



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

MÉSZÁROS ALEXANDRA ÁGNES

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

Témavezető: Dr. Kelemen-Erdős Anikó

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2023. 09. 25.

TARTALOMJEGYZÉK

BEVEZETÉS	5
A tudományos probléma megfogalmazása	5
A téma aktualitása.....	8
A kutatás célkitűzése	9
A kutatás felépítése.....	10
1. KUTATÁSI MÓDSZEREK	12
1.1. Szakértői mélyinterjú	12
1.2. Grounded theory és a kvalitatív kutatás megbízhatósága	13
1.2.1. Következetesség.....	16
1.2.2. Átvihetőség	19
1.2.3. Hitelesség.....	19
1.2.4. Megerősíthetőség	21
1.3. Kutatási kérdések	22
1.4. Minta	24
2. ELMÉLETI MEGALAPOZÁS	27
2.1. Az európai védelmi ipar stratégiai szerepe	27
2.2. Az ipari és gazdasági kémkedés.....	31
2.2.1. Az ipari és gazdasági kémkedés kutatási problémái.....	33
2.2.2. Az ipari kémkedés jelensége.....	37
2.2.3. A humán faktor szerepe	43
2.2.4. Ipari kémkedés elleni információvédelmi rendszer	47
2.3. Kontingencia elmélet	52
3. EREDMÉNYEK.....	56
3.1. Az ipari kémkedési esetek növekedése mögött azonosított tényezők.....	57
3.1.1. Külső kontingencia tényezők.....	59

3.1.2.	Belső kontingencia tényezők	63
3.2.	Az ipari kémkedés fenyegetésének észlelése és megelőzése	67
3.2.1.	Vezetői eszközök	69
3.2.2.	Információvédelmi eszközök	72
3.3.	Az ipari kémkedés fejlődése	76
3.3.1.	Fejlődő fenyegetések	77
3.3.2.	Újszerű védekezési eszközök.....	78
3.4.	Diskusszió	81
3.4.1.	A védelmi iparban az ipari kémkedési esetek növekedésének okai (K1). 81	
3.4.2.	A belső érintettek által elkövetett ipari kémkedés mögött azonosított faktorok (K2)	83
3.4.3.	Az ipari kémkedés megelőzésére és észlelésére alkalmazott eszközök és módszerek (K3).....	85
3.4.4.	Jövőbeni információbiztonsági fenyegetések várható természete (K4) ...	88
ÖSSZEGZETT KÖVETKEZTETÉSEK.....		91
Az információbiztonsági politika szerepe az ipari kémkedés kockázatának csökkentésében		91
Az információbiztonsági kultúra fejlesztésének lehetőségei		94
A védelmi kis- és középvállalkozásokra ható külső környezeti kontingencia tényezők vizsgálata		95
Az innovatív védelmi kis- és középvállalkozásoknál kialakítható információbiztonsági rendszer sajátosságai.....		96
Új tudományos eredmények		98
Az eredmények elméleti hasznosíthatósága		101
Az eredmények gyakorlati hasznosíthatósága		103
A kutatás limitációja		104
Jövőbeni kutatási irányok		106
AZ ÉRTEKEZÉS TÉMÁJÁHOZ KAPCSOLÓDÓ PUBLIKÁCIÓK.....		109

IRODALOMJEGYZÉK	111
RÖVIDÍTÉSJEGYZÉK.....	130
TÁBLÁZATJEGYZÉK.....	131
ÁBRAJEGYZÉK.....	131
FÜGGELÉK	132
Magyar vezérfonal I. szakasz.....	132
English Guide Phase I.....	134
Magyar vezérfonal II. és III. szakasz	136
English Guide Phase II. – III.	137
KÖSZÖNETNYILVÁNÍTÁS	138

BEVEZETÉS

Az ipari kémkedés nem egy új probléma. Az emberiség történetében, már az ókori civilizációk során, mikor megalapították az első vállalkozásokat, történtek olyan esetek, amikor valaki megpróbálta megszerezni vagy ellopni egy tevékenység folytatásához szükséges titkokat. Az egyik első dokumentált eset az időszámításunk előtti 4. században történt, amikor a kínai selyemhernyó tenyésztők és selyemkészítők titkait megfigyelték, majd alkalmazni kezdték Ázsia és Európa szerte [1]. A 18. és 19. században zajlott gyors ütemű iparosodás és technológiai fejlődés, továbbá az ezek hatására fokozódó gazdasági verseny következményeként a vállalkozások egyre nagyobb érdeklődést mutattak a versenytársak üzleti titkai iránt. A 20. században a két világháború, majd a hidegháború következményeként a gyorsan terjedő ipari kémkedés módszerei még kifinomultabbá váltak, különösen a védelmi ipar területén, ahol a kutatás és fejlesztésből származó lopott információ gazdasági, stratégiai és taktikai előnyhöz juttathatta a kémkedést szervező entitást. Napjainkra az ipari kémkedés a teljes globális gazdaság, és azon belül a védelmi ipar legfenyegetőbb problémájává nőtte ki magát. A globalizáció, az információs technológia fejlődése, a nemzetközi üzleti kapcsolatok bővülése, továbbá a geopolitikai feszültségek kiszámíthatatlan természete csak tovább fokozza az ipari kémkedés komplex problémáját, mely bár évszázadok óta a gazdaság része, napjainkra a módszerek jelentősen átalakuláson mentek keresztül, és hatékonyabbak, mint valaha voltak a történelem során.

A tudományos probléma megfogalmazása

A védelmi ipar minden nemzet számára stratégiai jelentőséggel bír. Az állampolgárok biztonságának védelme mellett számtalan társadalmi, politikai és gazdasági területen rendelkezik kiemelt szereppel. Több társadalmi réteget foglalkoztat, hozzájárul a kritikus infrastruktúra fejlesztéséhez, ezáltal a térség fejlődéséhez. A fejlett védelmi ipar az állam politikai és gazdasági hatalmának kifejező-, és érdekérvényesítő eszköze. Az ágazatban jellemző nemzetközi szövetségek és együttműködések támogatják a terület verseny- és innovációs képességét, továbbá a nemzetközi kereskedelmet. Az ipar úttörő szerepet tölt be a kutatásban, fejlesztésben, oktatásban, és a világúrból érkező fenyegetések megismerésében. Azonban 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 (KKV) számára, hogy tevékenységet folytassanak az ágazatban, amelyek azóta élen járnak az innovációk fejlesztése területén [2, 3, 4, 5, 6]. Az innovációs tevékenység folytatásának legértékesebb eleme – a humán erőforrás 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 ipar területén tevékenységet folytató kis- és középvállalkozásokat a gazdasági- és ipari kémkedés. Jelen kutatás során az **innovatív kis- és középvállalkozás** kifejezés azon szervezeteket foglalja magába, melyek tevékenységei, üzleti- és munkafolyamatai, termékei vagy szolgáltatásai új vagy újszerű megközelítésből valósulnak meg. Ezen védelmi vállalkozások agilis és rugalmas magatartást mutatnak, továbbá gyorsan képesek alkalmazkodni a változó vevői igényekhez és piaci feltételekhez. Figyelembe véve kisebb méretüket és fókuszált szakterületi specializálódásukat, a kis- és középvállalkozások nagyobb hajlandóságot mutatnak olyan kutatás, fejlesztés és innovációs projektek megvalósítására, amelyek a nagyobb védelmi vállalatok számára túl kockázatosnak számítanak.

Az ágazatban az új technológiák fejlesztése területén intenzív verseny jellemző az országok között, mert egy innováció elsőként való adaptálásával stratégiai és taktikai előnyt lehet kialakítani, ennél fogva gyakran alkalmazott információgyűjtési módszer a tudás illetéktelen eltulajdonítása. A gazdasági- és ipari kémkedés minden olyan vállalkozás számára kockázatot jelent, melyek versenyképes működése a kritikus információtól függ. Míg más iparágakban az információlopás komoly anyagi és hírnévbeli veszteséget képes okozni, addig a védelmi ipart fenyegető kémkedés a teljes nemzetbiztonságra veszélyt jelentő kockázatot testesít meg. A védelmi iparban a gazdasági- és ipari kémkedés áldozatának súlyos következményekkel kell szembe nézni mikroökonómiai és nemzeti szinten egyaránt. Kelemen-Erdős és Mészáros (2022) [7] eredményei alapján **gazdasági szempontból** (1) pénzügyi veszteséget, (2) piaci pozíció csökkenését, (3) a megrendelők bizalmának elvesztését, továbbá (4) negatív hírnevet okozhat a vállalkozásnak. **Stratégiai nézőpontból** vizsgálva (1) ellehetetlenítheti a védelmi felszerelések gyártását, (2) ellátási zavarokat és (3) taktikai lemaradást okozhat, (4) akadályozhatja az ipart a feladatainak ellátásában, (5) gyengítheti a szövetségesek közötti kapcsolatot ezáltal az állam regionális és geopolitikai pozícióját, továbbá a (6)

nemzetbiztonság csökkenését idézheti elő. Ezen kockázatok indokolják a gazdasági- és ipari kémkedés komplex jelenségének kutatását.

Jelen doktori értekezés során a védelmi iparban tevékenységet folytató kis- és középvállalkozásokat vizsgáltam kvalitatív módszerrel, melyek fő profilja az új eszközök, alkatrészek, részegységek, szoftverek vagy hardverek fejlesztése, továbbá tevékenységük részét képezheti a kis szériás sorozatgyártás. Ezen szervezeteket kiemelten fenyegeti a gazdasági- és ipari kémkedés, mely ellen védekezni szükséges, azonban az információbiztonsági fenyegetés dolgozatban bemutatott formájának komplex természete miatt a probléma megoldása nem olyan egyszerű. Sok vállalkozás a védekezést csak az interneten keresztül érkező támadásokra korlátozza [8, 9, 10, 11], azonban nem szabad figyelmen kívül hagyni a munkavállalók által megtestesített belső fenyegetést sem. Jelen kvalitatív kutatás újdonságtartalma, hogy a jogosulatlan információeltulajdonítás problémáját holisztikus megközelítésből vizsgálja, párhuzamot vonva az információs technológiai (IT) és a humán tényező között. A kutatás során az alanyok kiválasztása célzott mintavétellel történt, az adatgyűjtés vezérfonallal támogatott szakértő mélyinterjúk alkalmazásával valósult meg, 42 interjúalany részvételével. A gyűjtött empirikus adatok elemzése az abduktív jellegű, szisztematikus grounded theory (*megalapozott elmélet*) módszertan konstruktivista irányzatával zajlott.

Az európai védelmi ipar területén tevékenységet folytató kis- és középvállalkozások gazdasági- és 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 további 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 célom, hogy áthidaljam az elméleti megközelítés és a gyakorlati alkalmazhatóság közötti szakadékot. Ennek a perspektívának az újdonságtartalma, hogy az empirikus megközelítésre fókuszáltam, így az eredményeket a gyakorlatban hasznosítva hatékonyabban lehet védekezni az ipari kémkedés belső és külső fenyegetésével szemben egyaránt. Bár a kvalitatív kutatás eredményei nem tekinthetők reprezentatívnak, azonban pragmatikus jelentősége, hogy a védelmi vállalkozások döntéshozói útmutatóként használhatják egy hatékony információvédelmi program kidolgozásához, amely magában foglalja

szociotechnikai megközelítésből a digitális és fizikai eszközöket, továbbá belső érintettek viselkedésére és motiválására vonatkozó tényezőket egyaránt. Az eredmények szintén támogatást nyújtanak a vállalkozások vezetőinek az információbiztonságra vonatkozó szemléletmódjuk kiszélesítésében, hogy képesek legyenek megfelelő lépéseket tenni a kritikus információ védelme érdekében. Bár a dinamikusan változó piacon nehéz megjósolni a jövőbeni információbiztonsági fenyegetések alakulását, a kutatás során a napjainkban alkalmazott eszközökből és módszerekből következtetéseket vontam le, hogy a vállalkozásoknak milyen természetű fenyegetésekkel kell szembenézni az előre látható jövőben.

A téma aktualitása

A gazdasági- és ipari kémkedés elleni védekezést a megelőzés és észlelés szempontjából lehet megközelíteni. Egy olyan ipari kémkedés elleni belső rendszer kiépítése, mely segíthet megelőzni, időben észlelni és reagálni a támadásra, majd helyreállítani az esetlegesen okozott következményeket, összetett feladat, melynek során számos külső és belső tényező empirikus vizsgálata szükséges. A jól működő, átfogó rendszer kialakításának első problémája, hogy túl sok különböző természetű fenyegetés észlelhető, amelyeket számításba kell venni. Jelen kutatás folyamán újszerű megközelítést alkalmaztam, és az ipari- és gazdasági kémkedést, továbbá a fenyegetés elleni védekezést a szervezetre ható külső és belső kontingencia tényezők közé soroltam. A megközelítés újszerűsége abban rejlik, hogy a kontingencia elmélet 1960-as évektől való elterjedése óta a vállalkozásra ható változók jelentős átalakuláson mentek keresztül, így a hatékony szervezéshez a korábban definiáltak mellett szükséges figyelembe venni a jelenben ható tényezőket is. A fenyegetés csökkentéséhez a vállalkozások döntéshozóinak tanulmányozni szükséges az őket körülvevő környezetben érvényesülő gazdasági, politikai, geopolitikai változókat, a technológiai fejlődést, az ellátási láncba fűződő faktorokat, a kiberbűnözés fejlődését, a társadalmi tényezőket és a természeti katasztrófákat egyaránt, melyekkel szemben az átfogó információbiztonsági politika, az információbiztonsági kultúra, továbbá az információvédelmi szoftverek és berendezések támogatásával képesek a megelőzést és észlelést szolgáló gyakorlatokat alkalmazni.

A téma aktualitását szintén indokolja a 2022. februárban kirobban orosz-ukrán fegyveres konfliktus, melynek hatására a védelmi iparban előállított kritikus információ értéke ugrásszerűen növekedett, és vált keresetté az ágazat szereplői között, ami a gazdasági- és ipari kémkedési esetek fokozódásához vezetett. Következésképp nem volt meglepő, hogy

az Európa keleti határán zajló háború számottevő hatással volt a mélyinterjúk során az alanyok válaszaira. Így a geopolitikai körülmények alakulása okán az értekezés újszerű abból a szempontból, hogy az európai védelmi kis- és középvállalkozásokat fenyegető gazdasági- és ipari kémkedést háborús környezetben vizsgálja.

A mélyinterjúk folytatásának periódusában kezdett nagyobb médiafigyelmet kapni a mesterséges intelligencia, továbbá a technológia hatása a társadalom jövőjére, amely szintén hatást gyakorolt az alanyok beszámolóira.

A kutatás célkitűzése

Doktori értekezésem témájául azért választottam a bemutatott tudományos problémát, mert a védelmi ipar területén dolgozom, egy haditechnikai fejlesztéssel és gyártással foglalkozó vállalkozásnál vagyok értékesítési igazgató. A szervezet a saját értékesítésre szánt innovatív eszközök fejlesztése mellett más nemzetközi védelmi vállalatoknak is segít részegységek vagy teljes eszközök fejlesztésében, továbbá újonnan felmerülő igényekre is rövid időn belül elkészíti a kívánt technológia működő prototípusát. A vállalkozás magas innovációs hajlammal rendelkezik, így gyakran találkozom az ipari kémkedés különböző formáival.

Jelen kutatás fókuszja a védelmi iparban innovációk fejlesztésével foglalkozó kis-és középvállalkozásokra irányult. A vállalkozásokat képviselő szakértőkkel folytatott interjúk alatt gyűjtött empirikus adatok szolgáltak az elmélet definiálásának alapjául. A kutatás során célkitűzésem, hogy multidiszciplináris megközelítést alkalmazva azonosítsam azon faktorokat, amelyeket számításba kell venni egy olyan információvédelmi rendszer kialakításához, amely hatékonyan képes megelőzni és észlelni a kritikus információ eltulajdonítását célzó támadásokat, így csökkentve a szervezetet fenyegető ipari kémkedés súlyos következményeit. A célom eléréséhez a következő célkitűzéseket (C) definiáltam:

C1 Célom feltárni, hogy milyen faktorok azonosíthatók az ipari kémkedéssel összefüggésbe hozható esetek növekedése mögött a védelmi iparban. Az esetszámok gyarapodását okozó tényezők megismerése iránymutatást ad, hogy milyen természetű információbiztonsági fenyegetéseket szükséges számításba venni a rendszer tervezése során.

C2 Feladataim közé soroltam azonosítani, hogy milyen motivációk, körülmények és támogató tényezők ismerhetők fel a vállalkozás belső érintettjei által elkövetett ipari

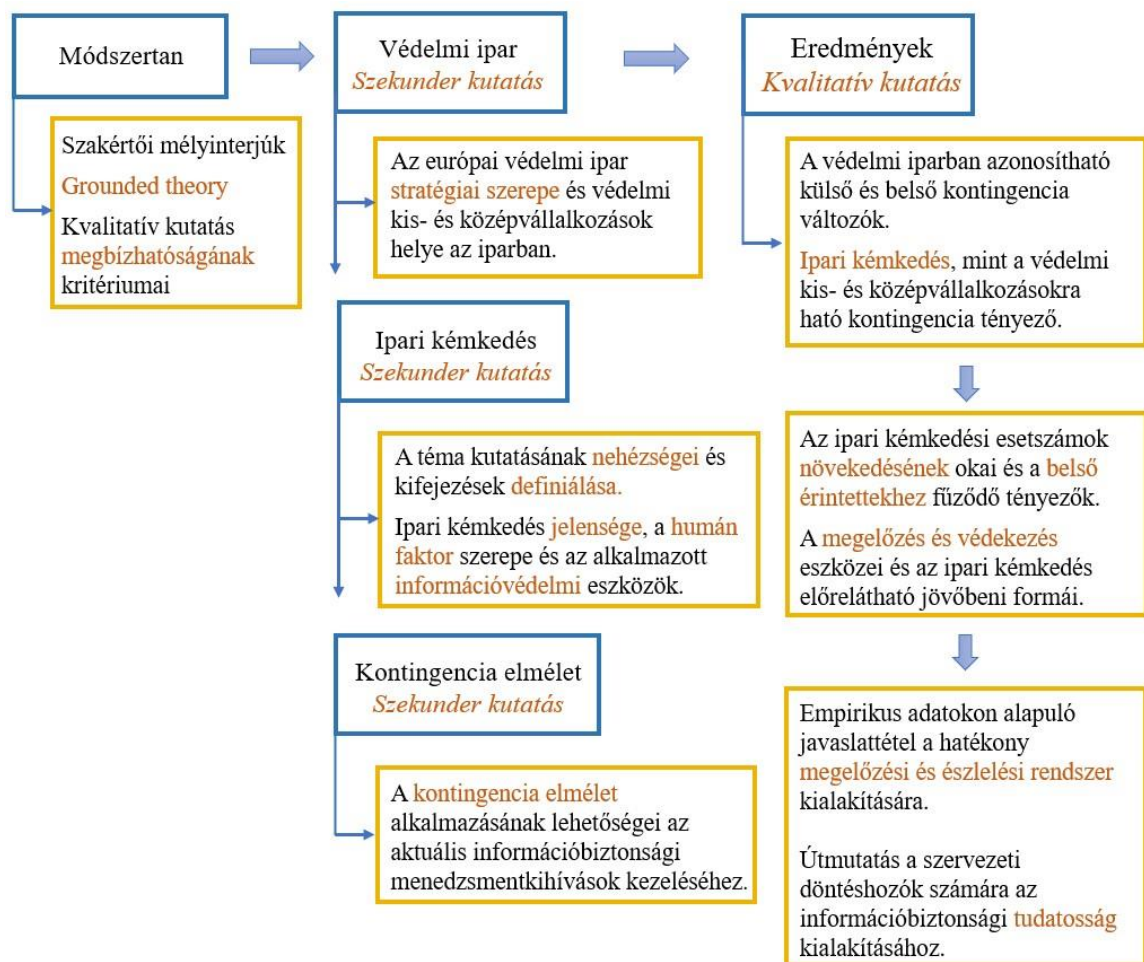
kémkedési esetek mögött. A definiált tudományos probléma vizsgálata során azért fontos az emberi tényező kutatása, mert a munkavállalók által megtestesített belső fenyegetés a legkritikusabb információbiztonsági probléma a vállalkozás szempontjából. Ennek oka, hogy hozzáféréssel rendelkezhetnek a szervezet információs infrastruktúrájához. Söilen (2016) [12] kutatása alapján az ipari kémkedési esetek jelentős többségét, mely az áldozatul esett vállalkozások felszámolását eredményezte, belső érintettek követték el.

C3 Célkitűzésem megismerni, hogy milyen gyakorlatokat alkalmaznak az innovatív védelmi vállalkozások a gazdasági- és ipari kémkedés kockázatának csökkentésére. A kérdés vizsgálata során a használt eszközökön és módszereken felül arról is következtetések vonhatók le, hogy a vállalkozások érintettjeinek milyen a percepciója az ipari- és gazdasági kémkedés jelentette kockázat kapcsán, továbbá mennyire tartják valós fenyegetésnek.

C4 Továbbá a dinamikusan változó környezeti kontingencia tényezők mellett a kutatómunkám célja előretekinteni, hogy a jelenben alkalmazott gazdasági- és ipari kémkedési módszerek fejlődéséből következtetve milyen természetű jövőbeni információbiztonsági fenyegetésekre szükséges felkészülni az innovatív védelmi vállalkozásoknak.

A kutatás felépítése

A dolgozatban az ipari- és gazdasági kémkedés komplex témakörét multidiszciplináris megközelítésből vizsgáltam, melynek során érintettem az informatikai, a katonai műszaki, a közgazdaság, a politika továbbá a pszichológiai tudományok területét, kiemelten vizsgálva a humán faktor szerepét. A doktori értekezés logikai felépítését és struktúráját az 1. ábra mutatja be.



1. ábra: Az értekezés koncepciója és struktúrája

Forrás: saját szerkesztés

1. KUTATÁSI MÓDSZEREK

A rendelkezésre álló statisztikák alapján ritkán történnek belső érintettek által elkövetett incidensek, azonban valószínűbb, hogy a 2.2.1. fejezetben részletesen ismertetett okok miatt a vállalkozások elvétve jelentik a hatóságok felé az ipari kémkedés gyanúját, ezáltal csak kvantitatív módszereket alkalmazva nem lehet átfogó képet adni a vizsgált problémáról [13, 14, 15, 16]. Ezzel szemben kvalitatív elemzés folytatása során olyan tényezőket lehet a felszínre hozni, melyekből levonhatók azon következtetések, amik a gyakorlatban segítik a védelmi vállalkozások döntéshozóit a megfelelő információvédelmi rendszer kialakításában. Kvalitatív kutatás folytatásának előnye, hogy az adatfelvétel során felszínre kerülő információk alapján irányítható annak további menete, amely hozzájárul a vizsgált jelenség mélyrehatóbb megértéséhez, miközben az alany tudása és tapasztalatai kiindulási pontul szolgálnak a kutatás további folytatásához [17]. Az így kapott eredmények alapot biztosítanak hipotézisek megfogalmazásához, a probléma kvantitatív elemzéséhez, magyarázásához, illetve a bizonyításhoz szükséges matematikai-statisztikai jellegű modellezéshez [17].

1.1. Szakértői mélyinterjú

Kvalitatív mélyinterjúk alkalmazása célravezető módszer érzékeny témák – mint a védelmi vállalkozások számára kritikus ipari kémkedés – mélyebb feltárására [17, 18], mivel az adatfelvétel során két személy nyíltan és őszintén beszélget egy, a közös érdeklődési körükbe tartozó témáról [19]. Ez a tudományos metódus hozzájárul a válaszadó személyes tapasztalatainak, véleményének, perspektívájának és hiedelmeinek mélyreható megismeréséhez, így az interjúk során gyűjtött adat az elmélet elsődleges forrásává válhat [20]. A mélyinterjúk alkalmával a kérdezőbiztos lehetővé teszi az interjúalany számára, hogy szabadon kifejtse a vizsgált problémával kapcsolatos gondolatait, miközben diszkréten irányítja a beszélgetést az előre definiált kutatási célok alapján [17, 21]. A félig strukturált mélyinterjúk alkalmazásának előnye, hogy támogatja a nagy mennyiségű személyes adat gyűjtését, mivel az interjúalany szabadon oszthatja meg tapasztalatait és véleményét, így könnyítve meg a vizsgált probléma kontextusba való helyezését [21].

A szakértői mélyinterjú általában vállalatvezetőkkel vagy valamely területen kimagasló tudással rendelkező szakemberekkel készül, melynek során a kutatási témában különösen jártas személyek véleményének és tapasztalatainak megismerése a cél [22]. A mintába

kiválasztott alanyok meglátásainak feltárása során a kutató birtokába kerülhet olyan iparági empirikus tudás, mely a valóságban szerzett szakmai tapasztalatok révén biztosít mélyebb betekintést a téma vizsgálatához [23]. A szakértői mélyinterjúk alkalmával a vezérfonal biztosítja, hogy a beszélgetés témája egyezzen a kutatott problémával. Az elméletet rigorózan véve kvalitatív kutatás során nincs szükség a vezérfonalra, mert korlátozza az interjúalany információátadását, azonban a gyakorlatban az adatfelvétel folyamán a teljes strukturátlanság nehézkes és adathiányhoz vezethet [24]. Szakértői mélyinterjúk alkalmával a moderátor nem lehet felkészületlen, hiszen a téma kifejtése során újabb kérdéseket szükséges feltenni, különben a beszélgetés elakad, illetve befejeződik; továbbá beszélgetések a vezérfonaltól eltérhetnek, a kérdések tartalmát, sorrendjét, és az interjú hosszát az interjúkészítő és a válaszadó interakciója folyamatosan befolyásolja [25]. A szakértői mélyinterjú egy olyan adatgyűjtési módszer, amely eredményei megfelelőek a grounded theory módszerrel való feldolgozásra [26].

1.2. Grounded theory és a kvalitatív kutatás megbízhatósága

Jelen kvalitatív kutatás során a gyűjtött adatok elemzése grounded theory (megalapozott elmélet) módszertannal történt. A grounded theory egy széles körben elismert, tudományosan megalapozott, abduktív jellegű, szisztematikus adatelemzési módszer [18, 27, 28, 29], mely alkalmazása során az elmélet empirikus adatokból fejlődik ki [30]. A módszer az elméleti és empirikus kutatás közötti szakadékot hivatott áthidalni [31], és lehetővé teszi a kutató számára, hogy alaposan megfigyeljen egy problémát, melynek során a szisztematikusan gyűjtött adatokból alakul ki az elmélet [30]. A módszer célja a koncepció azonosítása a problémák és lehetséges megoldási lehetőségek megértésén keresztül [25]. A grounded theory alkalmazása olyan kutatási munkák során ajánlott, amikor a vizsgált problémával kapcsolatban nem érhető el korábbi releváns elmélet [32].

A doktori értekezésben a gyűjtött adatok elemzése a grounded theory konstruktivista megközelítéséből történt, amely az empirikus világ első kézből való megtapasztalására épít [33]. A konstruktivista gondolkodásmód szerint a valóság nem objektív, hanem a kutató a saját nézőpontjából ragadja meg, szabadon meghatározva a jelentéstartalmat, amelyet a saját szemléletmódja és tapasztalata szerint formál, mialatt elismeri a korábbi ismeretek integrálását a kutatásba [34]. Az irányzat alkalmazása során a kódok, kategóriák és fogalomcsoportok a kutató szubjektumán átszűrődve alakulnak ki [35]. A konstruktivista megközelítés használata közben elkerülhetetlen, hogy a korábbi szekunder információk, ismeretek és tapasztalatok hatással legyenek a kutatás

eredményeire [36]. Az irányzat kódolási eljárása és mechanizmusai támogatják a korábbi ismeretek beépítését, így lehetővé téve a gyakorlati és elméleti megközelítését a vizsgált problémának [25]. Konstruktivista irányzatot alkalmazva a grounded theory induktív, mivel az elméletet a gyűjtött adatokból vezeti le, ugyanakkor deduktív, mert az elmélet fejlődése során az eredményeket összeveti a szakirodalommal [25, 29].

A narratív megközelítés lehetővé teszi az emberközeli, gyakorlatban alkalmazható eredmények generálását többek között a gazdasági és menedzsmenttudományok [37], továbbá a pszichológiai és társadalomtudományok [38] területén. A grounded theory módszertan alkalmazása során a narratív elemzési technikák hozzájárulnak a komplex probléma empirikus szemléletű feltárásához [39], így a módszert alkalmaztam a gyűjtött adatok elemzése folyamán. A megközelítés alapgondolata onnan ered, hogy a mindig racionálisan viselkedő és optimalizáló emberkép hibás, és nem ad teljes képet a gazdasági szereplőkről, mivel azokat pszichológiai és érzelmi hatások érik, ezáltal fontos megismerni azokat a narratív faktorokat, amelyek a nem racionális döntéseket formálják [40]. Mivel ez a módszer rugalmas, de ugyanakkor kellően stabil, így képes a definiált kutatási kérdésre vonatkozó tudományos eredmény alapját biztosítani [41]. A narratív elemzés, mely az emberi szándékokkal, cselekedetekkel, egyéni helyzetekkel és pszichés valósággal foglalkozik, az észlelt dolgokat egymással valamilyen relációba állítja, és azoknak közös jelentést tulajdonít [42]. Ez a módszer nem az egyetlen lehetséges valóságot írja le, hanem annak egy értelmezését [42]. Jelen kutatás során a narratívumokat induktív és deduktív módon is vizsgáltam. Induktív eljárás során a gyűjtött adatokat addig elemeztem, amíg fel nem fedeztem a strukturálást segítő szempontokat, majd a deduktív elemzés során ezeket összevettem a témába elérhető szakirodalommal [37].

Kvalitatív kutatás során a definiált eredmények megítélésének legfontosabb kritériuma a **megbízhatóság** [43, 44, 45], amely a következetességből, az átvihetőségből, a hitelességből, és a megerősíthetőségből tevődik össze [45, 46, 47]. Az eredmények megbízhatóságának biztosítása érdekében jelen kutatás figyelembe veszi ezen szempontokat, melyet az 1. táblázat ismertet. Bár a négy, kvalitatív kutatások megbízhatóságát biztosító kritérium külön alfejezetben kerül bemutatásra, azonban a bizonyításhoz szükséges módszerek nem határolhatók el egymástól, és átfedés lelhető fel közöttük.

Kvalitatív kutatás négy megbízhatósági kritériuma [45]	A kritérium követelménye és módszerei	A kritérium teljesítése jelen tanulmányban
Következetesség (<i>Dependability</i>)	Az eredmények következtetések és megbízhatók, a kutatás folyamata szigorúan dokumentált [30, 46]	○ A kutatás folyamata, az adatgyűjtés, az alanyok és az adatelemzés részletes bemutatása.
Átvihetőség (<i>Transferability</i>)	Az eredmények mennyire alkalmazhatók egyéb körülmények között [48], szélesebb populációra [47]. ○ Gyakorlati alkalmazhatóság kérdése [46]	○ Adatgyűjtés kilenc európai országban, a védelmi ipar számos területén; ○ a kutatás eredményei a védelmi iparban működő KKV-k vezetőit támogatják egy átfogó információbiztonsági rendszer kiépítésében.
Hitelesség (<i>Credibility</i>)	Az eredmények mennyire összeegyeztethetők a valósággal [48], mennyire képviselik az interjúalanyok valódi jelentését [45]. ○ Legoptimálisabb módszer kiválasztása [49] ○ Megfelelő alanyok kiválasztása [47, 49] ○ Elmélettel való összehasonlítás [25, 29] ○ Gyűjtött és feldolgozott adat mennyisége [49] ○ Reflektálás [30] ○ Trianguláció [46, 50] ○ Iteratív kérdések [47]	○ Módszertan kiválasztása előtt a témát korábban azonos vagy hasonló módszerrel feldolgozó szakirodalom vizsgálata; ○ kiemelkedő szakmai tapasztalattal rendelkező alanyok kiválasztása, akik készséggel vettek rész a kutatásban; ○ jelentős számú szakirodalom feldolgozása, majd releváns művek összehasonlítása az eredményekkel; ○ 42 mélyinterjú készítése; ○ szekunder és a primer módszer triangulációja; ○ iteratív kérdések használata.
Megerősíthetőség (<i>Confirmability</i>)	Az eredmények az alanyoktól származnak, és nincsenk befolyásolva a kutató által [45]. A következtetések kapcsolódnak az eredményekhez, és a kutatási azonos eredményekkel megismételhető [46]. ○ A kutatás folyamata szigorúan dokumentált [30, 46] ○ Trianguláció [47]	○ A megerősíthetőség bizonyításának limitációja, hogy longitudinális vizsgálatra lenne szükség mely jelen dolgozatban nem megvalósítható; ○ a három szakaszban készített mélyinterjúk azonos eredményei részben igazolják ezt a követelményt; ○ a kutatás folyamata alaposan dokumentált; ○ triangulációt a többforrású adatgyűjtés biztosítja.

1. táblázat: Kvalitatív kutatás megbízhatósági kritériumai

Forrás: Saját szerkesztés

1.2.1. Következetesség

Kvalitatív kutatás során a **következetesség** azt feltételezi, hogy az eredmények következtetések és megbízhatók, valamint a kutatás menete szigorúan dokumentált, lehetővé téve, hogy a kutatómunkában nem érintett személyek követni, ellenőrizni és bírálni tudják a folyamatot [30, 46]. A módszertan és a használt technikák részletes leírása hozzájárul, hogy az olvasó értékelje, hogy a kutató megfelelő vizsgálati gyakorlatokat követte-e, továbbá lehetővé teszi, hogy a kutatás ugyanazon kontextusban, módszerekkel és résztvevőkkel való megismétlése során hasonló eredményeket hozzon [47]. Jelen doktori értekezésben az eredmények megbízhatóságát a kutatási folyamat szigorú dokumentálása biztosítja a kutatás tervezésétől az eredmények értékeléséig. Bár a grounded theory alkalmazása során a probléma feltárását rögtön terepen, primer adatok gyűjtésével kell kezdeni, figyelmen kívül hagyva a korábbi eredményeket, azonban a publikációs alapelveket figyelembe véve ez a feltétel megvalósíthatatlan [33]. Jelen dolgozatban a primer kutatást megelőzte a témában rendelkezésre álló szakirodalom alapos vizsgálata, mivel a tudományos kutatások előírása szerint a grounded theory alkalmazása során a kutatási kérdéseknek az átfogó irodalmi feldolgozáshoz kell kapcsolódnia [51].

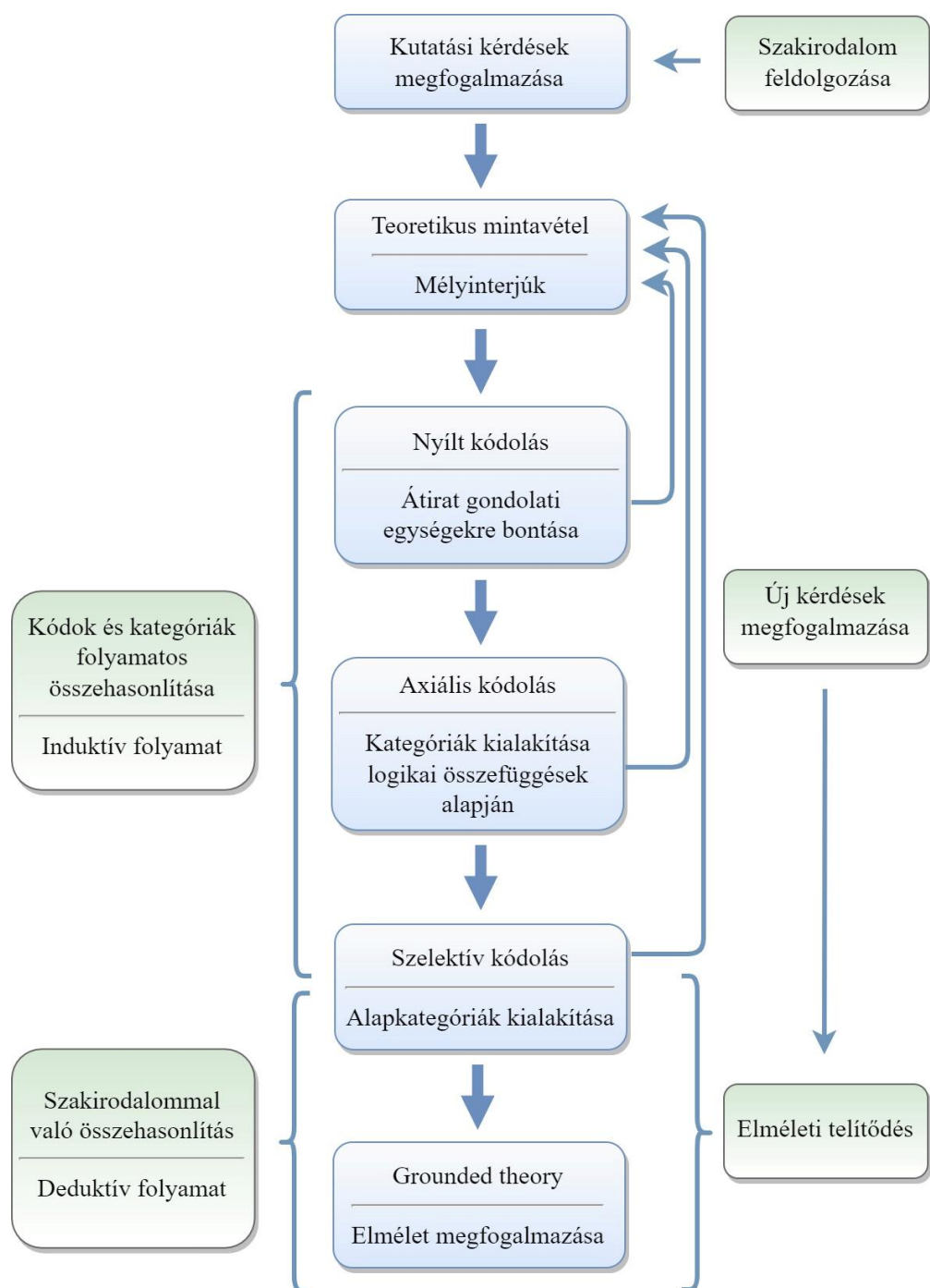
A teoretikus mintavétel a téma szakértőivel folytatott mélyinterjúk során valósult meg. Glaser és Strauss (1967) [30], a módszer megalkotói szerint a kvalitatív adatfelvétel nem csak válaszokat, hanem kérdéseket is szolgáltat, melyek segítségével újabb kutatási irányok azonosíthatók. A grounded theory nem határozza meg előre a minta jellemzőit, hanem az az elmélet fejlődésével folyamatosan alakul, az éppen feltárt eredmények és újonnan felmerülő kutatási kérdések vezetik a kutatót újabb alanyokig egészen az elméleti telítődésig [33]. Jelen kutatás során az adatfelvétel három szakaszban történt, azzal a céllal, hogy az eredmények elemzése során felmerülő újabb kérdésekkel gazdagítsa az elméletet, melyet az 1.4. fejezet ismertet részletesen.

