUNG, T. M. – MAHNKEN, T. G. – ROSS, A. L.: Assessing the State of Understanding of Defense Innovation; Study of Innovation and Technology in China Research Brief 10. 1. (2018) pp. 1–5.

[50] FRUNZETI, T. – COŞEREANU, L. – TOMOIAGĂ, T.: Impact of Disruptive Technologies on Defence; Land Forces Academy Review 26. 4. (2021) pp. 282 – 287.

[51] EUROPEAN COMMISSION: Result of the EDF 2022 Calls for Proposals, 2022. https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/result-edf-2022-calls-proposals_en (letöltve: 2023. 12. 15.).

[52] EUROPEAN COMMISSION: The EU Defence industry, 2023. https://defence-industry-space.ec.europa.eu/eu-defence-industry_en (letöltve: 2023. 12. 15.)

[53] BODORÓCZKI J.: A magyar különleges erők – 2035 (2. rész): Biztonságpolitikai-, hadseregszervezeti és technológiai kutatások elemzése; Hadmérnök 14. 2. (2019) pp. 56–73. ISSN: 1788-1919

[54] DURAKOVIC, B. – TRGO, E.: Perspectives and the Role of Bosnian Defense Industry in National Innovation System; Defense and Security Studies 1. (2020) pp. 26–33. DOI: https://doi.org/10.37868/dss.v1.id145

[55] KURÇ, Ç. – BITZINGER, R. A.: Defense Industries in the 21st Century: A Comparative Analysis – The second e-workshop; Comparative Strategy 37. 4. (2018) pp. 255–259. DOI: https://doi.org/10.1080/01495933.2018.1497318

[56] STRUYS, W.: The Future of the Defence Firm in Small and Medium Countries; Defence and Peace Economics 15. 6. (2004) pp. 551–564. DOI: https://doi.org/10.1080/1024269042000246648

[57] BETTS, S. C.: Contingency Theory: Science Or Technology?; Journal of Business & Economics Research 1. 8. (2003). DOI: https://doi.org/10.19030/jber.v1i8.3044

[58] TOSI, H. – SLOCUM, J.: Contingency Theory: Some Suggested Directions; Journal of Management 10. 1. (1984) pp. 9–26. DOI: https://doi.org/10.1177/014920638401000103

[59] FARKAS F.– BALOGH G. – RIDEG A.: Kontingencia-elmélet; Menedzsment alapvetések és funkciók. Pécs, Pécsi Tudományegyetem, Közgazdaságtudományi Kar 2015., pp. 52–53. ISBN: 978-963-642-758-0

[60] GRESOV, C.: Exploring Fit and Misfit with Multiple Contingencies; Administrative Science Quarterly 34. 3. (1989) pp. 431–453. DOI: https://doi.org/10.2307/2393152

[61] DONALDSON, L.: The Contingency Theory of Organizations; London, Sage Publicatios 2001. DOI: https://doi.org/10.4135/9781452229249

[62] BRENNER, S. W. – CRESCENZI, A. C.: State-Sponsored Crime: The Futility of the Economic Espionage Act; Houston Journal of International Law 28. 2. (2006)

[63] MICHALOWSKI, R. J. – KRAMER, R. C.: State-Corporate Crime: Wrongdoing at the Intersection of Business and Government; New Brunswick, NJ, Rutgers University Press 2006. ISBN: 978-0813538891

[64] BABBIE, E.: A társadalomtudományi kutatás gyakorlata; Budapest, Balassi Kiadó Kft 2020.

[65] KUHN, T. S.: The Structure of Scientific Revolutions; United States, University of Chicago Press 1962.

[66] GELENCSÉR K.: Grounded Theory; Szociológiai Szemle 1. (2003) pp. 143–154.

[67] MITEV A. Z.: Grounded theory, a kvalitatív kutatás klasszikus mérföldköve; Vezetéstudomány 43. 1. (2012) pp. 17–30.
DOI: https://doi.org/10.14267/VEZTUD.2012.01.02

[68] STRAUSS, A. – CORBIN, J.: Basics of Qualitative Research: Grounded Theory Procedures and Techniques; Newbury Park, Sage Publications 1990.

[69] CARL, S.: An Unacknowledged Crisis – Economic and Industrial Espionage in Europe. In: SPINELLIS, C. D., THEODORAKIS, N., BILLIS, E., PAPADIMITRAKOPOULOS, G. /szerk./: Europe in Crisis: Crime, Criminal Justice and the Way Forward. Athens, Ant. N. Sakkoulas Publishers L.P, 2. 2017., pp. 1315–1326. ISBN: 978-960-107-7

[70] KNICKMEIER. S.: Spies Without Borders? The Phenomena of Economic and Industrial Espionage and the Deterrence Strategies of Germany and Other Selected European Countries; Security Journal 33. 2. (2020) pp. 6–26. DOI: https://doi.org/10.1057/s41284-019-00199-1

[71] ELIFOGLU, I. H. – ABEL, I. – TAS¸SEVEN, Ö.: Minimizing Insider Threat Risk with Behavioral Monitoring; Review of Business: Interdisciplinary Journal on Risk and Society 38. 2. (2018) pp. 61–73.

[72] OMAR, M.: Insider Threats: Detecting and Controlling Malicious Insiders; New Threats and Countermeasures in Digital Crime and Cyber Terrorism (2015) pp. 162–172. DOI: https://doi.org/10.4018/978-1-4666-8345-7.ch009

[73] GLITZ, A. – MEYERSSON, E.: Industrial Espionage and Productivity; American Economic Review 110. 4. (2020) pp. 1055-1103.
DOI: https://doi.org/10.1257/aer.20171732

[74] STADLER, W. A.: The Quiet Threat: Fighting Industrial Espionage in America; Security Journal 25. (2012) pp. 90–93. DOI: https://doi.org/10.1057/sj.2011.26

[75] SADOK, M. – WELCH, C. – BEDNAR, P.: A Socio Technical Perspective to Counter Cyber Enabled Industrial Espionage; Security Journal 33. (2020) pp. 27–42. DOI: https://doi.org/10.1057/s41284-019-00198-2

[76] BABOS, S.: A katonai hírszerzés és a katonai elhárítás hadtudományi természete; Felderítő Szemle 17. 2. (2019) pp. 146– 158.

