ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

MÉSZÁROS ALEXANDRA ÁGNES

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

Témavezető: Dr. Kelemen-Erdős Anikó

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2024. 02. 01.

Szigorlati/komplex vizsgabizottság:

Elnök:

Prof. Em. Dr. Berek Lajos professor emeritus

Tagok:

Dr. Maros Dóra

Dr. habil. Garai-Fodor Mónika

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Em. Dr. Berek Lajos professor emeritus

Titkár:

Dr. Pető Richárd

Tagok:

Dr. Kolnhofer-Derecskei Anita

Prof. Dr. Velencei Jolán

Prof. Dr. Besenyő János

Bírálók:

Prof. Dr. Molnár Anna

Dr. habil. Szádeczky Tamás

Nyilvános védés időpontja:

2024

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

Alulírott **Mészáros Alexandra Ágnes** kijelentem, hogy az „**Ipari kémkedés vizsgálata a védelmi iparban működő innovatív kis- és középvállalkozások körében**" című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2024. február 4.

Mészáros Alexandra

(aláírás)

TARTALOMJEGYZÉK

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 egyik 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 jelentős átalakuláson mentek keresztül, és hatékonyabbak, mint valaha voltak a történelem során.

A tudományos probléma megfogalmazása

A védelmi ipar minden nemzet számára stratégiai jelentőségű. Az állampolgárok biztonságának védelme mellett számtalan társadalmi, politikai és gazdasági területen rendelkezik kiemelt szereppel. Több társadalmi csoportot 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 világűrből 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 számára is, hogy tevékenységet folytassanak az ágazatban, amelyek azóta kiemelkedő teljesítményt nyújtanak az innovációk fejlesztése területén [2, 3, 4, 5, 6]. Az innovációs tevékenység folytatásának legértékesebb eleme – a tudást előállító ember mellett – a kritikus információ, melynek védelme kulcsfontosságú feladat, azonban jelen gazdasági és geopolitikai körülmények között a legkorszerűbb információvédelmi rendszerek alkalmazása mellett is kiemelten fenyegeti a védelmi ipar területén tevékenységet folytató kis- és középvállalkozásokat a gazdasági- és ipari kémkedés. Az értekezés az európai védelmi ipar területén tevékenységet folytató, innovatív kis- és középvállalkozások szempontjából vizsgálja az ipari kémkedés fenyegetését, szociotechnikai megközelítést[1] alkalmazva, a humán faktort központba helyezve. A kutatás eredményei empirikus, a mélyinterjúk során gyűjtött adatokból fejlődtek (n=42), amelynek előnye, hogy nemcsak a korábban megfogalmazott szakirodalomból és jogszabályokból vontam le a következtetéseket, hanem a terepmunka során gyűjtött, gyakorlati tapasztalattal rendelkező személyek gondolatai szolgáltak túlnyomórészben az elméleti munka alapjául.

Jelen kutatás során az **innovatív kis- és középvállalkozás** (továbbiakban kkv) kifejezés azon szervezeteket foglalja magába, melyek tevékenységei, üzleti- és munkafolyamatai, termékei vagy szolgáltatásai új vagy újszerű megközelítésből valósulnak meg. Az Európai Bizottság definíciója alapján a kkv kategóriába olyan vállalkozások tartoznak, amelyek 250 főnél kevesebb személyt foglalkoztatnak, továbbá amelyek éves forgalma nem haladja meg az 50 millió eurót vagy éves mérlegfőösszege nem haladja meg a 43 millió eurót [7]. Az innovatív kkv-k általában kisebb méretű vállalkozások, azonban a növekedésük és fenntarthatóságuk érdekében aktívan vesznek részt kutatás, fejlesztés és innovációs (továbbiakban KFI) tevékenységekben, és az innovációk révén hozzájárulnak a gazdasági fejlődéshez [8]. Ezen vállalkozások fő profilja az új eszközök, alkatrészek, részegységek, szoftverek vagy hardverek fejlesztése, továbbá tevékenységük részét képezheti a kis szériás sorozatgyártás[2]. A definiált védelmi kkv-k elsősorban katonai

[1] A szociotechnikai megközelítés a társadalmi és technológiai rendszerek kölcsönhatását vizsgálja.

[2] A kutatás elsősorban, de nem kizárólagosan a magánkézben lévő kkv-ket vizsgálta Európa területén, amelyek lehetnek katonai beszállítók, azonban jelen empirikus kutatás fókusza szempontjából az államonként eltérő vonatkozó jogszabályok irrelevánsak, mert a kutatás célja induktív módon a megkérdezettek tapasztalatain alapuló eredmények feltárása, ami gyakorlatban eltérhet a jogszabályban definiáltaktól.

eszközök fejlesztésével és előállításával foglalkoznak, azonban készülnek olyan termékek is, melyeket nem kizárólag védelmi felhasználásra szántak. A **kettős (duális) felhasználású** termékek olyan alapanyagok, eszközök, szoftverek vagy technológiák, melyek békeidőben civil, háborús időben katonai célokra egyaránt alkalmazhatók. A kutatás során vizsgált kkv-k fejleszthetik a terméket közvetlenül megrendelésre vagy általuk észlelt piaci igény alapján. A védelmi kkv-k 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 kkv-k nagyobb hajlandóságot mutatnak olyan KFI projektek megvalósítására, amelyek a nagyobb védelmi vállalatok számára túl kockázatosnak számítanak.

A védelmi ipar ágazatokon átnyúló, diverzifikált, stratégiai iparág, amely magába foglalja a hagyományos hadiipart, – mely a védelmi erőket haditechnikai eszközzel, hadianyaggal és szolgáltatásokkal ellátó vállalatok összessége [9] – belbiztonságot és a fejlődőben lévő biztonsági ipart, a kritikus infrastruktúrát érintő kibervédelmet, katasztrófavédelmet, terrorelhárítást, valamint a repülőgép- és űripart egyaránt [10]. Ezek a területek mind az alkalmazott technológiák, mind a termékek és szolgáltatások tekintetében, különböző szinteken és formákban összefonódnak [10]. Jelen értekezés fókusza ezen alkalmazott technológiák és termékek fejlesztését, továbbá a hozzájuk kapcsolódó szolgáltatások és üzleti folyamatok megvalósítását végző kkv-kre irányul. A kutatás nem terjed ki a védelmi ipar által betöltött feladatok ellátásához kapcsolódó olyan kritikus információk védelmének kérdéseire, mint a belbiztonság biztosítása, katasztrófavédelem vagy terrorelhárítás.

Az információszerzés minden innovációs folyamat kiindulópontja, melynek számtalan módja létezik. Az ipari kémkedés ennek az információszerzésnek egy speciális esete, mely **információbiztonsági** szempontból jelentős kockázatot testesít meg a védelmi kkv-k számára. Haig (2017) [11] információbiztonságról megfogalmazott gondolatai alapján az információs társadalom alapvető éltető eleme az információ, melynek mennyisége és minősége létfontosságú a kkv-k számára, ezáltal kíméletlen harc folyik annak gyors megszerzéséért, biztonságos tárolásáért és hatékony felhasználásáért. Jelen értekezés az információ gyors megszerzésének egyik rendhagyó módszerét, az ipari kémkedést vizsgálja. Mivel napjainkban egyre markánsabban jelentkezik az igény az információ megóvására, hatékony védelmére, így törvényszerűen megjelentek azon tevékenységek,

amelyek az információhoz való illetéketeken hozzáférés és felhasználás akadályozására, esetleg tönkretételére irányulnak [11]. Következésképp az ipari kémkedés kockázatának csökkentését célzó empirikus eredmények kulcsszerepet játszanak az információbiztonság területén, ami szintén indokolja a tudományos probléma kutatását.

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 rendelkezhet. Számos szerző szerint a két fogalom közötti fő eltérés, hogy az előbbit állami szereplő, míg az utóbbit versenypiaci résztvevő kezdeményezi [1, 12, 13, 14, 15, 16], 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, 17, 18, 19].

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, 14, 15, 16], amely a hazai vállalatok üzleti titkainak vagy kormányzati szervek bizalmas információinak célzott megszerzésére irányul, hogy azt a megbízó állam tudatosan a saját céljára felhasználhassa [13, 20, 21].