A gyűjtött empirikus adatokból való elméletalkotás különböző szinteken történő analizálást igényel [52], mondatonként haladó adatelemzésre épül, továbbá a kutatás során folyamatosan új kategóriákat generál, mely eredményeként a vizsgált jelenséget általános elvi képletekkel magyarázza [31]. A módszertan szerint nem szabad az adatokat előre kialakított fogalomkörökbe erőltetni, azokat folyamatos összehasonlítás közben kialakított kategóriákba kell osztályozni [53]. Jelen kutatás Strauss és Corbin (1990) [51]

kódolási logikáját követi, mely az adatok logikai kategóriákba való osztályozását, új ötletekké való összeállítását majd az elmélet kialakítását foglalja magában.

A gyűjtött empirikus adatok kódolásának **első lépése** a nyílt kódolás, melynek során az átirat gondolati egységekre való bontása történik – amelyek egyszerűbb kifejezésektől több mondatig terjedhetnek – miközben kialakulnak a kezdetleges kategóriák [52]. A **következő lépés** az axiális kódolás, ami a kódok és kategóriák csökkentésére és összevonására irányuló köztes módszer [33, 51]. Axiális kódolás közben a gondolati egységek logikai összefüggések alapján történő fogalomkörökbe való osztályozása megy végbe, a köztük lévő hasonlóságok és különbségek felismerése és pontosítása során [54]. A **harmadik lépés** a szelektív kódolás, melynek során létrejönnek az alapkategóriák, amelyek a kialakuló elmélet forrását képviselik [33]. Ezután következhet az elmélet megfogalmazása, mely a fogalmak és kategóriák közötti kapcsolatok meghatározását jelenti [52].

A grounded theory módszertan alkalmazása során az elmélet akkor definiálható, amikor minden kategória elérte az elméleti telítődést. Az adatfelvétel és az -elemzés addig folyik, amíg az alanyok még hozzáadnak valamilyen új szempontot a kutatáshoz, illetve a kódok még magyarázó erővel bírnak [33]. Végül a hitelesség biztosítása érdekében az eredmények korábban megfogalmazott elméletekkel való összehasonlítása történik [29]. Az 2. ábra szemlélteti a grounded theory módszertan folyamatát.



2. ábra: Grounded theory módszer folyamata

Forrás: saját szerkesztés Glaser és Strauss (1967) [30]; Mitev (2012) [33]; Charmaz (2014) [29] és Kelemené Erdős (2014) [25] alapján

1.2.2. Átvihetőség

A kvalitatív kutatási eredmények szempontjából az **átvihetőség** kritériuma arra vonatkozik, hogy a tanulmányban leírt eredmények vagy jelenségek mennyire hasznosíthatók elméleti és gyakorlati felhasználás során más helyzetekben, továbbá a jövőbeni kutatásokban [45, 48]. Bár kvalitatív kutatás folytatásánál nem feltétlenül elvárás a reprezentativitás, ezzel szemben az átvihetőség kritériumának szempontjából bizonyítani kell, hogy az eredmények alkalmazhatók a szélesebb populációra [47]. Az átvihetőség teljesülését támogatja a résztvevők kiválasztásának és jellemzőinek, továbbá az adatgyűjtés körülményeinek részletes leírása, ezenfelül az eredmények gazdag bemutatása [49]. Ez a kritérium kritikus fontosságú a kutatási eredmények gyakorlati alkalmazásának szempontjából, mivel a szervezet döntéshozói csak egy vagy néhány kutatásból származó eredményre, következtetésre és javaslatra támaszkodhatnak, amelyek gyakorlati felhasználása a kutatási környezettől eltérő kontextusban kerül bizonyításra [46]. Jelen kutatás során az átvihetőséget biztosítja, hogy az adatfelvétel kilenc különböző európai országban, a védelmi ipar számos területét foglalta magába, mely részletes ismertetése az 1.4. fejezetben olvasható. Az 101. oldalon kerül bemutatásra az eredmények elméleti hasznosíthatósága, az 103. oldalon az eredmények gyakorlati alkalmazhatósága, és a 106. oldalon a definiált jövőbeni kutatási irányok.

1.2.3. Hitelesség

A kvalitatív kutatás **hitelessége** arra vonatkozik, hogy az eredmények milyen szinten összeegyeztethetők a valósággal [48], továbbá mennyire képviselik a kutatásban résztvevők által megosztott gondolatok valódi jelentését [45]. A kritérium biztosításának egyik módszere a kutatási problémához legjobban illeszkedő módszertan kiválasztása [49]. A témát korábban feldolgozó módszerek átvétele bevált gyakorlat a kvalitatív kutatások hitelességének biztosítására [32], amelyeknek azon szerzők kutatásiból kell származni, akik már eredményesen alkalmazták korábban hasonló problémák feldolgozása során [47]. (1) Connolly és szerzőtársai (2015) [55] a szervezeti érintettek információbiztonsághoz kapcsolódó attitűdjét vizsgálta; (2) Alsowail és Al-Shehari (2020) [56] szisztematikusan rendszerezte az ipari kémkedéshez fűződő kísérleteket azonosító technikákat; (3) Boakye és Gyan (2021) [57] az innovatív kis és középvállalatoknál kialakítható olyan program definiálásán dolgozott, mely csökkentheti a kutatott probléma kockázatát; (4) Khan és szerzőtársai (2022) [58] a belső fenyegetés nem szándékos formáját és annak következményeit vizsgálták; (5) Purl és Greitzer (2022)

[59] az ipari kémkedés dinamikáját és az azt elkövető entitások karakterisztikáit kutatták; (6) továbbá Robayo (2022) [60] a belső érintettek ipari kémkedéssel összefüggésbe hozható tevékenységének folyamatát elemezte a grounded theory módszertan használatával. A felsorolt tudományos művek nem csak a grounded theory alkalmazásában, hanem a gyűjtött empirikus adatok kódolásának logikájában és az eredmények vizuális szemléltetésében is hasznos tanácsokkal támogatták a doktori értekezést.

Glaser és Strauss (1967) [30] a jelen dolgozatban használt grounded theory módszertan alkalmazása során a reflektálást tartják a hitelesség alapjának, amely megtörtén az eredmények értelmezése során. A kvalitatív kutatások hitelességének biztosítását nehezíti, hogy a kritérium – a kvantitatív kutatásokhoz hasonlóan – deduktív módszerekben gyökerezik, és olyan külső követelményekre támaszkodik, amelyek a kvalitatív kutatásokból hiányoznak [61]. Azonban az alkalmazott grounded theory konstruktivista megközelítése deduktív természetű is egyben, mivel lehetővé teszi az elmélet fejlődése során az eredmények szakirodalommal való összevetését [25, 29]. A gyűjtött és feldolgozott adat mennyisége is fontos a hitelesség biztosítása érdekében. Az adatmennyiség, amely szükséges a kutatási kérdés megbízható megválaszolásához, különböző a vizsgált jelenségek komplexitásától, és a rendelkezésre álló adat minőségétől függően [49]. Iteratív kérdések segítségével lehetőség van kiszűrni, hogy az interjúalany az igazat osztja meg a kérdéssel kapcsolatban, melyek során a kutató visszatér a korábbi témákhoz, hogy felismerje az esetleg felmerülő ellentmondásokat [47].

Bár a véletlenszerű kiválasztás során a résztvevők nagyobb valószínűséggel képeznek reprezentatív mintát [62], a jelen dolgozatban definiált kutatási kérdések megválaszolására szakértői mélyinterjúk szükségesek a téma feltárásához. A véletlenszerű kiválasztás jelentős hátránya, hogy a kutatónak nincs ellenőrzése az alanyok szelektálása fölött, így előfordulhat, hogy olyan személy kerül a mintába, aki nem releváns a kutatás szempontjából vagy nem kíván együttműködni [47]. Jelen doktori értekezés folyamán az alanyok kiválasztása célzott mintavétel során történt, amely bár nem vezet reprezentatív eredmények megfogalmazásához, ugyanakkor alapot biztosít a téma további kvantitatív kutatásához.

Kvalitatív kutatás közben kiemelten fontos, hogy olyan alanyok vegyenek részt az adatfelvételben, akik valóban hajlandóak részt venni és szabadon késznek állnak a

tudásuk megosztására [47]. Olyan személyek kiválasztása, akik eltérő és gazdag tapasztalattal rendelkeznek, hozzájárul a kutatott probléma több különböző nézőpontból való megismeréséhez [49]. Az eredmények hitelessége szempontjából a kutató és az interjúalany között kialakuló hosszútávú kapcsolat segítheti a vizsgált probléma megértését [45], azonban ennek veszélye, hogy a kutató olyan mélyen belemerül a kultúrába, hogy szakami ítéletei befolyásolódnak [47].

A kvalitatív kutatások hitelességét a többforrású adatgyűjtéssel megvalósítható trianguláció biztosítja, mely különböző módszerek, technikák vagy források együttes használatát jelenti [46, 50]. Ezek erősíthetik vagy korrigálhatják egymást a kutatómunka során, továbbá alkalmazásukkal elkerülhető, hogy kevés vagy korlátozott információból történjen a következtetések levonása [50, 63]. A különböző adatforrások használata, továbbá az időben és térben széles spektrumú nézőpontok figyelembevétele megfelelőbb és stabilabb képet adhatnak a valóságról [64]. Az eltérő módszerek együttes használata ellensúlyozza azok korlátait, és egyben kihasználja a heterogén metódusok alkalmazásából származó előnyöket [63].

1.2.4. Megerősíthetőség

Az eredmények **megerősíthetőségéhez** bizonyítani szükséges, hogy a kutatás eredményei kizárólag a megkérdezett alanyoktól és azok körülményeitől függenek, és nincsenek befolyásolva a kutatás végző személy előítéletei, motivációi és érdekei által [45], továbbá a levont következtetések világosan kapcsolódnak az eredményekhez, és a kutatási folyamat közel azonos eredményekkel megismételhető legyen [46]. A kritérium biztosításához intézkedéseket kell tenni annak érdekében, hogy a vizsgálat eredménye az alanyok tapasztalatainak és ötleteinek foganata legyen, és ne befolyásolják a kutató saját jellemzői és preferenciái, így a trianguláció szerepe ismét hangsúlyozásra kerül ebben a kontextusban, hogy csökkentse a vizsgálatot végző személy elfogultságát [47]. Az eredmények megbízhatóságának limitációja jelen kutatás során a megerősíthetőség mélyrehatóbb bizonyítása, mivel az longitudinális vizsgálatot igényelne, amelyre ezen doktori értekezés keretei között nincs lehetőség. Azonban a három szakaszban készített mélyinterjúk közel azonos eredményei részben igazolják ezt a kritériumot. A kutatás során kapott eredmények megbízhatóságának szintén limitációja, hogy a téma érzékenysége miatt az interjúk során az alanyok eltitkolhattak vagy megváltoztathattak bizonyos, az ipari kémkedéshez kapcsolódó információkat, ami torzíthatja a gyűjtött adatokat.

1.3. Kutatási kérdések

A grounded theory szerint a végső megalapozott elmélet – az eredményként kapott *grounded theory* egyezik a módszertan elnevezésével – a kutatási kérdések alapján gyűjtött empirikus adatokból fejlődik ki, és nem célja előre megfogalmazott hipotézisek tesztelése. A módszertan alkalmazása során minden esetben az elmélet generálás a folyamat célja, és nem az előre definiált hipotézisek deduktív bizonyítása [31]. A kutatómunka alkalmával a kategóriák induktív módon, az állandó összehasonlítás eredményeként közvetlenül az empirikus adatokból fejlődnek, ezért nincs szükség a deduktív logikára, a hipotézisek tesztelésére [33]. A folyamat abduktív jellegének biztosítása érdekében is fontos elkerülni az előre megfogalmazott hipotézisek jelentette korlátozásokat [51]. A doktori értekezésben alkalmazott módszertan használata során a hipotézisek az elméletalkotás eredményei és nem kiindulópontjai [31]. Jelen dolgozatban a kutatási kérdések definiálását megelőzte a témában rendelkezésre álló szakirodalom alapos vizsgálata, mivel a grounded theory alkalmazása közben a kutatási kérdéseknek az átfogó irodalmi feldolgozáshoz kell kapcsolódnia [51]. A tudományos művek elemzése során azonosítva lettek az elméleti hiányosságok, melyek alapján a következő kutatási kérdések kerültek megfogalmazásra:

- K1:** Milyen tényezők vezettek a védelmi iparban az ipari kémkedéssel összefüggésbe hozható esetek növekedéséhez?
- K2:** Milyen motivációk, körülmények és egyéb támogató tényezők tárhatók fel a vállalat belső érintettjei által elkövetett ipari kémkedési incidensek mögött?
- K3:** Milyen módszereket tudnak az innovatív védelmi vállalkozások alkalmazni az ipari kémkedés megelőzésére és észlelésére?
- K4:** A dinamikusan változó kontingencia tényezők mellett a jelenleg alkalmazott ipari kémkedési módszerek és technikák alapján milyen természetű jövőbeni fenyegetésekre kell felkészülni az innovatív védelmi vállalkozások vezetőinek?

A szakértői mélyinterjúk során alkalmazott magyar és angol nyelvű vezérfonalakat a kutatási kérdések alapján fogalmaztam meg, melyek megtekinthetők a Függelékben. A 2. táblázat szemlélteti azon szekunder eredményeket, melyek támogatták az interjúk során érintett témák kialakulását. A félig-strukturált szakértői mélyinterjúk alatt az érintett témakörök azonosak voltak, azonban a beszélgetések időtartalma, a feltett kérdések, továbbá a kérdések pontos megfogalmazása az interjú alakulása szerint változott.

Szekunder eredmények	Szerzők	Interjúk során érintett témák
IPARI KÉMKEDÉS ESETEK SZÁMÁNAK NÖVEKEDÉSE		
Esetek száma növekszik	Thorleuchter – Van den Poel (2013), Konopatsch (2020), Shelupanov (2021)	Külső és belső kontingencia tényezők, melyek következményeként az üzleti titkok vagy egyéb információk nem tervezett szivárgása globálisan egyre gyakrabban fordul elő.
Technológia gyors ütemű fejlődése	Søilen (2016), Heickerö (2019), Szerb et al. (2020), Kelemen-Erdős – Mészáros (2022)	
Versenyelőny és technológiai lemaradás javítása	Sinha (2012), Choi – Teresa (2020), Kelemen-Erdős – Mészáros (2022)	
TÁMOGATÓ TÉNYEZŐK A BELSŐ ÉRINTETTEK MÖGÖTT		
Hanyagság, munkavégzés közben elkövetett hibák	Ashenden (2018), Elifoglu et al. (2018), Williams et al. (2019)	Tényezők, melyek szerepet játszanak a munkavállalók információbiztonsági tudatosságának kialakításában.
Új technológiák rendszerezése a szervezetenél	Williams et al. (2019), Samy et al. (2021)	Faktorok, melyek hozzájárulnak a munkavállalók szervezethez való hűtlenségéhez.
Nem megfelelő vezetési /szervezeti kultúra ami hűtlenséghez vezet	Nasheri (2004), Vashisth – Kumar (2013)	
Külső nyomás, zsarolás vagy megvesztegetés	Sinha (2012), Duckworth – De Silva (2019), Button (2020)	
MEGELŐZÉS ÉS VÉDEKEZÉS		
Fizikai védekezés	Androulidakis – Kioupakis (2016), Gheyas – Abdallah (2016), Elifoglu et al. (2018)	Hatékonyan alkalmazható védekezési eszközök és berendezések az ipari kémkedés megelőzésére és észlelésére.
Információbiztonsági kultúra	Schlienger – Teufel (2003), Ramachandran et al. (2008), AlHogail (2015), Glaspie – Karwowski (2018)	Olyan gyakorlatok, melyek során az információ tudatos védelmét a mindennapi munkavégzés részévé lehet alakítani.
Információtechnológiai (IT) háttérű védekezés	Androulidakis – Kioupakis (2016), Hills – Anjali (2017), Homoliak et al. (2020), Saxena et al. (2020)	
JÖVŐBENI INFORMÁCIÓBIZTONSÁGI KIHÍVÁSOK		
Mesterséges intelligencia	Zile – Strazdiņa (2018), Mohanta et al. (2019), Yalcinkaya – Maffei (2020), Fadi et al. (2022)	Mesterséges intelligencia alapú információbiztonsági eszközök alkalmazási területei és kockázatai.
Jövőbeni fenyegetések	Schindler – Ruhland (2022), Nejad (2023), Williams et al. (2023), Wilson – Hingnikar (2023)	Jövőbeni információbiztonsági fenyegetések természete, melyekre fel kell készülni a vállalkozásoknak.

2. táblázat: Interjúk témakörei

Forrás: Saját szerkesztés

1.4. Minta

Az adatgyűjtés célzott mintavétellel történt, mely lehetővé teszi, hogy a résztvevők a vizsgált téma szempontjából releváns tulajdonságaik szerint kerüljenek meghatározásra [65]. A módszer alkalmazása során a kutató saját döntése alapján választja ki a tervezett beszélgetéseken résztvevő azon személyek és szervezetek, akik képesek és hajlandók releváns információval hozzájárulni az előre definiált probléma kutatásához tudásuk és tapasztalataik alapján [66]. Azonban az alanyok tudása és szakmai tapasztalata mellett a minta meghatározása folyamán figyelembe kell venni a lehetséges résztvevők hajlandóságát, továbbá képességüket arra, hogy gondolataikat érthető és logikus módon tudják kommunikálni [67]. A kiválasztás során minél több kritériumnak szükséges megfelelni, annál célzottabbá válik a minta, melynek előnye, hogy kizárja a kutatásból a nem megfelelő elemeket, homogén mintát létrehozva [65].

Az átvihetőség minőségi kritérium biztosítása érdekében az alanyok kilenc európai országot és a védelmi ágazat számos területét képviselték, melyet a 3. táblázat szemléltet. A kutatás során az adatgyűjtés három szakaszban történt. A grounded theory módszertan lehetővé teszi, hogy az elemzési munka megkezdődjön már az adatfelvétel folyamán, így nem csak válaszokat, hanem újabb kérdéseket is szolgáltatva, melyek segítségével folytatható az adatgyűjtés a probléma még teljesebb feltárásához [30]. Kvalitatív kutatás során bár statisztikailag érvényes következtetések nem vonhatók le, azonban értékes betekintést nyújt az adott kérdéskörrel foglalkozó szakemberek gyakorlati tapasztalataiba, viselkedésébe, indítékaiba és gondolkodásmódjába [17].

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)			
1.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Vezérigazgató
2.	Magyarország	Precíziós fémalkatrész KFI és gyártás	Információbiztonsági szakértő
3.	Magyarország	Repülőipar – alkatrész KFI	Információbiztonsági szakértő
4.	Magyarország	Űripar – alkatrész KFI	Vezérigazgató
5.	Magyarország	Űripar – alkatrész KFI	Információbiztonsági szakértő
6.	Magyarország	Katonai jármű – alkatrész KFI	Vezérigazgató
7.	Magyarország	Katonai jármű – alkatrész KFI	Információbiztonsági szakértő
8.	Magyarország	Védelmi felszerelés KFI és gyártás	Tulajdonos/vezérigazgató
9.	Magyarország	Rakétaelhárító rendszer	Tulajdonos/vezérigazgató
III. szakasz (2023. I. negyedév)			
1.	Anglia	IT – hardverfejlesztés	Fejlesztőmérnök
2.	Anglia	Űripar – alkatrész KFI	Tulajdonos
3.	Német	Védelmi felszerelés KFI és gyártás	Értékesítési igazgató
4.	Magyar	Védelmi felszerelés KFI és gyártás	Tulajdonos
5.	Magyar	IT – szoftverfejlesztés	Fejlesztőmérnök
6.	Magyar	Precíziós fémalkatrész KFI és gyártás	Információbiztonsági szakértő

3. táblázat: Az interjúalanyok jellemzői

Forrás: saját szerkesztés (n=42)

A mélyinterjúk olyan személyekkel zajlottak, akik a védelmi iparban folytatott kutatás, fejlesztés és innovációs (KFI) tevékenységek területén rendelkeznek több éves – egyes alanyok esetén több évtizedes – kiemelkedő szakmai tapasztalattal. Összesen 42 mélyinterjú készült, az elméleti telítettség a 27. interjúnál valósult meg, ezután a válaszadók a kutatás fókuszát szigorúan véve nem szolgáltatottak új információt. Egy interjú átlagosan egy órát vett igénybe. Ezenfelül az adatok elemzése és a kategóriák kialakítása során lehetőségem volt többször újra felkeresni bizonyos alanyokat az újonnan felmerülő kérdésekkel, amely módszert lehetővé tesz az alkalmazott grounded theory. Az interjúk magyar és angol nyelven folytak, a vezérfonalak a Függelékben találhatóak. Az eltérő nyelvek közötti kommunikáció ekvivalenciája valamilyen szinten mindig

korlátozott, így az interjú keretrendszerét biztosító vezérfonal szövegének más nyelvekre való fordítása kihívást jelent a kutatóknak [68]. Azonban a nyelvi egyezőség elve kimondja, hogy az eltérő nyelvű vezérfonalak jelentésének azonosnak kell maradni az előre definiált probléma feltárására alkalmas adatok gyűjtéséhez [69]. A kutatómunka során törekedtem arra, hogy a vizsgált kutatási kérdések megfeleljenek a nyelvi ekvivalencia elvének.

A kutatott probléma érzékenysége miatt minden interjú elején az alanyok tájékoztatásra kerültek, hogy semmilyen bizalmas vagy személyes kérdés nem hangzik el az adatfelvétel során, továbbá beazonosításukra alkalmas információ nem kerül publikálásra. Az interjúk kezdetén szintén elhangzott, hogy jelen beszélgetés során nincs „rossz” vagy „jelentéktelen” válasz, minden ötlet hozzájárul a kutatáshoz. Ez a megközelítés segített abban, hogy az alanyok a kutatási projekt fontos szereplőinek érezzék magukat.

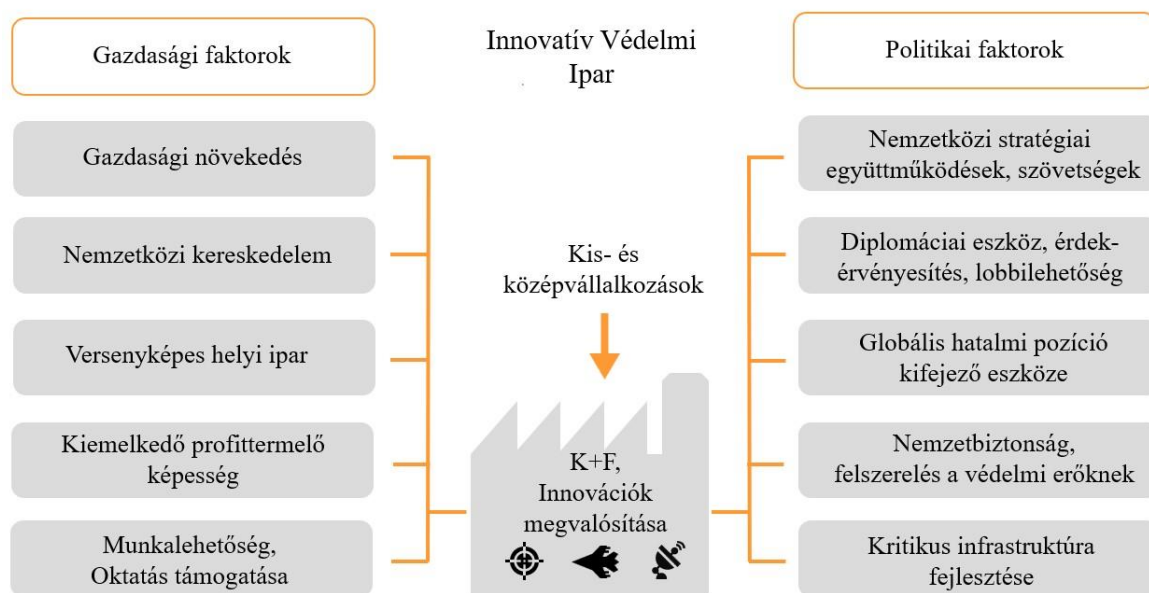
2. ELMÉLETI MEGALAPOZÁS

2.1. Az európai védelmi ipar stratégiai szerepe

A védelmi ipar attribútumait vizsgáló kutatók egyetértenek abban, hogy az ágazat stratégiai szerepet játszik valamennyi államban [70, 71, 72, 73, 74, 75]. A nemzetbiztonságban betöltött központi feladata mellett számos egyéb rendeltetésének teljesítésével biztosítja az ország lakosságának a jólétét. Az ipar támogatja a fenntartható gazdasági növekedést, serkenti a nemzetközi kereskedelmet, fontos szerepet játszik a polgárok védelmében, a belbiztonság biztosításában, továbbá fokozza a globalizációs folyamatokat [70, 71, 72, 76, 77, 78]. A tudásintenzív ágazat támogatja az oktatást, az egészségügyet, csökkenti a munkanélküliséget, ezenfelül munka- és kutatási lehetőséget teremt magasan képzett szakemberek számára [70, 71, 72]. A védelmi ipar kritikus infrastruktúrával látja el a lakosságot, amely magában foglalja a gyárakat és egyéb termeléshez szükséges létesítményeket, közlekedési hálózatokat¹, víz-, és energia hálózatokat, a kommunikációs rendszereket, iskolákat, oktatási központokat és kórházakat [79]. Az európai védelmi ágazat olyan gazdasági, politikai és technológiai tényezőket ölel fel, melyek kiemelten támogatják a helyi ipar globális versenyképességét [80], továbbá a szektorra jellemző intenzív kutatás, fejlesztés és innováció eredményeként számos technológiai újdonsággal látja el a társadalmat [6, 81, 82, 83].

A lokális védelmi ipar fejlesztése gazdasági és politikai szempontok figyelembevételével történik. Az ágazat megfelelő infrastruktúrával és kiemelkedő tudással és tapasztalattal rendelkező szakemberekkel támogatva kimagasló profitot képes realizálni [84, 85], ezenfelül a modern helyi védelmi ipar a nemzet politikai pozíciójának kifejező eszköze lehet [76, 86, 87, 88]. A jelenkori gazdasági és geopolitikai környezetben a védelmi eszközök exportja a diplomáciai kapcsolatok fontos területévé vált [89, 90, 91, 92], amely lehetőséget biztosít a nemzetközi viszonyok békés úton történő rendezésére [93]. A védelmi eszközök szövetséges államoknak történő exportja erősíti a nemzet regionális és globális politikai pozícióját [90, 94], támogatja a stratégiai szövetségek kötését és fenntartását [85, 95], növeli a nemzetbiztonságot a globális fenyegetésekkel szemben [96], továbbá fokozza a nemzet politikai befolyását, így biztosítva lobbilehetőséget a globális közösségben [97]. A 3. ábra szemlélteti az innovatív lokális védelmi ipar stratégiai sajátosságait gazdasági és politikai szempontból.

¹ Közúthálózat, sínhálózat, reptér, vízi közlekedés.



3. ábra: Az innovatív védelmi ipar gazdasági és politikai hatásai.

Forrás: saját szerkesztés Mészáros 2023 [82] és Mészáros 2023 [83] alapján

A hidegháború vége olyan változásokat hozott, melyek alapjaiban formálták át a globális védelmi ipart. Az átalakult körülmények, mint az ágazat fejlesztésére és fenntartására csoportosított állami költségkeretek radikális csökkentése, a korábbi magas kereslet elmozdulása a tömeggyártott eszközök irányából az innovatív, kisszéziás, precíziós védelmi rendszerek irányába, valamint a globalizációs hatások és a geopolitikai átrendeződés mind olyan változók, melyek kényszerítették a védelmi ágazat szereplőit, hogy alkalmazkodjanak az új feltételekhez [2, 87, 88, 98, 99]. Ezen körülmények hatására az országok csökkentették a protekcionizmus eszközeinek gyakorlását, amely új lehetőséget teremtett az iparban a nemzetközi együttműködések és szövetségek kialakítására, hogy azok ellensúlyozzák a kormányok redukált hozzájárulását [4, 87, 98, 100]. Az internacionális kooperációk következményeként megkezdődött a külföldi tőke beáramlása, ami hozzájárult a hosszútávon fenntartható lokális védelmi bázis kialakításához [88, 99, 101]. A stratégiai együttműködések eredményeként erősödött a védelmi piac szereplőinek versenyhelyzete, csökkent az ipar fenntartásához szükséges költségek és erőforrások mértéke, továbbá az ágazat természetéből eredő bizonytalanságot is mérsékeltek [102, 103, 104, 105, 106]. Az ipar fejlesztéséhez szükséges információ országhatáron kívüli forrásból való beszerzésének lehetősége innovációs hullámot eredményezett [103, 107, 108, 109]. A könnyebben hozzáférhető

technológiatranszfer a kevésbé iparosodott országokat is támogatta a helyi védelmi ipar fejlesztésében, így utat nyitva számukra a transznacionális védelmi hálózatba [73, 87]. Az ágazatban bekövetkezett átalakulás egy olyan technológiai forradalmat indított be, melynek eredményeként a védelmi ipar vezetővé vált a kutatás, fejlesztés és innovációk területén.

A védelmi ipar transzformációja lehetővé tette a magánszektor képviselő kis- és középvállalkozások, továbbá start-upok megjelenését a piacon [2, 83, 110], melyek szerepe és száma várhatóan növekedni fog a jövőben [111]. 2022-ben az Európai Unió területén több mint 2500 KKV [112], közvetlenül 463 ezer főt foglalkoztat a védelmi ipar területén [80]. Ezek a vállalkozások kiemelkedő innovációs hajlammal rendelkeznek és élen járnak a diszruptív védelmi innovációk fejlesztésében [2, 3, 5, 6, 82, 83, 113], amelyet nagyrészt belső kutatással és fejlesztéssel támogatnak [114]. Az európai védelmi iparnak célkitűzése, hogy képes legyen teljes mértékben a KKV-kból származó innovációkra támaszkodni [112]. Mivel a nagy védelmi vállalatok nem érdekeltek a szűk globális piacok, vagy személyre szabott igények kiszolgálásában [71, 110], a KKV-k versenyképesen működhetnek, ha a tevékenységüket rés piacokra, továbbá személyre szabott védelmi eszközök fejlesztésére összpontosítják [6, 81, 98, 99].

A dinamikus védelmi piacon való versenyképesség megőrzésének és a nemzetbiztonság fenntartásának fontos tényezője az innováció. A védelmi technológiai újdonságok területén kiemelkedő teljesítményt nyújtó állam felkészültebben képes reagálni a váratlan fenyegetésekre, stratégiaiilag függetlenebb és erősebb nemzetközi politikai pozíciót képes fenntartani [83]. Az ágazatban az innovációk alakulását olyan katalizáló faktorok befolyásolják, mint a politikai, gazdasági és társadalmi célokat magában foglaló nemzeti stratégia, geopolitikai viszonyok, környezeti fenyegetések, földrajzi adottságok, technológiai újdonságok növekvő komplexitása, továbbá váratlanul felmerülő taktikai problémák, melyek megoldása újszerű megközelítést igényel [108, 110, 113, 115]. A katalizáló tényezők olyan erőteljes külső befolyást gyakorolnak a védelmi innovációs rendszerre, amelyek az ökoszisztéma legmagasabb szintjére hatnak, és lehetőséget teremtenek az újdonságok rendszeresített eszközök közé való integrációjára [4].

A lokális innovatív védelmi ipar fejlesztése és fenntartása, továbbá az ellátási lánc zavartalan működésének biztosítása alapvető fontosságú a stratégiai autonómia és a nemzeti szuverenitás szempontjából [3, 88, 116, 117]. Bár a szektorban még mindig az

autarkia az irányadó politikai koncepció, azonban a nemzetek többsége korlátozott erőforrásokkal rendelkezik [118], és nem képesek arra, hogy kizárólag a belső erőforrásokra támaszkodva tartsanak fent egy hosszútávon versenyképes védelmi bázist. Ez arra kényszeríti a döntéshozókat, hogy csökkentsék a függetlenedési törekvéseiket, és nemzetközi együttműködésekre, továbbá szövetségek kialakítására törekedjenek [3, 101, 107, 116, 118]. A védelmi autarkia rendkívül költséges, és nehezen megvalósítható, ezzel szemben a nemzetközi együttműködések protekcionista hatással rendelkeznek, mivel lehetővé teszik a helyi védelmi ipar fenntartását a külföldi innovatív technológiák beépítése mellett, társadalmilag elfogadhatóbb költségeken [119, 120]. A globális védelmi ipar folyamatos átalakulásban van, naponta jelennek meg innovatív új technológiák, így az újdonságok minél korábbi adaptálása a nemzeti stratégia kulcsfontosságú részévé vált [90, 121, 122]. Azok a szervezetek, amelyek elsőként tesznek lépéseket az új technológiák átvételére, amik később dominánssá válnak, általában megőrzik versenyképességüket és sikeresek maradnak [123]. A nemzetek, melyek elsőként képesek rendszeresíteni az újdonságokat, jelentős stratégiai és taktikai előnyre képesek szert tenni [113].

A védelmi ipar számos, stratégiai szempontból fontos nemzetbiztonsági, politikai és gazdasági funkciót lát el, feladatai magában foglalják a polgárok védelmét, és a nemzetbiztonság biztosítását. Fontos szerepe van a kritikus infrastruktúrák megvalósításában és védelmében, a globális gazdaságban, támogatja az oktatást és az egészségügyet, továbbá munkalehetőséget biztosít. Számos kis- és középvállalkozást foglalkoztat, melyek kiemelkedő teljesítményt nyújtanak a kutatás, fejlesztés és innováció területén. A leginnovatívabb ágazat, mely új technológiákkal látja el a társadalmat. A védelmi autarkia bár erős globális pozíciót biztosíthat, magas költségei miatt kevés állam képes hosszútávon fenntartani, így a védelmi ipar területén a nemzetközi együttműködések és szövetségek stratégiai erősségé váltak, melyek elősegítik a tudás- és technológiatranszfert az innovációk megvalósításához, továbbá támogatják az ellátási lánc zavartalan működését. Azonban a nemzetközi együttműködések előnyei, és a megalakulásokat célzó erőfeszítések mellett is az európai védelmi ipar legfőbb jellemzője 2022-ben, hogy nagyrészt nemzeti alapon működnek, korlátozott számú országhatáron átnyúló együttműködéssel [112]. A versenyképesség létfontosságú a kialakulóban lévő közös biztonság- és védelempolitika szempontjából,

továbbá az Európai Unió célkitűzése, hogy a tagállamok fokozottabban működjenek együtt a helyi vállalatok hatékonyabb fellépése érdekében [80].

A védelmi ipar küldetése a kereslet kiszolgálása a megfelelő technikai színvonalú termékekkel és szolgáltatásokkal, a hatékony termelés és versenyképes árak biztosítása, továbbá az ellátás zavartalanságának fenntartása a mindenkor körülményektől függetlenül [3]. Az elmúlt években a védelmi piac keresleti és kínálati oldala, a védelmi felszerelések gyártása, és nemzetközi kereskedelme is dinamikus növekedést mutatott [71, 116, 124], amelyet az Európai Unió határán, 2022. februárban kirobbant fegyveres konfliktus csak tovább fokozott. A védelmi ipar stratégiai jelentőségű feladatainak ellátását a döntésekhez szükséges kritikus információ támogatja. Az információ védelme az ipar rendeltetésének teljesítését biztosító kulcsfontosságú feladat, azonban a legkorszerűbb információvédelmi rendszerek alkalmazása mellett is kiemelt kockázatot jelent az ipari és gazdasági kémkedés.

2.2. Az ipari és gazdasági kémkedés

Az ipari és gazdasági kémkedés a legkorábbi információszerzési tevékenységek közé sorolható, és bár a módszerek az évszázadok során jelentős átalakuláson mentek keresztül, napjainkban is meghatározó probléma. Az elmúlt évek során az ipari és gazdasági kémkedéssel összefüggésbe hozható incidensek gyakorisága, továbbá a nemzeti iparra, gazdaságra és a teljes nemzetbiztonságra gyakorolt negatív hatása globális szinten jelentős növekedést mutatott [11, 125, 126, 127]. A végbemenő dinamikus technológiai fejlődés még több eszközt teremtett az információlopás elkövetésére, tovább fokozva a problémát, amely az egyik legsúlyosabb fenyegetéssé nőtte ki magát az országok iparával és fenntartható fejlődésével szemben [128]. Az ipari és gazdasági kémkedés kiemelten fenyegeti azon szervezetek működését, mely feladatainak teljesítése a kritikus információ rendelkezésre állásától függ. Míg egyéb ágazatokban az információlopás elsősorban pénzügyi, és hírnévbeli veszteséget okozhat, addig a védelmi iparban bekövetkező ipari vagy gazdasági kémkedés a teljes nemzetbiztonságra veszélyt jelentő fenyegetést testesít meg. Az innovatív technológiák területén úttörőnek számító védelmi ipar az egyik legfenyegetettebb szektor a fenyegetés szempontjából [94, 129]. A fejezet során érintett témákat a 4. táblázat szemlélteti.