[77] CRANE, A.: In the Company of Spies: When Competitive Intelligence Gathering Becomes Industrial Espionage; Business Horizons 48. 3. (2005) pp. 233– 240. DOI: https://doi.org/10.1016/j.bushor.2004.11.005

[78] ANDROULIDAKIS, I. – KIOUPAKIS, F. E.: Industrial Espionage and Technical Surveillance Counter Measurers; Switzerland, Springer International Publishing 2016. DOI: https://doi.org/10.1007/978-3-319-28666-2

[79] KORONVÁRY P. – SZEGEDI P. – TÓTH J.: Kutatás és képzés – módszertani felvetések az elvárások és a képzési portfólió összehangolására a repülőműszaki képzésben; Hadmérnök 10. 4. (2015) pp. 237–246.

[80] DELANNON, N. – RAUFFLET, E.: Impeding Corporate Social Responsibility: Revisiting the Role of Government in Shaping Business — Marginalized Local Community Relations; Business Ethics, the Environment & Responsibility 30. 4. (2021) pp. 470–484. DOI: https://doi.org/10.1111/beer.12378

[81] MASON, J.: Qualitative Researching; London, Sage Publications Ltd 2002.

[82] SCANLAN, C. L.: Preparing for the Unanticipated: Challenges in Conducting Semi-Structured, In-Depth Interviews; London, SAGE Publications Ltd 2020.

[83] MORRIS, A.: A Practical Introduction to In-depth Interviewing; London, SAGE Publications Ltd 2015. ISBN: 9781446287637

[84] GÁTI M. – BAUER A.: Kvalitatív megközelítés a kis- és középvállalatok marketingdöntéseinek szervezeti értelmezéséhez, kiemelten kezelve a vállalatvezető szerepét; Vezetéstudomány - Budapest Management Review 48. 12. (2017) pp. 41–49. DOI: https://doi.org/10.14267/VEZTUD.2017.12.05

[85] MAXWELL, J. A.: Designing a Qualitative Study. In: BICKMAN, L., ROG, D. J. /szerk./: The Handbook of Applied Social Research Methods. Thousand Oaks CA, Sage Publications, 2008., pp. 214–253.
DOI: https://doi.org/10.4135/9781483348858.n7

[86] GOULDING, C.: Grounded Theory: Some Reflections on Paradigm, Procedures and Misconceptions; Working Paper Series, University of Wolverhampton 1999. ISSN: 1363–6839

[87] KELEMENNÉ ERDŐS A.: A közforgalmú közlekedési szolgáltatás és piac vizsgálata marketing és fenntarthatósági nézőpontból; Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest 2014.

[88] MALHOTRA, N. K.: Marketingkutatás; Budapest, KJK-Kerszöv Jogi és Üzleti Kiadó 2002. ISBN: 9632246470

[89] AL DABBAGH, Z. S.: The Role of Decision-Maker in Crisis Management: A Qualitative Study Using Grounded Theory (COVID-19 Pandemic Crisis as a Model); Journal of Public Affairs 20. 4. (2020) e2186. DOI: https://doi.org/10.1002/pa.2186

[90] BRATIANU, C.: Toward Understanding the Complexity of the COVID-19 Crisis: A Grounded Theory Approach; Management & Marketing 15. 1. Special Issue (2020) pp. 410–423. DOI: https://doi.org/10.2478/mmcks-2020-0024

[91] CHARMAZ, K.: Constructing Grounded Theory; Thousand Oaks, California, SAGE Publications Ltd 2014.

[92] GLASER, B. G. – STRAUSS, A. L.: The Discovery of Grounded Theory: Strategies for Qualitative Research; London, Weidenfed and Nicolson 1967. DOI: https://doi.org/10.4324/9780203793206

[93] YIN, R. K.: Case Study Research: Design and Methods (Applied Social Research Methods); London, SAGE Publications Ltd 2013.

[94] ALBERT A. – KELEMEN-ERDŐS A.: A kézműves sörgyártás vizsgálata gazdasági és élelmiszerbiztonsági szempontból; Acta Carolus Robertus 12. 2. (2022) pp. 60–73. DOI: https://doi.org/10.33032/acr.3246

[95] RIEGGER, A. S. – KLEIN, J. F. – MERFELD, K. – HENKEL, S.: Technology-enabled Personalization in Retail Stores: Understanding Drivers and Barriers; Journal of Business Research 123. (2021) pp. 140–155. DOI: https://doi.org/10.1016/j.jbusres.2020.09.039

[96] MCGINLEY, S. – WEI, W. – ZHANG, L. – ZHENG, Y.: The State Of Qualitative Research in Hospitality: A 5-year review 2014 to 2019; Cornell Hospitality Quarterly 62. 1. (2021) pp. 8–20. DOI: https://doi.org/10.1177/1938965520940294

[97] GUBA, E. G. – LINCOLN, Y. S.: Fourth Generation Evaluation; Newbury Park, California, SAGE Publications Ltd 1989.

[98] MOON, K. – BREWER, T. D. – JANUCHOWSKI-HARTLEY, S. R. – ADAMS, V. M. – BLACKMAN, D. A.: A Guideline to Improve Qualitative Social Science Publishing in Ecology and Conservation Journals; Ecology and Society 21.3. (2016) DOI: https://doi.org/10.5751/ES-08663-210317

[99] SHENTON, A. K.: Strategies for Ensuring Trustworthiness in Qualitative Research Projects; Education for Information 22. 2. (2004) pp. 63–75. DOI: https://doi.org/10.3233/EFI-2004-22201

[100] MERRIAM, S. B.: Qualitative Research and Case Study Applications in Education; San Francisco, Jossey-Bass 1998.

[101] GRANEHEIM, U. H. – LUNDMAN, B.: Qualitative Contentanalysis in Nursing Research: Concepts, Procedures and Measuresto Achieve Trustworthiness; Nurse

Education Today 24. 2. (2004) pp. 105–112.
DOI: https://doi.org/10.1016/j.nedt.2003.10.001

[102] SÁNTHA K.: A kvalitatív metodológiai követelmények problémái; Iskolakultúra 17. 6-7. (2007) pp. 168-177. ISSN: 1215-5233

[103] MITEV A. Z.: Végtelen történet: A narratív elemzés alkalmazhatósága a marketingkutatásban; Vezetéstudomány-Budapest Management Review 37. 10. (2006) pp. 33–41. DOI: https://doi.org/10.14267/VEZTUD.2006.10.04

[104] ELEKES G.: A Narratív Életútinterjú Módszere A Társadalomtudományok Kvalitatív Kutatásaiban; Szociálpedagógia 2018. 11. (2018) pp. 42–51.