Az **ipari kémkedés** számos átfedést mutat a gazdasági kémkedéssel [13, 20, 21], azzal a különbséggel, hogy a nemzetközi piacon versenyző vállalatok által szervezett tevékenység [14], amely üzleti titkok jogtalan elsajátítása révén egy másik vállalkozás javát szolgálja [1, 13, 20], üzleti céllal megy végbe [15], közvetlen kormányzati beavatkozás nélkül [13, 16, 20].

A nemzetközi szakirodalomban használt **stratégiai hírszerzés** *(strategic intelligence)* kifejezés, mely hatásköre a külföldi titkos politikai, technikai, gazdasági, tudományos és katonai információk tervszerű gyűjtése az állam hosszú távú, biztonsági aspektusokat is figyelembe vevő stratégiáinak kialakításához, továbbá az elhárítási feladatok ellátásához [22], több szempontból átfedést mutat a gazdasági kémkedéssel, amely a stratégiai hírszerzés részhalmazának is tekinthető.

Jelen kutatásban az **ipari kémkedés** kifejezést alkalmazom, 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 kifejezéshasználat 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.

Az ipari kémkedés jelentős károkat képes okozni az azt elszenvedő gazdálkodó szervezetnek, ez pedig kihatással lehet azon állam gazdaságára is, amelynek területén a szervezet működik, vagy amellyel kapcsolatban valamilyen tevékenységet fejt ki, így a magyar büntetőjogban a jogalkotó az ipari kémkedést társadalomra veszélyesnek minősítette, továbbá a természetes és jogi személy, illetve az állam gazdasági és utóbbi esetében nemzetbiztonsági érdekeinek védelme érdekében is, azt büntetni rendeli [23]. Magyarországon az ipari kémkedés nem jelenik meg önálló tényállásként a büntető törvénykönyvben, melynek oka annak változatos megjelenési formája, azonban a kémkedés ezen formájának tiltása a büntetőjogi szabályozás több tényállásában is megjelenik, melyekben közös, hogy a középpontban valamilyen titkos, a köz számára ismeretlen adat áll [23]. Az üzleti titok védelméről szóló **2018. évi LIV. törvény 5. pontja (6. §)** határozza meg az üzleti titokhoz fűződő jog megsértését, melynek az első pontja: „*Az üzleti titokhoz fűződő jogot megsérti, aki az üzleti titkot jogosulatlanul megszerzi, hasznosítja vagy felfedi*.” [24].

Az értekezésben **kritikus információ** minden olyan üzleti titok, amelynek az eltulajdonítása az azt előállító vállalkozástól egy másik entitás előnyét szolgálja, miközben kárt okoz a tudást jogosan birtokló szervezetnek. Az üzleti titok védelméről szóló **2018. évi LIV. törvény 1. pontja (1. §)** szerint az *„(1)* ***Üzleti titok*** *a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető –, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja. (2)* ***Védett ismeret (know-how)*** *az üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása.”* [24].

Az értekezésben 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, alapanyag beszállító, célpiac vagy egyéb marketinginformáció. A védelmi innovációk szempontjából a szellemi tulajdon[3]; a stratégiai, pénzügyi, ellátási lánccal kapcsolatos és marketingtevékenységére vonatkozó információk; továbbá az aktuális és jövőbeni tervek és infrastruktúrák állnak a kémkedés középpontjában [20, 25, 26], 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 [19]. A 94. oldalon bemutatott információbiztonsági piramis modell (11. ábra) keretrendszert nyújt a vállalkozás működéséhez szükséges üzleti titkok besorolásához.

A **védelmi innováció** Schumpeter (1939) [27] alapesetei alapján jelen értekezésben lehet új termék fejlesztése[4], új gyártási vagy értékesítési módszer alkalmazása, új piac megnyitása, továbbá új nyersanyag vagy félkész termék beszerzési forrás felkutatása.

Az 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 haditechnikai KFI minden szuverén államban fontos szerepet játszik a nemzetbiztonság rendszerében [28], így az ipart fenyegető kémkedés a teljes nemzetbiztonságra veszélyt jelentő kockázatot testesít meg. A védelmi iparban az ipari kémkedés áldozatának súlyos következményekkel kell szembe nézni makro- és mikroökonómiai szinten egyaránt. A témavezetőmmel folytatott korábbi kutatásunk [29] 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

[3] Tervrajz, forráskód, prototípus, szabadalom, találmány, kézirat, képlet, gyártástechnológia és egyéb fejlesztéssel kapcsolatos dokumentumok.

[4] Új termék lehet alapanyag, ötvözet, szoftver, alkatész, részegység (akár egy régóta rendszeresített eszköz továbbfejlesztéséhez) vagy egy teljesen új eszköz.

eredményeink indokolták a védelmi ipart fenyegető ipari kémkedés problémakörének további kutatását.

Az európai védelmi ipar területén tevékenységet folytató kkv-k ipari kémkedés elleni védekezéshez való viszonyát kvalitatív kutatás során ilyen mélységben korábban még nem vizsgálták. Bár számos megoldás található a rendelkezésre álló szakirodalomban a komplex fenyegetés megközelítésére, azonban a problémát még nem sikerült hatékonyan kezelni, ami szintén indokolja a kérdés további kutatását. Az ipari kémkedés problémaköre egy viszonylag új, és lassan fejlődő kutatási terület [30]. Számos szervezet alkalmaz költséges információvédelmi rendszereket, csak az információs technológia (továbbiakban IT) által jelentett veszélyre összpontosítva, figyelmen kívül hagyva a vállalati érintettek által megtestesített fenyegetést [31, 32]. Következésképpen a szakirodalom jelentős része a témát technológiai [17, 33], jogi [17, 34, 35], és a külső támadások aspektusából vizsgálja [36], kevés figyelmet fordítva a szervezeti érintettek által megtestesített belső fenyegetésre [33, 37, 38, 39]. 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, 40, 41]. Jelen kvalitatív[5] kutatás újdonságtartalma, hogy az ipari kémkedés problémáját holisztikus megközelítésből vizsgáltam, párhuzamot vonva az IT és a humán tényező között.

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

[5] A kvalitatív kutatás egy olyan feltáró módszer, mely a definiált tudományos probléma mélyebb megértését szolgálja. Kis mintán alapuló, nem reprezentatív metodika, mely nem alkalmaz statisztikai számításokat, továbbá nem hoz számszerűsíthető eredményeket, azonban lehetőséget teremt új tudományos területek feltárására.

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

Korábban Magyarországon a védelmi ipar, továbbá az ehhez szükséges szakirányú oktatás néhány kivétellel gyakorlatilag megszűnt. Azonban olyan kezdeményezések hatására, mint a 2016-ban elfogadott, a magyar ipar fejlesztéséről szóló Irinyi Terv, a szintén 2016-ban meghirdetett Zrínyi Honvédelmi és Haderőfejlesztési Program, vagy a 2023-ban induló hadiipari mérnök mesterképzés az Óbudai Egyetemen lehetőséget teremtenek, hogy a nagy tőkebefektetők mellett a hazai kkv-k is csatlakozhassanak a védelmi innovációs ökoszisztémához. A **védelmi innovációs ökoszisztéma** egy olyan környezet, mely szereplői együttműködnek a nemzetbiztonsági kérdésekkel kapcsolatos KFI tevékenységekben a védelmi képességek fejlesztésének céljából, mely kooperációk lehetővé teszik a gyors és hatékony reakciót a folyamatosan változó fenyegetésekre. Ezen környezetnek fontos szereplőik a definiált kkv-k, melyek versenyképes működéséhez szükséges megismerniük a biztonságukat fenyegető minden szervezeti külső és belső környezeti változót. Mivel az ehhez szükséges források nem elérhetők, nem nyilvánosak, hiányosak vagy esetenként szándékosan félrevezetők, ezek kutatása új módszertani megközelítést igényel. A védelmi kkv-k védelme, továbbá a fenyegetésekre és azok elhárítására történő felkészítése a sikeres működésük miatt elengedhetetlen, ezért az értekezésben kutatott téma nagy jelentőséggel bír.