Tényező	Probléma leírása	Szerző
KUTATÁSI PROBLÉMÁK		
Nincs általánosan elfogadott definíció	Nem áll rendelkezésre szakirodalom a jelenség pontos meghatározására.	Carl (2017), Hou – Wang (2020), Button (2020)
Kevés a releváns tanulmány	A probléma nehezen kutatható terület, amely korlátozott tudományos figyelmet kap.	Brancik – Ghinita (2011), Omar (2015), Söilen (2016), Carl (2017), Elifoglu et al. (2018), Button (2020), Glitz & Meyersson (2020), Knickmeier (2020), Barrachina et al. (2021), Lee et al. (2020)
Kevés a dokumentált eset	A statisztikák szerint nem gyakori jelenség, azonban számos ok miatt a szervezetek nem jelentik az eseteket, ami a statisztikák torzulásához vezet.	Crane (2005), Stadler (2012), Androulidakis – Kioupakis (2016), Bedford – Van Der Laam (2016), Söilen (2016), Babos (2019), Button (2020), Knickmeier (2020), Lyan – Frenkel (2020), Sadok et al. (2020)
IPARI KÉMKEDÉS JELENSÉGE		
Ipari kémkedés elkövetésének okai, motivációi	Számos érdek azonosítható az ipari kémkedés elkövetése mögött, mint a technológiai lemaradás gyors és költséghatékony csökkentése.	Sinha (2012), Pellegrino (2015), Roche (2016), Duckworth – De Silva (2019), Choi – Teresa (2020), Szerb et al. (2020), Barrachina et al. (2021)
Ipari kémkedés folyamata	Az innovatív információ eltulajdonításának menete és következményei.	Kelemen-Erdős – Mészáros (2023)
Ipari kémkedés típusai	Szervezetek vagy kormányok által szervezett vagy megbízott ipari kémkedés jellemvonásai.	Johnson (1998), Trim (2002), Brenner – Crescenzi (2006), Sinha (2012), Söilen (2016), Glitz – Meyersson (2020), Hou – Wang (2020), Ingesson (2023)
Ipari kémkedés módszerei	Az információlopás elkövetésére számos fizikai és információs technológiai módszert áll rendelkezésre, mely történhet belső szervezés, vagy külső kém megbízása során.	House (1995), Sinha (2012), Söilen (2016), Duckworth – De Silva (2019), Button (2020), Choi – Teresa (2020), Hou – Wang (2020), Lyan & Frenkel (2020), Kelemen-Erdős – Mészáros (2023)
HUMÁN FAKTOR SZEREPE		
Belső vagy külső elkövető	Amikor egy innovatív szervezetnél felmerül az ipari kémkedés gyanúja, vizsgálni szükséges, hogy az elkövető belső vagy külső személy.	Pasternak – Witkin (1996), Naseri (2004), Colwill (2009), Brancik – Ghinita (2011), Bedford – Van Der Laam (2016), Elifoglu et al. (2018), Noonan (2018), Duckworth – De Silva (2019), Button (2020), Kelemen-Erdős – Mészáros (2023)
Véletlen belső fenyegetés	Engedélyezett hozzáféréssel rendelkező belső érintett rossz szándék nélküli cselekedete kárt okoz az intézménynek.	House (1995), Colwill (2009), Omar (2015), Hills – Anjali (2017), Ashenden (2018), Elifoglu et al. (2018), Williams et al. (2019), Kelemen-Erdős – Mészáros (2023)
Szándékos belső fenyegetés	Engedélyezett hozzáféréssel rendelkező belső érintett tudatosan kárt okoz a szervezetnek.	Pasternak – Witkin (1996), Colwill (2009), Brancik – Ghinita (2011), Omar (2015), Hills – Anjali (2017), Ho – Warkentin (2017), Ashenden (2018), Elifoglu et al. (2018), Patil – Meshram (2018), Williams et al. (2019), Knickmeier (2020), Kelemen-Erdős – Mészáros (2023)

INFORMÁCIÓVÉDELMI RENDSZER		
Információbiztonsági kultúra	Magába foglal minden olyan intézkedést, melyek során információbiztonság az érintettek mindennapi munkavégzésének részévé válik.	Schlienger – Teufel (2003), Ramachandran et al. (2008), AlHogail (2015), Glaspie – Karwowski (2018)
Többrétegű információbiztonsági rendszer	Többrétegű védelmi rendszer kialakítása proaktívan védheti az információs infrastruktúrát.	Omar (2015), Androulidakis – Kioupakis (2016), Bedford – Van Der Laam (2016), Gheyas – Abdallah (2016), Elifoglu et al. (2018)
Innovatív megoldások, jövőbeni fenyegetések	Az információs technológia és mesterséges intelligencia alapú eszközök fejlődésével innovatív információvédelmi eszközök és ezzel párhuzamosan új fenyegetések jelennek meg.	Zile – Strazdiņa (2018), (2018), Mohanta et al. (2019), Yalcinkaya – Maffei (2020), Schindler – Ruhland (2022), Fadi et al. (2022), Nejad (2023), Williams et al. (2023), Wilson – Hingnikar (2023)
Kritikus infrastruktúra védelme	A védelmi iparban a kritikus infrastruktúrák olyan rendszerekből és eszközökből állnak, melyek romlása káros hatással lehet az ipar kritikus funkcióinak ellátására.	Mohanta et al. (2019), Yalcinkaya – Maffei (2020), Aoun et al. (2021), Dawson et al. (2021), Makrakis et al. (2021), Fadi et al. (2022), Lehto (2022), Williams et al. (2023)

4. táblázat: Ipari kémkedés attribútumai

Forrás: saját szerkesztés

2.2.1. Az ipari és gazdasági kémkedés kutatási problémái

Az ipari és gazdasági kémkedés egy olyan komplex probléma, mely vizsgálata multidiszciplináris megközelítést igényel, és nem rendelkezik általánosan elfogadott definícióval [13, 130, 131]. A téma kutatói egyetértenek abban, hogy ez egy kritikus és nehezen kutatható terület, mely a jelenség mélysége és negatív következményei ellenére korlátozott tudományos figyelmet kap [12, 13, 132, 133, 134, 135, 136, 137]. Az ipari és gazdasági kémkedés problémakörének nemzetközi vizsgálata nem tartozik a népszerű kutatási irányok közé, kevés az elérhető releváns tanulmány, és a publikált eredményekben a konzisztencia hiánya figyelhető meg [131, 138]. A kutatók a kérdés vizsgálatát interdiszciplinárisan elkülönülve végzik és nincsenek általánosan elfogadott következtetések, így a szerzők nehezen dolgoznak egymás eredményeivel [130]. A vizsgált jelenség hátterének szakirodalmi megalapozását, továbbá az empirikus tanulmányok és országspecifikus adatok összehasonlítását megnehezíti, hogy a tudományos eredmények ismertetése során a terminológiahasználat következetlen és nem konzisztens [131, 138].

A tudományos munkákban leggyakrabban alkalmazott két kifejezés, a gazdasági kémkedés (*economic espionage*), és az ipari kémkedés (*industrial espionage*) módszertanilag és tartalmilag szorosan összefügg, azonban eltérő jelentéssel bírhat. Számos szerző szerint a két fogalom közötti fő eltérés, hogy az előbbit állami szereplő, míg az utóbbit versenypiaci résztvevő kezdeményezi [1, 12, 13, 127, 139, 140], más kutatók nem tesznek különbséget a két kifejezés között és azt állítják, hogy mindig lehet bizonyos fokú kormányzati részvétel az ipari kémkedés során is [1, 10, 141, 142].

A szakirodalom elemzése alapján a **gazdasági kémkedés** a külföldi hírszerző szolgálatok által szervezett nemzetközi szintű, nemzetbiztonsági céllal történő, kormányok által folytatott, vagy irányított kémkedés [1, 13, 127, 139, 140], amely hazai vállalatok üzleti titkainak vagy kormányzati szervek bizalmas információinak célzott megszerzésére irányul, hogy azt a megbízó állam tudatosan a saját céljára felhasználhassa [13, 143, 144].

Az **ipari kémkedés** számos átfedést mutat a gazdasági kémkedéssel [13, 143, 144], azzal a különbséggel, hogy a nemzetközi piacon versenyző vállalatok által szervezett tevékenység [127], amely üzleti titkok jogtalan elsajátítása révén egy másik vállalkozás javát szolgálja [1, 13, 143], üzleti céllal megy végbe [139], közvetlen kormányzati beavatkozás nélkül [13, 140, 143].

Jelen kutatásban az **ipari kémkedés** kifejezés használata mellett döntöttem, amely 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. A doktori értekezésben az ipari kémkedés kifejezés használat nem tesz különbséget a versenytársak és a kormányok által szervezett kémkedés között, és a kémkedés tárgya elsősorban a védelmi innovációk fejlesztéséhez, előállításához és értékesítéséhez szükséges kritikus információ. A kémkedés mindkét formája súlyosan károsíthatja a vállalat hírnevét, megszakíthatja az innovációs folyamatokat és súlyos pénzügyi veszteségeket okozhat.

A kutatás szempontjából **kritikus információ** minden olyan tudás, amely eltulajdonítása az azt előállító vállalkozástól egy másik entitás előnyét szolgálja, miközben kárt okoz a tudást jogosan birtokló szervezetnek. Az ipari kémkedés által fenyegetett kritikus

információk leggyakoribb típusai a szellemi tulajdon (mint szabadalom, találmány, kézirat, képlet és gyártástechnológia); a stratégiai, pénzügyi, ellátási láncsal kapcsolatos és marketingtevékenységére vonatkozó információk; továbbá az aktuális és jövőbeni tervek és infrastruktúrák [137, 143, 145]. A védelmi innovációk szempontjából a tervrajzok, forráskódok, prototípusok, valamint az egyéb fejlesztéssel kapcsolatos dokumentumok állnak a kémkedés középpontjában, azonban egy elszánt elemző a folyamatban lévő szabadalmi kérelmekből, értékesítési előrejelzésekből, vevői információkból, a készletekkel és az ellátási lánc irányításával kapcsolatos információkból, továbbá a mérnökök és vezetők profiljaiból is képes értékes információt kinyerni [142].

Statisztikák alapján az ipari kémkedés nem gyakori jelenség, azonban valószínűbb, hogy az érintett szervezetek törekednek arra, hogy az esetek ne kerüljenek napvilágra, és a negatív következményektől tartva ritkán jelentik az incidenseket a hatóságoknak [12, 15, 16]. Mivel a legtöbb esetben nem jár azonnal észrevehető, kézzel fogható veszteséggel, számos vállalkozás egyáltalán nem, vagy csak hosszú idő után ismeri fel, hogy információlopás áldozatává váltak [14]. A probléma korai észlelését csak nehezíti, hogy az adatszerzés területén az új védelmi technológiák mellett folyamatosak a polgári, szélesebb körben elérhető új fejlesztések, amelyek sok esetben szofisztikáltabb és erőteljesebben titkosított kommunikációt tesznek lehetővé, mint a hatóságok által kezelt technológiák [146]. Amennyiben evidens bizonyíték áll a szervezet rendelkezésére, jellemzően a körülményes jogi folyamat, valamint a bizalom, hírnév és részvényárfolyamok csökkenése miatt igyekeznek az incidenseket elhallgatni, hogy elkerüljék a hozzá nem értésük és az üzleti titok lelepleződésének nyilvánosságra kerülését, vagy az illegális gyakorlat más területekre is kiterjedő kivizsgálását [12, 13, 14, 147].

Az esetek jelentésének hajlandóságát a nemzetközi sajtó részrehajlása is csökkenti, amely a vállalkozás által elkövetett cselekedetek törvénytelennek való felfogását társadalmilag konstruált és gyakran a hatalmi viszonyok mátrixába ágyazott kontextusba helyezi, amelyben az egyik fél nagyobb valószínűséggel képes a másikat deviánsnak, utánpótlónak bélyegezni [10]. Számos esetben a szervezetek belső eljárás keretében, a vonatkozó munkajog szerinti fegyelmi intézkedések figyelembevételével közelítik meg a problémát [133], vagy az áldozatok peren kívüli megállapodás kötésére törekednek az elkövetővel, amikor felmerül az ipari kémkedés gyanúja [147]. Amikor egy incidens hivatalos úton

való vizsgálatára kerül sor, az eljárás szigorú titoktartási intézkedések keretei között megy végbe, így jellemzően az elkövető vagy az áldozat kiléte nem kerül napvilágra, azonban a kutatók szerint nem gyakori az esetek hivatalos úton való kezelése [12, 13, 148].

Az ipari kémkedés problémaköre egy viszonylag új, és lassan fejlődő kutatási terület [149]. Számos szervezet alkalmaz költséges információvédelmi rendszereket, csak az információstechnológia (IT) által jelentett veszélyre összpontosítva, figyelmen kívül hagyva a vállalati érintettek által megtestesített fenyegetést [8, 9]. Következésképpen a rendelkezésre álló szakirodalom jelentős része a témát technológiai [10, 150], jogi [10, 138, 151], és a külső támadások aspektusából vizsgálja [152], kevés figyelmet fordítva a szervezeti érintettek által megtestesített belső fenyegetésre [15, 130, 132, 150]. Azonban a belső érintettek által megtestesített kockázat vizsgálata fontos faktor az ipari kémkedés témakörében, mivel az információlopási esetek nagy részéért globális szinten a munkavállalók vonhatók felelősségre [13, 153, 154].

A szervezeti érintettek révén megtestesített belső fenyegetés mélyreható feltárása nem egyszerű vállalkozás. Az általuk elkövetett ipari kémkedés – beleértve annak korábbi előzményeit, motivációit és szándékait – megértéséhez a szociálpszichológia, a kriminológia, a szervezeti viselkedés, a kommunikáció és más tudományos területek teoretikus megközelítéseit szükséges alkalmazni [155]. Ezenfelül a probléma komplexitásának köszönhetően, a gyakorlatban is használható megállapítások megfogalmazásához a vállalkozás jellemzőin felül a belső fenyegetések modellezése, az alkalmazottak sebezhetőségének értékelése és a szervezeten belüli biztonságtudatosság vizsgálata is fontos a kockázat mértékének azonosításához [132, 135, 156]. Azonban az elméleti keret hiányában nem áll rendelkezésre hatékony módszer vagy eszköz a kritikus információhoz hozzáféréssel rendelkező személyek megbízhatóságának vizsgálatára [157], ennél fogva a valós idejű cselekvések nehezen megfigyelhetők, a gyanús viselkedések gyakran észrevétlenül maradnak és bizonyítékok nehezen gyűjthetők.

2.2.2. Az ipari kémkedés jelensége

A védelmi iparban való tevékenység folytatásának feltétele a kritikus információ, melynek mennyisége és minősége kulcsfontosságú, gyors megszerzéséért, biztonságos tárolásáért és minél hatékonyabb felhasználásáért kíméletlen harc folyik [158]. A kritikus információ gyűjtése vagy előállítása hosszú és költséges folyamat, mely magában foglalja a külső környezet elemzését és a belső KFI tevékenységeket. Amennyiben a szervezet/állam sem belső, sem külső (nyílt) forrásból nem képes vagy hajlandó erőfeszítéseket tenni az igényelt technológiai innováció megvalósításához szükséges kritikus információ beszerzésére vagy előállítására, akkor merül fel az ipari kémkedés eszköztárának alkalmazása [159].

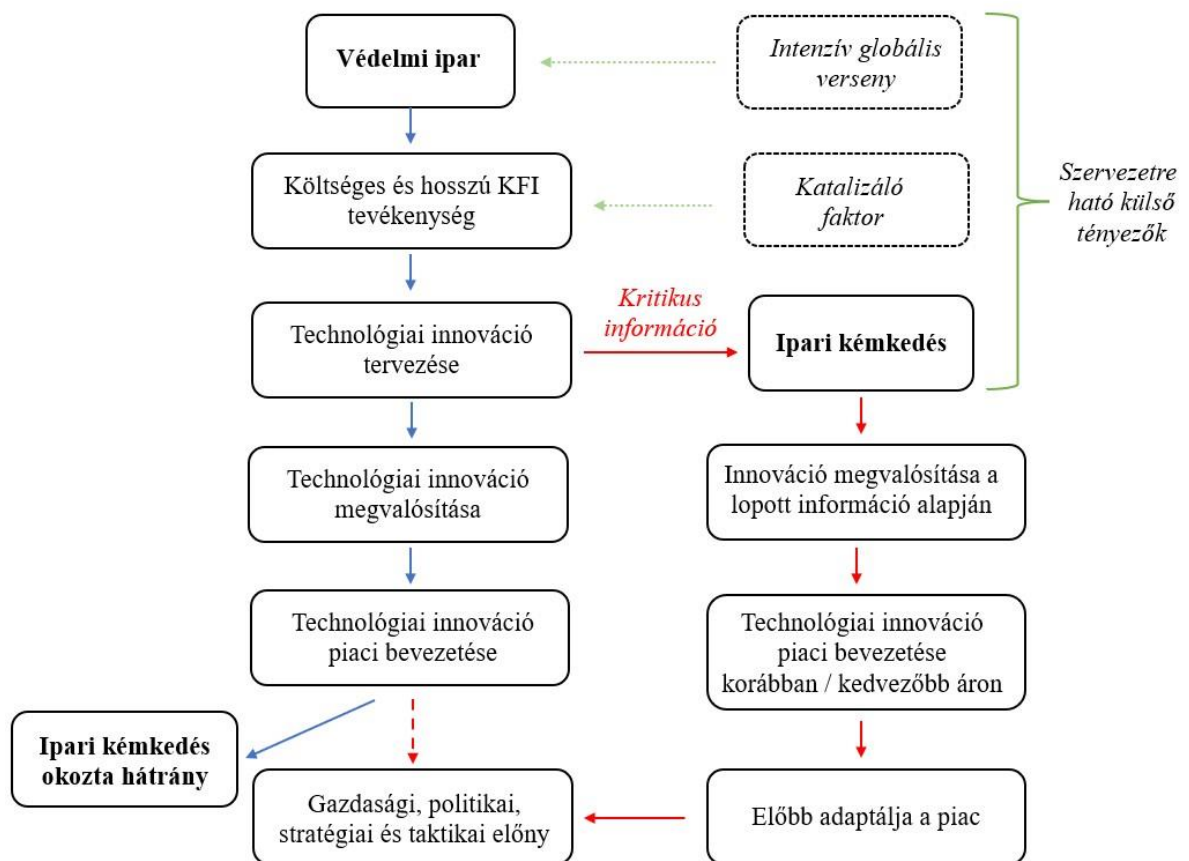
A szakirodalom a vizsgált tevékenységet jellemzően olyan etikátlan vagy törvénytelen gyakorlatnak mutatja be, amely lehetővé teszi a szervezetek/államok számára, hogy vásárlás vagy fejlesztés helyett kémkedés útján szerezzék be az innovatív információt [10]. A védelmi iparban az ipari kémkedés fő motivációi közé tartozik, hogy ezzel a módszerrel a szervezetek mérsékelhetik a technológiai lemaradásukat, javíthatják a versenyelőnyüket és elősegíthetik a bevétel gyors növekedését. Szintén előnye a tevékenységnek az elkövető szempontjából, hogy az új technológia elsőként való bemutatása során hatalmas piaci kapitalizációval piacvezetőkkel válhatnak és lobbilehetőséget szerezhetnek kormányzati szerveknél, hogy befolyásolják az iparágukkal kapcsolatos gazdasági döntéseket [142].

Bár a technológiai innovációk adaptálása számos előnyt jelent makró- és mikroökonómiai szinten egyaránt, ugyanakkor a gyors ütemű fejlődés jelentős mértékben fokozta az ipari kémkedés kockázatát, és annak negatív következményeit [160]. Az információlopás fenyegetése nem csak abból következik, hogy a szervezetek nagy mennyiségű kritikus információt tárolnak elektronikusan vagy felhőben, közvetlen a világhálózathoz csatlakozva – amit kihasználnak a kiber-kémek, akik kiléte gyakran ismeretlen marad [161] – hanem a széles körben elterjedő kommunikációs technológiai újdonságok biztonságossá, sok esetben fizikai érintkezés és egyéb nehézségek nélkül tettek hozzáférhetővé nagy mennyiségű kritikus információt [12], ami egyre több szervezetet bátorít fel arra, hogy kihasználja ezt a költség- és időhatékony információszerzési módszert [137].

Az, hogy egy szervezet mennyire kitett az információlopással kapcsolatos fenyegetéseknek, a vállalat innovációs képessége határozza meg. A védelmi iparban a

stratégiai jelentőségű technológiai újdonságok megvalósítása terén élen járnak a KKV-k [3, 82, 83, 113, 114], mivel azonban nem rendelkeznek a nagyvállalatok pénzügyi, humán és technológiai erőforrásával, így az ipari kémkedés jellemzőbb lehet [14, 140].

Kelemen-Erdős és Mészáros (2022) [7] eredményei szerint a védelmi ipar információs technológiától való függősége jelentős kockázatot rejt az ipari kémkedés szempontjából. Amennyiben a kritikus információ illetéktelen felhasználóhoz kerül, korlátozottá válik, vagy sérül, az akadályozhatja a teljes védelmi ágazatot a feladatai ellátásában. A védelmi ipart intenzív nemzetközi verseny jellemzi az új eszközök fejlesztése területén, mivel egy innováció megvalósítása és elsőként való adaptálása gazdasági és politikai előnyt szolgálhat a nemzet számára. Egy új technológia fejlesztése hosszú és költséges folyamat, amelyet jellemzően egy külső katalizáló faktor vált ki. Amikor egy szervezet vagy állam részt akar venni a védelmi innovációs versenyben, de nem állnak rendelkezésére a megvalósításához szükséges tapasztalattal és szaktudással rendelkező személyek, a költségvetési keret, továbbá elmaradottabb az ipar és a KFI területén, akkor dönthet úgy, hogy az ipari kémkedés eszköztárát alkalmazva szerzi be az információt, melynek folyamatát a 4. ábra ismerteti. Az információlopást elkövető fél számára ez a módszer gyors és költséghatékony megoldást kínál a szükséges tudás megszerzéséhez, amely lehetőséget nyújt számára az újdonság versenytársnál korábbi és/vagy – a költséges KFI folyamatok hiányában – kedvezőbb áron való piaci bevezetésére, amelyet az előbb adaptál, így jelentős profitot képes realizálni. Az innovációt előállító, megkárosított szervezet/állam nem csak a tervezett profit jelentős részét veszítheti el, hanem a KFI-be fektetett hatalmas költségeket, továbbá nem élvezheti a technológia elsőként bemutatásával járó stratégiai előnyöket. Emellett az illegálisan eltulajdonított információ felhasználása a piaci versenyt is torzítja.



4. ábra: Ipari kémkedés folyamata

Forrás: saját szerkesztés Kelemen-Erdős és Mészáros (2022) [7] alapján

A védelmi piacon magas belépési korlát jellemző, ami jelentősen megnehezíti, sok esetben ellehetetleníti az új szereplők megjelenését [162]. Az ágazatban már a piacra való belépés előtt számos esetben alkalmazott stratégia, hogy a szervezet ipari kémkedéssel szerzi be a szükséges információt, hogy képes legyen legyőzni a magas belépési korlátot és versenyelőnnyel kezdhesse a tevékenységét [137]. Az a szereplő, amely elsőként képes adaptálni egy új technológiát, anélkül, hogy jelentős erőforrást fordítana KFI tevékenységekre, potenciálisan globális előnyhöz juthat [163]. Az információszerzés ezen módszerét alkalmazó szervezet nem csak az innovatív információkhoz való gyorsabb és kevésbé költséges hozzáférés előnyét élvezni, amellyel hozzájárulhat a szervezet képességeinek fejlesztéséhez, hanem az így megtakarított összegeket átcsoportosíthatja egyéb projektekre [129].

Kelemen-Erdős és Mészáros [164, 165, 166] a korábbi kutatásaik során vizsgálták az innovatív vállalkozások által fejlesztett eszközök értékesítési lehetőségeit, mélyebben

elemezve az üzleti közvetítők és ügynökök tevékenységét információbiztonsági szempontból. A vizsgált üzleti tranzakciók során a terméket vagy technológiát értékesítő vállalkozást és a potenciális vevőt a gyakorlatban gyakran köti össze egy vagy több közvetítő [165]. A tevékenységük előnye, hogy felkeresnek és megosztanak olyan jövedelmező üzleti lehetőségeket és kapcsolatokat, amelyeket a vállalkozások egyénileg, előzetes ismeretség nélkül nem lettek volna képesek kialakítani [166]. Azonban munkájuk hátránya, hogy az üzletkötéshez szükséges kritikus információt felügyelet nélkül terjesztik, amely könnyen eljuthat olyan entitáshoz, aki rossz szándékkal használja fel a birtokába került tudást [164].

Az ipari kémkedés legegyszerűbb formája, amikor egyik szervezet kémkedik valamelyik versenytársa után. Érdekesebb eset, amikor egy külföldi kormány vagy szervezet kémkedik egy belföldi vállalkozás vagy állami KFI program után [142]. A kormányok által szervezett ipari kémkedés elemezhető mikrogazdasági és makrogazdasági kémkedés/hírszerzés szempontjából. A mikrogazdasági kémkedés során a kormányzatok által megbízott ügynökségek nyújtanak segítséget az alulteljesítő hazai vállalatoknak, vagy beavatkoznak a helyi szervezetek védelmében, a külföldi entitások által szervezett kémkedés elhárításában [167]. A makrogazdasági kémkedés olyan gazdasági, társadalmi, kulturális, politikai, ipari és technológiai adatok gyűjtését, elemzését, és értelmezését foglalja magában, amelyek közvetlenül felhasználhatók, és a teljes nemzet javát szolgálják [167].

Søilen (2016) [12] eredményei alapján a kémkedést szervező állam gyakran elmaradott a tudományok és az ipar területén, és a kémkedést – melynek célja a tanulás és felzárkózás – hatékonyabb stratégiának tekintik, mint a belső KFI képességek fejlesztését. Azonban ez hosszú távon a nemzeti védelmi ipar hanyatlásához vezet, mivel egyre kevesebb saját erőből megvalósított KFI programot eredményez [136]. Ezzel szemben Ingesson (2023) [168] szerint a nagyfokú ipari kémkedést nem szabad automatikusan a nemzeti innovációképességek hiányosságának tekinteni. Számos ország a vizsgált problémát a gazdasági tevékenységek legitim eszközének tekinti, és gyakran alkalmazza, – olyan módszereket is bevetve, melyeket más nemzetek jogrendszere törvénysértőnek tekint [141] – mivel felismerték a mikro- és makrogazdaságra gyakorolt pozitív következményeit [130, 141, 142, 169]. Más esetekben a kormányok kifejezetten ösztönzik a lokális vállalatokat az új technológiák kémkedés útján történő beszerzésére, a hazai védelmi képességek fejlesztése céljából [141, 142]. A kulturális különbségek is

hatást gyakorolnak az etikátlan és jogszerűtlen gyakorlatok megítélésére. A nemzetközi ügyletek során a szervezetek a saját kultúrájukban elfogadhatónak tekintett információgyűjtési módszereket részesítik előnyben [55, 170]. Az ipari kémkedés globális fenyegetését csak súlyosbítja, hogy a kapitalista országok törvénykezése hajlamos elbagatellizálni a jogtalan információeltulajdonítást, hogy a gazdasági/politikai hatalommal rendelkező, bűncselekményt elkövető személyek el tudják kerülni a hivatalos büntetőeljárást, és annak következményeit [171].

A hidegháború vége óta mind a kormányok, mind a vállalatok közötti ipari kémkedés széles körben elterjedt gyakorlattá vált. A kilencvenes évek elején kémek ezrei váltak munkanélkülivé, akik felszabadulva a hidegháborúban teljesített kötelezettségeik alól, tevékenységüket a külföldi kormányokat és vállalatokat célzó kémkedésen keresztül a saját nemzeti gazdaságuk újjáépítésére fordították [10], és látják el azóta is az ipar szereplőit az igényelt információval [12]. Elterjedt módszer, hogy a szervezetek/államok a belső hírszerző szerveik alkalmazása helyett külső személyt kérnek fel a kívánt információ megszerzésére, és a megbízók bármekkora összeget hajlandók fizetni az eltulajdonított információért cserébe a saját céljaik érvényesítése érdekében [130, 163].

A szervezeten belül bárki lehet kém. A kémek általában olyan bennfentesek, akiknek jó belső kapcsolataik vannak, megbízhatónak és semlegesnek tűnnek. Testet ölthetnek vezető, mérnök, takarító, karbantartó, biztonsági személyzet, gyakornok vagy bármilyen egyéb személyként, aki hozzáférhet a kritikus információkhoz [7]. Az innovatív technológiák eltulajdonítása szempontjából a legkritikusabb szervezeti belső érintettek (1) a mérnökök, akik hozzáférnek a terméktervezés és -fejlesztés kulcsfontosságú részleteihez; (2) a szervezeti jogászok, akik a folyamatban lévő szabadalmi bejelentésekkel, valamint egyéb bizalmas jogi kérdésekkel kapcsolatos információkkal rendelkeznek; (3) a műszaki és felhasználói kézikönyv készítői, akik számára elérhetők a különböző termékfejlesztési információk; (4) az értékesítési munkatársak, akik az értékesítési előrejelzésekkel és egyéb adatokkal dolgoznak; (5) továbbá, a vezetők, akik hozzáférnek a jövőbeni tervekhez és egyéb stratégiai információkhoz [142]. Azonban más szervezeti érintettől származó adat is egyéb forrásból gyűjtött információkkal kombinálva értékes és átfogó tudást nyújthat egy elemző számára.

Ipari kémkedés elkövetésének számtalan módszere áll rendelkezésre, amely eszköztára az etikátlan viselkedéstől a bűncselekményekig terjed. (1) Gyakran az innovációt

fejlesztő szervezet nincs is tisztában azzal, hogy a nyílt forráskódú platformok – mint a kiállítások, közösségi média felületek, értékesítési ajánlatok vagy marketinganyagok – milyen értékes információt kínálnak a piac más szereplőinek [172]. (2) Konferenciák és kiállítások során, ahol a szervezetek munkatársai informális légkörben érintkezhetnek egymással, a helyzetet az egyik szereplő kihasználhatja arra, hogy a beszélgetések során értékes információkat gyűjtsön a másik vállalkozásról [12]. (3) A kukabúvárkodás az ipari kémkedés klasszikus módszere, amelynek során az egyik szervezet a másik szemetét vizsgálja át, mivel a mai napig sok dokumentumot nyomtatnak ki a munkavállalók, amelynek jelentős része a kukában végzi [13]. (4) Több vállalkozást magában foglaló együttműködés keretein belül végzett kutatás és fejlesztés vagy egyéb üzleti tevékenység közelebb hozhatja egymáshoz a szervezeti érintetteket, ami bizalmas információk megosztásához vezethet, amelyet az egyik fél kihasználhat, hogy előnyre tegyen szert a másik féllel szemben [142]. (5) A versenytársak szakembereinek alkalmazása is gyakori módszer, annak ellenére, hogy ezzel megszegheti az előző szervezettel kötött versenytilalmi szerződést [13]. (6) A kémek prototípus tesztelése, ellopása vagy termék vásárlása útján visszafejtheti a versenytárs fejlesztését, hogy betekintést nyerjen az új technológiába [7, 172]. (7) A kémek helyezhetik a szervezet munkavállalóit elektronikus megfigyelés alá, többek között a helyiség vagy mobiltelefonok illegális lehallgatásával, kamerák elhelyezésével vagy az e-mailek és egyéb kommunikációs platformok megfigyelésével [13]. (8) Az ipari kémkedés egyik leggyakoribb és leggyorsabban fejlődő módszere a kibertámadás a szervezet információsrendszere ellen [142]. (9) A szükséges kritikus információ megszerzése történhet a belső érintett megbízása, zsarolása, megvesztegetése vagy kényszerítése útján is [13, 142, 161].

Az ipari kémkedés irányultsága elemezhető a szervezeten belül tevékenykedő, vagy külső elkövető szempontjából. A **belső kémkedés** során az érintett tudást sajátít ki érdekei érvényesítése vagy a vállalat megkárosítása érdekében, míg a **külső szereplő** által elkövetett információlopás alkalmával egy versenytárs vagy egy külföldi kormány saját technológiai vagy pénzügyi érdekeinek előmozdítása okán jogtalanul gyűjt információt egy másik entitástól [143]. Akár a szervezeten belülről, akár kívülről történik a kritikus információ eltulajdonítása, az a védelmi iparban súlyos következményeket vonhat maga után, így a probléma vizsgálata a humán faktor nézőpontjából elengedhetetlen a jelenség mélyebb megismeréséhez.

2.2.3. A humán faktor szerepe

Amikor egy szervezetnél felmerül az ipari kémkedés gyanúja, sokszor felvetődik a kérdés, hogy az elkövető belső vagy külső személy. A szervezet számára az egyik legkritikusabb és legnehezebben kezelhető fenyegetést jelenti, amikor egy belső érintett, amely a bizalmát élvezi, cselekszik az intézmény ellen. A kutatott probléma szempontjából **belső fenyegetést** testesít meg minden olyan személy, aki engedélyezett hozzáféréssel rendelkezik vagy rendelkezett a szervezet eszközeihez és információs rendszereihez, akiknek tettei vagy tétlensége, szándékai vagy gondatlansága negatív következményeket okozhat az intézménynek [11, 15, 56, 132, 134]. A belső fenyegetés olyan vállalkozáson belül tanúsított magatartásokban nyilvánulhat meg, amely eltér a szervezeti szabályzatban definiált viselkedéstől, és a kritikus információ szándékos vagy szándéktalan helytelen kezeléséhez, eltulajdonításához, jogosulatlan személy hozzáféréséhez és egyéb etikátlan vagy törvénytörő információkezelési cselekedethez vezethet [173]. Egy külső szereplő számára gyorsabb és költséghatékonyabb megoldás lehet egy bizalmi személy beépítése a szervezet sebezhetőségeinek feltárására, mint a számos információvédelmi rétegen keresztül történő támadás kezdeményezése [152]. A kritikus információ eltulajdonítása történhet belső érintett megbízása, zsarolása, megvesztegetése, vagy kényszerítése útján [13, 161]. Más esetekben a jó szándékú alkalmazottak munkavégzés közben tudatukon kívül válhatnak kémek célpontjává [58], vagy a szervezet belső érintettje kezdeményezi az ellopott információ értékesítését [174].

A belső fenyegetés megnyilvánulhat szándékosan elkövetett rosszakaró cselekedetek, és nem szándékos, véletlen elkövetett tevékenységek formájában, melyek engedély nélküli információkiáramláshoz vezetnek, és kárt okoznak a szervezetnek [134, 135, 150, 152, 175, 176]. A szándékosan és véletlen elkövetett ipari kémkedési esetek jellemzőit az 5. táblázat szemlélteti.

Elkövető	Ipari kémkedés formája	
	Szándékos	Véletlen
Külső	○ Információ szándékos és jogtalan eltulajdonítása, hogy egy másik entitás előnyét szolgálja [173] ○ Illegális vagy etikátlan tevékenység az információk szisztematikus gyűjtésére, elemzésére és felhasználására [143] ○ Nem képes vagy hajlandó erőfeszítéseket tenni az igényelt információ beszerzésére vagy előállítására [159] ○ Belfentes beépítése [152] ○ Belső személy megbízása, zsarolása, megvesztegetése, vagy kényszerítése [13, 161] ○ Versenytársak szakembereinek alkalmazása [13] ○ Külső személy megbízása [130, 163] ○ Szervezet illegális elektronikus megfigyelése [13] ○ IT innovációk biztonságossá tették [12], ami egyre több szervezetet bátorít fel [137] ○ Kibertámadás [142, 177]	○ Információ nyílt forráskódú platformokon való megosztása (kiállítások, közösségi média felületek, értékesítési ajánlatok vagy marketinganyagok) [172] ○ Konferenciák és kiállítások során értékes információ gyűjtése a másik szervezetről [12] ○ Több szervezetet magában foglaló együttműködés keretein belül végzett munka bizalmas információk megosztásához vezethet [142]
Belső	○ Jó kapcsolatokkal rendelkezik, és hozzáfér vagy hozzáférést biztosít az információhoz [174] ○ Belső fenyegetés információbiztonsági kockázati szintje magasabb, mint a külső támadásnál [133, 157] ○ Átfogó ismeretekkel, hozzáféréssel és ellenőrzési joggal rendelkezik és tisztában van a védelmi rendszerek hiányosságaival [157] ○ Elkövetési a foglalkoztatása korai szakaszában [178], vagy nyugdíjazás előtt [12]. ○ Az elkövető lehet a szervezet belső biztonsági rendszerét jól ismerő, magasan képzett személy [132, 135] vagy nem magasan képzett, hanem olyan alkalmazott, aki rossz szándékkal végzi a mindennapi feladatait [134]	○ Hanyagság vagy gondatlanság [150] ○ Munkavégzés közben elkövetett hibák [175] ○ Biztonságpolitika hiánya vagy nem betartása [135] ○ Nem megfelelő képzés vagy hiánya [135] ○ Stressz, munkavégzést támogató eszközök vagy okoseszközök elvesztése, ártatlan és naiv segíteni akarás a külső kérésekre vagy a zsarolás eszközeinek való kiszolgáltatottság [134] ○ Üzleti út során vállnak célponttá [172] ○ Új technológiák telepítése [175], alkalmazottak nem szívesen változtatnak a korábbi, szokásaikon [178]

5. táblázat: A szándékos és véletlen esetek jellemzői

Forrás: saját szerkesztés

A **véletlen** belső fenyegetést olyan belső vagy külső, jelenlegi vagy múltbéli szervezeti érintett testesít meg, aki engedélyezett hozzáféréssel rendelkezik vagy rendelkezett a szervezet információs rendszereihez, és rossz szándék nélküli cselekedete információszivárgáshoz vezet, amely kárt okoz az intézménynek [175]. Számos tevékenység vagy magatartás közvetlen vagy közvetett következménye vezethet véletlen információszivárogatási incidensekhez. Az alkalmazottak hanyagsága vagy gondatlansága [150], munkavégzés közben elkövetett hibák [175], a biztonságpolitika hiánya vagy nem betartása, a nem megfelelő képzés vagy annak hiánya [135] mind olyan faktorok, melyek növelik a belső fenyegetés kockázatát, és hozzájárulhatnak a kritikus információ illetéktelen kezekbe való kerüléséhez. A munkavállalói stressz, munkavégzést támogató eszközök vagy okoseszközök elvesztése, ártatlan és naiv segíteni akarás a kívülről érkező kérésekre vagy a zsarolás eszközeinek való kiszolgáltatottság [134] szintén súlyos szervezeti biztonsági résekhez vezethet. Más esetekben üzleti útjuk során vállalhatnak a vállalkozás érintettjei a kifinomult kémkedési módszerek célpontjává [172].