[105] SALLAY V. – MARTOS T.: A Grounded Theory (GT) módszertana; Magyar Pszichológiai Szemle 73. 1. (2018) pp. 11–28.
DOI: https://doi.org/10.1556/0016.2018.73.1.2

[106] HALÁSZ G. M.: A narratív közgazdaságtan szerepe; Köz-Gazdaság - Review of Economic Theory and Policy 16. 4. (2021) pp. 273–288.

[107] LÁSZLÓ J.: A történetek tudománya: Bevezetés a narratív pszichológiába; Budapest, Új Mandátum Könyvkiadó 2005. ISBN: 9799639494595

[108] FEHÉR B.: A narratív segítő beszélgetés; Esély 2010. 3. (2010) pp. 66–88.

[109] BHAL, K. T. – LEEKHA, N. D.: Exploring Cognitive Moral Logics Using Grounded Theory: The Case of Software Piracy; Journal of Business Ethics 81. (2008) pp. 635–646. DOI: https://doi.org/10.1007/s10551-007-9537-7

[110] GLASER, B. G.: Basics of Grounded Theory Analysis; Mill Valley, Sociology Press 1992.

[111] BASKERVILLE, R. – PRIES-HEJE, J.: Grounded Action Research: a Method for Understanding IT in Practice; Accounting, Management and Information Technologies 9. 1. (1999) pp. 1–23.
DOI: https://doi.org/10.1016/S0959-8022(98)00017-4

[112] CONNOLLY, L. – MICHAEL, L. – TYGAR, J. D.: Investigation of Employee Security Behaviour: A Grounded Theory Approach. In: FEDERRATH, H., GOLLMANN, D. /szerk./: ICT Systems Security and Privacy Protection. SEC 2015. IFIP Advances in Information and Communication Technology 455. Springer, Cham, 2015., pp. 283–296. DOI: https://doi.org/10.1007/978-3-319-18467-8_19

[113] ALSOWAIL, R. A. – AL-SHEHARI, T.: Empirical Detection Techniques of Insider Threat Incidents; IEEE Access 8. (2020) pp. 78385–78402.
DOI: https://doi.org/10.1109/ACCESS.2020.2989739

[114] BOAKYE-GYAN, K.: An Approach to a Comprehensive Framework for Insider Threat; Capitol Technology University ProQuest Dissertations Publishing, Marlyland, USA 2021.

[115] KHAN, N. – HOUGHTON, R. J. – SHARPLES, S.: Understanding Factors that Influence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks; Cognition, Technology & Work 24. (2022) pp. 393–421.

[116] PURL, J. – GREITZER, F. L.: The Dynamic Nature of Insider Threat Indicators; SN Computer Science - Cyber Security and Privacy in Communication Networks 3. 2. (2022). DOI: https://doi.org/10.1007/s42979-021-00990-1

[117] ROBAYO, T. A.: The Enemy Within: A Framework for Understanding the Lifecycle of the Malicious Insider Threat to Information Systems; Saint Leo University ProQuest Dissertations Publishing, St Leo, FL, USA 2022.

[118] MAYRING, P. – FREBZL, T.: Qualitative Inhaltsanalyse. In: BAUR, N., BLASIUS, J. /szerk./: Handbuch Methoden der empirischen Sozialforschung. Springer VS, Wiesbaden 2019., pp. 633-648. DOI: https://doi.org/10.1007/978-3-658-21308-4_42

[119] GUBA, E. G.: Criteria for Assessing the Trustworthiness of Naturalistic Inquiries; Educational Communication and Technology Journal 29. 2. (1981) pp. 75–91.

[120] DERVIN, B.: An Overview of Sense-Making: Concepts, Methods, and Results to Date; Dallas, Texas 1983.

[121] ABDULWAHAB Á. – PANDURICS A. – UGRAI P.: Vállalati és vállalatközi integráció. Budapesti Közgazdaságtudományi Egyetem, Budapest 1997.

[122] LLEWELLYN, S.: Managing the Boundary: How Accounting Is Implicated in Maintaining the Organization; Accounting, Auditing & Accountability Journal 7. 4. (1994) pp. 4–23. DOI: https://doi.org/10.1108/09513579410069821

[123] OTLEY, D.: The Contingency Theory of Management Accounting and Control: 1980–2014; Management Accounting Research 31. (2016) pp. 45-62. DOI: https://doi.org/10.1016/j.mar.2016.02.001

[124] ISLAM, J. – HU, H.: A Review of Literature on Contingency Theory in Managerial Accounting; African Journal of Business Management 6. 15. (2012) pp. 5159–5164. DOI: https://doi.org/10.5897/AJBM11.2764

[125] GALBRAITH, J.: Designing Complex Organizations; Boston, Addison-Wesley Pub. Co 1973.

[126] HAMILTON, R. T. – SHERGILL, G. S.: The Relationship between Strategy-Structure Fit and Financial Performance in New Zealand: Evidence of Generality and Validity with Enhanced Controls; Journal of Management Studies 29. 1. (1992), pp. 95–113. DOI: https://doi.org/10.1111/j.1467-6486.1992.tb00654.x

[127] HAYES, D. C.: The Contingency Theory of Managerial Accounting; The Accounting Review 52. 1. (1977) pp. 22–39.

[128] MINTZBERG, H.: The Structuring of Organizations; London: Pearson 1979.

[129] CHILD, J.: Culture, Contingency and Capitalism in the Cross-National Study of Organizations; Research in Organizational Behavior: An Annual Series of Analytical Essays and Critical Reviews 3. (1981) pp. 303–356.

[130] WONG, C. W. Y. – LAI, K. H. – CHENG, T. C. E.: Value of Information Integration to Supply Chain Management: Roles of Internal and External Contingencies; Journal of Management Information Systems 28. 3. (2012) pp. 161–200. DOI: https://doi.org/10.2307/41713846

[131] ALVES, M. W. F. M. – JABBOUR, A. B. L. D. S. – KANNAN, D. – JABBOUR, C. J. C: Contingency Theory, Climate Change, and Low-Carbon Operations Management; Supply Chain Management: An International Journal 22. 3. (2017) pp. 223–236. DOI: https://doi.org/10.1108/SCM-09-2016-0311

[132] ENGELSETH, P. – KRITCHANCHAI, D.: Innovation in Healthcare Services – Creating a Combined Contingency Theory and Ecosystems Approach; International Conference on Industrial and System Engineering 337. 1:012022. (2018). DOI: https://doi.org/10.1088/1757-899X/337/1/012022

[133] KONOPATSCH, C.: Fighting Industrial and Economic Espionage Through Criminal Law: Lessons to be Learned from Austria and Switzerland; Security Journal 33. (2020) pp. 83-118. DOI: https://doi.org/10.1057/s41284-019-00200-x

[134] SHELUPANOV, A. – NEMIROVICH-DANCHENKO, M. – GLUKHAREVA, S.: Decision-Making in the Recommendation System of Personnel Security of the Company; Journal of Physics: Conference Series 1989. (2021) DOI: https://doi.org/10.1088/1742-6596/1989/1/012045

[135] DOKKO, J. – SHIN, M. – PARK, S. Y.: An Intelligence Criminal Tracker for Industrial Espionage: Applying Digital Data Acquired Onsite to Target Criminals; Digital Forensics and Cyber Crime, 11th EAI International Conference, ICDF2C, 2020, Proceedings 352. 2021., pp. 224–230.