Az európai védelmi ipar transzformációja lehetővé tette a magánszektort képviselő kkv-k megjelenését a piacon [2, 42, 43], melyek szerepe és száma várhatóan növekedni fog a jövőben [44]. 2022-ben az Európai Unió területén több mint 2500 kkv [45], közvetlenül 463 ezer főt foglalkoztat a védelmi ipar területén [46]. Ezek a vállalkozások kiemelkedő innovációs képességekkel rendelkeznek [2, 3, 5, 47, 48, 49], amelyet nagyrészben belső kutatással és fejlesztéssel támogatnak [50]. Az európai védelmi iparnak célkitűzése, hogy képes legyen teljes mértékben a kkv-kból származó innovációkra támaszkodni [45]. Ennek eléréséhez az Európai Védelmi Alap 2022-ben 832 millió eurót [51], 2023-ban 1,2

milliárd eurót biztosított a védelmi célú KFI tevékenységekre [52]. A rohamosan fejlődő technológia jelentős hatást gyakorol a védelmi iparra, következésképpen a katonai összeütközések módszerei-, és eljárásai is változnak [53], amely megköveteli a helyi vállalkozásoktól az új technológiák fejlesztését. Mivel a nagy védelmi vállalatok nem érdekeltek a szűk piacok, vagy személyre szabott igények kiszolgálásában [43, 54], a kkv-k versenyképesen működhetnek, ha a tevékenységüket réspiacokra, továbbá személyre szabott védelmi eszközök fejlesztésére összpontosítják [6, 48, 55, 56].

Egy olyan ipari kémkedés elleni rendszer kialakítása, mely segíthet megelőzni, időben észlelni és reagálni a támadásra, majd helyreállítani az esetlegesen okozott következményeket, összetett feladat, mely kialakításának első problémája, hogy túl sok különböző természetű külső és belső fenyegetés észlelhető, amiket számításba kell venni. Jelen kutatás folyamán újszerű megközelítést alkalmaztam, és az ipari kémkedést, továbbá a fenyegetés elleni védekezést a szervezetre ható külső és belső kontingenciatényezők közé soroltam. A kontingenciaelmélet szerint a vállalkozás külső környezete nagymértékben befolyásolja annak működését [57, 58], így nincs egy minden körülmények között alkalmazható szervezeti stratégia, hanem a belső tényezőket folyamatosan a külső változókhoz szükséges alakítani a legjobb eredmény elérése érdekében [59, 60, 61]. A megközelítés újszerűsége abban rejlik, hogy a kontingenciaelmélet 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. Korábbi kutatásom során már vizsgáltam az innovatív védelmi kkv-kre ható kontingenciaváltozókat, melyek közül jelen értekezésben kimondottan az ipari kémkedés problémakörére fókuszálok [48]. A fenyegetés csökkentéséhez a vállalkozások döntéshozóinak tanulmányozni szükséges a környezetben érvényesülő gazdasági, politikai, geopolitikai kontingenciaváltozókat, a technológiai fejlődést, az ellátási lánchoz 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 kirobbant orosz-ukrán fegyveres konfliktus, melynek hatására a védelmi iparban előállított kritikus információ értéke ugrásszerűen növekedett, és vált keresetté az ágazat szereplői között, ami az 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 kkv-ket fenyegető ipari kémkedést háborús környezetben vizsgálja.

Korábbi kutatásom eredménye, hogy az orosz-ukrán háború kitörése óta egyre több befektetés áramlik a recesszióálló védelmi iparban működő kkv-kbe, ahol a befektetők előnyben részesítik azon vállalkozásokat, melyek termékeik duális felhasználású technológiaként alkalmazhatók [48]. Azonban egyes kettős felhasználású eszközök könnyen beszerezhetők vagy előállíthatók polgári piacon elérhető alapanyagokból, és alakíthatók át pusztító eszközzé. Ennélfogva, gazdasági és nemzetbiztonsági okokból egyaránt, ezen termékek fejlesztéséhez fűződő kritikus információk védelme szintén fontos feladat.

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 kvantitatív[6] módszerek a védelmi ipar számos területén hozhatnak empirikus és teoretikus felhasználásra alkalmas eredményeket. Azonban az ipari kémkedés mélyreható és összetett természete miatt olyan sok különböző, dinamikusan változó és nehezen számszerűsíthető faktort kell számításba venni, hogy ezen metodikák alkalmazása számos akadályba ütközhet. (1) Az 1.1. fejezetben részletesen kifejtett okok miatt a védelmi kkv-k erőfeszítéseket tesznek annak érdekében, hogy az ipari kémkedéssel összefüggésbe hozható esetek titokban maradjanak. Szintén korlátozza a számszerűsített adatokon alapuló módszerek alkalmazását, (2) hogy egyes országok az ipari kémkedést a gazdasági tevékenységek legitim eszközének tekintik [18, 19, 38, 62], (3) a kapitalista nemzetek törvénykezése hajlamos elbagatellizálni az ügyeket [63], továbbá (4) a védelmi ipar kritikus szerepe miatt az incidensekhez fűződő adatokhoz való hozzáférés szigorúan szabályozott. Ezen okok miatt az országspecifikus adatok nehezen összehasonlíthatók, továbbá az esetekhez fűződő dokumentációk gyakran hiányosak, közvetett vagy részleges formában állnak rendelkezésre, eltérnek a valóságtól vagy rejtettek, így nem áll a kutatók

[6] A kvantitatív kutatás egy olyan módszer, mely során számszerűsített adatokkal végeznek statisztikai méréseket reprezentatív mintán, a szélesebb sokaságra általánosítható eredményekkel.

rendelkezésére egy hozzáférhető adathalmaz. (5) A kommunikációs technológiák gyors fejlődése, (6) a kritikus információk gyakran nehezen számszerűsíthető értéke vagy (7) az információszerzési céllal történő humán viselkedések és interakciók szintén olyan változók, melyek nehezen számszerűsíthetők. Ezen okok miatt az ipari kémkedés vizsgálata során csak korlátozottan lehet kvantitatív módszereket alkalmazni, és kutatásához gyakran kvalitatív vagy kombinált módszerekre van szükség. Többek között ezek indokolják a grounded theory módszertan alkalmazását.

A kutatás során az alanyokat célzott mintavétellel választottam, az adatgyűjtést vezérfonallal támogatott szakértői mélyinterjúkkal valósítottam meg (n=42). A gyűjtött empirikus adatok elemzését a **grounded theory** (*megalapozott elmélet*) módszertan konstruktivista irányzatával folytattam. A grounded theory módszertan alkalmazásával az elmélet a mélyinterjúk alatt gyűjtött empirikus adatokból fejlődik. Az adatelemzést az átiratok gondolati egységekre történő bontásával kezdtem, majd azok több lépésben történő folyamatos összehasonlítása során definiáltam a kategóriákat és az azokat képző kódokat. A módszertan lehetővé tette számomra az adatelemzés adatgyűjtéssel egyidejű megkezdését, hogy elősegítse a folyamat során az új kutatási kérdések kialakulását, ezáltal a felmerülő újabb kérdésekre is válaszokat gyűjthettem. A grounded theory egy induktív módszertan, mert a konkrét, empirikus eredményekből indul, és a kutatott problémát irányító általános elvek meghatározására törekszik; továbbá deduktív megközelítés, mert leteszteli az elméleti jellegű sejtések érvényességét a korábban definiált eredményeken [64]. Ez olyan területek kutatása során alkalmazható tudományos módszertan, melyekben kevés vagy hiányos az elérhető szakirodalom, továbbá nem állnak rendelkezésre statisztikai adatok, mint a jelen értekezésben definiált probléma.