A versenyképesség fenntartásához szükséges a szervezetnek minél előbb adaptálni a technológiai innovációkat, azonban az új technológiák telepítése súlyos információbiztonsági sebezhetőséghez vezethet [175]. A munkavállalók fenntartásokkal kezelik az új, számukra ismeretlen technológiákat, mert nem szívesen változtatnak a korábbi, kényelmes munkavégzési szokásaikon [178], ebből kifolyólag az alkalmazott rendszereken végrehajtott változtatások növelik a véletlen elkövetett esetek számát. Amikor az alkalmazottnak a megszokottól eltérő módon kell végezni a mindennapi tevékenységüket, akkor kiemelkedő szerepe van a kockázati kommunikációnak a vállalkozást érinthető fenyegetésekről, és azok kivédéséről [176]. A szervezeti érintettek változástól való félelme komoly probléma, amelyet a vezetésnek kielégítően és felelősségteljesen szükséges kezelni.

A **szándékos** belső fenyegetést a szervezet olyan korábbi vagy jelenlegi érintettje személyesíti meg, aki jogosult hozzáféréssel rendelkezik vagy rendelkezett az intézmény információs rendszeréhez, és hozzáférést tudatosan olyan módon használja fel, amely megkárosítja a szervezetet [175, 179]. Az a belső érintett, aki kapcsolatba hozható a vállalkozás ellen elkövetett ipari kémkedéssel, általában jó kapcsolatokkal rendelkezik az intézményen belül, és hozzáfér vagy másoknak hozzáférést biztosít a szükséges információhoz [174]. A szándékos bennfentes fenyegetés – a szervezet rendszereinek alapos ismerete következményeként – információbiztonsági kockázati szintje

exponenciálisan magasabb a külső támadókénál [56, 133, 157]. Az általuk reprezentált magas kockázat abból ered, hogy jellemzően korlátlan hozzáféréssel és teljes ellenőrzési joggal rendelkeznek az információs rendszerek felett, ismerik a szervezet stratégiáját és a kulcsfontosságú üzleti folyamatokat, továbbá tisztában vannak az ezek védelmét szolgáló rendszerek hiányosságaival, így képesek azokat hatástalanítani vagy megkerülni [57, 157]. A belső érintett elkövethet információlopást a foglalkoztatása korai szakaszában amikor egy külső entitás építi be és használja fel az információval való visszaélésre [178], ugyanis a bennfentes elhelyezése gyakran alkalmazott módszere az ipari kémkedésnek [13]. Más esetekben a nyugdíjazáshoz közel álló, vezető beosztású személyek lopnak információt a szervezettől a nyugdíjas éveik anyagi biztonságának megalapozása érdekében [12]. Omar (2015) [135], Brancik és Ghinita (2011) [132] arra az eredményre jutottak, hogy a szándékos támadásokat általában a szervezet belső biztonsági rendszerét jól ismerő, magasan képzett személyek követik el, akik képesek hozzáférni a vállalkozás információs rendszeréhez. Ezzel szemben Elifoglu és szerzőtársai (2018) [134] eredményei alapján a szándékosan elkövetett ipari kémkedési eseteket nem magasan képzett, speciális eszközökkel felszerelt támadók, hanem olyan alkalmazottak követik el, akik rossz szándékkal végzik a mindennapi feladataikat.

A szándékos incidensek mögött álló tényezők széles skálán mozognak. A legtöbb esetben az anyagi kompenzáció motiválja az elkövetőt [12, 13], azonban hozzájárul a szervezettel szembeni lojalitás elvesztése, a szervezet iránt fellángoló negatív attitűd, vagy felmerül egy jó alkalom az információ eltulajdonítására és az elkövető birtokolja az ehhez szükséges szakmai ismereteket. Szervezeti tényezők, mint a negatív érzelmeket keltő vezetési gyakorlat, a nem megfelelő szervezeti kultúra és a jutalmazási rendszer hiánya is előidézheti a munkavállalói hűség csökkenését, és a szervezettel szembeni negatív érzelmek halmozódását, ami hajlandóságot ébreszt az intézmény megkárosítására [143, 180]. Az incidensek mögött állhatnak személyiségi tényezők, amelyek magában foglalják többek között a kielégítetlen célokat, ideológiai szerepvállalást, az elkövetett tettekért való felelősségvállalás hiányát, továbbá a munkavállaló kulturális háttérét és neveltetését [180]. A szervezet tudatos megkárosítása háttérben lehet egészségügyi probléma is, mint depresszió vagy személyiség zavar [173]. Más esetekben az elkövetők külső nyomás, zsarolás vagy megvesztegetés hatására folytatják káros tevékenységüket [13].

2.2.4. Ipari kémkedés elleni információvédelmi rendszer

Elméletben a védelmi iparban minden vállalkozásnak rendelkeznie kell átfogó szervezeti politikával az ipari kémkedés kezelésére, amely kiterjed valamennyi tevékenységre, azonban a gyakorlatban a hatékony útmutatás kidolgozása a legtöbb vállalkozás számára komoly kihívást jelent [142], és a biztonságpolitika megléte önmagában nem garantálja annak hatékonyságát. Ennek egyik oka, hogy a kockázatok valós üzleti folyamatoknak megfelelő értékelése és kezelése, továbbá a biztonsági funkciók ezen üzleti folyamatokba való integrálása nehézséget okoz a szervezeteknek, amely gyakorlati hatékonyságát csak úgy lehet biztosítani, hogy a kockázatok elemzése és a biztonságpolitika meghatározásába az összes belső érintett aktív bevonásával történik [14]. Az alkalmazott biztonságpolitika hatékonyságának hiánya eredhet abból a tényből is, hogy a kritikus üzleti információk védelmét sok szervezet csak információs technológiai szempontból közelíti meg, elsősorban a külső támadások kivédésére fókuszálva, figyelmen kívül hagyva a szervezeti érintettek által megismerésített belső fenyegetést, mikor ez az egyik legnagyobb információbiztonsági probléma [8, 9, 57, 176]. A vállalkozásoknak az alkalmazott biztonságpolitika definiálása során a humán és a technológiai szempontokat is egyaránt figyelembe kell venni [57, 59]. Az IT központú szemlélet kizárólagos hangsúlyozása hibákat és biztonsági réseket okozhat a rendszer tervezése és végrehajtása során, ami rávilágít a felhasználók bevonásának fontosságára a kockázatelemzésbe, mert ez a gyakorlatban hozzájárul a hatékonyabb biztonsági intézkedésekhez [14, 181].

Technikai szempontból az ipari kémkedés megelőzése és észlelése megköveteli a megfelelő fizikai és informatikai eszközök alkalmazását, az információbiztonsági szakemberek felelősségeinek pontos meghatározását, továbbá a munkavállalók képzését és tevékenységük monitorozását [148]. A felsorolt intézkedések szükségességét igazolja, hogy a technológiai fejlődéssel a belső érintettek által elkövetett incidensek is egyre komplexebbé válnak [182], költséghatékony és egyszerű hozzáférést biztosítva a vállalkozás kritikus információjához [183]. A szervezetek törekednek az aktuális fenyegetések elleni IT háttérű információbiztonsági rendszerek bevezetésére, ami mérsékli az ipari kémkedés jelentette fenyegetést, de a belső érintettek által megismerésített kockázat továbbra is jelentős marad [176].

A humán természet komplexitásának köszönhetően az információvédelem során az egyén a legösszetettebb faktor, és egyben a leggyengébb láncszem [150]. A sokrétű bennfentes fenyegetés problémaköréről nem állnak rendelkezésre széleskörű tudományos

eredmények, ami megnehezíti a hatékony védelmet nyújtó rendszer modellezését [157]. A fenyegetés megelőzéséhez szükséges lenne azonosítani azon alkalmazottakat, akik visszaélnék a kritikus információhoz való hozzáférési jogosultságukkal, de a kérdés vizsgálatának adatgyűjtési és mérési eszközei korlátozottak és sok esetben hatástalanok [184]. A probléma abban gyökerezik, hogy a szervezeti döntéshozók nem értik az emberi viselkedésből eredő fenyegetés természetét, így az IT központú védelmi rendszer megerősítésére összpontosítanak, holott a valódi megoldás nem kizárólagosan technológiai jellegű [178, 185], hanem holisztikus megközelítést igényel [152, 186]. Ez a megközelítés magában foglalja a technológiai és vállalatspecifikus tényezőket, a pszichológiai faktorok és az üzleti folyamatokat egyaránt [14, 58, 60].

Az információs technológiai biztonsági megoldások és a szociotechnikai megközelítés együttes alkalmazása támogatja a probléma holisztikus természetéből eredő szakadékok áthidalását, és egy biztonság tudatosabb szervezeti kultúra kialakítását, amely csökkentheti a véletlen elkövetett kritikus információszivárogtatási esetek gyakoriságát. Az elmúlt évtizedek intézményi átalakulásai következményeként, hatékonyságnövelő és információbiztonsági okokból, a hagyományos szervezeti kultúrákba integrálni kellett az IT szempontú megközelítést. Az információbiztonsági kultúra felölel minden olyan szociokulturális intézkedést, amely azzal támogatja a szervezetet, hogy az információbiztonság az érintettek mindennapi munkavégzésének természetes aspektusává váljon [187], amely magában foglalja a csoport információbiztonsággal kapcsolatos hiedelmeinek, elképzeléseinek és értékeinek tudatos alakítását [188]. A szervezeti kultúra újszerű megközelítésének célja az információs technológiai eszközökkel való emberi interakciók irányítása, és az érintettek tudatos viselkedésének ösztönzése az információbiztonság fenntartása érdekében [189]. Ez a megközelítés sokkal célravezetőbb, mint az emberi viselkedést utasító szabályozások, mivel a rendszer csak akkor lehet hatékony, ha az alanyok megértik, ismerik, és elfogadják a szükséges intézkedéseket, így megelőzhetővé válnak az információbiztonságra nézve kockázatot jelentő tevékenységek [156].

A szervezeti érintettek által elkövetett ipari kémkedés kockázata csökkenthető olyan rendszerek alkalmazásával, amelyek felismerik az esetek bekövetkezésének valószínűségét, mielőtt az megtörténne [134, 190]. Az esetek korai észlelését támogatja, amennyiben a vállalkozás az alkalmazott stratégiát, a technológiát, az üzleti folyamatokat, továbbá az emberi erőforrást szinkronizálja, és összehangolva kezeli [15].

Egy olyan többrétegű védelmi rendszer kialakítása, amely magában foglalja a szervezetre szabott biztonságpolitika megvalósítását, a kritikus információk kiemelt védelmét, a hozzáférésére felhatalmazott személyek fokozott ellenőrzését, a belső sebezhetőségek folyamatos felülvizsgálatát, továbbá az alkalmazottak tevékenységének nyomon követését, proaktívan védheti az információs infrastruktúrát a belső támadásoktól [135]. A munkavállalók magatartásának kisebb változásai is mutathatnak olyan mintákat, amelyeket érdemes szem előtt tartani [176], azonban a jelentősebb viselkedésszerű változások (mint verbális kirohanások, a biztonságpolitika szándékos megsértése, valamint az agresszív és konfrontatív magatartás) olyan figyelmeztető jelzések lehetnek, amelyek segíthetik egy szervezet ellen elkövetett incidens előrejelzését és prevencióját [173]. A belső érintettek közösségi média aktivitása is szolgáltat adatokat az ipari kémkedés gyanújának korai észleléséhez [191, 192], továbbá a munkavállaló büntetlen előéletéről való megbizonyosodás is nagyban csökkentheti a kockázatot [193]. Azonban az intenzív megfigyelés zavarhatja a munkavégzést, bizalmatlanságot ébreszt, és hatékonyságcsökkenéshez vezethet [194]. A megelőzésre használt rendszerek eredményének megbízhatóságát megkérdőjelezi, hogy az emberi tényező mélyen beágyazódik az információbiztonsági incidensek prevenciójára tervezett különböző szoftverek és hardverek technikai kialakításába [130].

A blokklánc (*blockchain*) egy olyan adatblokkokból álló, osztott adatbázis, amely új utakat nyit a vállalkozások számára az információbiztonsági kihívások, – mint az ipari kémkedés, a szellemi tulajdon lopása, az adatbiztonság sérülése és a zsarolóvírus támadások – megelőzése és észlelése területén [195]. A blokklánc decentralizált modellje magas szintű rugalmasságot és a munkafolyamatok átláthatóságát biztosítja, ezenfelül a láncalapú adatszerkezet integritást és az adatvédelem legmagasabb szintjét képes nyújtani [196, 197]. Az adatbázis információbiztonsági előnye, hogy alkalmazása során az adatok mindenkor titkosítva vannak, azonban a változatlan, eredeti állapotuk megmarad, továbbá a tranzakciók közvetlen résztvevők között, harmadik fél bevonása nélkül történnek, így biztosítva magasszintű védelmet a jogosulatlan hozzáféréstől [195]. A blokklánc technológia széleskörű alkalmazásának köszönhetően az elmúlt évek során a legtöbb innovatív iparágba beszivárgott [198]. Bár egyedülálló módon biztosítja az adatok védelmét, mivel új technológia, a szakirodalomban az értekezés írásának időpontjában kevés módszertan és keretrendszer állt rendelkezésre a blokklánc alkalmazásának értékelésére, és összehasonlítására a hagyományos rendszermegoldásokkal [195]. Bár a

blokklánc technológiának szembe kell nézni néhány vele született biztonsági kihívással, azonban a mesterséges intelligencia (*artificial intelligence*) alapú algoritmust alkalmazó megközelítések – mint a gépi tanulás (*machine learning*) – képesek a hálózaton belüli anomáliák nagy pontossággal történő észlelésére, a megfelelő biztonsági mechanizmusok beindítására, a veszélyeztetett elemek elkülönítésére és a potenciálisan jogosulatlanul végrehajtott tevékenységek előrejelzésére is [197, 199]. A gépi tanulás a közelmúltban kiemelt figyelmet kapott az információbiztonság területén, mivel képes akár komplex jelenségeket pontosan előre jelezni, és az adatokból olyan tudást előállítani, amely segítségével az emberekhez hasonló döntéseket hozhat [199].

A védelmi iparban az ipari kémkedés elleni védekezés részét képezi a létfontosságú infrastruktúra védelme [7], mert az olyan rendszerekből és eszközökből áll, melyek romlása káros hatással lehet az ipar kulcsfontosságú funkcióinak ellátására [182, 200]. A jelen dolgozat szempontjából a kritikus infrastruktúrák elsősorban az új technológiák fejlesztéséhez és előállításához szükséges területek, telephelyek, továbbá a gyártáshoz szükséges berendezéseket és gépeket foglalja magában. A létfontosságú létesítmények védelme még napjainkban is főként a véletlen balesetek és az ember által okozott fizikai támadások megelőzésére irányul, azonban mivel az értekezés szempontjából az informatikai rendszerek releváns szerepet játszanak az új technológiák előállításához szükséges infrastruktúrák működésében, a növekvő számú kiberfenyegetések kockázatát is figyelembe kell venni [200]. Az elmúlt években a kritikus információs létesítmények elleni támadások egyre gyakoribbá, kifinomultabbá, komplexebbé és célzottabbá váltak. A támadók fizikai behatolás nélkül is képesek kárt okozni vagy megzavarni a fizikai infrastruktúrát azáltal, hogy behatolnak a gyártási folyamatokat vezérlő digitális rendszerekbe, így távolról károsíthatják a speciális berendezéseket és megzavarhatják a létfontosságú folyamatokat [182].

Az ipar 4.0 olyan gyártórendszerekre utal, amelyekben a gépek intelligens és autonóm hálózatokat használnak, továbbá a digitális és fizikai környezet közötti kommunikáció lehetővé teszi az emberi beavatkozás nélküli döntéshozatalt. A mesterséges intelligenciával támogatva ezek a kiber-fizikai rendszerek előreláthatólag sokkal kifinomultabb reakciókat lesznek képesek létrehozni [201, 202]. Azonban a fizikai gyártási rendszerek kibertechnológiával való integrációja a megfelelő biztonsági ellenőrzések nélkül a kiber-fizikai támadások növekedéséhez vezetett, ami új és jelentős globális információbiztonsági fenyegetést jelent az innovatív vállalkozásokra [195, 202, 203]. A

fenyegetések fejlődése ellen a vállalkozásoknak szükséges lesz alkalmazni az újszerű védekezési lehetőségeket, – mint a mesterséges intelligencia és a blokklánc alapú platformok – melyek ipari felhasználás során is növelhetik az általános kiberbiztonsági képességeket [197]. A mesterséges intelligencia algoritmusok lehetővé teszik a blokklánc hálózatok számára, hogy nagy és összetett műveleteket hajtsanak végre, ami rendkívül hasznosnak bizonyult a gyártási feladatok automatizálásában [199].

Bár az értekezés írásának időpontjában alkalmazott technológiák is összetett információbiztonsági kihívás elé állítják a vállalkozások döntéshozóit, a már létező, és várhatóan a közeljövőben széles körben elterjedő eszközök újabb megpróbáltatásokat hoznak. A kvantumszámítógépek még fejlesztés alatt állnak, azonban speciális területeken már most jelentős teljesítménnyeljavulást mutatnak speciális feladatok elvégzésében, mint a korábban biztonságosnak gondolt titkosítási módszerek visszafejtése, ami potenciális veszélyt jelent az információbiztonság és az ipar 4.0 szempontjából [204]. Az intelligens rendszerek integrálódása a vállalkozások hétköznapi működésébe, áthidalva a digitális és fizikai környezet közötti szakadékot, szintén növeli az ipari kémkedés kockázatát [202]. Az egyre változatosabb hackertámadások, a szervezeti hatékonyság növelésére irányuló új szolgáltatások, továbbá az emberekhez hasonló azonosítást igénylő autonóm entitások és robotok megjelenése által jelentett biztonsági fenyegetések mind olyan faktorok, melyek minden eddiginél fontosabbá teszik döntéshozók információvédelmi erőfeszítéseit [177]. Az újszerű fenyegetések elleni védekezés minden esetben rugalmasságot, gyors reakciót és célzott biztonsági frissítéseket igényel [205].

Az ipari kémkedés egy olyan külső változó tényező, amely nagy mértékben befolyásolja a szervezet működését és stabilitását, így a kontingencia elméleti megközelítésnek fontos szerepe van a minden szervezeti folyamatot magában foglaló, többretegű információvédelmi rendszer kidolgozásában. A kontingencia elmélet alapelvein nyugvó információbiztonsági stratégia segíthet az innovatív vállalkozásoknak a külső fenyegetésre való gyors és hatékony reagálásban.

2.3. Kontingencia elmélet

A kontingencia elmélet alapján a szervezetek teljesítménye nagy mértékben függ a külső körülmények és az előre nem jelezhető események alakulásától, ezáltal nincs egy meghatározott stratégia, amit minden vállalkozás követ, hanem folyamatosan alkalmazkodniuk szükséges a külső dinamikus változó környezethez. Az elmélet szerint azon szervezeteknek van a legnagyobb esélyük a sikeres működésre, amelyek rugalmasan és gyorsan képesek reagálni a külső lehetőségekre és fenyegetésekre. Jelen kutatás egy újszerű megközelítést alkalmaz, és az ipari kémkedés problémakörét a környezeti kontingencia változók közé sorolja, amely szerint nincs egy általánosan elfogadott előrejelzési, megelőzési vagy védekezési rendszer, amely minden körülmények között hatékonyan védi a vállalkozás kritikus információit, hanem a rendszernek folyamatosan alkalmazkodnia kell a környezeti változásokhoz.

A klasszikus elméletek (Taylor, Fayol, Weber) a szervezetet egy zárt rendszernek tekintették, melynek határai összetartották a vállalkozás elemeit és elválasztották a környezeti tényezőktől [206]. Az 1960-as évektől, a kontingencia elmélet terjedésével a környezet egyre nagyobb figyelmet kapott, mivel elfogadottá vált, hogy a szervezet teljesítménye attól függ, hogy mennyire képes megfelelni a külső változóknak, és rugalmasan reagálni az onnan érkező fenyegetésekre, lehetőségekre és kihívásokra [207]. A kutatók ráébredtek arra, hogy a vállalkozás és a környezet között állandó a kölcsönhatás, a szervezethatárok változékonnyá és instabillá váltak, illetve a határoknak átjárhatónak kell lenni valamennyi irányból a hatékony működés érdekében [208]. Ez a modern menedzsment elmélet nem próbál egy univerzális, minden helyzetben és körülmények között jól működő módszert definiálni, inkább arra törekszik, hogy támogassa a döntéshozókat a különböző szituációk sajátosságainak beazonosításával, majd rámutat az ezekben a helyzetekben legmegfelelőbb reakciókra és válaszokra [206]. Az elméletet feldolgozó szakirodalom elemzése során azonban nem szabad figyelmen kívül hagyni, hogy az 1960-as évek óta a kontingencia elmélet hatóköre jelentősen kiszélesedett, a szervezetet körülvevő környezet átalakult és korábban ismeretlen fenyegetések jelentek meg, a gazdasági tényezők globalizálódtak, a vállalatok jellemzően laposabb szervezeti struktúrával rendelkeznek, továbbá a teljes ellátási lánc átfogása helyett csak egy meghatározott tevékenységre fókuszálnak [209].

Az elmélet a szervezeti viselkedést abból a szempontból vizsgálja, hogy a kontingencia tényezők hogyan befolyásolják a vállalkozás kialakítását és működését [210]. Az

alapvető állítása, hogy a környezet, amelyben az intézmény működik, határozza meg a legjobb szervezésmodot [211, 212], továbbá két alapfelvetése, hogy nincs egyetlen legjobb módja a szervezésnek, és a különböző módszerek nem egyformán hatékonyak [210, 213]. Az elmélet alapján nincs egy általánosan elfogadott, optimális módja a szervezeti tényezők kialakításának, továbbá a vállalkozás sikeres működése attól függ, hogy mennyire képes többek között az alkalmazott stratégiát, az intézmény struktúráját és a belső érintettek magatartását a külső környezeti kontingencia változókhöz illeszteni [206, 210, 214, 215]. A környezeti kontingencia változók és a szervezettervezési paraméterek közötti leghatékonyabb illeszkedés megtalálása a legnagyobb hatékonyságot eredményezheti [211]. A vállalkozás teljesítménye, bár különböző mértékben, de egyszerre több tényező összhangjának függvénye [212, 214]. A környezetébe hatékonyan illeszkedni képes szervezet magasabb termelékenységet érhet el, alkalmas lehet többletforrást generálni, ami fejlődéshez, terjeszkedéshez és az innovációs hajlam növekedéséhez vezethet [216]. Amikor a teljesítmény nem éri el az előre definiált értékeket, az a legtöbb esetben visszavezethető arra, hogy a vállalkozás nem képes gyorsan és rugalmasan reagálni a környezeti kontingenciák változásaira [214]. Az elmélet alapján egy módszer, amely az egyik intézmény számára biztosította a hatékony működés alapját, nem feltétlenül adaptálható egy másikra, mivel arra más tényezők hathatnak akár ugyanabban az időben [206].

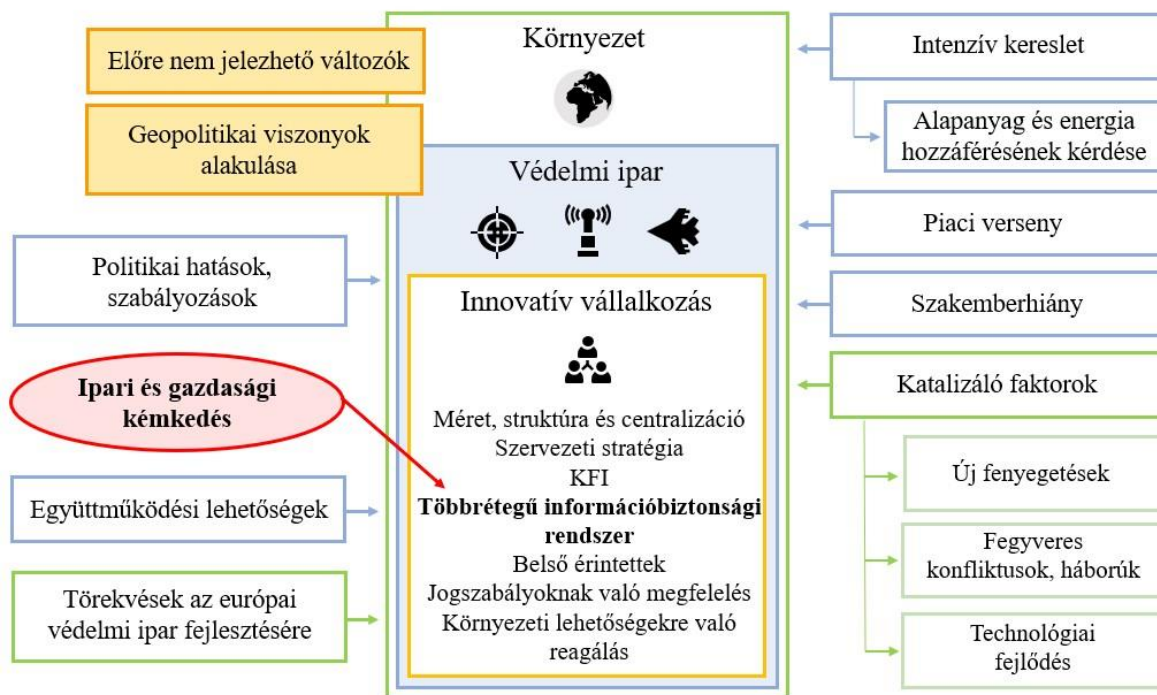
Bár a kontingencia elmélet kutatói egyetértenek abban, hogy a klasszikus iskolák felfogása téves abból a szempontból, hogy létezne egyetlen legjobb módja egy szervezet sikeres működtetésének [206, 210, 212, 213, 214, 215], azonban, hogy mely külső tényezőknek vagy belső adottságoknak van releváns szerepe a vállalkozás kialakításában, továbbá milyen szempontból szükséges ezeket kategorizálni, már számos eltérő vélemény létezik [212, 215].

(1) Hayes (1977) [217] három fő kategóriát fogalmazott meg, melyek a szervezeti belső tényezők, a kölcsönösen függőségi tényezők, és a külső tényezők. (2) Mintzberg (1979) [218] mélyebben elemezte a szervezetre ható kontingenciákat, és tizenegy kategóriát hozott létre, melyek a szervezet mérete, a szervezet által alkalmazott technológia, a külső környezet, a munka változékonysága, az alkalmazottak képzettségi szintje, a szervezet formalizáltsága, a döntéshozás központosításának foka, a szervezet által kínált termékek és szolgáltatások szabványosítása és komplexitása, az alkalmazott stratégia és a szervezeti kultúra. (3) Mintzberg (1979) [218] tizenegy kategóriáját Child (1981) [219]

kiegészítette a nemzeti kultúrával. (4) Donaldson (2001) [215] szintén három fő kategóriát hozott létre, melyek a szervezet mérete, stratégiája és annak környezete. (5) Betts (2003) [211] az alkalmazott technológiát, a szervezet környezetét, méretét és életkorát kategorizálta legfontosabb kontingencia tényezőknek. Az évek során számos új – a saját kutatási területükön releváns – kategóriát hoztak létre a kutatók, mint például (6) Wong és szerzőtársai (2012) [220] az ellátási láncot, a piaci versenyt, a versenytársakat, és az információáramlást; (7) Alves és szerzőtársai (2017) [221] a klímaváltozást, a károsanyag kibocsátást és fenntarthatóságot; (8) továbbá Engelseth és Kritchanchai (2018) [222] a kórházi infrastruktúrát, az egészségügyi szolgáltatások színvonalát, és a gyógyászati célú turizmust nevezték meg.

Az ismertetett kontingencia változókból levonható a következtetés, hogy az elmélet alkalmazása során a kutatóknak megvan az a szabadsága, hogy az általuk vizsgált területre leginkább ható környezeti változókat definiálják. Jelen kutatás egy újszerű megközelítést alkalmaz, és az ipari kémkedést a védelmi iparban működő szervezetre ható kontingencia tényezők közé sorolja.

Mészáros (2023) [82, 83] korábbi kutatása során vizsgálta az európai védelmi iparban működő kis- és középvállalkozásokra ható kontingencia tényezőket, melyeket az 5. ábra foglal össze. A vállalkozások működését a geopolitikai és gazdasági hatásokon felül számos előre nem jelezhető változó befolyásolja, így a versenyképes teljesítmény nyújtásához folyamatosan figyelni és értelmezni szükséges a környezeti kontingencia tényezőket. Azonban a jelen értekezés szempontjából legfontosabb kontingencia változó az ipari kémkedés, mely fokozottan fenyegeti az innovatív védelmi vállalkozásokat. A megfelelő információvédelmi rendszer hiánya mellett a problémát növeli a védelmi innovációk piacán jellemző intenzív verseny, továbbá a szektor bizonyos területein tapasztalható alacsony munkaerőkínálat.



5. ábra: A védelmi iparban működő szervezetre ható kontingencia tényezők

Forrás: saját szerkesztés Mészáros 2023 [82] és Mészáros 2023 [83] alapján

A következő fejezet a gyűjtött adatok elemzése alapján bemutatja a védelmi iparban tapasztalható ipari kémkedéssel összefüggésbe hozható esetek növekedése mögött azonosított külső és belső kontingencia tényezőket, továbbá ismerteti, hogy a vállalkozások döntéshozóinak milyen szempontokat szükséges figyelembe venni a szervezet információvédelmi rendszerének kialakítása során. Ezenfelül az eredmények bepillantást nyújtanak, hogy várhatóan a közeljövőben milyen ipari kémkedési módszerek jelentenek majd fenyegetést az innovatív védelmi vállalkozásokra, és hogyan lehet ezekre felkészülni.

3. EREDMÉNYEK

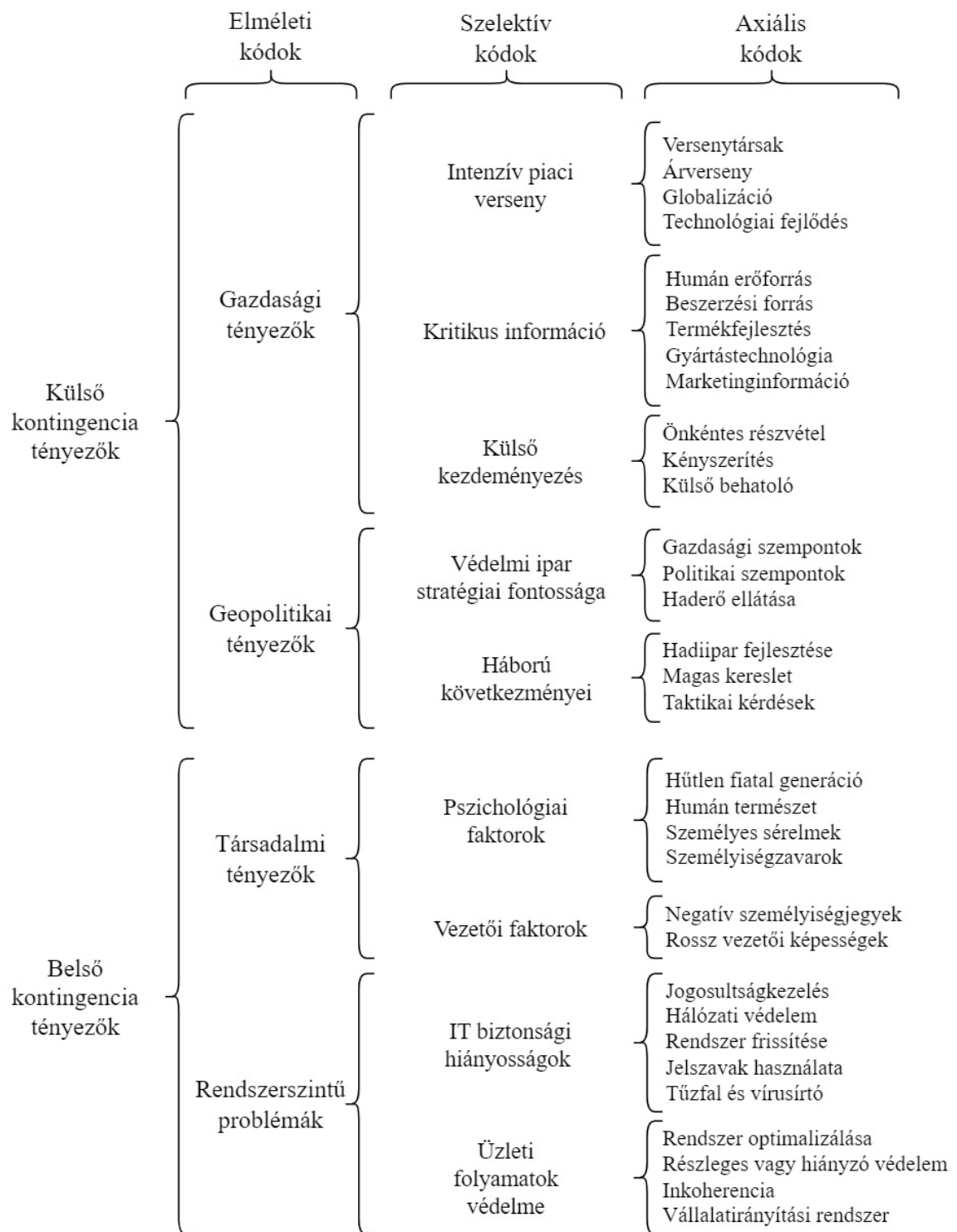
Jelen kutatás során az adatgyűjtés szakértői mélyinterjúk keretében valósult meg. Az interjúalanyok a védelmi kis- és középvállalkozásokat fenyegető ipari kémkedésről alkotott véleménye és tapasztalatai feltárása volt a cél. Mivel az adatgyűjtés megkezdése után néhány héttel kitört az orosz-ukrán fegyveres konfliktus, ennek okán az interjúk résztvevői gyakran asszociáltak a háborúra a kérdések megválaszolása során és osztották meg véleményüket az ipari kémkedésre gyakorolt következményeiről. Az adatok elemzése grounded theory módszertannal történt. A módszertan egyik megalkotója, Glaser (1992) [53] szerint az elemzés közben nem szabad az adatokat az előre definiált kutatási kérdések alapján kialakított kategóriákba erőltetni, azokat folyamatos összehasonlítás során kell osztályokba sorolni, így az azonosított elmélet részletes ismertetése néhol eltér a kutatási kérdések sorrendjétől, ugyanakkor a 3.4 Diszkusszió fejezetben azok sorrendjében kerülnek bemutatásra.

Az értekezés során az ipari kémkedés kifejezés magában foglalja a versenytársak és az állami szereplők által szervezett kémkedést is, melynek tárgya egy védelmi innováció fejlesztéséhez, gyártásához és a piacon való eredményes szerepléséhez szükséges kritikus információ. Ez a kritikus információ többek között lehet egy műszaki rajz (*blueprint*) a termékről vagy egy részéről a termékfejlesztés bármely szakaszában, gyártástechnológia vagy annak egy része, alapanyag ötvözet, alapanyag beszerzési forrás, beszállító, célpiac vagy egyéb marketinginformáció.

A kutatás célja egy hatékony információvédelmi rendszer definiálása, ami minden olyan eszközt és tevékenységet felölel, amellyel a vállalkozás képes az ipari kémkedés megelőzésére és észlelésére. Az eredmények ismertetése során alkalmazott idézetek azáltal segítik a megértést, hogy bevonják az alanyok hangját az elemzésbe, ezért Sántha és Tódor (2022) [223] javasolja, hogy a kutatók használják ezt az eszközt magyarázatok nyújtására és az alanyok perspektíváinak illusztrálására.

3.1. Az ipari kémkedési esetek növekedése mögött azonosított tényezők

Konopatsch (2020) [125], Shelupanov és szerzőtársai (2021) [126] kutatási eredményei alapján az elmúlt évek során a védelmi iparban az ipari kémkedéssel összefüggésbe hozható incidensek gyakorisága jelentős növekedést mutatott, továbbá Pellegrino (2015) [129], Kim és Kim (2021) [94] megállapításai szerint a védelmi ágazat az ipari kémkedés által egyik legfenyegetettebb szektor. Bár a kvalitatív kutatás nem alkalmas az esetszámok növekedésének vizsgálatára, azonban a jelenség mögött megbújó tényezők feltárására megfelelő módszer. Ezen megállapításokból kiindulva jelen kutatás vizsgálja, hogy milyen kontingencia változók állnak az ipari kémkedés gyakoriságának növekedése mögött. Az ipari kémkedéssel összefüggésbe hozható esetszámok fokozódásának hátterében azonosított tényezők (**K1**), és a belső érintettek által megtestesített fenyegetéshez fűződő faktorok (**K2**) nem kerülnek külön fejezetben bemutatásra, mivel az azonosított eredmények nem határolhatók el teljesen egymástól. A 6. ábra szemlélteti a témában azonosított eredmények kódját.



6. ábra: Az ipari kémkedési esetszámok növekedése mögött azonosított tényezők, a grounded theory elemzés kódfüaja

Forrás: saját szerkesztés (n=42)

3.1.1. Külső kontingencia tényezők

A jogosulatlan információeltulajdonítási esetek növekedő tendenciája mögött azonosított eredmények a vállalkozások szempontjából külső és belső kontingencia tényezőként kerültek meghatározásra. Az azonosított külső elméleti kódok a gazdasági és geopolitikai tényezők. A **gazdasági tényezők** az intenzív piaci verseny, a kritikus információ, és a külső kezdeményezés szelektív kódokból fejlődött.

A mélyinterjúk során megkérdezett szakemberek szerint az egyik magyarázat az ipari kémkedéshez fűződő esetszámok növekedésére a globális védelmi piacon tapasztalható **intenzív verseny**, mely a versenytársak, árverseny, globalizáció és technológiai fejlődés axiális kódokból alakult ki.

A védelmi iparban jellemző intenzív versenykörnyezetben, ahol napi gyakorisággal jelennek meg technológiai innovációk, a vállalkozások fokozottan ki vannak téve az ipari kémkedés fenyegetésének. Gazdasági szempontból az alanyok szerint a versenytársak számos tényezőtől motiválva – mint a *„technológiai előny megszerzése”* vagy *„piaci versenyelőny kialakítása”* – szervezhetnek ipari kémkedést, hogy megtudják a piac többi szereplőjének *„üzleti titkait, terveit és tevékenységeit”, „mit fejlesztenek és ki finanszírozza”,* továbbá *„éppen kivel dolgoznak együtt”*.