[136] SPEARS, J. L. – BARKI, H.: User Participation in Information Systems Security Risk Management; MIS Quarterly 34. 3. (2010) pp. 503–522. DOI: https://doi.org/10.2307/25750689

[137] WILLIAMS, B. – SOULET, M. – SIRAJ, A.: A Taxonomy of Cyber Attacks in Smart Manufacturing Systems. In: KNAPCÍKOVÁ, L., PERAKOVIC, D. /szerk./: 6th EAI International Conference on Management of Manufacturing Systems, EAI/Springer Innovations in Communication and Computing. Cham, Springer, 2023., pp. 77–97. DOI: https://doi.org/10.1007/978-3-030-96314-9_6

[138] WILSON, Y. – HINGNIKAR, A.: Looking into the Crystal Ball; Solving Identity Management in Modern Applications. Berkeley, CA, Apress 2023., pp. 317–334.

[139] ANDRADE, C.: The Inconvenient Truth About Convenience and Purposive Samples; Indian Journal of Psychological Medicine 43. 1. (2021) pp. 86–88. DOI: https://doi.org/10.1177/0253717620977000

[140] SHARMA, G.: Pros and Cons of Different Sampling Techniques; International Journal of Applied Research 3. 7. (2017) pp. 749–752.

[141] ETIKAN, I. – MUSA, S. A. – ALKASSIM, R. S.: Comparison of Convenience Sampling and Purposive Sampling; American Journal of Theoretical and Applied Statistics 5. 1. (2016) pp. 1–4. DOI: https://doi.org/10.11648/j.ajtas.20160501.11

[142] VERES Z. – HOFFMANN M. – KOZÁK Á.: Bevezetés a piackutatásba; Budapest, Akadémiai kiadó 2006. DOI: https://doi.org/10.1556/9789634540038

[143] REKETTYE G. – TÓTH T. – MALOTA E.: Nemzetközi Marketing; Budapest, Akadémiai kiadó 2008. DOI: https://doi.org/10.1556/9789630597401

[144] BRIONES-PEÑALVER, A. J. – BERNAL-CONESA, J. A. – NIEVES NIETO, C.: Knowledge and Innovation Management Model. Its Influence on Technology Transfer and Performance in Spanish Defence Industry; International Entrepreneurship and Management Journal 16. 2. (2020) pp. 595–615.
DOI: https://doi.org/10.1007/s11365-019-00577-6

[145] WANG, C. N. – NGUYEN, X. T. – LE, T. D. – HSUEH, M. H.: A Partner Selection Approach for Strategic Alliance in the Global Aerospace and Defense Industry; Journal of Air Transport Management 69. (2018) pp. 190–204.
DOI: https://doi.org/10.1016/j.jairtraman.2018.03.003

[146] AKMAN, E.: Emerging Trade Partnership between the South Korea and Turkey: The Case of Defense Industry; Güvenlik Stratejileri Dergisi 2016.

[147] CASTELLACCI, F. – FEVOLDEN, A.: Capable Companies or Changing Markets? Explaining the Export Performance of Firms in the Defence Industry; Defence and Peace Economics 25. 6. (2014) pp. 549–575.
DOI: https://doi.org/10.1080/10242694.2013.857451

[148] GUAY, T.: Defense Industry Developments in the U.S. and Europe: Transatlantic or Bipolar; Journal of Transatlantic Studies 3. 1. (2005) pp. 139–157.
DOI: https://doi.org/10.1080/14794010508656822

[149] OKUN, O. – ARUN, K.: Entrepreneurship and Intrapreneurship as Innovation Source in the Defense Industry and Military. In: OJO, S. /szerk./: Global Perspectives on Military Entrepreneurship and Innovation. Nigerian Defence Academy, Nigeria, 2021., pp. 190–215.
DOI: https://doi.org/10.4018/978-1-7998-6655-8

[150] YUAN, C. – LIU, S. – YANG, Y. – SHEN, Y.: On the Contribution of Defense Innovation to China's Economic Growth; Defence and Peace Economics 27. 6. (2016) pp. 820–837. DOI: https://doi.org/10.1080/10242694.2014.901644

[151] BREZNITZ, D.: Industrial R&D as a National Policy: Horizontal Technology Policies and Industry-state Co-evolution in the Growth of the Israeli Software Industry;

Research Policy 36. 9. (2007) pp. 1465–1482.
DOI: https://doi.org/10.1016/j.respol.2007.06.006

[152] STANFORD, S. M. – DICKS, E. – SUERMANN, P. C: Evaluating Management Risks in Megaprojects: Case of International Defense Construction; Construction Research Congress, 2022. DOI: https://doi.org/10.1061/9780784483954.056

[153] KHALID, M. A. – RAZAQ, M. A. J. A.: The Impact of Military Spending on Economic Growth: Evidence from the US Economy; Research Journal of Finance and Accounting 6. 7. (2015) pp. 183–190. ISSN: 2222-1697

[154] YAKOVLEV, P.: Arms Trade, Military Spending, and Economic Growth; Defence and Peace Economics 1. 4. (2007) pp. 317–338.
DOI: https://doi.org/10.1080/10242690601099679

[155] MĂNESCU, G. – STAN, S. E.: The Influence of Disruptive Technologies on the Preparation of the National Economy and of the Territory for Defense; International conference Knowledge-Based Organization 27. 1. (2021) pp. 204–209.
DOI: https://doi.org/10.2478/kbo-2021-0031

[156] KURÇ, Ç. – NEUMAN, S. G.: Defence Industries in the 21st Century: A Comparative Analysis; Defence Studies 17. 3. (2017) pp. 219–227.
DOI: https://doi.org/10.1080/14702436.2017.1350105

[157] REIS, J. C. G.: Politics, Power, and Influence: Defense Industries in the Post-Cold War; Social Sciences 10. 1. (2021). DOI: https://doi.org/10.3390/socsci10010010

[158] CHARILLON, F. – BALZACQ, T. – RAMEL, F.: Defense Diplomacy. In: CHARILLON, F., BALZACQ, T., RAMEL, F. /szerk./: Global Diplomacy. The Sciences Po Series in International Relations and Political Economy. Cham, Palgrave Macmillan, 2020., pp. 267–278.