Thomas Kuhn (1962) [65] gondolatai alapján a paradigma egy adott időszakra jellemző, tudományos körökben általánosan elfogadott zárt nézetrendszer arról, hogy egy meghatározott tudomány határai hol húzódnak. Azonban a paradigma a terület kutatása és az új elméletek fejlődése során egy ponton válságba juthat, és a további fejlődés érdekében változni kényszerül. Jelen doktori értekezésben a katonai műszaki tudományok körébe tartozó ipari kémkedés problémakörét a társadalomtudományok lencséjén keresztül is vizsgáltam, melynek során szintén érintettem az informatikai, a közgazdaság, a politika továbbá a pszichológiai tudományok területét, kiemelten vizsgálva a humán faktor szerepét. Az értekezés olyan szokatlan, új eredményeket hozhat, melyek a paradigma határainak feszegetésével, a tudományág bizonyos területeinek átrendezésével

kerülhetnek csak a rendszerbe. A definiált tudományos problémát hiányos és bizonytalan források jellemezik, így kutatása számos új tudományos eredményt hozhat. Ez azon kutatók számára, akik korábban behatárolt keretek között mozogtak, ellenérzést válthat ki, hiszen olyan megvilágításba helyez jelenségeket, melyek a korábbi tudásrendbe nem illeszthetők be.

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 képességekkel rendelkezik, így tevékenysége során az ipari kémkedés jelentős kockázatot jelent. Az évek alatt számos információlopási törekvést észleltünk, melyek eredményeként született meg jelen értekezés gondolata, mely széleskörű szakmai alapokra épít. A kutatás tervezése során a következő **célkitűzéseket (C)** fogalmaztam meg:

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

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

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

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

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

A téma kutatásának propozíciói

Mivel az ipari kémkedés témaköre a fent jelzett okok miatt nem, illetve csak felszínesen vizsgálható kvantitatív módon, ezért a hagyományos hipotetikus deduktív modell ezen probléma feltárása során nem hozna elméleti vagy gyakorlati felhasználásra alkalmas eredményeket. Ennélfogva a kvalitatív grounded theory módszertan alkalmazása mellett döntöttem, melynek empirikus adatgyűjtése során magam kerestem fel a védelmi kkv-ket, hogy a gyűjtött adatokat kódolva definiálhassam kutatásom eredményeként a megalapozott elméletet[7].

Kvalitatív kutatás során nem szempont a pontosan megfogalmazott hipotézisek tesztelése, inkább a kutató igyekszik egy folyamatban lévő, előre nem megjósolható jelenség megértésére, melynek során az alapoktól kezdve keresi az összefüggéseket, majd állítja fel elméletet [64].

A grounded theory módszertan szerint a végső megalapozott elmélet 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 [66]. Mivel 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 [67]. A folyamat abduktív jellegének biztosítása érdekében is fontos elkerülni az előre megfogalmazott hipotézisek jelentette korlátozásokat [68]. Az alkalmazott módszertan során a hipotézisek az elméletalkotás eredményei és nem kiindulópontjai [66].

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

[7] A kutatás eredményként kapott megalapozott elmélet (*grounded theory*) egyezik a módszertan elnevezésével.

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

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

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

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

A kutatás felépítése

Az értekezésben először indoklom a **módszertan** választást, majd ismertetem az alkalmazott grounded theory módszertan attribútumait, melynek során hangsúlyt fektettem a kvalitatív eredmények megbízhatóságának alátámasztására, annak négy kritériumán keresztül (következetesség, átvihetőség, hitelesség és megerősíthetőség). Ezt követően elemzem az értekezés elméleti keretét adó kontingenciaelméletet, melynek során újszerű megközelítést alkalmazva az ipari kémkedést az innovatív védelmi kkv-re ható kontingenciatényezőként azonosítottam, majd bemutatom a kutatási kérdéseket és a célzott mintavétel során kiválasztott mintát (n=42). Az **elméleti megalapozás** során először áttekintem az európai védelmi ipar átalakulását, stratégiai szerepét és a kkv-k lehetőségeit. Ezt követően vizsgálom az ipari kémkedés motivációit és megnyilvánulási formáit, ezután kontextusba helyezem a humán faktort a vizsgált tudományos probléma területén, majd ismertetem az ipari kémkedés kockázatának mérséklési lehetőségeit szociotechnikai megközelítésből, továbbá az Ipar 4.0 információbiztonsági kihívásait az ipari kémkedés szemszögéből. Az **eredmények** leírása során ismertetem a gyűjtött empirikus adatok alapján meghatározott, az ipari kémkedés gyakoriságának növekedése mögött azonosított külső és belső kontingenciatényezőket, az észlelés és megelőzés

eszközeit és módszereit, majd az ipari kémkedés fejlődő fenyegetéseit és az újszerű védekezési eszközöket. A **diszkusszió** fejezetben összefoglalom az eredményeket, továbbá elfogadom vagy elvetem a definiált propozíciókat. Az **összegzett következtetések** során javaslatot teszek az ipari kémkedés megelőzésére és észlelésére alkalmas rendszer kialakítására. Az értekezés végén bemutatom az új tudományos eredményeket öt tézisben összefoglalva, az eredmények elméleti és gyakorlati hasznosíthatóságát, a kutatás limitációit, továbbá a jövőbeni kutatási irányokat. 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

Az ipari kémkedés egy olyan komplex probléma, mely vizsgálata multidiszciplináris megközelítést igényel, és nem rendelkezik általánosan elfogadott definícióval [13, 38, 69]. 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, 25, 39, 70, 71, 72, 73]. Az ipari kémkedés problémakörének nemzetközi vizsgálata nem tartozik a népszerű kutatási irányok közé, kevés az elérhető objektív és releváns tanulmány, továbbá a publikált eredményekben a konzisztencia hiánya figyelhető meg [34, 69]. A kutatók a kérdés vizsgálatát interdiszciplinárisan elkülönülve végzik és nincsenek általánosan elfogadott következtetések, így a szerzők nehezen dolgoznak egymás eredményeivel [38]. A vizsgált jelenség hátterének szakirodalmi megalapozását, továbbá az empirikus tanulmányok és országspecifikus adatok összehasonlítását megnehezíti, hogy a tudományos eredmények ismertetése során a terminológiahasználat nem konzisztens [34, 69].

A fejezet elején kifejtem, hogy miért esett a választásom kvalitatív módszerek alkalamzására a definiált tudományos probléma kutatásához. Ezt követően ismertetem a szakértői mélyinterjúk sajátosságait. A szakirodalom alapján áttekintem a grounded theory módszertant annak négy megbízhatósági kritériumán keresztül. A fejezet második felében bemutatom a kutatási kérdéseket (**K1-K4**), az ezek megfogalmazását indokló szakirodalmi hátteret, valamint a minta sajátosságait (n=42).

1.1. Kvalitatív kutatás folytatásának indoklása

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, 37, 74]. 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 [75]. 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 [76]. Amennyiben evidens bizonyíték áll a szervezet rendelkezésére, jellemzően a körülményes jogi folyamat, valamit 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, 75, 77].

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, utánzónak bélyegezni [17]. Számos esetben a szervezetek belső eljárás keretében, a vonatkozó munkajog szerinti fegyelmi intézkedések figyelembevételével közelítik meg a problémát [70], vagy az áldozatok peren kívüli megállapodás kötésére törekednek az elkövetővel, amikor felmerül az ipari kémkedés gyanúja [77]. 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, 78].

A nyilvánosan elérhető adatok alapján ritkán történnek belső értintettek által elkövetett incidensek, azonban valószínűbb, hogy az 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, 37, 74, 75]. 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 [79]. Az így kapott eredmények alapot biztosítanak a probléma kvantitatív elemzéséhez és a bizonyításhoz szükséges matematikai-statisztikai jellegű modellezéshez [79].

1.2. Szakértői mélyinterjú

Kvalitatív mélyinterjúk alkalmazása célravezető módszer érzékeny témák – mint a védelmi vállalkozások számára kritikus ipari kémkedés – mélyebb feltárására [79, 80], mivel az adatfelvétel során két személy a közös érdeklődési körükbe tartozó témáról beszélget [81]. 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 vállhat [82]. 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 [79, 83]. 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 [83].