A kvalitatív adatok elemzése alapján az árverseny szintén olyan gazdasági kontingencia tényező, amely azonosítható az esetszámok emelkedése hátterében. Az ipari kémkedés eszköztárának alkalmazásával eltulajdonított információ megszerzése jelentősen kevesebb erőforrást igényel, mint annak előállítása. A módszer segítségével *„alacsonyabb költségen képes technológiai innovációt fejleszteni”,* továbbá *„költséges piackutatás folytatása nélkül rendelkezésre állnak a marketinginformációk”,* következményként a kémkedést szervező vállalkozás *„jelentősen alacsonyabb áron értékesítheti a terméket, mint a technológiát fejlesztő versenytárs és sokkal többen fogják vásárolni”* – véli az egyik interjúalany.

A védelmi ipar globalizációja folytán a vállalkozások nemcsak a nemzethatárokon belül folytatnak tevékenységet, hanem más országokban és kultúrákban is, ahol eltérő jogi és etikai elveket követnek, ezáltal sokkal nehezebb feladat az együttműködések vagy egyéb közösen folytatott üzleti tranzakciók során a kritikus információ védelme. Az alanyok tapasztalatai alapján a *„növekvő kiszervezési gyakorlat”,* az *„új piacok megszerzése”,* és

a „több országon áthaladó ellátási láncok” mind olyan tényezők, melyek növelik a gazdasági célú kémkedés kockázatát.

A technológiai fejlődés ipari kémkedéshez való viszonyát az interjúalanyok két eltérő nézőpontból közelítették meg. Az axiális kód elemezhető az ágazatban jellemző magasfokú innovációs hajlam szempontjából. Az egyik alany beszámolója szerint a *„védelmi iparban nap mint nap jelennek meg új technológiák, melyekkel a versenytársak gyakran csak ipari kémkedéssel képesek lépést tartani”*. Az alkategória továbbá vizsgálható a kommunikációs technológiák evolúciója által megtestesített fenyegetés nézőpontjából. Az interjúalanyok kiemelték, hogy a vállalkozások *„nagyon sok információt tárolnak digitális formában”*, továbbá *„rendszeresen jelennek meg új és egyre komplexebb, a civil piacon elérhető technológiák az ipari kémkedés elkövetésére”*, melyek alkalmazása könnyen hozzáférhetővé tették az információszerzés ezen illegális módszerét.

Az interjúk résztvevői egyetértettek abban, hogy a **kritikus információ** növekvő értéke közvetlenül hozzájárul az esetszámok növekedéséhez. A védelmi iparban innovációs tevékenységet folytató kis- és középvállalkozások vizsgálata során az azonosított szelektív kódok a humán erőforrás, a beszerzési források, a termékfejlesztési információk, a gyártástechnológia és a marketinginformációk axiális kódokból fejlődött.

A humán erőforrás a vállalkozás által alkalmazott, speciális szaktudást igénylő pozíciót betöltő munkavállalók képességeire utal. Az interjúalanyok elmondása szerint a védelmi iparban foglalkoztatott mérnökök sok esetben az alkalmazásuk során sajátítják el a technológiák fejlesztéséhez szükséges tudást, mivel Európa-szerte jellemzően kevés az erre irányuló képzés, ezáltal ezt a speciális területet alacsony munkaerőkínálat jellemzi. Az interjúalanyok hangsúlyozták, hogy *„a vállalkozások számára nagyon értékesek az általuk képzett fejlesztőmérnökök”*. Azonban a mérnökök tudása mellett – mivel ők nem rendelkeznek bevetési tapasztalattal – *„a fejlesztési folyamatban gyakran vesznek részt a védelmi erőknél szerzett gyakorlattal rendelkező személyek, ami szintén lehet probléma a kémkedés szempontjából”* – osztotta meg az egyik résztvevő.

Az alanyok tapasztalatai szerint a pandémia, majd az orosz-ukrán háború által okozott ellátási problémák hatására az alapanyag és alkatrész beszerzéshez kapcsolódó információk iránt magas a kereslet a védelmi piac szereplői között. Szintén kiemelték, hogy a termékfejlesztéshez kapcsolódó tudás és a gyártástechnológia jelenősége

gazdasági és geopolitikai szempontból is meghatározó, így ezt is nagymértékben fenyegeti az információlopás kockázata. Ez olyan tudás ipari kémkedés útján történő elsajátítását jelenti, *„amelyekkel a vállalkozás termelékenyebben és költséghatékonyabban képes szervezni a gyártást”, vagy „támogatja a vállalkozást az új technológia fejlesztési képességeinek növelésében”*. Amennyiben a versenytárs *„csak egy lépést, vagy egy részegység előállításának módszerét képes ellesni, azzal is jelentősen gyorsabbá és költséghatékonyra képes tenni a saját gyártási folyamatát”* – számolt be az egyik résztvevő. Egy másik alany véleménye alapján *„az ágazatban egy új technológia fejlesztése hosszú és költséges folyamat, melynek során az innováció újdonságtartalmától függően számos magas költségű tévút merülhet fel, melyek lehetősége csökkenthető a versenytársaktól lopott tudás felhasználásával”*. Az interjúk alapján elmondható, hogy az ipar stratégiai jellegéből adódóan a fő vásárlók az állami szereplők, amely okán számos vállalkozásnak nehézséget okoz az új termék célpiacnak való bemutatása. A versenytársak marketinginformációi iránt egyaránt magas a kereslet a védelmi iparban. A kritikus információ szelektív kód szorosan kapcsolódik az intenzív piaci versenyhez és a geopolitikai tényezőkhez.

Az ipari kémkedéshez fűződő esetszámok növekedésének okai közé került kategorizálásra a **külső kezdeményezés**. Bár az értekezés primer kutatás során nem vizsgálta az elkövetési módszereket, ez a kategória utal a jogtalan információeltulajdonítás végrehajtásának módjára is. Az interjúk alapján a belső érintett által elkövetett kémkedést jelentősen motiválja a külső entitás által kínált pénzbeli kompenzáció. Az alanyok beszámoltak, hogy a belső érintett átadhatja az információt önkéntesen, vagy történhet az információ megszerzése kényszerítés – *vesztegetés* vagy *zsarolás* – útján. Szintén külső entitás által kezdeményezett ipari kémkedés egy külső elkövető szervezetbe való beépülése, fizikai behatolása, vagy az interneten keresztül történő támadás. A résztvevők elmondták, hogy ez megvalósulhat *„egy új munkavállaló beépülése során”,* követhetik el *„információbiztonságra szakosodott vállalkozások”,* *„állami engedélyezett hatóságok”* vagy *„auditáló szervezetek munkatársai”*. A külső kezdeményezés jelensége csak közvetve járul hozzá az ipari kémkedési esetszámok növekedéséhez, a valódi ok abban keresendő, hogy a piac szereplői egyre nagyobb összeget hajlandók fizetni az eltulajdonított információért. Ez az eredmény szintén átfedést mutat az intenzív piaci versennyel és a geopolitikai tényezőkkel.

A **geopolitikai tényezők** elméleti kód a védelmi ipar stratégiai jelentősége és a háború következményei szelektív kódokból fejlődött. Az interjúalanyok szerint az esetszámok növekedésének szempontjából a probléma gyökere, hogy a **védelmi ipar stratégiai fontossággal** rendelkezik minden európai államban, következményképp az ágazatban létrehozott információt kiemelten fenyegeti az állami szereplők és a versenytársak által szervezett ipari kémkedés egyaránt. A gazdasági előnyök közül kiemelték, hogy „*az ágazat magas bevételtermelő képességgel rendelkezik*”, „*az iparban fejlesztett innovációk számos egyéb területen alkalmazhatók*”, továbbá „*mérséklő hatással van a gazdasági recesszióra*”. Politikai szempontból a „*nemzetközi kapcsolatok kialakításának eszköze*”, „*erősebb stratégiai pozíciót biztosít*” és „*lehetővé teszi az állampolgárok biztonságának fenntartását*”. Az ipar stratégiai szerepei közé tartozik a helyi haderő ellátása innovatív felszerelésekkel. Az egyik interjúalany úgy nyilatkozott, hogy „*ha a helyi védelmi ipar képes a fegyveres erőket ellátni a legújabb technológiákkal, azzal támogatja a haderő hadrafoghatóságát és ütőképességét, így az állampolgárok mindenkori biztonságát*”. Ezenfelül, a védelmi erők hazai termékekkel való ellátása a helyi vállalkozások versenyképességét is növeli.

A 2022. februárban kirobbant orosz-ukrán **háború** alapjaiban forgatta fel az európai védelmi ipart, melynek hatására növekedett az igény a védelmi kis- és középvállalkozások által előállított innovatív információ iránt. A szakértői mélyinterjúk során megkérdezett alanyok elmondták, hogy a fegyveres konfliktus felhívta az európai döntéshozók figyelmét az ipar elhanyagoltságára, előtérbe helyezve annak fejlesztését. Ugyanakkor az ipar szereplőire helyezett nyomás, és a területre áramló nagy mennyiségű tőke ellenére a lokális védelmi ipar fejlesztése nem kivitelezhető rövid távú megoldásokkal. Ezt a lemaradást az államok vagy vállalkozások sok esetben ipari kémkedés útján szerzett tudással próbálják pótolni.

Ahogy a kritikus információ elmélet kódnál már említésre került a jelenség, a geopolitikai események hatására a kereslet nagymértékű növekedésnek indult a védelmi felszerelések és az előállításukhoz szükséges alapanyagok iránt egyaránt, amely mindkét szempontból jelentős hiányt és ellátási problémákat eredményezett. „*A megnövekedett kereslet kiszolgálása nehézséget okoz a beszállítóknak, melyet sok esetben csak ipari kémkedéssel gyorsan megszerzett információval képesek kielégíteni*” – osztotta meg az egyik interjúalany. Ez a jelenség fenyegeti a vállalkozások által végzett innovációs

tevékenységet is, mivel *„egy hirtelen jelentkező igényre sokszor csak eltulajdonított információval képesek rövid időn belül technológiát fejleszteni”*.

Az alanyok beszámoltak, hogy a háború során a taktikai előny megszerzése fontos tényező, amelynek eszköze lehet az egymással szemben álló felek által alkalmazott új technológiák ütőképessége. Mivel az orosz-ukrán háború az első nem aszimmetrikus fegyveres konfliktus a második világháború óta, az alkalmazott technológiák kritikus szerepet játszanak az összecsapások kimenetében, mely fokozza a taktikai előny megszerzésére irányuló ipari kémkedés jelentette fenyegetést.

3.1.2. Belső kontingencia tényezők

A kutatás során azonosított szervezeti belső tényezők, melyek hozzájárulnak az ipari kémkedéshez fűződő esetszámok növekedéséhez a társadalmi tényezők és a rendszerszintű problémák elméleti kódok, melyek elsősorban a belső érintettek által elkövetett ipari kémkedéssel állnak összefüggésben, azonban vonatkoztathatók a külső kezdeményező által elkövetett esetekhez is. A **társadalmi tényezők** elméleti kód a pszichológiai faktorok és a vezetői faktorok szelektív kódokból fejlődött. A **pszichológiai faktorok** kategória a hűtlen fiatal generáció, a humán természet, a személyes sérelmek és a személyiségzavarok axiális kódokat foglalja magában.

Az interjúalanyok egybehangzóan beszámoltak arról a jelenségről, – függetlenül a saját életkoruktól – hogy a fiatal munkavállalók vállalkozással szembeni hűségének csökkenése jelentős információbiztonsági kihívást jelent a döntéshozóknak. Tapasztalataik szerint a fiatalabb generációk tagjai *„gyakran váltanak munkahelyet”*, többek között azért, hogy *„rövid időn belül számos vállalkozásnál tegyenek szert kiemelkedő szakmai tapasztalatra”*. Az alanyok elmondták, hogy sok esetben hiába iratnak alá titoktartási vagy versenytilalmi szerződést, mivel annak megszegése nehezen szankcionálható, főleg, ha az érintett más országban vállal munkát. Az interjúk során az alanyok nem nevezték meg pontosan, hogy melyik korosztályra utalnak, *„új generációnak”*, *„fiatal generációnak”* vagy *„friss diplomásoknak”* nevezték őket, így feltételezhető, hogy az Y és Z generációra utaltak. Ezzel szemben az *„idősebb generációk”* (feltételezhetően az X generáció) olyan környezetben nevelkedtek, amelyben az *„hűség értéket képviselt”*. Ez az eredmény fokozza a belső érintettek által véletlen és szándékosan elkövetett esetek kockázatát is, továbbá összefüggésben áll a

globalizáció axiális kóddal, mert globális szinten lehetőséget biztosít a munkaerő szabad áramlásának.

A humán természetből eredő információbiztonsági kockázat a belső érintettek munkavégzés közben elkövetett hibáira utal, melynek okaként a megkérdezettek olyan tényezőket osztottak meg, mint a „*fáradtság*”, „*nyomás*”, „*stressz*”, „*figyelmetlenség*”, „*túlhajszoltság*”, „*kevés szakképzett alkalmazott*”, továbbá „*az alkalmazottak is csak emberek, és néha hibáznak*”. A válaszadók többféleképpen reagáltak a belső érintettek által elkövetett hibákból eredő információszivárogtatás problémájára, ugyanis felmerült bennük a kérdés, hogy valóban véletlen esetről lenne szó, vagy az alkalmazott szándékosan követte el, és próbálja leplezni. Ez az eredmény összefüggésben áll a vezetői faktorral, az IT biztonsági hiányosságok szelektív kóddal, továbbá hatást gyakorol rá az intenzív piaci versenyből eredő nyomás.

A gyűjtött adatok elemzése során kialakult személyes sérelmek axiális kód a belső érintettek vállalkozásnál töltött ideje alatt, a szervezettel, vezetőkkel vagy munkatársakkal szemben kialakuló negatív emóciókra és attitűdre utal, amely növelheti a belső fenyegetés kockázatát. Az alanyok olyan gondolatokat osztottak meg, mint a „*negatív tapasztalat a vállalkozásnál*”, „*rossz kapcsolat a munkatársakkal*”, vagy „*nem megfelelő szervezeti kultúra*”, melyek hatására „*harag*” és „*bosszúvágy*” fejlődik a belső érintettben. A személyiségzavarok axiális kód az interjúalanyok azon tapasztalataiból alakult ki, mely szerint egyre több alkalmazottat jellemeznek olyan vonások, mint a „*pszichopata*”, „*nárcisztikus*”, „*depressziós*”, vagy „*nem megfelelő neveltetés következményei*”. A személyes sérelmek vagy személyiségzavarok jellemzőivel rendelkező szervezeti érintettek magas kockázatot jelentenek a döntéshozók számára, mivel jelentősen növeli annak hajlandóságát a vállalkozás megkárosítására, azonban jelen doktori értekezés multidiszciplináris megközelítése ellenére úgy döntöttem, hogy a pszichológia tudományterülete túl tágas, hogy beférjen jelen dolgozat kereti közé, így ezt a problémát nem magyarázom részletesebben, azonban megértése rendkívül fontos a hatékony megelőzési és észlelési rendszer modellezéshez.

A **vezetői faktorok** szelektív kód a negatív személyiségjegyek és a rossz vezetői képességek axiális kódokból alakult ki és olyan, a vállalkozások vezetői vagy menedzseri által végzett „*tevékenységekre*”, „*kommunikációra*”, „*az alkalmazottakkal való kapcsolatra*” és ezek „*stílusára*” vonatkozik, amelyek hatására negatív emóciók

alakulhatnak ki a munkavállalóban. Ez a szelektív kód közvetlen kapcsolatban áll a személyes sérelmek és a személyiségzavarok axiális kódokkal, mert amennyiben a vezető rendelkezik ezen karakterisztikák valamelyikével, úgy cselekedetei és viselkedése szintén kockázatot jelent a vállalkozásnak. A vezetői faktor összefüggésben áll a geopolitikai tényezőkkel, melyek a védelmi ipar természeténél fogva jelentősen befolyásolják a vezetők cselekedeteit.

A **rendszerszintű problémák** a belső kontingencia tényezők közé került osztályozásra, mely az alkalmazott információvédelmi eszközök és az üzleti folyamatok kapcsolatát foglalja magában. Az elméleti kód az IT biztonsági hiányosságok és az üzleti folyamatok védelme szelektív kódokból épül fel.

A válaszadók különböző nézőpontokból közelítették meg az **IT biztonsági hiányosságokat**, azonban abban egyetértettek, hogy növelik az ipari kémkedés, azon belül a belső érintettek által elkövetett szándékos és véletlen incidensek kockázatát egyaránt. Az interjúk során az ipari kémkedéshez kötődő esetek növekedésének okaként nevezték meg a következőket:

- nem megfelelő jogosultságkezelést, mely a kritikus információkhoz való hozzáférés szabályozására szolgál;
- a belső hálózat internethez való csatlakozásának kérdését;
- az alkalmazott információbiztonsági rendszer frissítésének problémáit (ha a frissítés során a rendszer felhasználási módja módosul, rákényszerítve a belső érintetteket, hogy változtassák meg az addig megszokott munkavégzési szokásaikat, az platformot biztosíthat a véletlen elkövetett információszivárogtatási eseteknek, ezzel szemben a frissítés elhanyagolása sebezhetővé teszi a rendszert);
- gyenge jelszavak használatát;
- és a nem megfelelően konfigurált tűzfalak, vírusírtók, és egyéb szoftverek alkalmazásának kérdését.

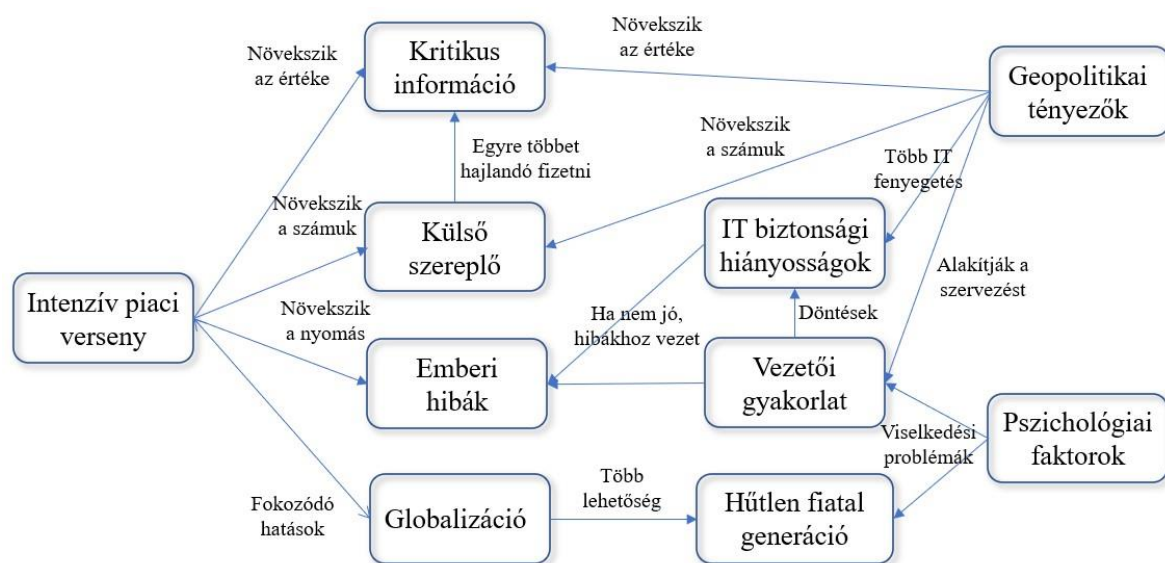
Mivel a vizsgált védelmi vállalkozások tevékenységei közé tartozik a technológiai újdonságok fejlesztése, gyártása és számos esetben az értékesítése is, mely **üzleti folyamatok** jellemzően egy összehangolt, belső digitális hálózattal támogatva mennek végbe, fontos szempont az információbiztonsági rendszer különböző műveletekhez való

optimalizálása. Az alanyok a rendszer optimalizálásának hiányosságai között említették, hogy *„nem veszi figyelembe a vállalkozás sajátosságait”, „nincs minden egyes folyamatra külön kalibrálva”* továbbá *„nehezen kezelhető az alkalmazottak számára”*. Az üzleti folyamatok részleges védelme vagy a különböző műveletekhez kialakított rendszerek inkoherenciája szintén okozhat biztonsági réseket, fokozva az ipari kémkedés kockázatát. Néhány alany beszámolt az interjúk során, hogy nem tartják biztonságosnak a vállalatirányítási rendszerek alkalmazását. *„A jelentős számú alrendszerrel rendelkező vállalatirányítási rendszerek nem biztonságosak, mivel minden adat egy felületen érhető el, és ezek alkalmazása során nehezen védhető a kritikus információ”* – számolt be az egyik interjúalany.

A rendszerszintű problémák számos platformot teremtenek a belső fenyegetés megnyilvánulásának, szorosan kapcsolódnak a külső kezdeményezés alkategóriához, továbbá a vezetői faktorhoz, mivel a jelenség mögött állhat az a probléma, hogy *„a vezetőség nem tartja az ipari kémkedést valós kockázatnak, így nem költ sokat az ilyen rendszerekre”* – véli az egyik alany.

Az ipari kémkedési esetek növekedése mögött azonosított külső és belső kontingencia tényezők mind közvetlen vagy közvetett kölcsönhatásban állnak egymással, melyek közül a 7. ábrán látható kapcsolatok kerültek kiemelésre. A védelmi piacon uralkodó intenzív verseny következményeként növekszik a kritikus információ értéke, továbbá szintén emelkedik a külső entitások száma, melyek egyre jelentősebb összeget hajlandók fizetni az információért. A külső szereplők jelenlétét fokozzák a geopolitikai tényezők is, mint a háború által előidézett keresletnövekedés. A piaci verseny okozta nyomás növeli a belső érintettek által elkövetett hibák valószínűségét, amelyet szintén fokozhat az IT rendszer biztonsági hiányosságai, továbbá a munkavállalók által elfogadhatatlan vezetési gyakorlat. Az IT alapú információbiztonsági rendszer minőségét a vezetői döntések formálják. A geopolitikai körülmények alakulása növeli az IT fenyegetések számát, továbbá befolyással van a védelmi iparban működő vállalkozások vezetésére. Az intenzív piaci verseny és a védelmi piac globalizációja olyan tényezők, amelyek gerjesztő hatással rendelkeznek egymás irányába. Többek között a globalizáció által kínált lehetőségek eredményeként a fiatal generációk hűsége csökkent a vállalkozással szemben. Amennyiben a fiatal munkavállalók még pszichológiai problémával, – mint harag vagy személyiségzavar – is rendelkeznek, úgy még jelentősebb információbiztonsági

kockázatot jelentenek a vállalkozásnak, mely karakterisztikák és azok következményei jellemezhetik a vezetőket is.



7. ábra: A növekedés tényezői közötti hipotetikus összefüggések

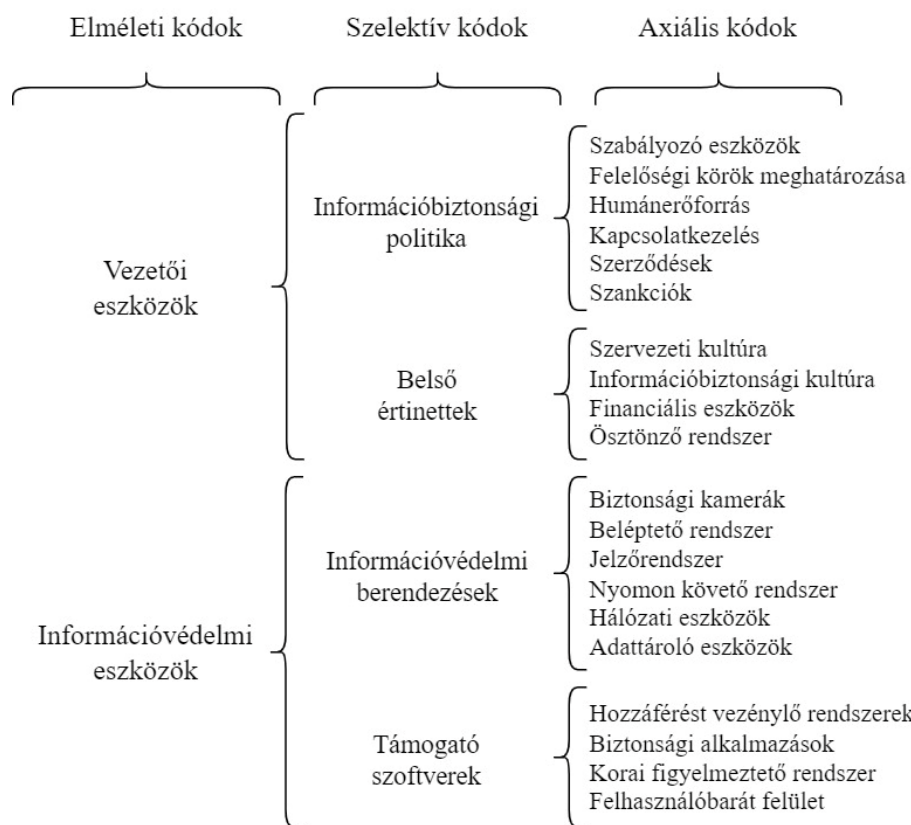
Forrás: saját szerkesztés (n=42)

A védelmi iparban tapasztalható ipari kémkedési esetek növekedése mögött található tényezők feltárása és megértése nélkülözhetetlen része a fenyegetés elleni hatékony információvédelmi rendszer kialakításának. A következő fejezet bemutatja, hogy a gyűjtött empirikus adatok alapján mely szempontokat szükséges figyelembe venni, továbbá milyen lehetőségek állnak a vállalkozások rendelkezésére az ipari kémkedés megelőzésére és az incidensek észlelésére.

3.2. Az ipari kémkedés fenyegetésének észlelése és megelőzése

Hills és Anjali (2017) [176], Homoliak és szerzőtársai (2020) [8], továbbá Saxena és szerzőtársai (2020) [9] véleménye szerint a vállalkozások által alkalmazott információbiztonsági rendszer sok esetben csak információs technológiai szempontból, a külső támadásokra fókuszálva közelítik meg az ipari kémkedés jelentette fenyegetést, figyelmen kívül hagyva a belső érintettek által képviselt problémát. Lara és szerzőtársai (2020) [185], továbbá Samy és szerzőtársai (2020) [178] publikációja alapján ennek oka, hogy a döntéshozók nem értik az emberi viselkedésből eredő fenyegetés természetét, így az IT központú védelmi rendszer megerősítésére összpontosítanak, mikor Omar (2015)

[135] szerint a megoldást egy olyan többretegű információbiztonsági rendszer jelentheti, amely felkészült a belső érintettek és a külső entitások jelentette fenyegetésre egyaránt. A fejezetet bemutatja, hogy a megkérdezett szakértők beszámolói alapján milyen eszközöket és módszereket alkalmaznak a védelmi vállalkozások az ipari kémkedés megelőzésére és észlelésére (**K3**). Az azonosított elméleti, szelektív és axiális kódokat a kódfa szemlélteti (8. ábra).



8. ábra: az ipari kémkedés elleni védekezés és megelőzés tényezői, a grounded theory elemzés kódja

Forrás: saját szerkesztés (n=42)

Jelen kvalitatív kutatás során a kérdésben a vezetői és az információvédelmi eszközök elméleti kódok kerültek azonosításra, melyek alapot biztosíthatnak a vállalkozásra optimalizált információbiztonsági rendszer kialakításához.

3.2.1. Vezetői eszközök

A **vezetői eszközök** elméleti kód az információbiztonsági politika és a belső érintettek szelektív kódokból alakult ki. Az **információbiztonsági politika** magában foglalja a szabályozó eszközöket, a felelősségi körök meghatározását, a humánerőforrást, a kapcsolatkezelést, a szerződéseket és a szankciókat.

Az interjúalanyok elmondása szerint a szabályozó eszközök olyan pontosan definiált szabályokat és előírásokat jelentenek, melyek többek között *„meghatározzák a kritikus üzleti információ kezelésére vonatkozó irányelveket”, „a vállalkozás azon területeit és üzleti folyamatait, amelyekre különösen oda kell figyelni”, a felmerülő kockázatok értékelésének és kezelésének protokollját és a szükséges biztonsági intézkedéseket”* továbbá *„az ipari kémkedés bekövetkezése esetén életbelépő válságkezelési protokollt”*.

A megkérdezettek egyetértettek abban, hogy az ipari kémkedés elleni védekezés fontos része a felelősségi körök meghatározása. Elmondásuk alapján minden üzleti folyamatnál definiálni indokolt az adott belső érintettek hatáskörét és felelősségét, továbbá a feladat elvégzéséhez szükséges kritikus információhoz való hozzáférés körülményeit, feltételeit és felhasználási módját, így meghatározható, hogy egy esetleges információszivárogtatási incidens során ki vonható felelősségre. Ebbe a kategóriába került besorolásra a jól működő ügyirat kezelés, ugyanis az interjúalanyok szerint *„nagyon sok információt kezelnek a vállalkozások papíron”,* továbbá *„még mindig nincs minden digitalizálva, és a papír alapú információk kezelése is fontos információbiztonsági szempontból”*.

A humánerőforrás az új munkavállalók felvétele során alkalmazható gyakorlatokra vonatkozik, melyekkel csökkenthető annak kockázata, hogy egy személy ártó szándék által vezérelve csatlakozzon a vállalkozáshoz. Az alanyok beszámoltak, hogy egy új ember alkalmazása előtt példának okáért *„szükséges ellenőrizni, hogy részt vett-e korábban ipari kémkedésben, bűncselekményben”* vagy *„az ipar jellegéből adódóan van-e kapcsolata bármilyen szélsőséges csoporttal”*.

A kapcsolatkezelés a külső érintettekkel való közös tevékenység folytatásának információbiztonsági szempontú szabályozására vonatkozik. A résztvevők hangsúlyozták a kommunikációs csatorna megválasztásának fontosságát, mivel az együttműködések során a kritikus információ egymástól különálló egységek között áramlik. Az alanyok véleménye eltért abban a kérdésben, hogy mely csatornák biztonságosak, azonban abban egyeztek a véleményük, hogy a *„különböző szolgáltatók*

által biztosított online tárgyalók, melyek használata elterjed a pandémia ideje alatt”, információbiztonsági szempontból nagyon kockázatos. Szintén eszköze lehet a kapcsolatkezelésnek a közös tevékenység megkezdése előtt a másik entitás megbízhatóságának ellenőrzése, amely történhet „*audit*” formájában vagy amennyiben a tevékenység jellege lehetővé teszi, a kritikus információk „*nem teljes, korlátozott formában történő*” rendelkezésre bocsátása.

A szerződések azon dokumentumokat foglalják magukban, melyekkel a szervezet a belső és külső érintettekkel szemben is védheti a kritikus üzleti információt, mint a „*titoktartási*” és a „*versenytilalmi szerződés*”. Azonban az interjúalanyok tapasztalta szerint sok esetben, – például „*külföldön*” vagy „*Európai Unió kívüli*” szerződésszegés esetén – nehéz szankcionálni ezen dokumentumok megszegését.

A szankciók azon eljárásokat rendszerezik, melyeket a vállalkozás jogilag megtehet abban az esetben, ha az egyik belső vagy külső érintett ipari kémkedés gyanújába keveredik. A mélyinterjúk során a megkérdezett szakértők szerint az „*első lépés lehet csak egy szó- vagy írásbeli figyelmeztetés*”, amely a „*fegyelmi eljárásig*”, a „*munkaviszony megszűnéséig*”, vagy az eset az „*illetékes hatóságok felé való jelentéséig*” terjedhet. „*Amennyiben a védelmi vállalkozások között elterjed egy szakemberről, hogy információt tulajdonított el és adott át egy külső szereplőnek, azt a személyt az ipar többi szereplője a jövőben fenntartással fogja kezelni*” – számolt be az egyik alany, utalva az ágazat szűk körű, zárt jellegére. Szankciók megfogalmazása, amely az „*alkalmazottak megfélemlítésén alapszik*”, csak abban az esetben rendelkezik kockázatcsökkentő hatással, ha az „*emberek tisztában vannak a cselekedeteik következményével*”. Mindazonáltal szankciók definiálása negatívan is hathat a munkavállalók viselkedésére és teljesítményére, amely fokozza a személyes sérelmek kialakulásából eredő kockázatot.

A **belső érintettek** szelektív kód a szervezeti kultúra, az információbiztonsági kultúra, a pénzügyi eszközök, továbbá az ösztönző rendszer axiális kódokból fejlődött.

A szervezeti kultúra olyan, a belső érintettek közötti kapcsolatokhoz köthető tényezőket foglal magában, melyek biztosításával a vállalkozáshoz fűződő pozitív attitűdöt és lojalitást lehet növelni. A válaszadók szerint ennek része a „*világos és hatékony kétirányú kommunikáció*”, „*pozitív kapcsolatok a vállalkozáson belül*”, „*pozitív és ösztönző kultúra*”, továbbá „*egymás tisztelete*”. A szervezeti kultúrának szintén fontos része „*az*

alkalmazottak hibáinak diszkrét kezelése”, továbbá hibák esetén a „nyilvános felelősségre vonás és megalázás kerülése”.

Az információbiztonsági kultúra a belső érintettek információbiztonsághoz fűződő tudatosságát, viselkedését és attitűdjét foglalja magában, mely fejlesztése kiemelt szerepet játszik az ipari kémkedés megelőzésében és észlelésében. Ennek fontos részét képezik a belső érintettek oktatása, az információbiztonsági tudatosság kialakítása, és a figyelemfelhívás az információszivárgás káros következményeire. Az alanyok egyetértettek abban, hogy az információbiztonság legfontosabb faktora a belső érintettek oktatása, többek között olyan tényezőkre, mint *„az információvédelmi rendszerek használata”, „a kritikus információk felhasználására”, „a fizikai dokumentumok kezelése”, „a különböző platformokon történő biztonságos kommunikáció”, „az engedély nélkül megosztott információk következményei”, továbbá „a megvesztegetés és zsarolás elleni védekezés”.* A munkavállalók oktatása nem egyszeri feladat, hanem folyamatosan ismétlődő része a munkavégzésnek, melynek során *„a biztonsági rendszeren végrehajtott változtatásokat és a folyamatosan megjelenő új fenyegetéseket is szükséges ismertetni”* – osztotta meg az egyik alany. *„Az alkalmazottak számára biztosítani szükséges olyan eszközöket, melyek segítségével azonosítani tudják a gyanús tevékenységeket – számolt be egy másik résztvevő.* Továbbá kiemelték, hogy az oktatási módszer is fontos, *„egy interaktív, színes és szórakoztató prezentáció során jobban fel lehet kelteni az emberek figyelmét, mint száraz oktatóanyagokkal, amit kiküldenek nekik e-mailben és általában meg sem nyitják”.* Az alkalmazottak információbiztonsági tudatossága többek között tesztelhető *„szervezett külső megkeresésekkel”, vagy „károsnak álcázott e-mailekkel”.*

Az alkalmazottak oktatása mellett az információbiztonsági szabályok megszegésével járó káros következményekre való figyelemfelhívás is nélkülözhetetlen eleme az információbiztonsági kultúra kialakításának, melynek az alanyok elmondása szerint részét képezi elmagyarázni, hogy *„bizonyos információk miért vannak bizalmasnak jelölve”, „miért fontos az adatok védelme” és „kiszivárogtatása milyen károkat okozhat a vállalkozásnak”.* A vezetők feladata a *„kritikus információk egyértelmű jelölése”.* Ezen gyakorlatok alkalmazásával a belső érintettek képesek lesznek olyan módon végezni a mindennapi feladataikat, hogy közben tudatosan óvják a vállalkozás kritikus információit.

A válaszadók tapasztalatai szerint a belső érintettek által elkövetett ipari kémkedés mögött leggyakrabban külső pénzügyi ösztönzés azonosítható, így a finansziális eszközök biztosítása, mint a versenyképes fizetés és egyéb juttatások, közvetlenül támogatják a munkavállalók vállalkozáshoz való hűségét és motivációját. *„A munkavállalói hűség kérdése túl van gondolva, versenyképes fizetést kell nekik biztosítani, és akkor hűségesek lesznek”* – számolt be az egyik alany.

Az alkalmazottak elismerésére kialakított ösztönző rendszer fontos faktor a belső érintettek hűségének és motivációjának növelésében, melynek az interjúk alapján eszközei lehetnek a *„többdimenziós sikermutatók használata”*, az *„alkalmazottak munkájának elismerése”*, *„elégedetlenségük figyelése és kezelése”*, továbbá *„fejlődési és a vállalkozáson belüli előrelépési lehetőség biztosítása”*. Szintén növeli a munkavállalói hűséget *„a reális és elérhető, egyéni és kollektív célok kialakítása, továbbá a cél elérése esetén a megígért kompenzáció azonnali biztosítása”* – mondta az egyik alany.

3.2.2. Információvédelmi eszközök

Az információs infrastruktúra védelmének kritikus része a vállalkozás által alkalmazott **információvédelmi eszközök**. Az elméleti kód az információvédelmi berendezések és a támogató szoftverek szelektív kódokból fejlődött, melyek használata során az előbbi hatékony működését támogatja az utóbbi. Az alkalmazott eszközök nem csak a külső támadásoktól védik a vállalkozás kritikus információit, hanem egy jól átgondolt rendszer a belső érintettek munkavégzés közben elkövetett hibáiból, és a szándékosan kezdeményezett információszivárogtatási esetekből eredő kockázatot is képes csökkenteni.

Az **információvédelmi berendezések** azon eszközöket ölelik fel, melyek az interjúalanyok elmondása szerint támogatják a vállalkozást az ipari kémkedés észlelésében és megelőzésében. A biztonsági kamerák használata széles körben elterjedt gyakorlat a területek monitorozására, azonban az alanyok beszámoltak arról, hogy ez az eszköz alkalmas a belső érintettek magatartásában történő változások megfigyelésére is, mely részletesen a korai figyelmeztető rendszer axiális kód során kerül bemutatásra.

A beléptető rendszer olyan fizikai berendezések együttese, melyek célja a vállalkozás területeire való belépés ellenőrzése és az illetéktelen személyek behatolásának megakadályozása. Az interjúk során az alanyok a beléptető rendszer olyan tulajdonságait osztották meg, mint a *„kártyás”*, *„chipes”*, *„kódos”*, *„biometrikus”* vagy *„ezek*

kombinációja”, „alkalmazása során naplózza a belépéseket”, továbbá „szabályozható, hogy melyik alkalmazott mely időpontokban léphet be a vállalkozás területére”. Az alanyok a számítógépekbe és egyéb digitális platformokra való belépés eszközeként is említették a „biometrikus hitelesítő eszközöket” és „kártyákat” melyek a személyazonosság ellenőrzésére szolgálnak. Néhány interjúalany elmondta, hogy a beléptető része lehet a látogatói rendszer, mely „a vállalkozás területére érkező látogatókat azonosítja, adataikat rögzíti, mozgásukat követi és a cégen belüli tevékenységüket ellenőrzi tartózkodásuk során”. Ezen eszközök segítenek megakadályozni az olyan jogosulatlan személyek behatolását a vállalkozás területére, akik veszélyeztethetik az üzleti folyamatok szakadatlan működését és az információbiztonságot.