[159] HARUTYUNYAN, G. E. – DAVTYAN, A. G.: Issues of International Cooperation in Defense Industry: Critical Review; Ars Administrandi 11. 2. (2019) pp. 287–305.
DOI: https://doi.org/10.17072/2218-9173-2019-2-287-305

[160] PAJTINKA, E.: Military Diplomacy and its Present Functions; Security Dimensions 20. 1. (2016) pp. 179–194. DOI: https://doi.org/10.24356/SD/20/9

[161] MATSUDA, Y.: An Essay on China's Military Diplomacy: Examination of Intentions in Foreign Strategy; NIDS Security Repors 7. 1. (2006) pp. 1–40.

[162] MUTHANA, K. A.: Military Diplomacy; Journal of Defence Studies 5. 1. (2011) pp. 1–15.

[163] KIM, S. Y. – KIM, Y. H.: A Study on the Understanding of the Analysis of the Future Operational Environment for Smart Defense Innovation and the Application of the ROK MND, 스마트 국방혁신을 위한 미래 작전환경 분석의 이해와 군 적용방안에 대한 고찰; Journal of Information Technology Services

(한국IT서비스학회지) 20. 1. (2021) pp. 55–65.
DOI: https://doi.org/10.9716/KITS.2021.20.1.055

[164] XU, Y. – LIU, Z. – SU, C. – PETRU, S.: Military Industry Bubbles: are they Crowding out Utility Investments?; Economic Research-Ekonomska Istraživanja 35. 1. (2022) pp. 692–708. DOI: https://doi.org/10.1080/1331677X.2021.1931913

[165] PAMP, O. – DENDORFER, F. – THURNER, P. W.: Arm your Friends and Save on Defense? The Impact of Arms Exports on Military Expenditures; Public Choice 177. (2018) pp. 165–187. DOI: https://doi.org/10.1007/s11127-018-0598-1

[166] TERZIEV, V. – NICHEV, N.: Main Features of the Offsets in Defense Trade; IJASOS- International E-Journal of Advances in Social Sciences 3. 8. (2017) pp. 502-507. DOI: https://doi.org/10.18769/ijasos.336983

[167] TAKSÁS B.: A hadiipar fejlesztésének feltételei és működésének követelményei; Honvédségi Szemle – Hungarian Defence Review 148. 2. (2020) pp. 125–135. DOI: https://doi.org/10.35926/HSZ.2020.2.12

[168] CARRIL, R. – DUGGAN, M.: The Impact of Industry Consolidation on Government Procurement: Evidence from Department of Defense contracting; Journal of Public Economics 184. 104141. (2020) pp. 1–17.
DOI: https://doi.org/10.1016/j.jpubeco.2020.104141

[169] HAYWARD, K.: The Globalisation of Defence Industries; Survival, Global Politics and Strategy 43. 2. (2001) pp. 115–132.
DOI: https://doi.org/10.1093/survival/43.2.115

[170] JIANYU, Z. – BAIZHOU, L – XI, X. – GUANGDONG, W.– TIENAN, W.: Research on the Characteristics of Evolution in Knowledge Flow Networks of Strategic Alliance Under Different Resource Allocation; Expert Systems with Applications 98. (2018) pp. 242–256.
DOI: https://doi.org/10.1016/j.eswa.2017.11.012

[171] XIE, X. – WANG, L. – ZENG, S.: Inter-Organizational Knowledge Acquisition And Firms' Radical Innovation: A Moderated Mediation Analysis; Journal of Business Research 90. (2018) pp. 295–306.
DOI: https://doi.org/10.1016/j.jbusres.2018.04.038

[172] MARTINS, D. M. – FARIA, A. C. – PREARO, L. C. – ARRUDA, A. G.: The Level of Influence of Trust, Commitment, Cooperation, and Power in the Interorganizational Relationships of Brazilian Credit Cooperatives; Strategy & Bussiness Economics - Revista de Administração 52. 1. (2017) pp. 47–58.
DOI: https://doi.org/10.1016/j.rausp.2016.09.003

[173] PANICO, C.: Strategic Interaction in Alliances: Strategic Management Journal 38. 8. (2017) pp. 1646–1667. DOI: https://doi.org/10.1002/smj.2610

[174] DORNBUSCH, F. – NEUHÄUSLER, P.: Composition of Inventor Teams and Technological Progress – The Role of Collaboration between Academia and Industry; Research Policy 44. 7. (2015) pp. 1360–1375. DOI: https://doi.org/10.1016/j.respol.2015.04.003

[175] MARTÍNEZ-NOYA, A. – NARULA, R: What More can we Learn from R&D Alliances? A Review and Research Agenda; BRQ Business Research Quarterly 21. 3. (2020) pp. 195–212. DOI: https://doi.org/10.1016/j.brq.2018.04.001

[176] DELGADO-MARQUEZ, B. L. – HURTADO-TORRES, N. E. – PEDAUGA, L. E. – CORDON-POZO, E.: A Network View of Innovation Performance for Multinational Corporation Subsidiaries; Regional Studies 52. 1. (2018) pp 47–67. DOI: https://doi.org/10.1080/00343404.2016.1272756

[177] ARDITO, L. – MESSENI PETRUZZELLI, A.: Breadth of External Knowledge Sourcing and Product Innovation: The Moderating Role of Strategic Human Resource Practices; European Management Journal 35. 2. (2017) pp. 261–272. DOI: https://doi.org/10.1016/j.emj.2017.01.005

[178] HOROWITZ, M. C. – PINDYCK, S.: What is a Military Innovation and why it Matters; Journal of Strategic Studies 46. 1. (2023) pp. 85-114. DOI: https://doi.org/10.1080/01402390.2022.2038572

[179] BELLAIS, R. – FIOTT, D.: The European Defense Market: Disruptive Innovation and Market Destabilization; The Economics of Peace and Security Journal 12. 1. (2017) pp. 37–45.

[180] BITZINGER, R. A.: The Modern Defense Industry: Political, Economic, and Technological Issues, Santa Barbara, California, ABC-CLIO, LLC 2009.