A szakértői mélyinterjú általában vállalatvezetőkkel vagy valamely területen kimagasló tudással rendelkező szakértőkkel készül, melynek során a kutatási témában különösen jártas személyek véleményének és tapasztalatainak megismerése a cél [84]. 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 [85]. A szakértői mélyinterjúk alkalmával a vezérfonal biztosítja, hogy a beszélgetés témája egyezzen a kutatott problémával. Az elméletet rigorózusan véve kvalitatív kutatás során nincs szükség a vezérfonalra, mert korlátozza az interjúalany információátadását, azonban a gyakorlatban az adatfelvétel folyamán a teljes strukturálatlanság nehézkes és adathiányhoz vezethet [86]. Az adatgyűjtési módszer alkalamzása során a moderátor nem lehet felkészületlen, hiszen a téma kifejtése során újabb kérdéseket szükséges feltenni, különben a beszélgetés elakad, illetve befejeződik; továbbá a beszélgetések a vezérfonaltól eltérhetnek, a kérdések tartalmát, sorrendjét, és az interjú hosszát az interjúkészítő és a válaszadó interakciója folyamatosan befolyásolja [87]. Az interjúk során az interjúkészítő megalapozza a beszélgetés fő irányát, majd végigköveti az interjúalany által felvetett témakörökön keresztül, így az interjúterv rugalmas, iteratív és folytonos, nem előre meghatározott [64]. A szakértői mélyinterjú egy olyan adatgyűjtési módszer, amely eredményei megfelelőek a grounded theory módsztannal való feldolgozásra [88].

1.3. Grounded theory módszertan 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 [80, 89, 90, 91], melynek az alkalmazása során az elmélet empirikus adatokból fejlődik ki [92]. A módszer az elméleti és empirikus kutatás közötti szakadékot hivatott áthidalni [66], és lehetővé teszi a kutató számára, hogy alaposan megfigyeljen egy problémát, melynek során a szisztematikusan gyűjtött adatokból alakul ki az elmélet [92]. A metódus célja a koncepció azonosítása a problémák és lehetséges megoldási lehetőségek megértésén keresztül [87]. A grounded theory módszertan alkalmazása olyan kutatási munkák során ajánlott, amikor a vizsgált problémával kapcsolatban nem érhető el korábbi releváns elmélet [93].

A doktori értekezésben a gyűjtött adatok elemzése a grounded theory módszertan konstruktivista megközelítéséből történt, amely az empirikus világ első kézből való megtapasztalására épít [67], mely használata közben elkerülhetetlen, hogy a korábbi szekunder információk, ismeretek és tapasztalatok hatással legyenek a kutatás eredményeire [94]. Az irányzat kódolási eljárása és mechanizmusai támogatják a korábbi ismeretek beépítését, így lehetővé téve a gyakorlati és elméleti megközelítését a vizsgált problémának [87]. Konstruktivista irányzatot alkalmazva a grounded theory **abduktív**, mert logikai következtetéseket von le a megfigyelt jelenségről; **induktív**, mivel az elméletet a gyűjtött adatokból vezeti le; ugyanakkor **deduktív**, mert az elmélet fejlődése során az eredményeket összeveti a szakirodalommal [87, 91].

Kvalitatív kutatás során a definiált eredmények megítélésének legfontosabb kritériuma a **megbízhatóság** [95, 96, 97], amely a következetességből, az átvihetőségből, a hitelességből, és a megerősíthetőségből tevődik össze [97, 98, 99]. Az eredmények megbízhatóságának biztosítása érdekében jelen kutatás figyelembe veszi ezen szempontokat, 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 [97]	**A kritérium követelménye és módszerei**	**A kritérium teljesítése jelen tanulmányban**
Következetesség (*Dependability*)	Az eredmények következetesek és megbízhatók, a kutatás folyamata szigorúan dokumentált [92, 98]	○ A kutatás folyamata, az adatgyűjtés, az alanyok és az adatelemzés részletes bemutatása.
Átvihetőség (*Transferability*)	Az eredmények mennyire alkalmazhatók egyéb körülmények között [100], szélesebb populációra [99]. ○ Gyakorlati alkalmazhatóság kérdése [98]	○ 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 (*Credibility*)	Az eredmények mennyire összeegyeztethetők a valósággal [100], mennyire képviselik az interjúalanyok a téma valódi jelentését [97]. ○ Optimális módszer kiválasztása [101] ○ Megfelelő alanyok kiválasztása [99, 101] ○ Elmélettel való összehasonlítás [87, 91] ○ Gyűjtött és feldolgozott adat mennyisége [101] ○ Reflektálás [92] ○ Trianguláció [98, 102] ○ Iteratív kérdések [99]	○ 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 (*Confirmability)*	Az eredmények az alanyoktól származnak, és nincsnek befolyásolva a kutató által [97]. A következtetések kapcsolódnak az eredményekhez, és a kutatás azonos eredményekkel megismételhető [98]. ○ A kutatás folyamata szigorúan dokumentált [92, 98] ○ Trianguláció [99]	○ A megerősíthetőség bizonyításának limitációja, hogy longitudinális vizsgálatra lenne szükség mely jelen értekezésben 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

A narratív megközelítés lehetővé teszi az emberközeli, gyakorlatban alkalmazható eredmények generálását többek között a gazdasági és menedzsmenttudományok [103], továbbá a pszichológiai és társadalomtudományok [104] területén. A grounded theory módszertan alkalmazása során a narratív elemzési technikák hozzájárulnak a komplex probléma empirikus szemléletű feltárásához [105], 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 [106]. Mivel ez a módszer rugalmas, ugyanakkor kellően stabil, így képes a definiált kutatási kérdésre vonatkozó tudományos eredmény alapját biztosítani [107]. A narratív elemzés, mely az emberi szándékokkal, cselekedetekkel, egyéni helyzetekkel és pszichés valósággal foglalkozik, az észlelt tényezőket egymással valamilyen relációba állítja, és azoknak közös jelentést tulajdonít [108].

1.3.1. Következetesség

Kvalitatív kutatás során a **következetesség** azt feltételezi, hogy az eredmények következetesek és megbízhatók, valamint a kutatás menete szigorúan dokumentált, lehetővé téve, hogy a kutatómunkában nem érintett személyek követni, ellenőrizni és bírálni tudják a folyamatot [92, 98]. 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 [99]. Jelen doktori értekezésben az eredmények megbízhatóságát a kutatási folyamat szigorú dokumentálása biztosítja a kutatás tervezésétől az eredmények értékeléséig. Bár a grounded theory módszertan 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 [67]. Jelen értekezésben 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 [68].

Glaser és Strauss (1967) [92], a módszer megalkotói szerint a kvalitatív adatfelvétel nem csak válaszokat, hanem kérdéseket is szolgáltat, melyek segítségével újabb kutatási

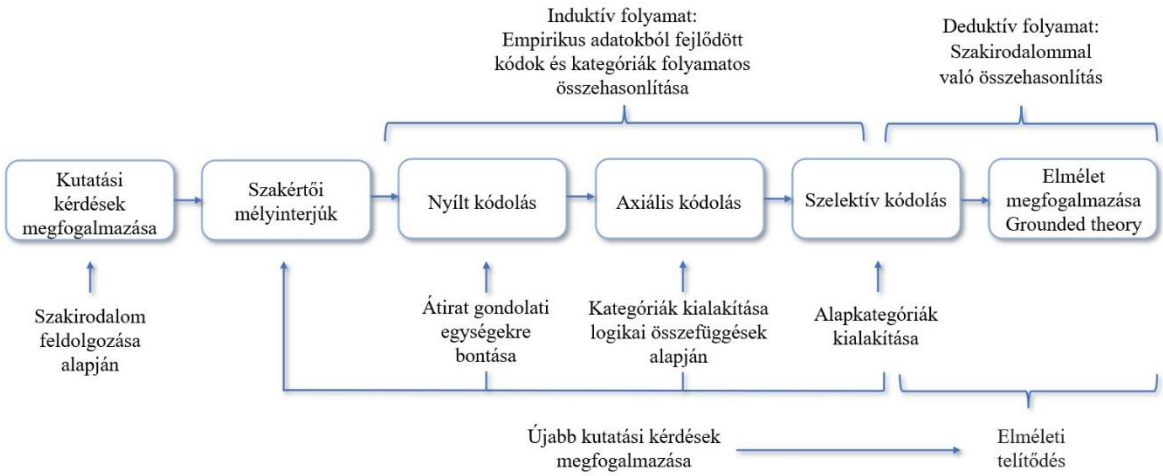
irányok azonosíthatók. A grounded theory módszertan nem határozza meg előre a minta jellemzőit, hanem az az elmélet fejlődésével folyamatosan alakul, az éppen feltárt eredmények és újonnan felmerülő kutatási kérdések vezetik a kutatót az újabb alanyokig egészen az elméleti telítődésig [67]. Jelen kutatás során az adatfelvétel három szakaszban történt, azzal a céllal, hogy az eredmények elemzése során felmerülő újabb kérdésekkel gazdagítsa az elméletet.