A résztvevők megosztották tapasztalataikat a jelzőrendszer alkalmazásának fontosságáról, mely *„azonnali figyelmeztetést küld a szervezetnek, amennyiben valaki megpróbál behatolni a vállalkozás területére vagy hozzáférni annak eszközeihez, így azonnali reakciót tesz lehetővé”* – számolt be az egyik alany. Bizonyos esetekben indokolt lehet az alkalmazottak (gépjárművek) vagy dokumentumok *„nyomon követése GPS vagy RFID technológiával”,* mely szintén használható *„a munkavégzési területekre való belépés és mozgás megfigyelésére”.*

A hálózati eszközök a vállalkozás belső rendszerén keresztül teszik lehetővé a számítógépek és egyéb berendezések kommunikációját. Az egyik interjúalany elmondása szerint *„olyan gyorsan fejlődnek az interneten keresztül történő támadások, hogy az ellen nem képes egy tűzfal vagy egyéb szoftver teljes biztonságot nyújtani”,* ezért *„fontos egy független, belső hálózat kialakítása, amely nem csatlakozik az internethez”* – számolt be egy másik. Az alanyok kiemelték az olyan adattároló eszközök használatát, amelyek internethez való hozzáférés nélkül tárolják a szervezet kritikus információit.

Az információbiztonsági hálózat kialakításának fontos része a fizikai berendezések és a **támogató szoftverek** konfigurációja. Az alanyok beszámolója alapján a hozzáférést vezénylő rendszerek axiális kód azon szoftvereket foglalja magában, melyek a beléptető, a nyomon követő, a jelző- és a látogatói rendszer üzemelését támogatják. A biztonsági alkalmazások azon programokat öleli fel, melyek különböző módokon védik a vállalkozást az interneten keresztül történő támadásoktól, szándékos károkozástól, adatvesztéstől és információlopástól. Az interjúk alapján a biztonsági alkalmazások

többek között olyan feladatokat látnak el, mint a *„biztonsági protokoll megsértésének felismerése”, „védelem a külső támadásokkal szemben”, „hozzáférési jogosultságok letiltása”* és a *„rendszer sérülékenységeinek azonosítása”*.

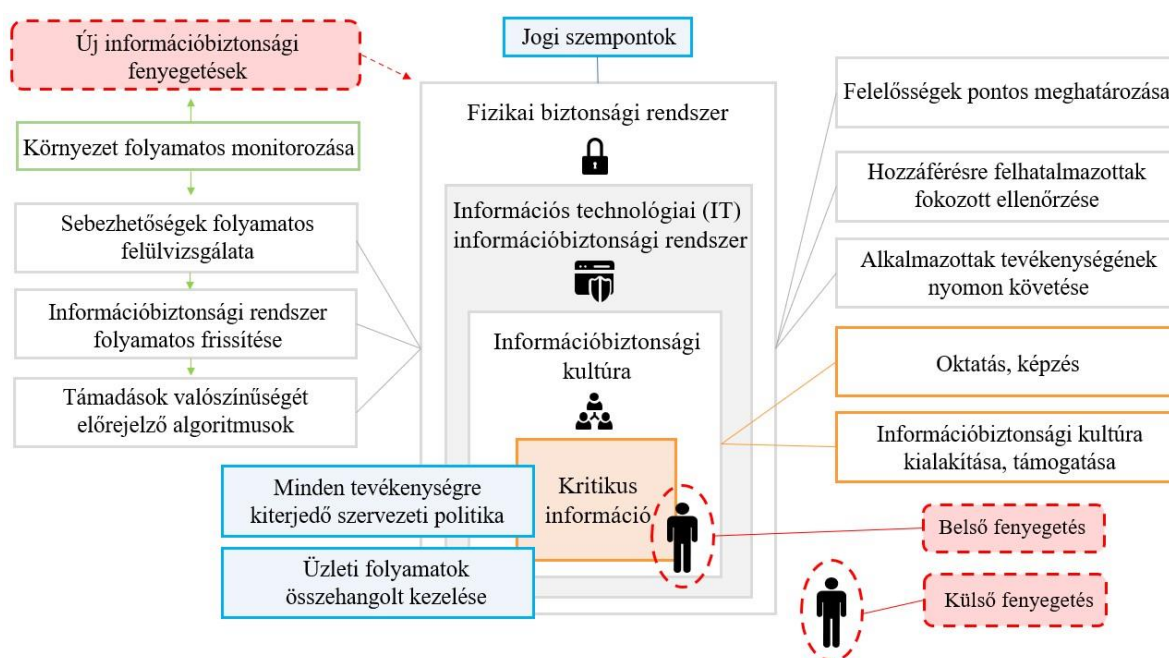
A mélyinterjúk során megkérdezett szakemberek szerint a vállalkozásoknak lehetőségük van korai figyelmeztető rendszert (*early warning sign system*) alkalmazni, amely elsősorban a belső érintettek kamerákkal történő megfigyelésén alapszik. A válaszadók tapasztalatai alapján a módszer többek között *„növeli a biztonságot”, „lehetővé teszi az ipari kémkedéssel összefüggésbe hozható kísérletek időben való észlelését”, „figyelemmel kísérhető a szabályok betartása”, „értékelhető a munkavégzés hatékonysága”* továbbá *„szabályszegés esetén lehetővé teszi az azonnali beavatkozást”*. Elmondásuk alapján a kamerák használata nem csak megelőző jellegű, hanem egy esetleges ipari kémkedési incidens során a *„felvételek bizonyítékként szolgálhatnak”,* így támogatva a kialakult helyzet kezelését. A belső érintettek monitorozása során lehetőség van a korai figyelmeztető jelzések észlelésére és elemzésére, mely a magatartásbeli változásokra utal. *„Ezek olyan jelek, amelyek önmagukban nem rendelkeznek jelentőséggel, azonban, ha kirajzolódik egy trend, akkor a vállalkozásnak érdemes a munkavállaló viselkedésére kiemelt figyelmet fordítani”* – osztotta meg az egyik megkérdezett. A korai figyelmeztető jelzések lehetnek *„hirtelen változások az alkalmazott viselkedésében”, „agresszív viselkedés”, „szokatlan időpontban való munkavégzés”* vagy *„nagy érdeklődés mutatása pozíciójuk vagy munkájuk hatáskörén kívül eső témák iránt”*.

Az interjúk során felmerült a kérdés, hogy a mesterséges intelligencia fejlődése milyen hatással lesz a belső érintettek rossz szándékának korai észlelésére, melyben az alanyok egymással szemben álló véleményeket osztottak meg. Egyesek szerint a mesterséges intelligencia alapú rendszerek rövidesen képesek lesznek azonosítani és előrejelezni a belső érintettek rossz szándékú cselekedeteit, míg mások szerint az emberi természet annyira komplex, hogy egy ilyen jellegű jól működő rendszer kialakítása nagyon távol áll a jelenben alkalmazott technológiáktól. Szintén beszámoltak, hogy a belső érintettek monitorozása csökkentheti a visszaéléseket, azonban negatívan is hathat a munkavégzésre, mivel *„frusztrációt kelthet”, „zavarhatja őket”, „növelheti a nyomást”* és *„csökkentheti a motivációt”*.

A kutatás eredményei alapján a munkavégzés során használt digitális felületek felhasználóbarát kialakításának céljai között említendő *„az emberi hibákból eredő*

kockázat csökkentése” és „az információhoz való illetéktelen hozzáférés megakadályozása”. Az interjúalanyok elmondása szerint többek között fontos az „egyszerű használat”, „logikus elrendezésű felület”, és „az automatikus biztonsági mentések és frissítések biztosítása”. Szintén ide került kategorizálásra az „erős jelszavak használata”, a „többlépéses azonosítás” és a „felhasználók hitelesítése”.

A 9. ábra szemlélteti a holisztikus megközelítésű, többretegű információbiztonsági rendszert, mely magában foglalja a fizikai elemeket, az IT megközelítést és az információbiztonsági kultúrát egyaránt.



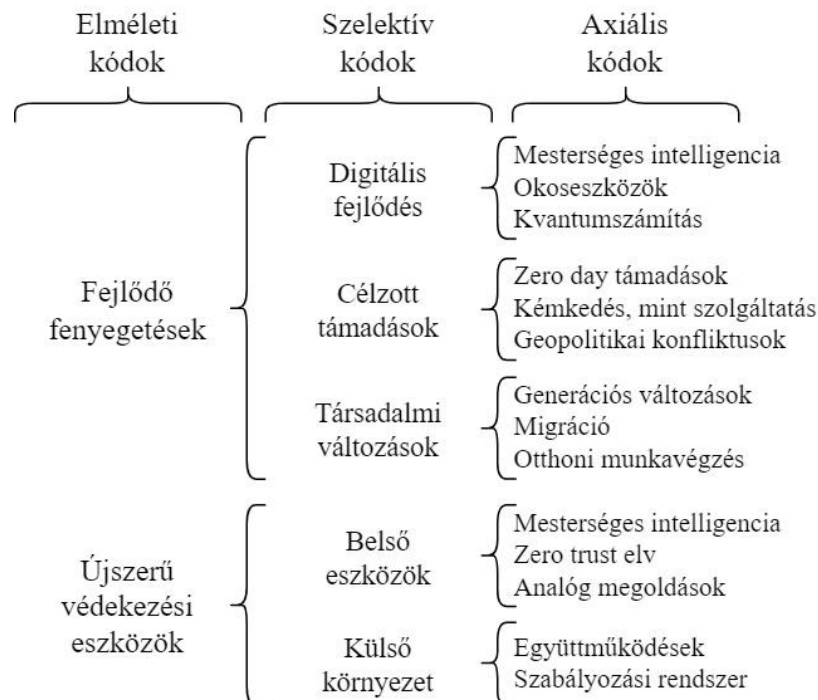
9. ábra: Többretegű információbiztonsági rendszer

Forrás: saját szerkesztés (n=42)

A folyamatosan változó környezetben a vállalkozásoknak kiemelkedően fontos a külső és a belső fenyegetésekkel szembeni védekezés. Azonban a döntéshozóknak nem csak a jelenben ható információbiztonságot fenyegető támadásokra kell felkészülni, hanem a technológiai fejlődéssel és társadalmi átalakulással járó jövőbeni fenyegetésekre is, melyek természetére a jelenleg rendelkezésre álló információkból, eszközökből és uralkodó körülményekből lehet következtetni.

3.3. Az ipari kémkedés fejlődése

A védelmi vállalkozások döntéshozóinak rendkívül fontos szerepe van az új technológiák megvalósításához és egyéb üzleti folyamatokhoz szükséges kritikus információ megóvásában, és a jövőben az információbiztonsági fenyegetések előrehaladásával a feladatuk még komplexebb és meghatározóbb lesz (**K4**). Williams és szerzőtársai (2023) [202] az ipari kémkedés növekedésének kockázatát az intelligens rendszerek üzleti folyamatokba való integrálásában látják. Wilson és Hingnikar (2023) [177] szerint az egyre különfélebb hackertámadások, továbbá az az autonóm entitások és robotok megjelenése növeli a vállalkozások ellen elkövetett ipari kémkedési esetek számát. Bár az alanyoknem tartanak a robotok megjelenésétől, azonban a legnagyobb információbiztonsági fenyegetést a digitális technológia fejlődésében látják. Megjegyzem, hogy bár az interjúk során az ipari kémkedéssel összefüggésbe hozható jövőbeni fenyegetésekről kérdeztem az alanyokat, a gyűjtött adatok és azonosított eredmények már napjainkban is kockázatot jelentenek a vállalkozásoknak. A kódfa ismerteti az azonosított kategóriákat (10. ábra).



10. ábra: Jövőbeni fenyegetések, a grounded theory elemzés kódfája

Forrás: saját szerkesztés (n=42)

3.3.1. Fejlődő fenyegetések

A **fejlődő fenyegetések** elméleti kód a digitális fejlődés, a célzott támadások és a társadalmi változások szelektív kódokból fejlődött.

Bár a **digitális technológiák előrehaladása** eddig is súlyos fenyegetést jelentett az ipari kémkedés szempontjából, az alanyok véleménye szerint ez a trend csak tovább fokozódik a jövőben. Az interjúkészítés periódusában váltak egyik napról a másikra népszerűvé a mesterséges intelligencia alapú chatbotok, melynek hatása érezhető volt a beszámolókon. A legsúlyosabb jövőbeni ipari kémkedéshez fűződő fenyegetést a mesterséges intelligencia evolúciójában látták, amely „*célzottabb*” és „*hatékonyabb*” információeltulajdonítást tesz lehetővé. A résztvevők szerint szintén egyre súlyosabb információbiztonsági kockázattal jár az okoseszközök jelenléte. Elmondásuk szerint a mobiltelefonok és egyéb eszközök „*civilek által történő lehallgatása korábban nehezen megoldható feladat volt*”, azonban erre „*egyre modernebb technológiák válnak széles körben elérhetővé*”. Néhány megkérdezett beszámolt a kvantumszámítás növekvő fenyegetéséről, melynek veszélye az egyik alany szerint abban gyökerezik, hogy „*olyan bonyolult problémákat képes megoldani, amelyet a hagyományos számítógépek nem tudnak, és így bármilyen titkosítási rendszert képes lesz feltörni*”.

A **célzott támadások** szelektív kód az ipari kémkedési kísérletek egyre specifikusabb természetére utal. A válaszadók beszámoltak a nulladik napi (*zero day*) támadásokról, melyek a rendszer olyan sebezhetőségeit kihasználva tulajdonítanak el kritikus információt, amit a fejlesztők még nem ismertek fel, így a támadás időpontjában a biztonsági réseket még nem azonosították.

A kémkedés, mint szolgáltatás axiális kód az alanyok azon véleményén alapszik, hogy jövőben várhatóan egyre több entitás fog a jogtalan és célzott információeltulajdonításra „*szakosodni*”, mely szolgáltatást a piac szereplői igénybe vehetik. Ezek a támadások egyre célzottabbá válnak, amelyeket „*speciális ipari vagy ágazati tudással rendelkező emberek*” követnek el, közben „*törekedve arra, hogy tevékenységük hosszú távon észrevehetetlen maradjon*”. Ez a kategória magában foglalja a személyes kémkedést és az interneten keresztül történő hackertámadást egyaránt.

A geopolitikai konfliktusok is vitathatatlanul hatással vannak a védelmi ipar területén történő ipari kémkedésre, mely az orosz-ukrán háború elhúzódásával, továbbá az országok közötti szövetségek bizonytalanságával szintén problémát fognak jelenteni a

döntéshozóknak. Az alanyok kiemelték, hogy a fegyveres konfliktus következményeként számos kém és hacker jelent meg az ágazatban, akik a felek szövetségesei és támogatói ellen egyre több támadást kezdeményeznek. Az egyik résztvevő hangsúlyozta, hogy *„jelen geopolitikai környezetben a vállalkozásoknak csak olyan piaci szereplőkkel javasolt üzleti tevékenységet folytatni, amelyek nem függenek olyan beszállítóktól vagy szolgáltatóktól, akik közvetlenül kapcsolódnak vagy érintettek a konfliktus által”*.

A **társadalmi változások** ugyancsak információbiztonsági kihívás elé fogják állítani a védelmi vállalkozások vezetőit. Mint ahogy a pszichológiai faktorok között korábban már bemutatásra került, a fiatal munkavállalók hűségének kérdése is növeli a belső fenyegetés kockázatát, azonban az újabb generációk, valamint az eltérő kulturális háttérű személyek munkaerőpiacra való belépése is változásokat hoz az információbiztonsági kultúra dinamikájában. A válaszdók megosztották a migrációval kapcsolatos foglalkoztatás kockázatát, amely abból ered, hogy megtalálható közöttük a *„kétkezi munkásoktól kezdve a phd-vel rendelkező mérnökökig minden réteg, viszont lehetetlen a háttérüket ellenőrizni”* – osztotta meg az egyik interjúalany. Bár a résztvevők közül néhányan jelezték, hogy a kockázatok miatt nem foglalkoztatnának olyan személyt, akinek nem ellenőrizhető a háttere, azonban hozzátették, hogy a munkaerőhiány miatt számos, a védelmi iparhoz közvetlenül vagy közvetve kapcsolódó területen elkerülhetetlen az alkalmazásuk.

Az alanyok véleménye szerint a távoli munkavégzés (*home office*) – számos ok miatt, mint egy pandémia, energiaválság vagy szélsőséges időjárás – része marad a társadalomnak, rákényszerítve a vállalkozásokat, hogy lehetővé tegyék az információs infrastruktúrához való távoli hozzáférést. A távmunkát végző alkalmazottak *„kevésbé figyelnek a biztonságra”*, és *„jellemzően nem rendelkeznek hálózati szintű biztonsági ismeretekkel”*, ami belső fenyegetések és a külső támadások szempontjából is jelentős kockázattal jár.

3.3.2. Újszerű védekezési eszközök

Az **újszerű védekezési eszközök** kutatásának célja olyan eszközök és módszerek feltárása volt, melyek támogatják a védelmi vállalkozások döntéshozóit az új fenyegetésekre való felkészülésben. A **belső eszközök** között került azonosításra a mesterséges intelligencia, a zéró bizalom elv (*zero trust*) és az analóg megoldások.

Mint ahogy a fejlődő fenyegetéseknél már említésre került, az újszerű védekezési eszközök kutatása során is hatással volt a válaszokra a mesterséges intelligencia, mely jelentős médiafigyelmet kapott az adatgyűjtés időszakában. Bár a technológia már elérhető volt az adatfelvétel során, azonban egyik vállalkozás sem alkalmazott ilyen eszközöket az ipari kémkedés megelőzésére és észlelésére, de a legtöbb alany tervezi a jövőbeni bevezetését. Egyik résztvevő beszámolt, hogy *„a mesterséges intelligencia előnye, hogy olyan nagy mennyiségű adatot képes elemezni, amelyre az emberi elme már nem képes, így rövid időn belül felismeri, jelzi és blokkolja a potenciális fenyegetést jelentő eseményeket, jelentősen lerövidítve a reakció időt”*.

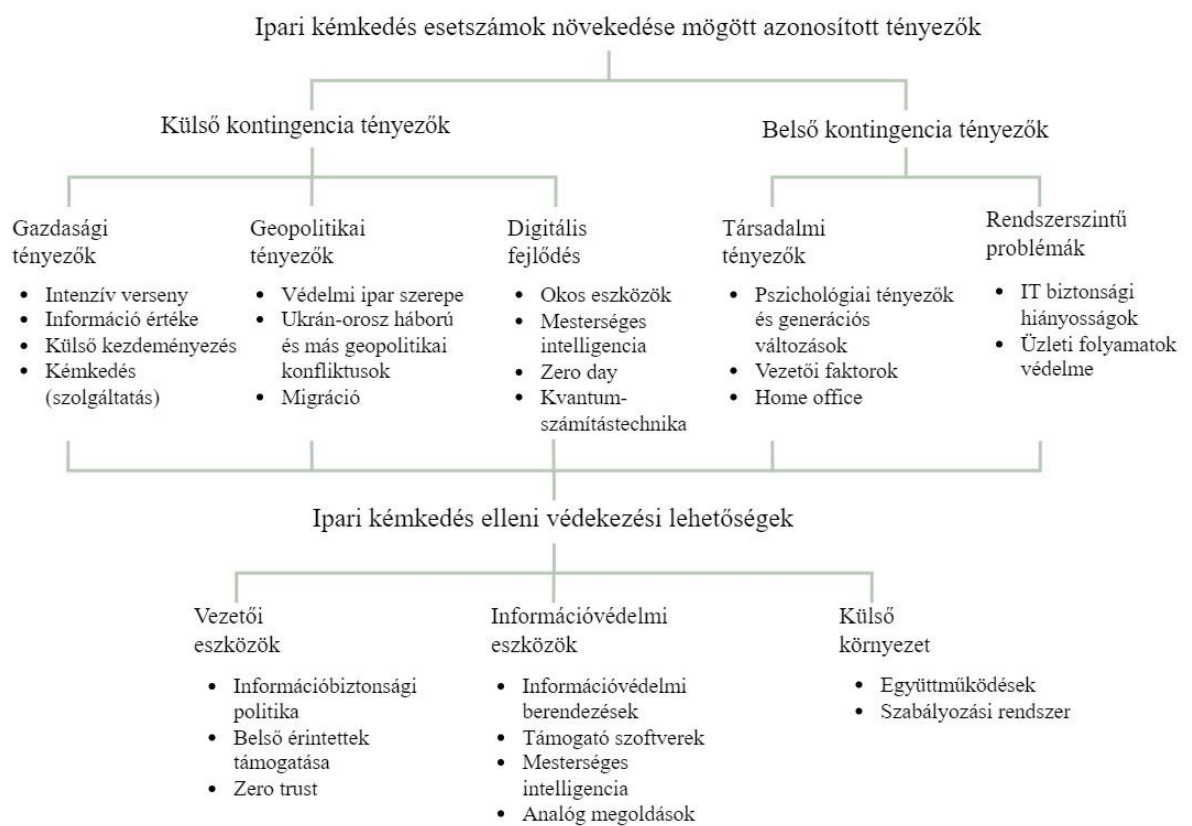
A zéró bizalom elv (*zero trust*) alkalmazása, amely a belső érintettek digitális eszközökkel szemben természetessé vált bizalmának csökkentésére irányul, szintén szerepelt az alanyok tervei között. Ez ellentétben áll a menedzsment megközelítésekkel, mely éppen a bizalom szerepét hangsúlyozza a szervezeti kultúrában és működésben [224]. A döntéshozók jellemzően úgy ítélik, hogy a belső hálózaton belül minden felhasználó és eszköz megbízható, míg a külső felhasználók és eszközök a lehetséges kockázatok közé vannak sorolva, azonban a megközelítés hiányossága, hogy a behatolók kihasználhatják a rendszer biztonsági sebezhetőségeit [225]. A zéró bizalom elv a munkavégzés során véletlen elkövetett információszivárgási esetek kockázatát csökkentheti.

Néhány alany megosztotta az aggodalmát, mely szerint a jövőben olyan információbiztonsági fenyegetéseket kell majd kezelni a vállalkozásoknak, amelyekkel szemben a kritikus információ továbbítása és felhasználása során *„vissza kell majd tért a régi, analóg módszerekhez”*, mint a *„papír alapú megoldások”* és az *„információ személyes átadása”*. Azonban ennek hátránya, hogy a *„régimódszerek”* alkalmazásával vissza fognak térni a *„régimódszerek”* és a *„tranzakció elveszíti a valós idejű jellegét”*.

Az ipari kémkedés eszköztárának és módszereinek fejlődésével szemben nem elegendő a vállalati szintű felkészültség, a külső környezeti tényezőknek is fejlődni szükséges a fenyegetéssel. Az együttműködések a védelmi ipar területén történő közös tevékenység folytatására utalnak, melyek során a *„a vállalkozások próbálták az információvédelmi megoldásaikat eltitkolni”*. Azonban a jövőben ez nem megoldható, mert a rendszerek közötti inkohérenca biztonsági résekhez vezet és jelentősen növeli az ipari kémkedés kockázatát. Az interjúalanyok véleménye szerint egyre nagyobb szükség van az állami

szintű lépésekre, „törvények és szabályozások elfogadásra” az ipari kémkedés szankcionálása érdekében, továbbá az „az információlopásért kiszabható büntetések” és a „szervezetek által kötelezően betartandó intézkedések” területén.

Mivel a kutatás során alkalmazott kvalitatív grounded theory módszertan lehetővé teszi az adatelemzés empirikus adatgyűjtéssel egyidejű megkezdését, továbbá a jövőre vonatkozó kutatási kérdések az interjúk II. szakaszától kaptak nagyobb figyelmet, ezért ezek a növekedést okozó tényezőktől, továbbá az észlelés és megelőzés eszközeitől külön fejezetben kerültek bemutatásra. Azonban a 11. ábra az grounded theory módszertan alkalmazásával definiált eredményeket összefoglalva mutatja be.



11. ábra: A grounded theory alkalmazásával definiált elmélet összefoglalása

Forrás: saját szerkesztés (n=42)

3.4. Diszkusszió

A megalapozott elmélet² összehasonlítása a témában rendelkezésre álló szakirodalommal a kvalitatív eredmények hitelességét, továbbá a kutatás deduktív jellegét biztosítja. A grounded theory használata során a kódolási eljárások és a módszertan mechanizmusai lehetővé teszik a korábbi elméletek beépítését az új eredmények közé, így támogatva a probléma gyakorlati és teoretikus megközelítésű vizsgálatát [25]. A kutatás során feltártak alátámasztják Button (2020) [13], Hou és Wang (2020) [130], továbbá Carl (2017) [131] állítását, mely szerint az ipari kémkedés komplex problémájának vizsgálata multidiszciplináris megközelítést igényel. Az eredmények érintik az informatika, a katonai műszaki, a közgazdaság, a politika továbbá a pszichológia tudományok területét, amelyből levonható a következtetés, hogy az ipari kémkedés elleni hatékony információbiztonsági rendszer kialakítása ezen diszciplínák együttműködésével valósulhat meg.

3.4.1. A védelmi iparban az ipari kémkedési esetek növekedésének okai (K1)

Jelen kutatás empirikus adatok alapján vizsgálta a védelmi iparban tapasztalható ipari kémkedéshez fűződő esetszámok növekedésének mögöttes tényezőit, melyek között külső kontingencia tényezőként kerültek azonosításra a gazdasági tényezők. Az intenzív piaci verseny során a szereplőknek, a piaci pozíció megőrzéséhez vagy növeléséhez, továbbá az árversenyben való előnyös szerepléshez szükséges ismeretekkel rendelkezni a versenytársak tevékenységeiről, amelyet gyakran az ipari kémkedés etikátlan vagy illegális eszköztárát alkalmazva valósítanak meg. A jelenséget csak súlyosbítja, hogy a piacon megjelentek azon speciális területi tudással rendelkező entitások, amelyek szolgáltatásként kínálják a megrendelő által igényelt információ beszerzését.

A védelmi iparban zajló globalizációs folyamatok eredményeként a vállalkozások az országhatárokon túl is terjeszkedhetnek³. A külföldi, főként az Európai Unió kívüli tevékenység folytatása azért jelent kiemelt kockázatot, mert számos nemzet az ipari kémkedést a gazdasági tevékenységek legitim eszközének tartja [130, 141, 142, 169], továbbá a nemzetközi ügyletek során a szervezetek a saját kultúrájukban elfogadható információkezelési módszereket részesítik előnyben [55, 170]. Egy ilyen természetű információlopás esetén – példának okáért amikor egy kisvállalkozás indít eljárást egy

² A grounded theory alkalmazása során nyert eredmények.

³ Azonban nem szabad elfelejteni, hogy a védelmi ipar területén való tevékenység folytatása a legtöbb országban engedélyekhez kötött, melyek megszerzése hosszú és komplex folyamat.

külföldi állam ellen – a jogi folyamat rendkívül körülményes, költséges és sok esetben eredménytelen.

A védelmi technológiák és a kommunikációs eszközök gyorsütemű fejlődése szintén olyan tényezők, amelyek hozzájárulnak az esetszámok növekedéséhez. Heickerö (2019) [128], továbbá Szerb és szerzőtársai (2020) [160] szintén arra az eredményre jutottak, hogy a gyorsütemű technológiai evolúció még több eszközt teremtett az ipari kémkedés elkövetésére, amely az egyik legsúlyosabb fenyegetéssé nőtte ki magát az országok iparával és fenntartható fejlődésével szemben. Az átalakulás hatására az ipari kémkedés eszköztára egyszerűen elérhetővé vált bármely piaci szereplő számára, ami egyre több vállalkozást bátorít fel arra, hogy kihasználja ezt a költség- és időhatékony információszerzési módszert.

A kritikus információ – mely magában foglalja többek között az innovatív vállalkozás legértékesebb eszközét, a humán erőforrást, a különböző beszerzési forrásokat, a termékfejlesztést, gyártástechnológiát és a marketinginformációkat – nélkülözhetetlen az üzleti folyamatok zavartalan működéséhez és a szervezeti képességek fejlesztéséhez, azonban létrehozása hosszú és költséges eljárás, amely szintén ösztönzően hat a vállalkozásokra, hogy az ipari kémkedés eszköztárához folyamodjanak. Haig (2007) [158] korábbi kutatása során szintén arra az eredményre jutott, hogy a védelmi iparban való tevékenység folytatásának feltétele a kritikus információ, melynek gyors megszerzéséért kíméletlen harc folyik.

Az ipari kémkedéssel összefüggésbe hozható esetszámok növekedéséhez a védelmi ipar területén szintén hozzájárulnak a folyamatosan alakuló geopolitikai tényezők, mely gazdasági, politikai és a helyi haderő ellátása okán is stratégiai fontossággal rendelkezik, ezáltal fokozott fenyegetésnek van kitéve. A rendelkezésre álló szakirodalom alapján az elmúlt években a védelmi piac keresleti és kínálati oldala is dinamikus növekedést mutatott [3, 71, 124], melyet a 2022. februárban kirobbant orosz-ukrán fegyveres konfliktus csak tovább fokozott, kritikus ellátási problémákat okozva az ágazatban az alapanyag és a felszerelések területén egyaránt. Ezenfelül a háború előtérbe helyezte az európai védelmi ipar elhanyagoltságát, melyre válaszul a döntéshozók számára prioritássá vált a lokális ipar fejlesztése. A politikai nyomás ellenére ez azonban nem kivitelezhető rövid időn belül, ami a piac szereplőit az információ minél gyorsabb beszerzésére kényszeríti. A háború során taktikai előny szerezhető az innovatív védelmi technológiák

bevetésével, továbbá a másik fél által használt védelmi eszközök természetének ismeretével, mely szintúgy növeli az információlopás kockázatát. Azonban geopolitikai konfliktus hatására fokozódó különböző információs infrastruktúrákat érő támadások célja nem csak az információeltulajdonítás, hanem sok esetben a rombolás.

A belső kontingencia tényezők közé osztályozott rendszerszintű problémák növelik a külső kezdeményezés, továbbá a belső szándékos és véletlen elkövetett esetek kockázatát egyaránt. Az IT biztonsági hiányosságok sebezhetővé teszik a vállalkozást, a rendszer üzleti folyamatokra való hangolásának elmaradása biztonsági réseket okozhat. Azonban az információbiztonsági rendszer kialakítása során az IT eszközök mellett figyelembe kell venni a humán tényezőt, az üzleti folyamatokat, továbbá a környezeti kontingenciák alakulását is. A témát kutató szerzők szintén egyetértenek abban, hogy a rendszer kialakítása során nem szabad csak az IT szempontokra fókuszálni, a humán faktornak is kiemelt figyelmet szükséges szentelni [8, 9, 57, 176, 178, 185].

A dinamikusan fejlődő fenyegetések korában az alkalmazott információvédelmi rendszerek és eszközök folyamatos fejlesztést igényelnek. Amennyiben ez megköveteli a belső érintettek munkavégzési rutinjának átalakítását, az hozzájárulhat a véletlen elkövetett esetek növekedéséhez, mert az emberek nem szeretik a hétköznapi rutinjukban bekövetkező változásokat. Samy és szerzőtársai (2021) [178], továbbá Williams és szerzőtársai (2019) [175] is arra az eredményre jutottak, hogy a vállalkozásnak minél előbb adaptálni szükséges az új fenyegetések elleni megoldásokat, azonban ez súlyos információbiztonsági sebezhetőséghez vezethet, mert a munkavállalók fenntartásokkal kezelik az új, számukra ismeretlen technológiákat, és nem szívesen változtatnak a korábbi, kényelmes munkavégzési szokásaikon.

3.4.2. A belső érintettek által elkövetett ipari kémkedés mögött azonosított faktorok (K2)

A belső érintettek által elkövetett ipari kémkedés mögött – függetlenül annak szándékos vagy véletlen természetétől – számos különböző támogató változó tárható fel. Az eredmények alapján a leggyakoribb motiváló tényező az eltulajdonított információért cserébe kínált anyagi kompenzáció, ugyanerre az eredményre jutott Button (2020) [13] és Søylen (2016) [12] is. Bár a szakirodalom szerint [134, 135, 150, 152, 175, 176] az alkalmazottat legtöbb esetben ártani akaró, rossz szándék vezérli, mikor a vállalkozás ellen cselekszik, az interjúalanyok jelen kutatás során ezt a feltételezést teljesen

elvetették. Véleményük szerint túl súlyos következményekkel járhat ez a cselekedet, hogy a vállalkozás belső érintettje csak rossz szándékból kövesse el, az esetek mögött gyakran azonosítható anyagi kompenzáció, pszichológiai probléma vagy külső kezdeményezés.

A munkavállalók anyagi kompenzációja a kutatás során két szempontból elemezhető: (1) külső tényezőként (amikor egy külső entitás ajánl ellentételezést az információért); (2) belső változóként (a vállalkozás által kínált munkabér és egyéb juttatások).

A külső kezdeményező, aki összefüggésbe hozható az ipari kémkedéssel, kínálhat anyagi kompenzációt az információért cserébe, kémkedhet megbízásból, használhatja a zsarolás vagy megvesztegetés eszközeit, továbbá beépülhet olyan ellenőrző szervbe, amely a vállalkozás szervezését és működését vizsgálja. A döntéshozók kezében a versenyképes munkabér egy eszköz a munkavállalói hűség növelésére.

A belső érintettek által elkövetett ipari kémkedés mögött azonosíthatók pszichológiai faktorok a (1) fiatal generációk lojalitásának csökkenése, (2) több generáció vagy kultúra együtt történő munkavégzése, (3) a napi tevékenység közben elkövetett hibák, (4) személyes sérelmek és (5) személyiségzavarok.

Ezen változók gyakori előfordulása jelentős információbiztonsági kockázatot jelent az innovatív védelmi vállalkozásoknak. Vashisth és Kumar (2013) [180] korábbi kutatásuk során az incidensek mögött szintén feltártak a személyiséghez fűződő változókat, mint a kielégítetlen célok, ideológiai szerepvállalás és az elkövetett tettekért való felelősség hiánya. Noonan (2018) [173] a szervezet tudatos megkárosítása mögött olyan egészségügyi problémákat tárt fel, mint a depresszió és a különböző típusú személyiségzavarok.

A munkavégzés közben véletlen kezdeményezett információszivárogtatás kockázata növekedhet a versenypiaci nyomással, az iparágban jellemző képzett munkaerőhiánnyal (túlterhelt munkavállalók), a nem megfelelő vezetési gyakorlattal, továbbá rosszul kialakított információs rendszerrel. Ashenden (2018) [150] az alkalmazottak hanyagságát és gondatlanságát, Omar (2015) [135] a biztonságpolitika be nem tartását, továbbá Elifoglu és szerzőtársai (2018) [134] a munkavállalói stresszt, a munkavégzést szolgáló okoseszközök elvesztését és a naivitást azonosította, melyek véletlen esetek elfordulásához vezethetnek. A nem szándékos incidenseknél azonban felmerülhet a kérdés, hogy ténylegesen véletlen történtek-e.

A védelmi vállalkozások vezetőinek cselekedeteire és viselkedésére szintén hatást gyakorolnak a fejezetben fentebb felsorolt pszichológiai faktorok, továbbá a versenypiaci nyomás, a geopolitikai tényezők alakulása, és az anyagi kompenzáció. Abban az esetben, ha ezen tényezők miatt nem mutat etikus viselkedést a munkavállalók felé, nem támogatja az információbiztonsági kultúra kialakulását hatékony oktatással, továbbá nem csoportosít erőforrásokat az információbiztonsági rendszer megfelelő kivitelezésére, úgy jelentős kockázatnak teszi ki a vállalkozást. Nasheri (2004) [143], továbbá Vashisth és Kumar (2013) [180] szintén arra az eredményre jutottak, hogy a vezetési gyakorlat, mely negatív emóciókat idéz elő a munkavállalóban, hajlandóságot ébreszthet bennük a vállalkozás megkárosítására.

3.4.3. Az ipari kémkedés megelőzésére és észlelésére alkalmazott eszközök és módszerek (K3)

Az ipari kémkedés megelőzésére és észlelésére alkalmazható, a vezetők rendelkezésére álló eszközök közül kiemelt fontosságú a minden üzleti folyamatra kiterjedő információbiztonsági politika. Jelen kutatás alapján ez magában foglalja a (1) felelősségi körök meghatározását; (2) a humán erőforrás menedzselését; (3) a külső és belső kapcsolatok kezelését; (4) a szerződéses eszközöket; (5) és az incidensek szankcionálását.

Omar (2015) [135] korábbi kutatása során szintén vizsgálta, hogy milyen fejezeteket szükséges tartalmaznia a vállalkozásra szabott biztonságpolitikának, és a kritikus információk kiemelt védelmét, a hozzáférésére felhatalmazott személyek fokozott ellenőrzését, a belső sebezhetőségek folyamatos felülvizsgálatát, továbbá az alkalmazottak tevékenységének nyomon követését azonosította.

Az innovatív védelmi vállalkozások által az ipari kémkedés megelőzésére használt eszközök és módszerek kutatásából arról is levonható következtetés, hogy a döntéshozók mennyire tartják súlyos fenyegetésnek az ipari kémkedést. Az alkalmazott információvédelmi rendszerekből feltételezhető, hogy a megkérdezettek ismerik a fenyegetés természetét, azonban nem tartják magas kockázatnak, hogy az érintett vállalkozás áldozatul essen az ipari kémkedésnek. Mészáros és Tick (2021) [226] a magyar szervezetek körében végzett korábbi kvantitatív kutatása alapján a vezetők tisztában vannak az ipari kémkedés jelentette kockázattal, azonban a belső érintettek által megtestesített fenyegetést nem tartják jelentősnek.

A belső érintettek lojalitásának és motivációjának tudatos ösztönzése hatékonyan csökkentheti a vállalkozás ellen szándékosan elkövetett incidensek kockázatát. A menedzserek fontos feladata az olyan szervezeti kultúra kialakítása, melyben a belső érintettek „*jól érzik magukat*”. Az információbiztonsági kultúra fejlődésének támogatása oktatással és a potenciális kockázatokra való figyelemfelhívással segít beépíteni az információ tudatos védelmét a munkavállalók mindennapi tevékenységébe. Szintén hasznos vezetői eszközök a versenyképes bérezés biztosítása, továbbá a motiváló és ösztönző rendszerek alkalmazása.