[181] CAHYASUSILA, A. B. – SIAHAAN, T. – JUPRIYANTO: Analysis of Strategic Environment and Characteristics of the World's Defense Industry; The International Journal of Business Management and Technology 6. 1. (2022) pp. 291–299. ISSN: 2581-3889

[182] FIOTT, D.: Strategic Autonomy: Towards 'European sovereignty' in defence?; European Union Institute for Security Studies (EUISS). Paris 2018.

[183] FAURE, S. B. H.: La coopération internationale dans le secteur de l'armement; Questions de Recherche 46. 1. (2015) pp. 1–45.

[184] DEVORE, M. R.: Armaments After Autonomy: Military Adaptation and the Drive for Domestic Defence Industries; Journal of Strategic Studies 44. 3. (2021) pp. 325–359. DOI: https://doi.org/10.1080/01402390.2019.1612377

[185] PORKOLÁB I.: Az Innováció Hatása a Hadviselésre; Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata 26. 1-2. (2016) pp. 19–28. ISSN: 1215-4121

[186] NAIR, A. – AHLSTROM, D.: Delayed Creative Destruction and the Coexistence of Technologies; Journal of Engineering and Technology Management 20. 4. (2003) pp. 345–365. DOI: https://doi.org/10.1016/j.jengtecman.2003.08.003

[187] TIAN, N. – WEZEMAN, S. T. – WEZEMAN, P. D. – FLEURANT, A. –KUIMOVA, A. – DA SILVA, D. L.: Trends in International Arms Transfers, 2019; SPIRI Fact Sheet, Stockholm International Peace Research Institute, Stockholm 2020., pp. 1–12. DOI: https://doi.org/10.55163/YJYW4676

[188] MAKHSUD, U.: Basic Concepts of Information Security; International Journal of Academic and Applied Research (IJAAR) 5. 1. (2021) pp. 5–8. ISSN: 2643-9603

[189] SZŰCS E. – ZÁHONYI L.: Információbiztonság fejlődés-történeti vizsgálata– Mérföldkövek, események és válaszok; Biztonságtudományi Szemle 3.3. (2021) pp. 81–91.

[190] HEICKERÖ, R.: Cyber Espionage and Illegitimate Information Retrieval; Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications (2019) pp. 1725–1736. DOI: https://doi.org/10.4018/978-1-5225-7909-0.ch091

[191] PELLEGRINO, M.: The Threat of State-Sponsored Industrial Espionage; European Union Institute for Security Studies, 2015. https://op.europa.eu/en/publication-detail/-/publication/9de4b721-6256-43f0-b7df-988e3c4c9451 (letöltve: 2023. 09. 23.)

[192] ROCHE, E. M.: Industrial Espionage; Journal of U.S. Intelligence Studies 22. 1. (2016) pp. 59-63.

[193] SZERB L. – KOMLÓSI É. – PÁGER B.: Új Technológiai Cégek az Ipar 4.0 Küszöbén – A Magyar Digitális Vállalkozási Ökoszisztéma Szakértői Értékelése; Vezetéstudomány / Budapest Management Review 51. 6. (2020) pp. 81– 96. DOI: https://doi.org/10.14267/VEZTUD.2020.06.08

[194] DUCKWORTH, N.– DE SILVA, E.: Teaching New Dogs Old Tricks: The Basics of Espionage Transcend Time; National Security: Breakthroughs in Research and Practice (2019) pp. 479–496. DOI: https://doi.org/10.4018/978-1-4666-9661-7.ch005

[195] BUDAVÁRI K. – TAKSÁS B. – HEGEDÛS E.: A magyar védelmi ipar innovációs környezetének vizsgálata; Hadtudomány 32. 1. (2022) pp. 113–134. DOI: https://doi.org/10.17047/HADTUD.2022.32.1.113

[196] CHOI, Y. B. – TERESA, W.: The Rise of Industrial Espionage and How to Prevent It; International Journal of Cyber Research and Education 2. 2. (2020) pp. 9–16. DOI: https://doi.org/10.4018/IJCRE.2020070102

[197] KELEMEN-ERDŐS A. – MÉSZÁROS A. Á.: Ethics and Social Responsibility of Information Intermediaries in International Businesses; Arab Journal of Administration 41. (2021) pp. 239–248. ISSN: 1110-5453

[198] KELEMEN-ERDŐS A. – MÉSZÁROS A. Á.: A közvetítő partnerek információval kapcsolatos kockázatai a nemzetközi üzleti tranzakciók során; Biztonságtudományi Szemle 2. 4. (2020) pp. 29–38. ISSN: 2676-9042

[199] KELEMEN-ERDŐS A. – MÉSZÁROS A. Á.: A közvetítőpartnerek alkalmazásának aspektusai a nemzetközi üzleti tranzakciók során; Vállalkozásfejlesztés a XXI. században 2021. 1. (2021) pp. 66–83.

[200] JOHNSON L. K.: Secret Agencies: U.S. Intelligence in a Hostile World; London, Yale University Press 1998.

[201] INGESSON, T.: Innovators, Copycats, or Pragmatists? Soviet Industrial Espionage and Innovation in the Military Aerospace Sector during the Cold War; International Journal of Intelligence and CounterIntelligence 36. 3. (2023) pp. 816–846. DOI: https://doi.org/10.1080/08850607.2022.2109081

[202] SIVANESAN, G.: The human factor in espionage; Computer Fraud & Security 2011. 2. (2011) pp. 15–16. DOI: https://doi.org/10.1016/S1361-3723(11)70018-5

[203] SCHWARTZ, M. S.: The State of Business Ethics in Israel: A Light Unto the Nations?; Journal of Business Ethics 105. 4. (2012) pp. 429–446.

[204] HOUSE, W.: Annual Report to Congress on Foreign Economic Collection and Industrial Espionage; Washington DC, National Counterintelligence Center, Government Printing Office 1995.

[205] MÉSZÁROS, A. Á. – KELEMEN-ERDŐS, A.: Industrial Espionage from a Human Factor Perspective; Journal of International Studies 16. 3. (2023) pp. 97–116. DOI: https://doi.org/10.14254/2071-8330.2023/16-3/5

[206] NOONAN, C. F.: Spy the Lie: Detecting Malicious Insiders; Pacific Northwest National Laboratory, Richland, Washington, United States 2018.

[207] PASTERNAK, G. – WITKIN, G.: The Lure of the Steal; US News & World Report, United States 45. 1996.