A gyűjtött empirikus adatokból való elméletalkotás különböző szinteken történő analizálást igényel [109], kifejezésenként haladó adatelemzésre épül, továbbá a kutatás során folyamatosan új kategóriákat generál, mely eredményeként a vizsgált jelenséget általános elvi képletekkel magyarázza [66]. A módszertan szerint nem szabad az adatokat előre kialakított fogalomkörökbe erőltetni, azokat folyamatos összehasonlítás közben kialakított kategóriákba kell osztályozni [110]. Jelen kutatás Strauss és Corbin (1990) [68] 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 [109]. A **következő lépés** az axiális kódolás, ami a kódok és kategóriák csökkentésére és összevonására irányuló köztes módszer [67, 68]. 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 [111]. A **harmadik lépés** a szelektív kódolás, melynek során létrejönnek az alapkategóriák, amelyek a kialakuló elmélet forrását képviselik [67]. Ezután következhet az elmélet megfogalmazása, mely a fogalmak és kategóriák közötti kapcsolatok meghatározását jelenti [109].

A társadalomtudományok területén kvalitatív kutatás folytatása során folytonos visszacsatolás valósul meg az adatgyűjtés és az elmélet megfogalmazása között [64]. 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 [67]. Végül a hitelesség biztosítása érekében az

eredmények korábban megfogalmazott elméletekkel való összehasonlítása történik [91]. A 2. ábra szemlélteti a grounded theory módszertan folyamatát.



2. ábra: Grounded theory módszertan folyamata

Forrás: saját szerkesztés Glaser és Strauss (1967) [92]; Mitev (2012) [67]; Charmaz (2014) [91] és Kelemenné Erdős (2014) [87] alapján

1.3.2. 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 [97, 100]. Bár kvalitatív kutatás folytatásánál nem feltétlenül elvárás a reprezentativitás, ezzel szemben az átvihetőség kritériumának szempontjából bizonyítani kell, hogy az eredmények alkalmazhatók a szélesebb populációra [99]. Az átvihetőség teljesülését támogatja a résztvevők kiválasztásának és jellemzőinek, továbbá az adatgyűjtés körülményeinek részletes leírása, ezenfelül az eredmények gazdag bemutatása [101]. Ez a kritérium kritikus fontosságú a kutatási eredmények gyakorlati alkalmazásának szempontjából, mivel a szervezet döntéshozói sok esetben csak egy vagy néhány kutatásból származó eredményre, következtetésre és javaslatra támaszkodhatnak, amelyek gyakorlati felhasználása a kutatási környezettől eltérő kontextusban kerül bizonyításra [98]. Jelen kutatás során az átvihetőséget biztosítja, hogy az adatfelvétel kilenc különböző európai országban, a védelmi ipar számos területét foglalta magába, mely részletes ismertetése az 1.6. fejezetben olvasható. A 101. oldalon kerül bemutatásra az eredmények elméleti hasznosíthatósága, a 103. oldalon az eredmények gyakorlati alkalmazhatósága, és a 106. oldalon a definiált jövőbeni kutatási irányok.

1.3.3. Hitelesség

A kvalitatív kutatás **hitelessége** arra vonatkozik, hogy az eredmények milyen szinten összeegyeztethetők a valósággal [100], továbbá mennyire képviselik a kutatásban résztvevők által megosztott gondolatok valódi jelentését [97]. A kritérium biztosításának egyik módszere a kutatási problémához legjobban illeszkedő módszertan kiválasztása [101]. A témát korábban feldolgozó módszerek átvétele bevált gyakorlat a kvalitatív kutatások hitelességének biztosítására [93], amelyeknek azon szerzők kutatásaiból kell származni, akik már eredményesen alkalmazták korábban hasonló problémák feldolgozása során [99]. (1) Connolly és szerzőtársai (2015) [112] a szervezeti érintettek információbiztonsághoz kapcsolódó attitűdjét vizsgálta; (2) Alsowail és Al-Shehari (2020) [113] szisztematikusan rendszerezte az ipari kémkedéshez fűződő kísérleteket azonosító technikákat; (3) Boakye és Gyan (2021) [114] az innovatív kkv-knál kialakítható olyan program definiálásán dolgozott, mely csökkentheti a kutatott probléma kockázatát; (4) Khan és szerzőtársai (2022) [115] a belső fenyegetés nem szándékos formáját és annak következményeit vizsgálták; (5) Purl és Greitzer (2022) [116] az ipari kémkedés dinamikáját és az azt elkövető entitások karakterisztikáit kutatták; (6) továbbá Robayo (2022) [117] 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) [92] a jelen értekezésben használt grounded theory módszertan alkalmazása során a reflektálást tartják a hitelesség alapjának, amely megtörtént 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 [118]. Azonban az alkalmazott grounded theory konstruktivista megközelítése deduktív természetű is egyben, mivel lehetővé teszi az elmélet fejlődése során az eredmények szakirodalommal való összevetését [87, 91]. 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 [101]. Iteratív kérdések segítségével, melyek során a kutató visszatér a korábbi

témákhoz, hogy felismerje az esetleg felmerülő ellentmondásokat, valamint non-verbális jelek alapján lehetőség van valamelyest kiszűrni, hogy az interjúalany az igazat osztja meg a kérdéssel kapcsolatban [99].

A kvalitatív kutatások hitelességét a többforrású adatgyűjtéssel megvalósítható trianguláció biztosítja, mely különböző módszerek, technikák vagy források együttes használatát jelenti [98, 102]. Ezek erősíthetik vagy korrigálhatják egymást a kutatómunka során, továbbá alkalmazásukkal elkerülhető, hogy kevés vagy korlátozott információból történjen a következtetések levonása [102, 119]. A különböző adatforrások használata, továbbá az időben és térben széles spektrumú nézőpontok figyelembevétele megfelelőbb és stabilabb képet adhatnak a valóságról [120]. Az eltérő módszerek együttes használata ellensúlyozza azok korlátait, és egyben kihasználja a heterogén metódusok alkalmazásából származó előnyöket [119].

1.3.4. Megerősíthetőség

Az eredmények **megerősíthetőségéhez** bizonyítani szükséges, hogy a kutatás eredményei kizárólag a megkérdezett alanyoktól és azok körülményeitől függenek, és nincsnek befolyásolva a kutatást végző személy előítéletei, motivációi és érdekei által [97], továbbá a levont következtetések világosan kapcsolódnak az eredményekhez, és a kutatási folyamat közel azonos eredményekkel megismételhető legyen [98]. 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 [99]. 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.

1.4. Az ipari kémkedés, mint kontingenciatényező

A kontingenciaelmélet 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 dinamikusan változó környezethez. Az elmélet alapján azon szervezeteknek van a legnagyobb esélyük a sikeres működésre, amelyek rugalmasan és gyorsan képesek reagálni a külső lehetőségekre és fenyegetésekre. A fejezetben a kontingenciaelmélet szakirodalmi hátterét tekintem át, majd levonom a következtetést, hogy az elmélet alkalmazása során a kutatóknak megvan az a szabadsága, hogy az általuk vizsgált területre leginkább ható környezeti változókat definiálják.

A klasszikus elméletek (Taylor, Fayol, Weber) a szervezetet egy zárt rendszernek tekintették, melynek határai összetartották a vállalkozás elemeit és elválasztották a környezeti tényezőktől [59]. Az 1960-as évektől, a kontingenciaelmélet 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 [121]. 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 lennie valamennyi irányból a hatékony működés érdekében [122]. Ez a modern menedzsmentelmélet 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 [59]. Az elméletet feldolgozó szakirodalom elemzése során azonban nem szabad figyelmen kívül hagyni, hogy az 1960-as évek óta a kontingenciaelmélet hatóköre jelentősen kiszélesedett, a gazdasági tényezők globalizálódtak, a szervezetet körülvevő környezet átalakult és korábban ismeretlen fenyegetések jelentek meg, a teljes ellátási lánc átfogása helyett csak egy meghatározott tevékenységre fókuszálnak, továbbá a vállalatok jellemzően laposabb szervezeti struktúrával rendelkeznek [123].