Az ipari kémkedés megelőzésének és észlelésének fontos részét képezik a vállalkozás által alkalmazható információvédelmi eszközök, melyek hatékonyan védenek a külső, továbbá a szándékos és véletlen belső esetektől egyaránt, ezenfelül lehetővé teszik az azonnali beavatkozást. Az információvédelmi berendezések és a támogató szoftverek csak a megfelelő konfiguráció mellett képesek magasszintű védelmet biztosítani. A hozzáférést vezénylő rendszerek jelen kutatás során azon szoftvereket foglalják magukban, melyek a beléptető, a nyomon követő, a jelző- és a látogatói rendszer üzemelését támogatják. A biztonsági alkalmazások feladata védeni a vállalkozás kritikus információját az interneten keresztül történő támadásoktól, szándékos károkozástól, adatvesztéstől és információlopástól. A munkavégzést szolgáló digitális felületek felhasználóbarát kialakításával megelőzhetők az alkalmazottak által elkövetett hibák.

A korai figyelmeztető rendszer lehetővé teszi a belső érintettek tevékenységének megfigyelését, melynek során észlelhetők olyan viselkedésbeli változások, amelyek önmagukban nem rendelkeznek jelentőséggel, azonban gyakori előfordulás esetén érdemes figyelmet fordítani az érintett munkavállaló tevékenységére. Gheyas és Abdallah (2016) [190], továbbá Elifoglu és szerzőtársai (2018) [134] korábban már kutatták a korai figyelmeztető rendszer alkalmazásának előnyeit, mely a belső érintettek magatartását vizsgálva hívja fel a figyelmet az eset bekövetkezésének magas valószínűségére. Hills és Anjali (2017) [176] szerint már a kisebb magatartásbeli változások is mutathatnak olyan mintákat, amiket érdemes szem előtt tartani, azonban Noonan (2018) [173] kiemelte, hogy a jelentősebb változások – mint verbális kirohanások, a biztonságpolitika szándékos megsértése, vagy agresszív és konfrontatív magatartás – olyan figyelmeztető jelek, amelyeket már nem szabad figyelmen kívül hagyni. Pang és szerzőtársai (2014) [192], továbbá Carstens és szerzőtársai (2021) [191] eredményei alapján az alkalmazottak közösségi média aktivitásának analizálása is szolgáltathat adatokat az ipari kémkedés

gyanújának korai felismerésére. A belső érintettek monitorozása támogatja az ipari kémkedési kísérletek időbeni észlelését és azonnali beavatkozást tesznek lehetővé, azonban a folyamatos megfigyelés negatív hatással lehet a munkavégzésre.

A mesterséges intelligencia alapú eszközöket egyre több döntéshozó tervezi beépíteni az alkalmazott információvédelmi rendszerbe, mivel képes lesz felismerni és automatikusan blokkolni a potenciális fenyegetéseket. Aoun és szerzőtársai (2021) [201], továbbá Williams és szerzőtársai (2023) [202] szerint a mesterséges intelligenciával támogatott rendszerek sokkal kifinomultabb reakciókat lesznek képesek létrehozni egy információbiztonsági támadás esetén. Mohanta és szerzőtársai (2019) [197], továbbá Fadi és szerzőtársai (2022) [199] publikációi alapján a mesterséges intelligenciára épülő algoritmusok képesek a hálózaton belüli anomáliák észlelésére, a szükséges biztonsági mechanizmusok beindítására, a veszélyeztetett elemek elkülönítésére és a potenciálisan jogosulatlanul végrehajtott tevékenységek előrejelzésére is, melyek indokolhatják alkalmazását az ipari kémkedés kockázatának csökkentésére. Azonban abban a kérdésben, hogy ez a technológia hatékonyabbá fogja tenni a jövőben a belső érintettek rossz szándékának korai észlelését, a válaszadók véleménye megoszlott. Egyes alanyok úgy gondolták, hogy az emberi természet túl komplex ahhoz, hogy egy mesterségesen kialakított rendszer felismerje a cselekedeteik alapján a szándékaikat, bár a mesterséges intelligencia folyamatos fejlődése, ha nem is feltétlenül teljes mértékben, de közelebb visz az esetek feltárásához. Ezzel szemben Fadi és szerzőtársai (2022) [199] rámutatnak, hogy a mesterséges intelligencia az innovatív iparágak területén alkalmazva a közeljövőben képes lehet az adatokból olyan tudást előállítani, amelynek segítségével az emberekhez hasonló döntéseket hozhat.

Együttműködések során a fenyegetés csökkenthető a külső partner felülvizsgálatával, továbbá szerződéses eszközök alkalmazásával a tevékenység megkezdése előtt. Szintén hasznos eszköz az ügylet során használt kommunikációs csatornák pontos meghatározása és védelmének biztosítása. Közös tevékenység folytatása esetén a vállalkozások mérsékelheti az ipari kémkedés kockázatát az alkalmazott információbiztonsági eszközök összehangolásával. A 6. táblázat összefoglalja a kutatás során feltárt megelőzési és észlelési eszközöket az elsődleges feladatuk alapján.

Megelőzés eszközei	Észlelés eszközei
Minden üzleti folyamatra kiterjedő információbiztonsági politika	
○ Szabályozó eszközök ○ Felelősségi körök meghatározása ○ Humán erőforrás menedzsment ○ Kapcsolatkezelés ○ Szerződések ○ Kritikus információ kiemelt védelme [135] ○ Belső sebezhetőségek folyamatos felülvizsgálata [135]	○ Szankciók ○ Jogi lehetőségek [148]
Információvédelmi berendezések	
○ Belső offline hálózat ○ Külső adattárolóeszközök	○ Biztonsági kamerák ○ Beléptető rendszer ○ Jelző rendszer ○ Nyomon követő eszközök (személy, dokumentum vagy személygépkocsi)
Támogató szoftverek	
○ Hozzáférést vezénylő rendszerek ○ Információbiztonsági szoftverek ○ Felhasználóbarát felület ○ A potenciális eseteket előre jelző rendszerek [134, 190]	○ Blokklánc [195, 196, 197] ○ Gépi tanulás és mesterséges intelligencia [197, 199]
Belső érintettek	
○ Belső érintettek hűségének növelése ○ Szervezeti kultúra ○ Információbiztonsági kultúra ○ Versenyképes bérezés ○ Ösztönző rendszer ○ Munkavállalók előéletének ellenőrzése [193]	○ Belső érintettek monitorozása ○ Korai figyelmeztető rendszer ○ Tevékenység nyomon követése [135, 148] ○ Közösségi média aktivitás megfigyelése [191, 192]

6. táblázat: Az ipari kémkedés megelőzésének és észlelésének eszközei

Forrás: Saját szerkesztés a mélyinterjúk (n=42) és a szakirodalom alapján

3.4.4. Jövőbeni információbiztonsági fenyegetések várható természete (K4)

Bár a dinamikusan változó környezeti kontingencia tényezők mellett lehetetlen pontos hosszútávú előrejelzéseket készíteni, azonban a dolgozat írásának időpontjában jellemző ipari kémkedési módszerekből és eszközökből rövidebb távra előre lehet vetíteni. A digitális fejlődéssel az információlopás elkövetésére is több eszköz fog rendelkezésre állni, (1) mint az okostelefonok, melyek lehallgatására egyre modernbb technológiák válnak széles körben elérhetővé; (2) a kvantumszámítás, amely bármilyen titkosítást képes lesz feltörni; (3) vagy a *zero day* támadások, melyek a fejlesztők által még fel nem ismert rendszerhibákat használják ki.

Ugyanakkor az alanyok a legsúlyosabb jövőbeni fenyegetést a mesterséges intelligencia fejlődésében látják, mely hatékonyabb és célzottabb támadásokat tesz majd lehetővé.

Szintén az ipari kémkedés komplex problémakörét bővíti azon entitások piaci megjelenése, amelyek ágazatspecifikus információ megszerzését teljesítik szolgáltatás formájában.

Az ipar 4.0 jellemzője a gyártási berendezések digitális technológiákkal való összekapcsolása, mely számos hatékonyságnövelő előnye mellett információbiztonsági kihívásokat is jelent a védelmi vállalkozások döntéshozóinak. Williams és szerzőtársai (2023) [202] az innovatív védelmi vállalkozásoknál jellemző kisméretű automatizált gyártási rendszerek kibertechnológiával való integrációját kutatták, és arra az eredményre jutottak, hogy a megfelelő biztonsági ellenőrzések nélkül az új típusú rendszer a kibertizikai támadások növekedéséhez vezetett, ami új és jelentős globális fenyegetést jelent a védelmi vállalkozások számára.

A társadalmi változások szintén kihívások elé fogják állítani a védelmi vállalkozások vezetőit. A fiatal munkavállalók hűségének kérdése és az új generációk munkaerőpiacra való belépése is jelentősen meg fogja változtatni az információbiztonsági kultúra dinamikáját. A környezeti kontingenciák alakulásából levonható a következtetés, hogy a fiatalabb generációk körében gyakrabban fognak előfordulni személyes sérelmek, személyiségi zavarok és egyéb mentális problémák. A geopolitikai konfliktusok alakulásának hatására előreláthatólag a kémek és hackerek jelenléte tovább fog fokozódni a védelmi ipar területén. Az interjúalanyok véleménye szerint szintén információbiztonsági kockázatot jelent, ha a potenciális munkavállaló előéletének ellenőrzése nem biztosítható, egy olyan speciális ágazat területén, mint a védelmi ipar.

Az otthoni munkavégzés feltételezhetően részévé fog válni a társadalomnak annak ellenére, hogy az alanyok nem támogatják a tevékenység folytatásának ezen formáját az információbiztonsági kockázatok miatt. Tóth és Csiszárík-Kocsir (2022) [227] kvantitatív módszerrel kutatták a *home office* kérdését, és arra az eredményre jutottak, hogy a vezetők részéről ez a forma jelentősebb kontrollt igényel, továbbá a belső érintettek az otthoni munkavégzés során sokkal nagyobb számban követnek el olyan hibákat, amelyek információszivárgáshoz vezethetnek.

A mesterséges intelligencia evolúciója számos információbiztonsági fenyegetést hoz, azonban magasabb szintű védelmet is jelenthet, melyet a legtöbb interjúalany alkalmazni kíván a jövőben. Szintén problémát okozhat, hogy a belső érintettek megbíznak a digitális technológiákban, melyre megoldást kínál a *zero trust* elv alkalmazása, mely csökkentheti

a véletlen esetek kockázatát. A kritikus információk továbbítására számos megkérdozett javasolta a személyes átadást, azonban az előnyei mellett ez a módszer is számtalan kockázatot rejt.

Az Európai Unió számos kezdeményezéssel támogatja a területén működő védelmi vállalkozások közötti együttműködések kialakítását [112], így várhatóan a jövőben a kooperációk száma növekedni fog. Azonban a jövőben nem megoldható, hogy a közös tevékenységet folytató vállalkozások ne konfigurálják az információvédelmi rendszerüket, mert az alkalmazott eszközök közötti inkoherencia biztonsági résekhez vezethet.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A doktori értekezésben az ipari kémkedés jelentette fenyegetést vizsgáltam a védelmi iparban tevékenységet folytató kis- és középvállalkozásokra fókuszálva, kvalitatív kutatási módszert alkalmazva. Céloom olyan, empirikus adatokon alapuló, gyakorlatban alkalmazható eredmények definiálása volt, melyek támogatják a védelmi vállalkozások vezetőit az ipari kémkedés elleni küzdelemben. Az eredményekből arra a következtetésre jutottam, hogy az ipari kémkedés kockázatát alapvetően három különböző szinten szükséges kezelni. Ezek lehetnek az átfogó információbiztonsági politika, a belső érintettek jelentette fenyegetés, és a külső környezeti fenyegetés kezelése.

A kontingencia elméleti megközelítést alkalmazva nem törekszem egy univerzális, minden körülmények között és helyzetben jól működő információvédelmi rendszert definiálni, mivel minden vállalkozásra más belső és külső tényezők hathatnak ugyanabban az időben, így ez nem megvalósítható. Azonban céloom a döntéshozók számára olyan eszközrendszert meghatározni, melynek segítségével képesek a különböző helyzetek sajátosságait beazonosítani, és ezen szituációkban a legmegfelelőbb eszközöket alkalmazni. A fejezetben bemutatom az eredmények alapján megfogalmazott iránymutatást a vállalatspecifikus, holisztikus és szociotechnikai megközelítésű információbiztonsági rendszer kialakításához, mely figyelembe veszi a külső környezeti tényezőket, az üzleti folyamatokat és a belső érintetteket egyaránt.

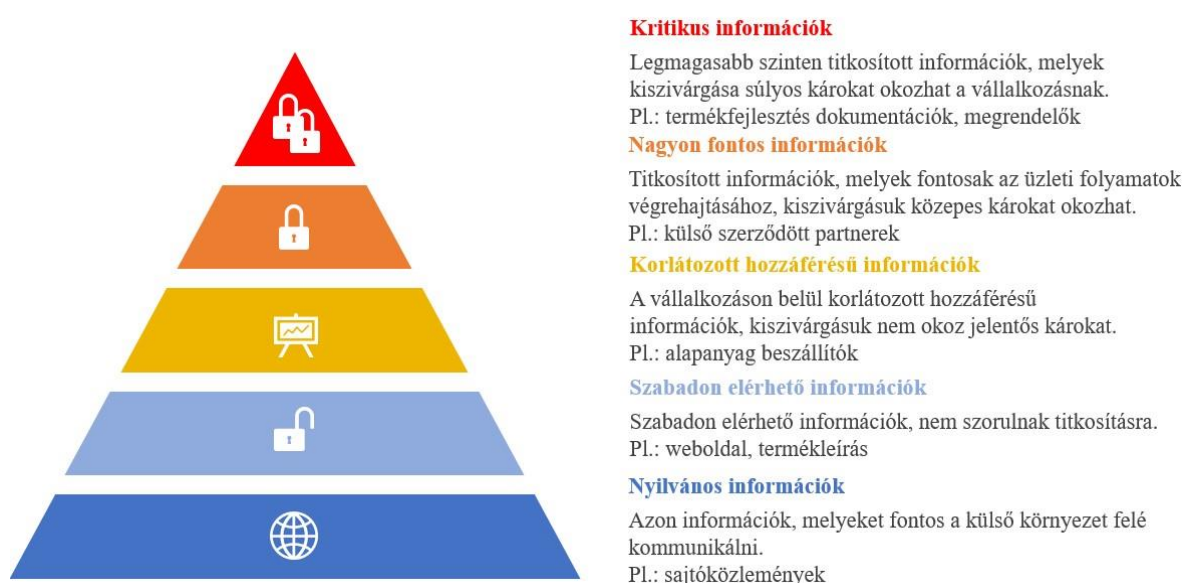
Az információbiztonsági politika szerepe az ipari kémkedés kockázatának csökkentésében

Az ipari kémkedés megelőzésére és észlelésére irányuló tevékenységet a belső kontingencia tényezőkre fókuszálva szükséges kezdeni, melynek célja azon folyamatok, eszközök és információk meghatározása, amelyeket védeni indokolt a fenyegetéstől

Első lépésben azonosítani indokolt minden, a vállalkozás zavartalan működéséhez nélkülözhetetlen belső tevékenységet, továbbá azok folytatásához szükséges összes eszközt és információt. A vizsgálat során azt szükséges felmérni, hogy milyen következményekkel járhat és károkat okozhat a szervezetnek, amennyiben bármely eszköz vagy információ illetéktelen kezekbe kerül. A rendszeres kockázatértékelést azért fontos elvégezni, hogy egy esetleges incidens bekövetkezte esetén kezelni lehessen a problémát, mielőtt még súlyosabb negatív hatása lenne a vállalkozásra nézve. A belső vizsgálat során szintén azonosítani szükséges azon vállalati gyenge pontokat, ahol

potenciálisan magasabb a kockázata a külső behatolásnak vagy információszivárgásnak. Célszerű ezen területek fokozott figyelme és gyakori felülvizsgálata.

Az információk osztályozására alkalmas módszer az információbiztonsági piramis modell használata, melynek során a piramis csúcsában kerülnek kategorizálásra a kritikus információk és azok titkos természete lefelé haladva csökken. A 12. ábra a teljesség igénye nélkül mutat be egy példát az információbiztonsági piramis modell alkalmazásáról.



12. ábra: Információbiztonsági piramis modell alkalmazása

Forrás: saját szerkesztés

Az üzleti folyamatokra vonatkozó információbiztonsági vizsgálat és a kockázatelemzés eredményeit fontos világosan kommunikálni az összes belső érintett felé, mert hatékonyan csak akkor képes működni a rendszer, amennyiben a munkavállalók megértik, hogy bizonyos információk miért kerültek kritikus besorolás alá. Ennek releváns részét képezi a lehetséges következményekre való figyelemfelhívás, továbbá minden információ besorolásának jól látható és könnyen értelmezhető jelölése.

A vizsgálat eredményei alapján meg lehet fogalmazni az **információbiztonsági politikát**, melyben a következő dokumentumoknak van kiemelt szerepe az ipari kémkedés elleni védekezésben. (1) A kritikus információ védelmére vonatkozó előírások, amik magában

foglalják a hozzáférési jogosultság menedzselését és az ügyiratkezelést. Ezen szabályok definiálják a feladat elvégzéséhez szükséges információhoz való hozzáférés körülményeit, feltételeit és felhasználási módját, ezáltal egy információszivárogtatási incidens során meghatározható a felelősségre vonható személyek köre. Bizonyos védelmi vállalkozásoknál indokolt lehet alkalmazni a legkisebb jogosultság elvét (*principle of least privilege*), mely irányelv szerint az alkalmazottak csak azon információkhoz férhetnek hozzá, mely szükséges a tevékenység elvégzéséhez. (2) A kockázatelemzés alapján a vállalkozás azon területeinek és üzleti folyamatainak definiálása, melyek gyakori felülvizsgálatot igényelnek az információszivargás elkerülése érdekében. (3) Az új munkavállalók ellenőrzésére, felvételére és alkalmazására vonatkozó szabályozások, melyekkel csökkenthető a rossz szándékkal rendelkező egyén beépülésének valószínűsége a vállalkozásba. (4) A belső érintettek feladatának, hatáskörének és felelősségének pontos definiálása. (5) A kapcsolatkezelésre vonatkozó előírások, melyek a külső érintettekkel való tevékenység folytatásának információbiztonsági szempontú menedzselését tartalmazzák. Mivel jelen geopolitikai környezetben jelentős a védelmi ipar területén történő vállalkozások közötti együttműködések ösztönzése, a dokumentumban definiálni szükséges a kooperációkra vonatkozó információbiztonsági irányelveket. (6) A külső szervezeti érintettek felülvizsgálatára vonatkozó szabályok definiálását indokolja, hogy az ipar speciális természete miatt sok megkérdőjelezhető szándékú és hátterű entitás folytat tevékenységet a területen. (7) Az információbiztonsági politikát ajánlott kiegészíteni a kockázatelemzés alapján azon dokumentummal, amely az ipari kémkedés bekövetkezése esetén életbe lépő, az üzleti folyamatok folytonosságát biztosító válságkezelési protokollt definiálja. (8) A szabályzat szintén tartalmazhatja az információlopás által okozott következmények értékelését támogató leírást. (9) Indokolt a vállalkozás által fejlesztett technológiai újdonságok, prototípusok tesztelésére vonatkozó szabályok rögzítése a dokumentumban, ugyanis fennállhat az innováció visszafejtésének veszélye. (10) Az állami közbeszerzésekre írt pályázati anyagok szabályozása is részét képezheti, mivel ezen ügyletek során a kritikus információ külső szereplővel való megosztása történik. (11) Fontos meghatározni, hogy az alkalmazott szerződéseknek (pl.: titoktartási és versenytilalmi szerződés vagy partnerségi megállapodás), mely részeket kell tartalmaznia, amikkel a szervezet a belső és külső érintettekkel szemben is védheti a kritikus üzleti információt. (12) Szankciók definiálása is indokolt az információbiztonsági politikában, melyeket jogilag elkövethet a vállalkozás, amennyiben egy szervezeti érintett az ipari kémkedés gyanújába keveredik.

(13) A dokumentumnak részét képezheti a belső érintettek vállalkozáshoz kötődő, külső tevékenységeinek felülvizsgálata, mint a konferenciákon és kiállításokon való részvétel vagy üzleti célú utazások. Ezek során szükséges feltárni, hogy mely vállalkozások képviselőivel kerültek kapcsolatba és milyen volt a beszélgetés természete, melyből levonható a következtetés, hogy véletlenül nem adott-e ki kritikus információt egy versenytársnak.

Az információbiztonsági politika szintűgy csak akkor célravezető, amennyiben a belső érintettek megismerik és mindennapi munkavégzés során alkalmazzák a benne foglaltakat, ami az alappillére az információbiztonsági kultúrának.

Az információbiztonsági kultúra fejlesztésének lehetőségei

Az innovatív védelmi vállalkozások vezetőinek számottevő támogatást nyújthat a munkavégzés során, amennyiben a szervezeten belül kialakul a jól működő információbiztonsági kultúra. Ez olyan belső csoportot jelent, melynek tagjai lojálisak és tisztelik a vállalkozást, tisztában vannak az ipari kémkedés kockázatával és negatív következményeivel, ezáltal az információ védelme a mindennapi munkavégzésük természetes aspektusává válik. Az információbiztonsági kultúra fejlesztésének legfontosabb eszköze a belső érintettek folyamatos oktatása (1) az alkalmazott információbiztonsági rendszer helyes használatára (mely magában foglalja a fizikai eszközök használatát és a számítógépes ismereteket egyaránt); (2) a titkos információk kezelésének helyes módjára (ügyszerkezelés, tárolás, felhasználás, továbbítás, archiválás, megsemmisítés); (3) a külső érintettekkel való kommunikációnak és egyéb tevékenység folytatásának információbiztonsági aspektusaira; (4) és a zsarolás és megvesztegetés elleni védekezésre.

Szintén fontos részét képi a munkavállalók figyelmének felhívása (1) az információbiztonsági politikában foglaltakra; (2) az információk kritikus természetének okára; (3) a vállalkozást fenyegető információbiztonsági kockázatokra és azok káros következményeire; (4) az okoseszközök és közösségi média használatának veszélyeire; (5) és az esetleges belső incidensek elkövetése után járó szankciókra.

Az információbiztonsági kultúra támogatásának szignifikáns módszere a világos, folyamatos és tiszteletteljes kommunikáció a vállalkozás összes belső érintettjével. A felelősségek és feladatok pontos definiálása is hozzájárul, hogy a munkavállalók tisztában legyenek az elvárásokkal. A belső érintettek munkáját motiváló és elismerőrendszerek

bevezetése, a személyre szabott egyéni célok megfogalmazása, továbbá a versenyképes bér biztosítása hozzájárul a munkavállalók vállalkozáshoz fűződő pozitív attitűdjének támogatásához. A megfelelő kultúra kialakításához a vezetőknek figyelembe kell venni és helyesen menedzselni a szervezeten belüli konfliktusokat, továbbá a generációs és kulturális különbségeket. Szintén ajánlott módszer a zero bizalom elv (*zero trust*) bevezetése, mely mérsékelheti az alkalmazottak digitális eszközök felé kialakult túl nagy bizalmából eredő hibák előfordulását.

Amennyiben a körülmények elkerülhetetlenné teszik az otthoni munkavégzés (*home office*) folytatását, úgy javasolt a munkavállalók oktatása az ezzel járó információbiztonsági kockázatokra.

A védelmi kis- és középvállalkozásokra ható külső környezeti kontingencia tényezők vizsgálata

A belső információbiztonsági rendszer tervezése és megvalósítása előtt az innovatív védelmi vállalkozások vezetőinek kiemelt fontosságú feladata a külső környezeti kontingencia tényezők tanulmányozása, melyhez keretrendszert biztosít jelen értekezés, ugyanis hatékonyan csak azon fenyegetés ellen képesek védekezni, melynek ismerik a természetét. Az ipari kémkedés kockázatának csökkentése mellett a környezet monitorozása során a vállalkozás felismerhet olyan katalizáló faktorokat, melyek ötletet adnak innovációk fejlesztéséhez. A felsorolt tényezőket indokolt megfigyelni és értelmezni:

- **Gazdasági tényezők**, mint versenytársak tevékenysége, piaci környezet, árpolitika, lehetséges célpiacok, export lehetőségek, együttműködések, finanszírozási források, infláció és makrogazdasági feltételek.
- **Politikai faktorok**, példának okáért jogszabályok és szabályozások, export szabályozások és nemzetközi szankciók, nemzeti stratégia, védelmi ipar fejlesztési stratégia, diplomáciai kapcsolatok és együttműködések, védelmi kiadások és finanszírozási források, beszerzési politika és tenderek.
- **Geopolitikai változók**, mint nemzetközi konfliktusok és háborúk, továbbá jelen helyzetben ide került besorolásra az energiaválság.
- **Ellátási lánc**, többek között nyers- és alapanyag ellátás, logisztikai útvonalak biztonsági kérdései és beszállítók.

- **Technológiai fejlődés**, példának okáért a piac szereplőinek új fejlesztései, egymással szemben álló felek által bevetett innovációk, mesterséges intelligencia és ipari kémkedésre alkalmas újdonságok.
- **Kiberbűnözés**, az interneten történő támadások evolúciója.
- **Társadalmi tényezők**, például munkaerő kínálat, oktatás, generációs változások, kulturális különbségek és migráció.
- **Természeti katasztrófák**, melyek ellátási bizonytalansághoz vezetnek vagy a károk enyhítésére alkalmasak lehetnek bizonyos védelmi innovációk.

Ezen változók mind okozhatnak egy államnak/vállalkozásnak olyan információkra való igényt, melyet nem képesek vagy hajlandók előállítani, így annak beszerzésére az ipari kémkedés eszközeihez és módszereihez folyamodhatnak.

Az innovatív védelmi kis- és középvállalkozásoknál kialakítható információbiztonsági rendszer sajátosságai

Az információbiztonsági rendszer tervezése egy rendkívül komplex folyamat, melynek során az értekezésben bemutatott vállalati belső és külső kontingencia tényezők vizsgálata értékes információval látja el a döntéshozókat. Ezenfelül az ipari kémkedés elleni hatékony védekezés csak úgy valósítható meg, ha a rendszer részei az üzleti folyamatokra vannak hangolva, továbbá a különböző részek között nem alakul ki inkoherencia. Ez magában foglalja a dolgozatban részletesen bemutatott fizikai elemeket és szoftvereket, továbbá azok konfigurációját. Információbiztonsági szempontból előnyösebb, amennyiben a rendszer kialakítását és folyamatos karbantartását a szervezet belső érintettje végzi, azonban a kis- és középvállalkozások nem mindig rendelkeznek az erre szükséges költségvetéssel. Ebben az esetben végezheti a tevékenységet egy külső szerződött partner, azonban a közös munka megkezdése előtt csökkentheti az információlopás kockázatát a megbízott vállalkozás alapos ellenőrzése és szerződéses eszközök alkalmazása.

A vezetőknek törekedni kell arra, hogy minden alkalmazott csak annyi kritikus információhoz férjen hozzá, amennyit az aktuális feladata megkövetel (legkisebb jogosultság elve). Szintén fontos figyelemmel kísérni, hogy a belső érintettek a munkavégzéshez megfelelő mentális állapotban vannak-e, azonban ez támogatható a munkavállalói elégedettséget fejlesztő gyakorlatok alkalmazásával. Bár az alkalmazottak viselkedését megfigyelő rendszerek hatékonysága megkérdőjelezhető, azonban az együtt

dolgozó egyének is észrevehetnek egymáson olyan magatartásbeli változásokat, amelyeket érdemes a vezetőknek kezelni, diszkrét módon. A nyilvános felelősségre vonás semmilyen körülmények között sem javasolt, mert következményképp a belső érintett a vállalkozás ellen fordulhat.

Bár az ipari kémkedésre alkalmas eszközök fejlődnek, azonban az elmúlt évtizedben nem jelent meg a területen olyan diszruptív innováció, amely alapjaiban formálná át a vállalkozások által alkalmazható információvédelmi eszközöket. Az internet és az okoseszközök továbbra is fenyegetést jelentenek, a fizikai berendezések rendszerét fel lehet törni, és a megbízott rossz szándékú személyek kémkednek az igényelt információ után. Ebből levonható a következtetés, hogy amennyiben egy vállalkozás kialakít egy jól megtervezett, átgondolt, rugalmas és bővíthető, minden üzleti folyamatra és a belső érintettek tevékenységére is kiterjedő információbiztonsági rendszert, az folyamatos felülvizsgálat és karbantartás mellett legalább középtávon csökkentheti az ipari kémkedés fenyegetését. Mivel a kis- és középvállalkozásoknak korlátozott erőforrásokkal kell gazdálkodniuk, így olyan hatékony és megfizethető védelmi megoldásokra van szükségük, amelyek megfelelnek az egyedi igényeiknek. Ez a szemlélet jelentősen csökkentheti az információbiztonság fenntartásának pénzügyi terheit. A 13. ábra szemlélteti az információbiztonsági rendszer kialakításának folyamatát.

1. Mit kell védeni?

Belső kontingencia tényezők vizsgálata, kockázatelemzés és információk besorolása.

Információbiztonsági politika

2. Kinek kell védeni?

Vezetők és alkalmazottak, oktatás, figyelemfelhívás és tudatosság, motiváció és elismerés.

Információbiztonsági kultúra

4. Mivel kell védeni?

Információbiztonsági rendszer, vállalatspecifikus, minden folyamatra kiterjedő, átgondolt, rugalmas és bővíthető, hogy sokáig szolgálja a vállalkozást.

Folyamatos karbantartás és felülvizsgálat.

3. Mitől kell védeni?

Külső kontingencia változók folyamatos megfigyelése és elemzése. Katalizáló faktorok észlelése.

Külső információigény → ipari kémkedés.



13. ábra: Információbiztonsági rendszer kialakítása.

Forrás: saját szerkesztés

Sokan feltételezik, hogy a mesterséges intelligencia gépi tanulással támogatva nagy előrelépést hoz az információbiztonság területén, ugyanis képes lesz észlelni és időben beavatkozni az általa gyanúsaként vélt események esetén. Azonban véleményem szerint nem fog tudni a közeljövőben olyan döntést hozni, amely kizárja a folyamatból a felelősségre vonható humán tényezőt. A meghatározó döntés megalkotásának joga az arra felhatalmazott belső érintett kezében marad.

Új tudományos eredmények

Összegzésként bemutatom a szekunder és a primer kutatás alapján definiált téziseket. A témában releváns szakirodalom feldolgozása az értekezés elméleti keretének kialakításában nyújtott segítséget. A kvalitatív kutatás során célkitűzésem azon eredmények feltárása volt, melyek a gyakorlati alkalmazás során támogatják az innovatív védelmi kis- és középvállalkozások vezetőit a kritikus információ ipari kémkedéstől való védelmében.

Tézis 1.

A védelmi iparban tevékenységet folytató innovatív kis- és középvállalkozásoknak stratégiai szerepük miatt kiemelt figyelmet szükséges fordítani a kritikus információ védelmére, amihez minden olyan külső környezeti változót folyamatosan monitorozni és elemezni szükséges, melyek közvetlenül vagy közvetve hatást gyakorolnak a tevékenység folytatására. A geopolitikai feszültségek létfontosságúvá tették, hogy minden európai ország képes legyen saját haderejével védekezni a háború eszkalálódása esetén. Azonban ennek teljesítése érdekében a korábban leépített és elhanyagolt védelmi ipar fejlesztése kiemelkedő jelentőségűvé vált, melyben meghatározó szerepet töltenek be a védelmi innovációk területén kiemelkedő kis- és középvállalkozások. Az agilis védelmi KKV-k a külső környezeti kontingenciák elemzésével gyorsan képesek reagálni a felmerült igényekre. A stratégiai szerepük miatt a védelmi vállalatokat kiemelten fenyegeti a gazdasági- és ipari kémkedés veszélye, mely kockázatának csökkentése kritikus fontosságú feladat. A külső fenyegetés eredhet gazdasági, politikai, geopolitikai, társadalmi, technológiai vagy természeti változókból. Összegezve, bármely külső kontingencia tényezőből, mely olyan hirtelen jelentkező információigényt vált ki az ágazat valamelyik szereplőjéből, amelyet nem képes vagy hajlandó a rendelkezésre álló erőforrásokkal kielégíteni, ezáltal ipari kémkedést idézhet elő. A környezet folyamatos elemzése nem csak információbiztonsági szempontból

támogatja a vállalkozást, hanem lehetőséget biztosít azon katalizáló faktorok észlelésére, melyek hatására megszülehet az innovatív ötlet.

(Lásd: 3. ábra, 28. oldal; 6. ábra, 58. oldal; 7. ábra, 67. oldal; 11. ábra, 80. oldal. Kapcsolódó publikációk: P2, P5, P6, P7, P8)

Tézis 2.

A védelmi iparban tevékenységet folytató innovatív kis- és középvállalkozásoknak az információvédelmi rendszer kialakítása során minden olyan belső folyamatot, továbbá az azokat támogató humán tényezőt, információt, berendezést és eszközt vizsgálni szükséges, melyek a vállalkozás zavartalan működéséhez nélkülözhetetlenek. Ezen szempontok figyelembevételével lehet megfogalmazni az információbiztonsági politikát, továbbá kialakítani az információbiztonsági rendszert. **Az ipari kémkedés kockázatának hatékony mérséklése csak szociotechnikai szemlélettel kialakított, vállalatspecifikus rendszerrel lehetséges.** Fontos része a hatékony védekezésnek a komprehenzív információvédelmi rendszer, melynek részei az üzleti folyamatokra hangoltak, fizikai és digitális elemei megfelelően konfiguráltak. Az információbiztonsági kultúra támogatásával a kritikus információk védelme az alkalmazottak tudatos és tudatalatti tevékenységének természetes részévé válhat.

(Lásd: 9. ábra, 75. oldal; 6. táblázat, 88. oldal; 13. ábra, 97. oldal. Kapcsolódó publikációk: P1, P3, P4)

Tézis 3.

Az ipari kémkedés szempontjából a kiemelkedő innovációs hajlammal rendelkező védelmi kis- és középvállalkozások számára a legkritikusabb tényező a humán faktor, mely megnyilvánulhat szándékosan elkövetett esetek, és véletlen hibákból eredő incidensek formájában. A humán tőke a legértékesebb eszköze egy innovatív vállalkozásnak, azonban bennfentes ismeretei és a rendszerhez való hozzáférése miatt jelentős kárt képes okozni szervezetnek. A belső érintettek cselekedhetnek külső befolyás alatt vagy önkéntesen. Követhetnek el információlopást személyiségzavarok, személyes sérelmek, generációs vagy kulturális különbségek okán, a vezetővel szemben kialakult negatív attitűd miatt, vagy munkavégzés során elkövetett hibájuk vezethet információszivárgáshoz. Mindazonáltal az alkalmazottak ritkán követnek el ipari

kémkedést pusztán rossz szándék által vezérelve, jellemzően az anyagi vagy egyéb jellegű kompenzáció motiválja őket.

(Lásd: 6. ábra, 58. oldal; 5. táblázat, 44. oldal. Kapcsolódó publikációk: P1, P3, P4)

Tézis 4.

Az ipari kémkedés elleni védekezésben meghatározó szerepet töltenek be az innovatív védelmi kis- és középvállalkozások döntéshozói. Képességeik fejlesztése és figyelmük felhívása a fenyegetés természetére és a lehetséges következményekre nagyban növelheti vállalkozás biztonságát. A vezetőknek tisztában kell lenni az ipari kémkedés növekedésének globális trendjeivel, továbbá azon külső kontingencia tényezőkkel, amelyek ezt okozzák. Feladataik közé tartozik a belső tényezők vizsgálata, a kockázatok értékelése, a sérülékeny pontok azonosítása, és ezeket figyelembe véve az információbiztonsági politika definiálása és folyamatos aktualizálása. Tevékenységüket nagyban támogatja az információbiztonsági kultúra, mely megvalósításának egyik fő eszköze a belső érintettek oktatása. Az információbiztonsági rendszer kialakításának és rendszeres felülvizsgálatának a döntéshozók fokozott felügyelete mellett kell történni.

(Lásd: 13. ábra, 97. oldal. Kapcsolódó publikációk: P1, 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 válnak célzottabbá és hatékonyabbá. Az évtizedek óta zajló technológiai fejlődés tagadhatatlan (például dróntechnológia), azonban ezek használatát ipari kémkedésre nem elterjedt. A gyakorlatban az évtizedek óta alkalmazott módszereket használják kémkedésre, mint a személyes beépülés, helységek megfigyelése, interneten keresztül történő behatolás vagy kukabúvárkodás. Mivel a kis- és középvállalkozások jellemzően korlátozott erőforrásokkal rendelkeznek, ezáltal nem minden esetben tudnak forrásokat csoportosítani a legmodernebb információbiztonsági eszközök alkalmazására. Ezzel szemben egy jól átgondolt, rugalmas és bővíthető vállalatspecifikus rendszer folyamatos fejlesztés és karbantartás mellett éveken keresztül hatékonyan mérsékelheti az ipari kémkedés jelentette kockázatot. Azonban a napjainkban jellemző dinamikus technológiai

fejlődés mellett bármikor megjelenhet egy olyan diszruptív innováció, amellyel szembeni védekezésre nincsenek felkészülve a dolgozat írásának időpontjában alkalmazott információvédelmi rendszerek, ami szintén alátámasztja az 1. tézist, mely szerint a döntéshozók feladata a környezeti fenyegetések folyamatos monitorozása.

Az eredmények elméleti hasznosíthatósága

Jelen kvalitatív kutatás eredményei a védelmi iparban működő innovatív kis- és középvállalkozásokat 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, 132, 133, 134, 135, 136, 137, 149], így a jelen doktori értekezésben definiált eredmények hozzájárulnak a tudományos probléma elméleti hiányosságainak mérsékléséhez.