[208] WILLIAMS, M. L. – LEVI, M. – BURNAP, P. – GUNDUR, R. V.: Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory; Deviant Behavior 40. 9. (2019) pp. 1119–1130. DOI: https://doi.org/10.1080/01639625.2018.1461786

[209] HILLS, M. – ANJALI, A.: A Human Factors Contribution to Countering Insider Threats: Practical Prospects from a Novel Approach to Warning and Avoiding; Security Journal 30. 1. (2017) pp. 142–152. DOI: https://doi.org/10.1057/sj.2015.36

[210] HO, S. M. – WARKENTIN, M.: Leader's Dilemma Game: An Experimental Design for Cyber Insider Threat Research; Information Systems Frontiers 19. 2. (2017) pp. 377–396. DOI: https://doi.org/10.1007/s10796-015-9599-5

[211] SAMY, G. N. – MAAROP, N. – SHANMUGAM, B. – RADHAKRISHNAN, M.– PERUMAL, S. – RAHIM, F. A.: Multidimensional Insider Threat detection model for organization; Journal of Theoretical and Applied Information Technology 99. 20. (2021) pp. 4770–4785.

[212] PATIL, D. – MESHRAM, S. B.: Network Packet Analysis for Detecting Malicious Insider; 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 2018., pp. 1-8. DOI: https://doi.org/10.1109/I2CT.2018.8529451

[213] VASHISTH, A. – KUMAR, A.: Corporate Espionage The Insider Threat; Business Information Review 30. 2. (2013) pp. 83–90. DOI: https://doi.org/10.1177/0266382113491816

[214] LEHTO, M.: Cyber-Attacks Against Critical Infrastructure. In: LEHTO, M., NEITTAANMÄKI, P. /szerk./: Cyber Security: Critical Infrastructure Protection, Computational Methods in Applied Sciences. Springer, 56. 2022., pp. 3–42. DOI: https://doi.org/10.1007/978-3-030-91293-2_1

[215] MAICAN, O. H.: Legal Aspects of Economic Espionage; Perspectives of Law and Public Administration 8. 2. (2019) pp. 385–392.

[216] RAJNAI Z.: Információbiztonság tudatosság; Műszaki Tudományos Közlemények 7. (2017) pp. 37–42. ISSN: 2393-1280

[217] WARKENTIN, M. – MUTCHLER, L.: Research in Behavioral Information Security Management. In: TOPI, H., TUCKER, A. /szerk./: Computing Handbook. Taylor and Francis, 2014.

[218] ALHOGAIL, A.: Design and Validation of Information Security Culture Framework; Computers in Human Behavior 49. (2015) pp. 567– 575. DOI: https://doi.org/10.1016/j.chb.2015.03.054

[219] CROSSLER, R. E. – JOHNSTON, A. C. – LOWRY, P. B. – HU, Q. –WARKENTIN, M. – BASKERVILLE, R.: Future Directions for Behavioral Information Security Research; Computers & Security 32. 1. (2013) pp. 90–101. DOI: https://doi.org/10.1016/j.cose.2012.09.010

[220] LARA, E. – AGUILAR, L. – SANCHEZ, M. A, – GARCÍA, J. A.: Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things; Sensors 20. 2. (2020) pp. 1–22. DOI: https://doi.org/10.3390/s20020501

[221] SCHLIENGER, T. – TEUFEL, S.: Information Security Culture - From Analysis to Change; South African Computer Journal 31. (2003) pp. 46-52.

[222] RAMACHANDRAN, S. – RAO, S. – GOLES, T.: Information Security Cultures of Four Professions: A Comparative Study; Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), 2008., pp. 454-454. DOI: https://doi.org/10.1109/HICSS.2008.201

[223] GLASPIE, H. W. – KARWOWSKI, W.: Human Factors in Information Security Culture: A Literature Review; In: NICHOLSON, D. /szerk./: Advances in Human Factors in Cybersecurity. AHFE 2017. Advances in Intelligent Systems and Computing 593. Springer, Cham 2017.
DOI: https://doi.org/10.1007/978-3-319-60585-2_25

[224] GHEYAS, I. A. – ABDALLAH, A. E: Detection and Prediction of Insider Threats to Cyber Security: a Systematic Literature Review and Meta-Analysis; Big Data Analytics 1. 6. (2016). DOI: https://doi.org/10.1186/s41044-016-0006-0

[225] CARSTENS, D. S. – MILLER, J. R. – MAHLMAN, J. A. – SHAFFER, M. J.: Internet, Social Media, and Mobile Device Addiction Effects on a Workplace; International Journal of Social Media and Online Communities 13. 1. (2021) pp. 37–50. DOI: https://doi.org/10.4018/IJSMOC.2021010103

[226] PANG, A. – HASSAN, A. – BINTE, N. B. – CHONG, A. C. Y.: Negotiating Crisis in the Social Media Environment: Evolution of Crises Online, Gaining Credibility Offline; Corporate Communications: An International Journal 19. 1. (2014) pp. 96–118.

[227] LAUFER E. – SZÁDECZKY T. – VÁCZI D.: Emberi kockázati tényezők digitális információ szivárgás potenciáljának mérésére; Biztonságtudományi Szemle 3.3. (2021) pp. 55–65.

[228] LEE, C. M.: Criminal Profiling and Industrial Security; Multimedia Tools and Applications 74. 5. (2015) pp. 1689–1696.
DOI: https://doi.org/10.1007/s11042-014-2014-2

[229] CHAN, M.: Corporate Espionage and Workplace Trust/Distrust; Journal of Business Ethics 42. 1. (2003) pp. 45–58. DOI: https://doi.org/10.1023/A:1021611601240

[230] MAKRAKIS, G. M. – KOLIAS, C.– KAMBOURAKIS, G. – RIEGER, C. – BENJAMIN, J.: Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents; IEEE Access 9. (2021) pp. 165295–165325.
DOI: https://doi.org/10.1109/ACCESS.2021.3133348

[231] AOUN, A. – ILINCA, A.– GHANDOUR, M. – IBRAHIM, H.: A Review of Industry 4.0 Characteristics and Challenges, with Potential Improvements using Blockchain Technology; Computers & Industrial Engineering 162. 107746. (2021) DOI: https://doi.org/10.1016/j.cie.2021.107746

[232] YALCINKAYA, E. – MAFFEI, A.: Blockchain Suitability Assessment of Manufacturing Functions Defined by the ISA95 Standard; Industrial Engineering &

Management Systems 19. 4. (2020) pp. 825–846.
DOI: https://doi.org/10.7232/iems.2020.19.4.825