Az elmélet a szervezeti viselkedést abból a szempontból vizsgálja, hogy a kontingenciatényezők hogyan befolyásolják a vállalkozás kialakítását és működését [124]. Az alapvető állítása szerint a környezet, amelyben az intézmény működik, határozza meg a legjobb szervezésmódot [57, 58]. Emellett két alapfelvetése, hogy nincs

egyetlen legjobb módja a szervezésnek, és a különböző módszerek nem egyformán hatékonyak [124, 125]. A környezeti kontingenciaváltozók és a szervezettervezési paraméterek közötti legoptimálisabb illeszkedés megtalálása a legnagyobb hatékonyságot eredményezheti [57]. A vállalkozás teljesítménye, bár különböző mértékben, de egyszerre több tényező összhangjának függvénye [58, 60]. A környezetébe hatékonyan illeszkedni képes szervezet magasabb termelékenységet érhet el, alkalmas lehet többletforrást generálni, ami fejlődéshez, terjeszkedéshez és az innovációs hajlam növekedéséhez vezethet [126]. 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 [60].

Bár a kontingenciaelmélet kutatói egyetértenek abban, hogy a klasszikus iskolák felfogása téves abból a szempontból, hogy létezne egyetlen legjobb módja egy szervezet sikeres működtetésének [58, 59, 60, 61, 124, 125], 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 [58, 61], melyek többek között az alábbiak:

(1) Hayes (1977) [127] három fő kategóriát fogalmazott meg, melyek a szervezeti belső tényezők, a kölcsönösen függőségi tényezők, és a külső tényezők. (2) Mintzberg (1979) [128] 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) [128] tizenegy kategóriáját Child (1981) [129] kiegészítette a nemzeti kultúrával. (4) Donaldson (2001) [61] szintén három fő kategóriát hozott létre, melyek a szervezet mérete, stratégiája és annak környezete. (5) Betts (2003) [57] az alkalmazott technológiát, a szervezet környezetét, méretét és életkorát kategorizálta legfontosabb kontingenciatényezőknek. Az évek során számos új – a saját kutatási területükön releváns – kategóriát hoztak létre a kutatók, mint például (6) Wong és szerzőtársai (2012) [130] az ellátási láncot, a piaci versenyt, a versenytársakat, és az információáramlást; (7) Alves és szerzőtársai (2017) [131] a klímaváltozást, a károsanyag kibocsátást és fenntarthatóságot; (8) továbbá Engelseth és Kritchanchai (2018) [132] a

kórházi infrastruktúrát, az egészségügyi szolgáltatások színvonalát, és a gyógyászati célú turizmust nevezték meg.

Az ismertetett kontingenciaváltozókból 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 során egy újszerű megközelítést alkalmaztam, és az ipari kémkedés problémakörét a környezeti kontingenciaváltozók közé soroltam, 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.

1.5. Kutatási kérdések

Jelen értekezésben a kutatási kérdések definiálását megelőzte a témában rendelkezésre álló szakirodalom alapos vizsgálata, mivel a grounded theory módszertan alkalmazása közben a kutatási kérdéseknek az átfogó irodalmi feldolgozáshoz kell kapcsolódnia [68]. A 2. táblázat szemlélteti azon szekunder eredményeket, melyek megalapozták a **kutatási kérdések** definiálását.

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 kontingenciatényezők, 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 rendszeresítése a szervezetnél	Williams et al. (2019), Samy et al. (2021)	
Nem megfelelő szervezeti magatartás és kultúra, ami hűtlenséghez vezet	Nasheri (2004), Vashisth – Kumar (2013)	Faktorok, melyek hozzájárulnak a munkavállalók szervezethez való hűtlenségéhez.
Külső nyomás, zsarolás vagy megvesztegetés	Sinha (2012), Duckworth – De Silva (2019), Button (2020)	Attribútumok, melyek elősegítik a munkavállaló szándékosan elkövetett információbiztonsági támadásait a szervezet ellen.

MEGELŐZÉS ÉS VÉDEKEZÉS		
Fizikai védekezés	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) hátterű védekezés	Hills – Anjali (2017), Homoliak et al. (2020), Saxena et al. (2020)	
JÖVŐBENI INFORMÁCIÓBIZTONSÁGI KIHÍVÁSOK		
Mesterséges intelligencia	Zīle – 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: Kutatási kérdések megalapozása

Forrás: Saját szerkesztés

A tudományos problémát vizsgáló szerzők eredményei alapján az ipari kémkedés gyakorisága növekszik [14, 133, 134], azonban azt nem vizsgálták, hogy milyen tényezők okozzák az esetszámok növekedését (**K1**). A tudományos magyarázatok alapja, hogy a vizsgált jelenségek determináltak, vagyis valami előidézi őket [64]. Ezen tényezők megismerése iránymutatást ad, hogy milyen természetű információbiztonsági fenyegetéseket szükséges számításba venni az információvédelmi rendszer tervezése során annak érdekében, hogy a vállalkozás képes legyen megelőzni és észlelni a kritikus információt célzó támadásokat, így csökkentve a szervezetet fenyegető ipari kémkedés súlyos következményeit. Ezek feltárása azért is lényeges, mert a kontingenciaelmélet alapján nagymértékben befolyásolják a szervezet működését [57, 58].

Az emberi tényező kutatása azért szükséges, mert a munkavállalók által megtestesített belső fenyegetés a legkritikusabb információbiztonsági probléma a vállalkozás szempontjából (**K2**). Dokko és szerzőtársai (2021) [135] eredményei alapján az ipari kémkedéshez fűződő esetek 85%-át követik el jelenlegi vagy volt munkavállalók, azonban kevés a szervezeti érintettek által megtestesített fenyegetés mögötti okokat vizsgáló szakirodalom [33, 37, 38, 39].

Számos vállalkozás használ olyan információvédelmi rendszereket, melyek kizárólag az IT fenyegetésekre összpontosítanak [31, 32], azonban ez a megközelítés hibákat és biztonsági réseket okozhat [75, 136]. Ennélfogva jelen kutatás fókusza arra a kérdésre is kiterjed, hogy a kkv-k milyen szociotechnikai megközelítésű információvédelmi intézkedésekkel képesek csökkenteni az ipari kémkedés kockázatát (**K3**).

Az egyre változatosabb technológiai innovációk hatására feltételezhetően tovább fog fokozódni az ipari kémkedés fenyegetése [137, 138], amely hatására egyre jelentősségteljesebbé vállnak a döntéshozók által tett információvédelmi erőfeszítések. Így jelen kutatás során arra is válaszokat kerestem, hogy milyen természetű jövőbeni fenyegetésekre szükséges felkészülni az innovatív védelmi vállalkozások vezetőinek (**K4**).

A szakértői mélyinterjúk során alkalmazott magyar és angol nyelvű vezérfonalakat a kutatási kérdések alapján fogalmaztam meg, melyek megtekinthetők az 1–4. számú mellékletekben. 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.

A tudományos művek elemzése során azonosításra kerültek az elméleti hiányosságok, melyek alapján a következő kutatási kérdések fogalmaztam meg:

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 kontingenciatényezők mellett a jelenleg alkalmazott ipari kémkedési módszerek és technikák alapján milyen természetű jövőbeni fenyegetésekre kell felkészülni az innovatív védelmi vállalkozások vezetőinek?

1.6. Minta

Az adatgyűjtés célzott mintavétellel történt, mely lehetővé teszi, hogy a résztvevők a vizsgált téma szempontjából releváns tulajdonságaik szerint kerüljenek meghatározásra [139]. A módszer alkalmazása során a kutató választja ki a tervezett beszélgetéseken résztvevő azon személyeket, illetve szervezeteket, akik képesek és hajlandóak releváns információval hozzájárulni az előre definiált probléma kutatásához tudásuk és tapasztalataik alapján [140]. 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 [141]. 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 [139].