A kutatás során kontingencia elméleti megközelítésből vizsgáltam a védelmi ipar területén tevékenységet folytató innovatív kis- és középvállalkozásokat fenyegető ipari kémkedés külső és belső kockázatait. Az 1960-as években definiált menedzsment módszer a döntéshozókat támogatja a vállalkozásra ható tényezők azonosításában, hogy az aktuális körülményekhez legjobban illeszkedő szervezési módszert legyenek képesek meghatározni, azonban az elmúlt évtizedek során ezek a faktorok jelentős átalakuláson mentek keresztül. Jelen dolgozatban az ipari kémkedést a kontingencia elmélet alapján elemeztem, levonva a következtetést, hogy a módszer a napjaink dinamikusan változó környezetében is aktuális és releváns megközelítés. Az értekezés azon külső és belső kontingencia tényezőkkel egészíti ki a problémát vizsgáló szakirodalmat, melyek globális szinten hozzájárulnak az ipari kémkedéshez fűződő esetszámok növekedéséhez. A kutatómunka során az orosz-ukrán fegyveres konfliktust is a védelmi iparban működő kis- és középvállalkozásokra ható kontingencia változóként azonosítottam, amely probléma területén akadémiai megközelítésből szintén elméleti hiányosság azonosítható.

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

A dolgozatban 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 [10, 150], jogi [10, 138, 151], és a külső tényezők szempontjából vizsgálják [152], kevés tudományos figyelmet fordítva a belső fenyegetésre [11, 15, 130, 137, 150]. Azonban az értekezésben definiált elmélet magában foglalja a belső érintettek által elkövetett szándékos és véletlen incidensek mögött azonosított tényezőket is. A belső érintettek által előidézett **véletlen** esetek bekövetkezhetnek emberi természetből eredő változók okán (mint hiba elkövetése, hanyagság, naivság, felelőtlenség, fáradtság, stressz vagy *multitasking*), gazdasági vagy geopolitikai faktorok okozta nyomás hatására, különböző generációk vagy kultúrák közös munkavégzése során történő félreértések miatt, vagy az alkalmazott információbiztonsági és IT rendszer hiányos/nem megfelelő kialakítása platformot biztosít a nem kívánt incidenseknek. A **szándékos** eseteket motiválhatja a gazdasági vagy geopolitikai kontingencia változók miatti magas kereslet a kritikus információ iránt, állhat mögötte a munkavállalók hűségének kérdése, nem megfelelő vezetési gyakorlat, pénzügyi nyereségvágy, személyes sérelmek (például etikátlan vezetői viselkedés miatt) vagy különböző személyiségzavarok. Az ipari kémkedés pszichológiai szempontú megközelítéséből kevés a tudományos publikáció, mely hiányosságot jelen dolgozat kíván mérsékelni.

A kutatás eredményei hozzájárulnak a menedzsment tudományok fejlesztéséhez a gazdasági és ipari kémkedés kockázatának csökkentésére alkalmazható, empirikus adatokon alapuló gyakorlatok definiálásával, továbbá az ipari kémkedés elkövetésére alkalmas eszközök és módszerek közeljövőben várható természetének bemutatásával, alapot biztosítva a kutatóknak a téma mélyebb kifejtésére. Bár a digitalizáció szempontjából elérhető tudományos publikációk a jövőbeni információbiztonsági fenyegetésekről [177, 202, 205], 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 keretrendszer 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.

Az eredmények gyakorlati hasznosíthatósága

Az értekezés eredményei betekintést nyújtanak a védelmi ipart fenyegető ipari kémkedés komplex jelenségébe, így hasznos információkkal szolgálhatnak az innovatív vállalkozások vezetőinek. Ennek okán fontosnak érzem, hogy a definiált elmélet a tudományos körök mellett azon döntéshozók számára is elérhető legyen, akiknek a mindennapi üzleti gyakorlatára lehet jelentős hatással. 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 fókuszba kiterjedt a vállalkozásokat fenyegető külső és belső kontingencia tényezőkre egyaránt, ezáltal keretrendszer nyújt azon változók azonosításához, amelyekkel szemben védeni szükséges a kritikus információt. A globális esetszámok növekedését okozó gazdasági és geopolitikai fakorok 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, IT rendszer fejlesztésének szempontjait ismertető eredmények gyakorlati jelentősége, hogy felhívja a döntéshozók figyelmét a belső érintettek IT ismereteinek hiányosságaira, így a véletlen elkövetett hibák csökkentése alkalmas könnyen kezelhető és felhasználóbarát rendszer kialakításának fontosságára. A dolgozat szintén támogatást nyújt azon berendezések és szoftverek információbiztonsági tényezők alapján történő kiválasztásában, melyek segíthetik a rendszer tervezését és végrehajtását. Az információvédelmi rendszer kialakítása során a kis- és középvállalkozásoknál gazdasági szempontokat is figyelembe kell venni, mivel ezek

bevezetése és üzemeltetése finansziális terhet jelenthet. Az értekezésben bemutatott rendszer megvalósítása során azonban lehetőségük van a vezetőknek a rendelkezésükre álló erőforrások alapján meghatározni az eszközöket és módszereket, melyek a költséghatékonyság mellett is megfelelő mértékben csökkentik az ipari kémkedés kockázatát.

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.

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. A definiált elmélet támogatja a vállalkozások döntéshozóit a fenyegetés természetének megértésében, így segítve őket abban, hogy hatékonyabban értékeljék az üzleti kockázatokat és megfelelő döntéseket hozzanak az információbiztonság javítása érdekében.

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

A kutatás limitációja

Minden kutatás során fontos azonosítani a lehetséges korlátokat, amelyek befolyásolhatják az eredmények megbízhatóságát és általános érvényességét. Jelen értekezés elkészítése során az interjúalanyok készséggel álltak rendelkezésre, azonban feltételezhető, hogy a téma érzékeny jellege miatt bizonyos tényezőket nem osztottak meg vagy megváltoztattak, ami torzíthatja az eredményeket. Ugyanez a jelenség

vonatkoztatható a szekunder kutatásra is, mivel a vállalkozások jellemzően nem jelentik az eseteket a hatóságoknak, és amennyiben ez mégis megtörténik, úgy a nyomozás dokumentumai titkosításra kerülnek. Ha az incidens médiafigyelmet kap, akkor még nehezebb kiszűrni annak valóságtartalmát, ezáltal a témában korábban publikált eredmények sem minden esetben tükrözik a teljes valóságot. Szintén ezen okoknál fogva a definiált probléma kvantitatív kutatása gyakorlati felhasználásra alkalmatlan eredményeket hozhat.

A definiált tudományos probléma kutatásának korlátai között azonosítható, hogy a lehetséges negatív körülményektől tartva vállalkozások ritkán jelentik az ipari kémkedés gyanúját a hatóságok felé, ha mégis értesítik a hatóságokat, az incidens hivatalos vizsgálata szigorú titoktartási intézkedések keretei között megy vége [12, 13, 14, 15]. Szintén torzíthatja az eredményeket, hogy az információ jogtalan eltulajdonítása nem jár azonnal észrevehető, kézzel fogható veszteséggel, így előfordul, hogy a vállalkozás egyáltalán nem, vagy csak hosszabb idő után szembesül a történetekkel [14]. Ezen limitációk nehezítik a terület kvantitatív és kvalitatív vizsgálatát egyaránt.

A szakirodalom feltárása során azzal a nehézséggel szembesültem, hogy az ipari kémkedés nem rendelkezik általánosan elfogadott definícióval [13, 130, 131], a terminológiahasználat nem konzisztens, kevés az elérhető releváns tanulmány [131, 138], és a tudományos probléma vizsgálata interdiszciplinárisan elkülönülve történik [130].

Az ipari kémkedés komplex problémakörének multidiszciplináris természete okán számos különböző tudományterületet érint, így a vizsgálat során jelen értekezés keretei miatt néhány tényező feltáratlanul maradhatott. Ennek ellenére a dolgozat írása közben legjobb tudásom szerint törekedtem az eredmények minél teljesebb körű bemutatására, azonban bizonyos tudományterületeken (mint pszichológia és informatika) a definiált elmélet mutathat hiányosságokat.

A kutatásban számos európai ország képviselője mellett nagy számban vettek részt magyar megkérdezettek, ami korlátozhatja az eredmények átvihetőségét. A társadalmi és kulturális különbségek Európán belül is hatással lehetnek az ipari kémkedés megítélésére és a védekezési gyakorlatokra, így ezeket is figyelembe kell venni az eredmények értelmezése közben.

A kvalitatív eredmények megerősíthetőségének mélyreható bizonyítása longitudinális vizsgálatot igényelne, amelyre jelen dolgozat keretei között nem volt lehetőség, azonban

a három szakaszban készített mélyinterjúk közel azonos eredményei részben igazolják ezt a kritériumot.

A bemutatott limitációk ellenére a kutatómunka során végig törekedtem az ipari kémkedés komplex problémájának és a kockázatcsökkentési lehetőségek minél mélyebb feltárására.

Jövőbeni kutatási irányok

Jelen kvalitatív kutatás átfogó képet ad az ipari kémkedés természetéről és az innovatív védelmi kis- és középvállalkozások által alkalmazható védekezési lehetőségekről, azonban a kutatási probléma terjedelme és jelen értekezés keretei okán a feltárt tényezőket részletekbe menően nem vizsgálja. Fontosnak tartom kiemelni azokat a területeket, melyek további kutatásra szorulnak a probléma teljes körű megértéséhez és a fenyegetés hatékony kezeléséhez.

További kutatásra javaslom a belső érintettek által elkövetett ipari kémkedés pszichológiai aspektusainak vizsgálatát. A belső fenyegetés mögött álló motivációk és pszichológiai faktorok mélyebb megértése segítheti a vállalkozások döntéshozóit azon esetek korai észlelésében, amikor egy ártó szándékú alkalmazott potenciálisan veszélyt jelent a vállalkozásra.

Az információbiztonsági kultúra fejlesztésének lehetőségei szintén olyan kutatási irányt jelentenek, melyek a gyakorlatban hasznosítható eredményekkel szolgálhatnak a vállalkozások számára. Olyan alkalmazható módszerek és fejleszthető képességek definiálása lenne célravezető, amelyek hozzájárulnak ahhoz, hogy a belső érintettek valamennyi tettének részévé váljon az információ tudatos és tudatalatti védelme egyaránt.

További kutatásra javaslom az ipari kémkedés hatását a modern gyártórendszerekre. Az ipar 4.0 része a fizikai gyártási rendszerek kibertechnológiával való integrációja, ami számos új információbiztonsági kihívást jelent a védelmi vállalkozásoknak.

A környezetben végbemenő társadalmi átalakulások is hoznak olyan új információbiztonsági fenyegetéseket, melyek mélyebb feltárása fontos az ipari kémkedés elleni hatékony védekezés szempontjából. Ez magában foglalja a munkaerőpiacon tapasztalható generációs különbségeket, továbbá a különböző kultúrák közös munkája során tapasztalható eltérések jelentette újszerű menedzsment kihívásokat.

Szintén aktuális kutatási terület lehet az elhúzódó orosz-ukrán konfliktus hatása a különböző európai stratégiai iparágakat fenyegető ipari kémkedésre. A geopolitikai feszültségek miatt fokozódó probléma által kiemelten fenyegetett ágazatok feltárása, továbbá az ipari kémkedés különböző dimenzióinak megértése lehetővé teszi a vállalkozásoknak, hogy jobban felkészüljenek az egyedi kihívásokra és a változó körülményekre.

Az értekezés során alkalmazott kvalitatív kutatási technika hasznos eszköz volt az ágazatspecifikus empirikus adatok feltárásához, azonban a módszer természeténél fogva nem eredményez reprezentatív eredményeket. Mindazonáltal a definiált elmélet jó alapot biztosít bizonyos érintett területek további kvantitatív vizsgálatához. A kvantitatív vizsgálat folytatása előtt ajánlom a kutatók figyelmébe a jelen értekezésben bemutatott kutatási limitációkat, mert az ismertetett tényezők a számszerűsített eredmények számottevő torzulásához vezethetnek, ami jelentősen csökkentheti a kutatás gyakorlati alkalmazhatóságát.

A kutatómunkám során felmerült egy érdekes tudományos probléma az innovációk megítélésével kapcsolatban, amely vonatkoztatható az ipari kémkedés eszköztárára, a védekezési eszközökre és a diszruptív védelmi technológiai újdonságokra egyaránt. Azt feltételezi, hogy bár mindhárom említett kategóriában vannak diszruptív innovációk, azonban a gyakorlati felhasználás során ezekre nem mindig van igény, mert sokan ragaszkodnak a jól bevált régi eszközökhöz, és nem szívesen változtatnak azok alkalmazásán. Azonban ez ellentmond az értekezésben bemutatott vállalkozások küldetésével, az innovatív működésre való törekvéssel. Ez szintén egy olyan multidiszciplináris probléma, amely számos tudományos terület együttműködését igényeli, mivel vizsgálható a műszaki, pszichológiai és a társadalomtudományok fókuszából egyaránt. Úgy gondolom, hogy a jelen innovatív technológiai környezetben ez egy olyan irány, amelyet érdemes tovább kutatni, mind az ipari kémkedés, mind a védelmi technológiák szempontjából.

Az értekezés célja, hogy az ipari kémkedés multidiszciplináris problémájának mélyebb megértését tegye lehetővé. A kutatás során szerzett elméleti ismeretek támogatják a tudományos közösség fejlődését, miközben arra ösztönzhetik a kutatókat, hogy további mélyreható elemzéseket folytassanak az ipari kémkedés területén. Az empirikus eredmények segíthetik az innovatív védelmi kis- és középvállalkozások vezetőit a

probléma megértésében és az ipari kémkedés jelentette információbiztonsági kihívások elleni hatékony védelmi stratégiák kifejlesztésében. A dolgozat hozzájárul ahhoz, hogy a jövőben hatékonyabb megoldásokat lehessen meghatározni az ipari kémkedés kockázatának mérséklésére, amelyek lehetővé teszik a kutatott probléma veszélyeinek és hatásainak csökkentését, támogatva egy fenntarthatóbb és biztonságosabb ipari környezet kialakulását. Az értekezés eredményei fontosak lehetnek az ipari kémkedés elleni globális erőfeszítésekben, miközben megerősítik a vállalkozások védekezőképességét a 21. század információbiztonsági kihívásaival szemben.

AZ ÉRTEKEZÉS TÉMÁJÁHOZ KAPCSOLÓDÓ PUBLIKÁCIÓK

- [P1] Anikó Kelemen-Erdős – Alexandra Ágnes Mészáros (2023): Industrial Espionage from a Human Factor Perspective. *Journal of International Studies*– Megjelenés alatt
- [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 (2023): The Significance of 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 (2023): A kontingencia elmélet alkalmazása az innovatív kis- és középvállalkozások vizsgálata során az európai védelmi iparban. *HADMÉRNÖK* 18(3) – Megjelenés alatt
- [P7] Mészáros Alexandra Ágnes – Tóth István Márk – Csiszár-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 – Csiszár-Kocsir Ágnes (2022). A védelmi ipar lokális gazdaságra gyakorolt hatásának kvalitatív vizsgálata. *Vállalkozásfejlesztés a XXI. században*, 2022/2, pp. 193-206.
- [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

IRODALOMJEGYZÉK

- [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] 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)
- [8] 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>
- [9] 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>
- [10] 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>
- [11] KELEMEN-ERDŐS A. – MÉSZÁROS A. Á.: Industrial Espionage from a Human Factor Perspective; Journal of International Studies (2023) (Megjelenés alatt.)
- [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] 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>
- [15] 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
- [16] 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>
- [17] 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.
- [18] 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>
- [19] MASON, J.: *Qualitative Researching*; London, Sage Publications Ltd 2002.
- [20] SCANLAN, C. L.: *Preparing for the Unanticipated: Challenges in Conducting Semi-Structured, In-Depth Interviews*; London, SAGE Publications Ltd 2020.
- [21] MORRIS, A.: *A Practical Introduction to In-depth Interviewing*; London, SAGE Publications Ltd 2015. ISBN: 9781446287637
- [22] 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>
- [23] 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>
- [24] GOULDING, C.: *Grounded Theory: Some Reflections on Paradigm, Procedures and Misconceptions*; Working Paper Series, University of Wolverhampton 1999. ISSN: 1363–6839.
- [25] KELEMENNÉ ERDŐS A.: *A közforgalmú közlekedési szolgáltatás és piac vizsgálata marketing és fenntarthatósági nézőpontból*; Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest 2014.

- [26] MALHOTRA, N. K.: Marketingkutató; Budapest, KJK-Kerszöv Jogi és Üzleti Kiadó 2002. ISBN: 9632246470
- [27] 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>
- [28] 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>
- [29] CHARMAZ, K.: Constructing Grounded Theory; Thousand Oaks, California, SAGE Publications Ltd 2014.
- [30] GLASER, B. G. – STRAUSS, A. L.: The Discovery of Grounded Theory: Strategies for Qualitative Research; London, Weidenfeld and Nicolson 1967.
DOI: <https://doi.org/10.4324/9780203793206>
- [31] GELENCSEK K.: Grounded Theory; Szociológiai Szemle 1. (2003) pp. 143–154.
- [32] YIN, R. K.: Case Study Research: Design and Methods (Applied Social Research Methods); London, SAGE Publications Ltd 2013.
- [33] 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>
- [34] CHARMAZ, K. – THORNBERG, R.: The Pursuit of Quality in Grounded Theory; Qualitative Research in Psychology 18. 3. (2021) pp. 305–327.
DOI: <https://doi.org/10.1080/14780887.2020.1780357>
- [35] KENESEI Z. – STIER Z.: Kultúraközi szolgáltatásélmények vizsgálata a megalapozott elmélet módszerével; Vezetéstudomány 46. 3. (2015) pp. 2–17.
DOI: <https://doi.org/10.14267/VEZTUD.2015.03.01>
- [36] 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>
- [37] 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>
- [38] ELEKES G.: A Narratív Életútinterjú Módszere A Társadalomtudományok Kvalitatív Kutatásaiban; Szociálpedagógia 2018. 11. (2018) pp. 42–51.
- [39] 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>

- [40] HALÁSZ G. M.: A narratív közgazdaságtan szerepe; *Köz-Gazdaság - Review of Economic Theory and Policy* 16. 4. (2021) pp. 273–288.
- [41] LÁSZLÓ J.: A történetek tudománya: Bevezetés a narratív pszichológiába; Budapest, Új Mandátum Könyvkiadó 2005. ISBN: 9799639494595
- [42] FEHÉR B.: A narratív segítő beszélgetés; *Esély* 2010. 3. (2010) pp. 66–88.
- [43] 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>
- [44] 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>
- [45] GUBA, E. G. – LINCOLN, Y. S.: *Fourth Generation Evaluation*; Newbury Park, California, SAGE Publications Ltd 1989.
- [46] 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>
- [47] 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>
- [48] MERRIAM, S. B.: *Qualitative Research and Case Study Applications in Education*; San Francisco, Jossey-Bass 1998.
- [49] GRANEHEIM, U. H. – LUNDMAN, B.: Qualitative Contentanalysis in Nursing Research: Concepts, Procedures and Measures to Achieve Trustworthiness; *Nurse Education Today* 24. 2. (2004) pp. 105–112.
DOI: <https://doi.org/10.1016/j.nedt.2003.10.001>
- [50] SÁNTHA K.: A kvalitatív metodológiai követelmények problémái; *Iskolakultúra* 17. 6-7. (2007) pp. 168-177. ISSN: 1215-5233
- [51] STRAUSS, A. – CORBIN, J.: *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*; Newbury Park, Sage Publications 1990.
- [52] 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>
- [53] GLASER, B. G.: *Basics of Grounded Theory Analysis*; Mill Valley, Sociology Press 1992.

- [54] 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](https://doi.org/10.1016/S0959-8022(98)00017-4)
- [55] 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
- [56] 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>
- [57] BOAKYE-GYAN, K.: An Approach to a Comprehensive Framework for Insider Threat; Capitol Technology University ProQuest Dissertations Publishing, Maryland, USA 2021.
- [58] 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.
- [59] 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>
- [60] 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.
- [61] 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
- [62] BOUMA, G. D. – DIXON, B. R. – ATKINSON, G. B. J.: A Handbook of Social Science Research; Oxford, Oxford University Press 1995. ISBN: 019828000
- [63] GUBA, E. G.: Criteria for Assessing the Trustworthiness of Naturalistic Inquiries; Educational Communication and Technology Journal 29. 2. (1981) pp. 75–91.
- [64] DERVIN, B.: An Overview of Sense-Making: Concepts, Methods, and Results to Date; Dallas, Texas 1983.
- [65] 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>

- [66] SHARMA, G.: Pros and Cons of Different Sampling Techniques; *International Journal of Applied Research* 3. 7. (2017) pp. 749–752.
- [67] 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>
- [68] VERES Z. – HOFFMANN M. – KOZÁK Á.: *Bevezetés a piackutatásba*; Budapest, Akadémiai kiadó 2006. DOI: <https://doi.org/10.1556/9789634540038>
- [69] REKETTYE G. – TÓTH T. – MALOTA E.: *Nemzetközi Marketing*; Budapest, Akadémiai kiadó 2008. DOI: <https://doi.org/10.1556/9789630597401>
- [70] BRIONES-PENALVER, 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>
- [71] 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>
- [72] 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>
- [73] AKMAN, E.: Emerging Trade Partnership between the South Korea and Turkey: The Case of Defense Industry; *Güvenlik Stratejileri Dergisi* 2016.
- [74] 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>
- [75] 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>
- [76] 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>
- [77] 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>

- [78] 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>
- [79] 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>
- [80] EUROPEAN PARLIAMENT: Fact Sheets on the European Union, 2022.
<https://www.europarl.europa.eu/factsheets/en/sheet/65/defence-industry> (letöltve: 2023. 09. 23.)
- [81] 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.
- [82] MÉSZÁROS A. Á.: A kontingencia elmélet alkalmazása az innovatív kis- és középvállalkozások vizsgálata során az európai védelmi iparban; *Hadmérnök* 18. 3. (2023) (Megjelenés alatt.)
- [83] MÉSZÁROS A. Á.: The Significance of Innovation in the Defence Industry from the End of the Cold War to the War in Ukraine; *Journal of Regional Security* (2023) (Megjelenés alatt.)
- [84] 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
- [85] 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>
- [86] 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>
- [87] 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>
- [88] 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>
- [89] 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.

- [90] 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>
- [91] 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>
- [92] MATSUDA, Y.: An Essay on China's Military Diplomacy: Examination of Intentions in Foreign Strategy; *NIDS Security Repors* 7. 1. (2006) pp. 1–40.
- [93] MUTHANA, K. A.: Military Diplomacy; *Journal of Defence Studies* 5. 1. (2011) pp. 1–15.
- [94] 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>
- [95] 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>
- [96] 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>
- [97] 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>
- [98] 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>
- [99] 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>
- [100] 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>
- [101] 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>

- [102] 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>
- [103] 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>
- [104] 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 & Business Economics - Revista de Administração 52. 1. (2017) pp. 47–58.
DOI: <https://doi.org/10.1016/j.rausp.2016.09.003>
- [105] PANICO, C.: Strategic Interaction in Alliances; Strategic Management Journal 38. 8. (2017) pp. 1646–1667. DOI: <https://doi.org/10.1002/smj.2610>
- [106] 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>
- [107] 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>
- [108] DELGADO-MARQUEZ, B. L. – HURTADO-TORRES, N. E. – PED AUGA, 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>
- [109] 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>
- [110] LESKE, A. D. C.: A Review on Defense 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>
- [111] BAKOS C. A.: Modern könnyűgyalogység a jövő konfliktusaiban, háborúiban; Honvédségi Szemle - Hungarian Defense Review 146. 1. (2018) pp. 3–11.
- [112] EUROPEAN COMMISSION: Defence Industry and Space, 2022. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en (letöltve: 2023. 09. 23.)

- [113] 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.
- [114] FRUNZETI, T. – COȘEREANU, L. – TOMOIAGĂ, T.: Impact of Disruptive Technologies on Defence; Land Forces Academy Review 26. 4. (2021) pp. 282 – 287.
- [115] 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>
- [116] 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.
- [117] BITZINGER, R. A.: The Modern Defense Industry: Political, Economic, and Technological Issues, Santa Barbara, California, ABC-CLIO, LLC 2009.
- [118] 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
- [119] FIOTT, D.: Strategic Autonomy: Towards 'European sovereignty' in defence?; European Union Institute for Security Studies (EUISS). Paris 2018.
- [120] FAURE, S. B. H.: La coopération internationale dans le secteur de l'armement; Questions de Recherche 46. 1. (2015) pp. 1–45.
- [121] 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>
- [122] PORKOLÁB I.: Az Innováció Hatása a Hadviselésre; Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata 26. 1-2. (2016) pp. 19–28. ISSN: 1215-4121
- [123] 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>
- [124] 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>
- [125] 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>

- [126] 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>
- [127] 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>
- [128] 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>
- [129] 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.)
- [130] HOU, T. – WANG, V.: Industrial Espionage –A Systematic Literature Review (SLR); *Computers & Security* 98. 102019 (2020)
DOI: <https://doi.org/10.1016/j.cose.2020.102019>
- [131] 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
- [132] 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>
- [133] 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>
- [134] 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.
- [135] 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>

- [136] 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>
- [137] 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>
- [138] 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.
- [139] 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>
- [140] 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>
- [141] 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>
- [142] 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>
- [143] 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>
- [144] 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.
- [145] 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>
- [146] BABOS, S.: A katonai hírszerzés és a katonai elhárítás hadtudományi természete; *Felderítő Szemle* 17. 2. (2019) pp. 146– 158.

- [147] 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>
- [148] ANDROULIDAKIS, I. – KIOUPAKIS, F. E.: *Industrial Espionage and Technical Surveillance Counter Measures*; Switzerland, Springer International Publishing 2016. DOI: <https://doi.org/10.1007/978-3-319-28666-2>
- [149] 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
- [150] 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>
- [151] 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.
- [152] 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>
- [153] 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>
- [154] 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>
- [155] WARKENTIN, M. – MUTCHLER, L.: Research in Behavioral Information Security Management. In: TOPI, H., TUCKER, A. /szerk./: *Computing Handbook*. Taylor and Francis, 2014.
- [156] 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>
- [157] 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>
- [158] HAIG Z.: Az információs társadalmat fenyegető információalapú veszélyforrások; *Hadtudomány* 17. 3. (2007) pp. 37– 56.

- [159] ROCHE, E. M.: Industrial Espionage; *Journal of U.S. Intelligence Studies* 22. 1. (2016) pp. 59-63.
- [160] 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>
- [161] 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>
- [162] BUDAVÁRI K. – TAKSÁS B. – HEGEDŰS 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>
- [163] 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>
- [164] 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
- [165] 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
- [166] 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.
- [167] JOHNSON L. K.: *Secret Agencies: U.S. Intelligence in a Hostile World*; London, Yale University Press 1998.
- [168] 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>
- [169] BRENNER, S. W. – CRESCENZI, A. C.: State-Sponsored Crime: The Futility of the Economic Espionage Act; *Houston Journal of International Law* 28. 2. (2006).
- [170] 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.
- [171] 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

- [172] HOUSE, W.: Annual Report to Congress on Foreign Economic Collection and Industrial Espionage; Washington DC, National Counterintelligence Center, Government Printing Office 1995.
- [173] NOONAN, C. F.: Spy the Lie: Detecting Malicious Insiders; Pacific Northwest National Laboratory, Richland, Washington, United States 2018.
- [174] PASTERNAK, G. – WITKIN, G.: The Lure of the Steal; US News & World Report, United States 45. 1996.
- [175] 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>
- [176] 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>
- [177] WILSON, Y. – HINGNIKAR, A.: Looking into the Crystal Ball; Solving Identity Management in Modern Applications. Berkeley, CA, Apress 2023., pp. 317–334.
- [178] 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.
- [179] 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>.
- [180] 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>
- [181] 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>
- [182] 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
- [183] MAICAN, O. H.: Legal Aspects of Economic Espionage; Perspectives of Law and Public Administration 8. 2. (2019) pp. 385–392.
- [184] 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>
- [185] 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>
- [186] 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.
- [187] SCHLIENGER, T. – TEUFEL, S.: Information Security Culture - From Analysis to Change. In: ELOFF, J., VENTER, H., LABUSCHAGNE, L., ELOFF, M. /szerk./: Information Security South Africa - Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference, Sandton Convention Center, Johannesburg, South Africa, 9-11 July 2003. ISSA: 183-195.
- [188] 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>
- [189] 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
- [190] 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>
- [191] 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>
- [192] 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.
- [193] 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>

- [194] 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>
- [195] 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>
- [196] CROSBY, M. – NACHIAPPAN – PATTANAYAK, P. – VERMA, S. – KALYANARAMAN, V.: BlockChain Technology: Beyond Bitcoin; *Applied Innovation Review* 2. (2016) pp. 7–19.
- [197] 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>
- [198] 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>
- [199] 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>
- [200] 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>
- [201] 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>
- [202] WILLIAMS, B. – SOULET, M. – SIRAJ, A.: A Taxonomy of Cyber Attacks in Smart Manufacturing Systems. In: KNAPČÍKOVÁ, 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
- [203] 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>
- [204] 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

- [205] NEJAD, B.: Introduction to Satellite Ground Segment Systems Engineering: Principles and Operational Aspects (Space Technology Library, 41); Cham, Springer 2023.
- [206] 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
- [207] ABDULWAHAB Á. – PANDURICS A. – UGRAI P.: Vállalati és vállalatközi integráció. Budapesti Közgazdaságtudományi Egyetem, Budapest 1997.
- [208] 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>
- [209] 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>
- [210] 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>
- [211] 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>
- [212] 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>
- [213] GALBRAITH, J.: Designing Complex Organizations; Boston, Addison-Wesley Pub. Co 1973.
- [214] 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>
- [215] DONALDSON, L.: The Contingency Theory of Organizations; London, Sage Publicatios 2001. DOI: <https://doi.org/10.4135/9781452229249>
- [216] 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>
- [217] HAYES, D. C.: The Contingency Theory of Managerial Accounting; The Accounting Review 52. 1. (1977) pp. 22–39.
- [218] MINTZBERG, H.: The Structuring of Organizations; London: Pearson 1979.

- [219] 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.
- [220] 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>
- [221] 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>
- [222] 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>
- [223] 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>
- [224] BUCK, C. – OLENBERGER, C. – SCHWEIZER, A. – VÖLTER, F. – EYMANN, T.: Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust; Computers & Security 110. 102436. (2021) DOI: <https://doi.org/10.1016/j.cose.2021.102436>
- [225] CHEN, Y. – HU, H. C. – CHENG, G. Z.: Design and Implementation of a Novel Enterprise Network Defense System by Maneuvering Multi-Dimensional Network Properties; Frontiers of Information Technology & Electronic Engineering 20. (2019) pp. 238–252. DOI: <https://doi.org/10.1631/FITEE.1800516>
- [226] 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
- [227] 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.

RÖVIDÍTÉSJEGYZÉK

1. IT Információs technológia
2. KFI Kutatás, fejlesztés és innováció
3. KKV Kis- és középvállalkozás

TÁBLÁZATJEGYZÉK

1. táblázat: Kvalitatív kutatás megbízhatósági kritériumai	15
2. táblázat: Interjúk témakörei	23
3. táblázat: Az interjúalanyok jellemzői	25
4. táblázat: Ipari kémkedés attribútumai	33
5. táblázat: A szándékos és véletlen esetek jellemzői.....	44
6. táblázat: Az ipari kémkedés megelőzésének és észlelésének eszközei	88

ÁBRAJEGYZÉK

1. ábra: Az értekezés koncepciója és struktúrája	11
2. ábra: Grounded theory módszer folyamata.....	18
3. ábra: Az innovatív védelmi ipar gazdasági és politikai hatásai.	28
4. ábra: Ipari kémkedés folyamata	39
5. ábra: A védelmi iparban működő szervezetre ható kontingencia tényezők.....	55
6. ábra: Az ipari kémkedési esetszámok növekedése mögött azonosított tényezők, a grounded theory elemzés kód fája	58
7. ábra: A növekedés tényezői közötti hipotetikus összefüggések	67
8. ábra: az ipari kémkedés elleni védekezés és megelőzés tényezői, a grounded theory elemzés kód fája.....	68
9. ábra: Többretegű információbiztonsági rendszer	75
10. ábra: Jövőbeni fenyegetések, a grounded theory elemzés kód fája	76
11. ábra: A grounded theory alkalmazásával definiált elmélet összefoglalása.....	80
12. ábra: Információbiztonsági piramis modell alkalmazása.....	92
13. ábra: Információbiztonsági rendszer kialakítása.....	97

FÜGGELÉK

Magyar vezérfonal I. szakasz

(2022. I.-II. negyedév)

1. Mi annak az oka, hogy jelentősen növekedett világszerte azoknak az eseteknek a száma, amikor valamilyen módon üzleti titkok és információk szivárognak ki a védelmi vállalatoktól?
 - a. Milyen *okok, tényezők, körülmények* állhatnak mögötte?
2. Mit gondol, miért fenyegeti az ipari kémkedés kiemelten a védelmi kis- és középvállalkozásokat? (*Milyen szerepük van az ágazatban?*)
3. Tud olyan, akár véletlen vagy szándékosan elkövetett üzleti titok kiszivárogtatási esetről, amely az ön környezetében történt? (*El tudja mondani a részleteket?*)
4. Véleménye szerint milyen tényezők vezetnek egy vállalatnál az információ biztonság csökkenéséhez?
5. Véleménye szerint milyen tényezők játszanak szerepet a munkavállalók információbiztonsághoz való viszonyában a vállalatnál? (*hűség kérdése?*)
6. Mi a véleménye azokról az esetekről, melyek során a vállalat alkalmazottjai **véletlen** elkövetett hiba során szivárogtatják ki a bizalmas üzleti információt a vállalattól?
 - a. Mi az oka, miért történnek a véletlen üzleti információ kiszivárogtatási esetek?
 - b. Milyen következményekkel járhatnak a véletlen üzleti információ kiszivárogtatási esetek?
7. Mi a véleménye azokról az üzleti titok kiszivárogtatási esetekről, amelyeket **rossz szándékkal** követnek el a munkavállalók, hogy szándékosan ártsanak a szervezetnek?
 - a. Véleménye szerinte milyen körülmények, motivációk váltják ki a munkavállalóból azt a viselkedést, hogy szándékosan szivárogtasson üzleti információt a vállalattól?

- b. Hogyan lehet szankcionálni?
 - c. Azoknak a munkavállalóknak, akik elkövetnek szándékos üzleti információ szivárogtatást, van valamilyen speciális jellemzőjük? *(kor, pozíció, hány éve dolgoznak a szervezetnél,)*
8. Milyen információvédelmi eszközöket alkalmaz a vállalkozás, ahol ön dolgozik? *(Berendezések, szoftverek, beléptetők...)*
9. Rendelkeznek írott információbiztonsági politikával? *(Mire terjed ki?)*
10. Hogyan kezelik a belső fenyegetés kérdését? *(Szankcionálás, motiválás, hűség)*

English Guide Phase I.

(2022 Q1-Q2)

1. What is the reason behind the significant increase worldwide in the number of cases where business secrets and information leak from defense companies in some way?
 - a. What *reasons, factors, and circumstances* could be behind this?
2. Why do you think industrial espionage particularly threatens defense small and medium-sized enterprises? (*What role do they play in the industry?*)
3. Are you aware of any incidents of business secrets being leaked, whether accidentally or intentionally, that have occurred in your environment? (*Can you provide details?*)
4. In your opinion, what factors contribute to a decrease in information security within a company?
5. What factors do you think play a role in employees' attitudes towards information security within the company? (*A matter of loyalty?*)
6. What is your opinion about cases where company employees **accidentally** leak confidential business information?
 - a. What do you think is the reason behind these accidental business information leakage incidents?
 - b. What could be the consequences of accidental business information leakage incidents?
7. What is your opinion about cases where employees **intentionally** leak business secrets to harm the organization?
 - a. According to your view, what *circumstances and motivations* drive employees to engage in such behavior of intentionally leaking business information from the company?
 - b. How can they be sanctioned?
8. Do employees who intentionally leak business information have any specific characteristics? (*age, position, years of service with the organization, etc.*)

9. What information security tools does the company where you work utilize?
(Equipment, software, access controls, etc.)
10. Do they have a written information security policy? *(What does it cover?)*
11. How does the company address the issue of internal threats? *(Sanctions, motivation, loyalty)*

Magyar vezérfonal II. és III. szakasz

(2022. III. – 2023. I. negyedév)

1. Milyen tényezők az ipari kémkedési eseten növekedését a védelmi iparban?
 - a. Külső?
 - b. Belső?
 - c. Hogyan befolyásolja a háború?
2. Milyen lehetőségek állnak a vállalkozás rendelkezésére az ipari kémkedés elleni védekezésben?
 - a. Vezetők szerepe?
 - b. Megelőzés?
 - c. Észlelés?
3. Véleménye szerint milyen jövőbeni információbiztonsági fenyegetésekkel kell a védelmi vállalkozásoknak szembe nézni?
 - a. Ezt milyen tényezőkből lehet előre jelezni?
 - b. Hogyan lehet ellenük védekezni?
4. Milyen szerepe van az ipari kémkedés jövőjében a mesterséges intelligenciának?
5. Milyen szerepe van az ipari kémkedés elleni védekezés jövőjében a mesterséges intelligenciának?

English Guide Phase II. – III.

(2022 Q3 – 2023 Q1)

1. What factors contribute to the increase in industrial espionage in the defense industry?
 - a. External factors?
 - b. Internal factors?
 - c. How does the war affect it?
2. What options are available to businesses for defense against industrial espionage?
 - a. The role of leaders?
 - b. Prevention?
 - c. Detection?
3. In your opinion, what future information security threats should defense companies be prepared for?
 - a. How can these threats be anticipated based on certain factors?
 - b. How can they defend against these threats?
4. What role does artificial intelligence play in the future of industrial espionage?
5. What role does artificial intelligence play in the future of defending against industrial espionage?

KÖSZÖNETNYILVÁNÍTÁS

Szeretném megköszönni Dr. Kelemen-Erdős Anikónak, hogy a BSc képzésemtől kezdve a doktori kutatásom megvalósulásáig minden szakaszban mellettem állt, és nem csak tudását és tapasztalatát osztotta meg velem, hanem mindig támogatott, biztatott és hitt bennem. Anikó doktori értekezése példaként szolgált számomra a munkám során.

Szintén szeretném megköszönni az összes interjúalanyomnak, akik a publikációk és az értekezés megvalósulásához hozzájárultak értékes ötleteikkel, tapasztalataikkal és gondolataikkal.