[233] DAWSON, M. – BACIUS, R. – LGOUVEIA, L. B. – VASSILAKOS, A.: Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors; Land Forces Academy Review 26. 1. (2021) pp. 69–75, 2021.
DOI: https://doi.org/10.2478/raft-2021-0011

[234] MOHANTA, B. K. – JENA, D. – PANDA, S. S. – SOBHANAYAK, S.: Blockchain Technology: A Survey on Applications and Security Privacy Challenges; Internet of Things 8. 100107 (2019) DOI: https://doi.org/10.1016/j.iot.2019.100107

[235] FADI, O. – KARIM, Z. – ABDELLATIF, E. G. – MOHAMMED, B.: A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments; IEEE Access 10. (2022) pp. 93168–93186.
DOI: https://doi.org/10.1109/ACCESS.2022.3203568

[236] CROSBY, M. – NACHIAPPAN – PATTANAYAK, P. – VERMA, S. – KALYANARAMAN, V.: BlockChain Technology: Beyond Bitcoin; Applied Innovation Review 2. (2016) pp. 7–19.

[237] ZĪLE, K. – STRAZDIŅA, R.: Blockchain Use Cases and Their Feasibility; Applied Computer Systems 23. 1. (2018) pp. 12–20.
DOI: https://doi.org/10.2478/acss-2018-0002

[238] OLÁH J. – POPP J. – ERDEI E.: Az Ipar 5.0 megjelenése: ember és robot együttműködése; Logisztika Trendek és legjobb gyakorlatok kiadvány 5. 1. (2019) pp. 12–19. ISSN: 2416-0555

[239] SCHINDLER, P. – RUHLAND, J.: The Threat of Quantum Computing to SMEs. In: ARAI, K. /szerk./: Intelligent Computing. SAI 2022. Lecture Notes in Networks and Systems 506. Springer, Cham, 2022.
DOI: https://doi.org/10.1007/978-3-031-10461-9_28

[240] NEJAD, B.: Introduction to Satellite Ground Segment Systems Engineering: Principles and Operational Aspects (Space Technology Library, 41); Cham, Springer 2023.

[241] SÁNTHA K. – TÓDOR E. M.: Szövegek a szövegben. Kvalitatív kutatásmódszertani szempontok az idézetek szerepéről; Iskolakultúra 32. 6. (2022) pp. 72–82. DOI: https://doi.org/10.14232/ISKKULT.2022.6.72

[242] MÉSZÁROS A. Á. – TICK A.: Az ipari kémkedéssel szembeni felkészültség vizsgálata a magyar szervezetek körében; Biztonságtudományi Szemle 4. 3. (2021) pp. 57–72. ISSN 2676-9042

[243] TICK, A. – MÉSZÁROS, A. Á.: Hungarian Organizations' Attitude toward the Protection against Industrial Espionage; IEEE 20th Jubilee World Symposium on

Applied Machine Intelligence and Informatics SAMI (2022) Proceedings (2022) pp. 243-248.

[244] TÓTH I. M. – CSISZÁRIK-KOCSIR, Á.: Teleworking and the Home Office - The Digital Possibilities in Work Organization; 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022. Budapest, IEEE Hungary Section 2. 2022., pp. 277–280.

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

[P1] Mészáros, Alexandra Ágnes – Kelemen-Erdős, Anikó (2023): Industrial Espionage from a Human Factor Perspective. Journal of International Studies, 16(3), 97-116. Doi:10.14254/2071-8330.2023/16-3/5

[P2] Kelemen-Erdős Anikó – Mészáros Alexandra Ágnes (2022): Az ipari és gazdasági kémkedés vizsgálata a védelmi iparban. FELDERÍTŐ SZEMLE (1588-242X) 2022/4. szám, pp. 95–110.

[P3] Andrea Tick – Alexandra Ágnes Mészáros (2022): Hungarian Organizations' Attitude toward the Protection against Industrial Espionage. IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022) Proceedings, pp 243-248, ISBN: 9781665497046 ISBN: 9781665497039

[P4] Mészáros Alexandra Ágnes – Tick Andrea (2021): Az ipari kémkedéssel szembeni felkészültség vizsgálata a magyar szervezetek körében. Biztonságtudományi szemle, 3. évf. 4. szám, pp. 57-72, ISSN 2676-9042

[P5] Mészáros Alexandra Ágnes (2024): Innovation in the Defence Industry from the End of the Cold War to the War in Ukraine. Journal of Regional Security – Megjelenés alatt

[P6] Mészáros Alexandra Ágnes (2024): A kontingenciaelmélet alkalmazása az innovatív kis- és középvállalkozások vizsgálata során az európai védelmi iparban. HADMÉRNÖK, 18(3), 103–119. Doi: https://doi.org/10.32567/hm.2023.3.8

[P7] Mészáros Alexanda Ágnes – Tóth István Márk – Csiszárik-Kocsir Ágnes (2023): The impact of investments in the defense industry on local economies. The Macrotheme Review 11(1), pp. 52-61.

[P8] Mészáros Alexandra Ágnes – Tóth István Márk – Csiszárik-Kocsir Ágnes (2022). A védelmi ipar lokális gazdaságra gyakorolt hatásának kvalitatív vizsgálata. Vállalkozásfejlesztés a XXI. században, 2022/2, pp. 193-206.

8.2 További tudományos közlemények

[P9] Anikó Kelemen-Erdős – Alexandra Ágnes Mészáros (2021): Ethics and Social Responsibility of Information Intermediaries. International Businesses. Arab Journal of Administration, Vol 41, pp. 239-248, ISSN: 1110-5453

[P10] Kelemen-Erdős Anikó – Mészáros Alexandra Ágnes (2021): A közvetítőpartnerek alkalmazásának aspektusai a nemzetközi üzleti tranzakciók során. Vállalkozásfejlesztés a XXI. században, 2021/1 kötet: Üzleti megoldások és gyakorlati tapasztalatok a menedzsment területén, pp. 66-83, ISBN: 9789634492795

[P11] Anikó Kelemen-Erdős – Alexandra Ágnes Mészáros (2020): A közvetítő partnerek információval kapcsolatos kockázatai a nemzetközi üzleti tranzakciók során. Biztonságtudományi Szemle (2676-9042): 2(4) pp. 29-38 (2020), ISSN: 2676-9042

[P12] Mészáros Alexandra Ágnes (2020): Communication Problems Arising from Cultural Differences During English Negotiations. FIKUSZ 2019 – Symposium for Young Researchers Proceedings, Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar, pp 157-166. ISBN: 9789634491750