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 [92]. Kvalitatív kutatás során bár statisztikailag érvényes következtetések nem vonhatók le, azonban értékes betekintést nyújt az adott kérdéskörrel foglalkozó szakértők gyakorlati tapasztalataiba, viselkedésébe, indítékaiba és gondolkodásmódjába [79].

A mélyinterjúk olyan személyekkel zajlottak, akik a védelmi iparban folytatott 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 szolgáltattak 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.

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

3. táblázat: Az interjúalanyok jellemzői

Forrás: saját szerkesztés (n=42)

Az interjúk magyar és angol nyelven folytak, a vezérfonalak az 1–4. számú mellékletekben találhatók. 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 [142]. Azonban a nyelvi egyezőség elve kimondja, hogy az eltérő nyelvű vezérfonalak jelentésének azonosnak kell maradni az előre definiált probléma feltárására alkalmas adatok gyűjtéséhez [143]. 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 tájékoztatva lettek, 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 átalakulása, stratégiai szerepe és a kis- és középvállalkozások lehetőségei

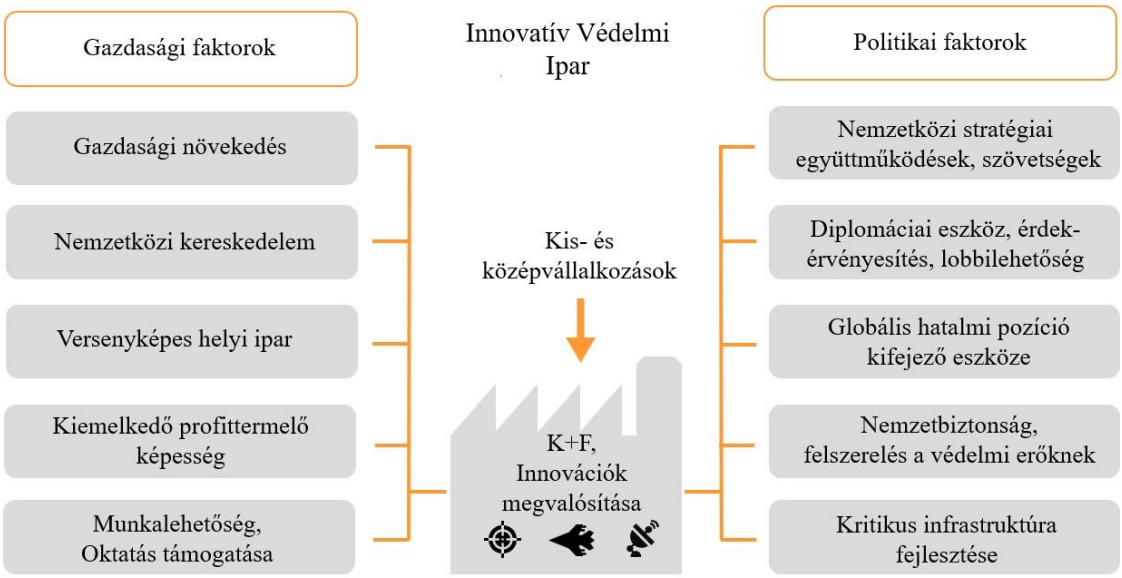
A fejezetben kifejtem az európai védelmi ipar által betöltött szerepet, majd ismertetem azokat a gazdasági, politikai és nemzetbiztonsági szempontokat, amelyeket az államok figyelembe vesznek a védelmi ipar fejlesztése során. Ezt követően röviden áttekintem a védelmi ipar szerkezetében bekövetkezett átalakulást, mely lehetőséget teremtett a kkv-k számára, hogy versenyképesen működhessenek az ágazatban, továbbá bemutatom a védelmi innovációk lokális fejlesztésének előnyeit.

A védelmi ipar attribútumait vizsgáló kutatók egyetértenek abban, hogy az ágazat stratégiai szerepet játszik valamennyi államban [54, 144, 145, 146, 147, 148]. 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 [54, 144, 145, 149, 150, 151]. A tudásintenzív ágazat támogatja az oktatást, az egészségügyet, csökkenti a munkanélküliséget, ezenfelül munka- és kutatási lehetőséget teremt magasan képzett szakértők számára [54, 144, 145]. A védelmi ipar kritikus infrastruktúrával látja el a lakosságot, amely magában foglalja a gyárakat és egyéb termeléshez szükséges létesítményeket, közlekedési hálózatokat[8], víz-, és energia hálózatokat, a kommunikációs rendszereket, iskolákat, oktatási központokat és kórházakat [152]. Az európai védelmi ágazat olyan gazdasági, politikai és technológiai tényezőket ölel fel, melyek kiemelten támogatják a helyi ipar globális versenyképességét [46], továbbá a szektorra jellemző intenzív KFI eredményeként számos technológiai újdonsággal látja el a társadalmat [6, 42, 47, 48].

A lokális védelmi ipar fejlesztése gazdasági, politikai és nemzetbiztonsági szempontok figyelembevételével történik. Az ágazat megfelelő infrastruktúrával és kiemelkedő tudással és tapasztalattal rendelkező szakértőkkel támogatva kimagasló profitot képes realizálni [153, 154], ezenfelül a modern helyi védelmi ipar a nemzet politikai pozíciójának kifejező eszköze [149, 155, 156, 157]. A jelenkori gazdasági és geopolitikai környezetben a védelmi eszközök exportja a diplomáciai kapcsolatok fontos területévé

[8] Közúthálózat, sínhálózat, reptér, vízi közlekedés.

vált [158, 159, 160, 161], amely lehetőséget biztosít a nemzetközi viszonyok békés úton történő rendezésére [162]. A védelmi eszközök szövetséges államoknak történő exportja erősíti a nemzet regionális és globális politikai pozícióját [159, 163], támogatja a stratégiai szövetségek kötését és fenntartását [154, 164], növeli a nemzetbiztonságot a globális fenyegetésekkel szemben [165], továbbá fokozza a nemzet politikai befolyását, így biztosítva lobbilehetőséget a globális közösségben [166]. A 3. ábra szemlélteti az innovatív lokális védelmi ipar stratégiai sajátosságait gazdasági és politikai szempontból.



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

Forrás: saját szerkesztés

Az innovatív védelmi ipar fejlesztését nemzetbiztonsági szempontból indokolja, hogy a minőségi haditechnikai eszközök lokális fejlesztése jobban igazodik a helyi haderő igényeihez, hozzájárul az ellátásbiztonság fenntartásához és erősíti egy nemzet haderejének hadrafoghatóságát és műveleti képességét [28]. A technológiai fölény mindig is fontos tényező volt a hadviselés során, azonban az ipar dinamikus fejlődésének eredményeként technológiai szakadék nyílt a világ hadseregei között. Így ahhoz, hogy a helyi haderő képes legyen a feladata ellátására, elengedhetetlen, hogy a legmodernebb haditechnikai eszközökkel legyen felszerelve, ezáltal a védelmi iparnak fontos feladata, hogy olyan felszerelést adjon a katonák kezébe, amelyek megfelelnek a kor technológiai színvonalának [167]. Védelmi innovációk fejlesztése során fontos szempont, hogy figyelembe vegyék a haderő igényeit. Mérnöki szempontból lehet egy innováció érdekes, azonban nem biztos, hogy valós harctéri körülmények között beváltja a hozzáfűzött reményeket [42].

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, kisszériás, precíziós védelmi rendszerek irányába, valamit a globalizációs hatások és a geopolitikai átrendeződés mind olyan változók, melyek kényszerítették a védelmi ágazat szereplőit, hogy alkalmazkodjanak az új feltételekhez [2, 55, 56, 156, 157]. 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, 55, 156, 168]. Az internacionális kooperációk következményeként megkezdődött a külföldi tőke beáramlása, ami hozzájárult a hosszútávon fenntartható lokális védelmi bázis kialakításához [56, 157, 169]. 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 mérsékelték [170, 171, 172, 173, 174]. Az ipar fejlesztéséhez szükséges információ országhatáron kívüli forrásból való beszerzésének lehetősége innovációs hullámot eredményezett [171, 175, 176, 177]. A könnyebben hozzáférhető technológiatranszfer a kevésbé iparosodott országokat is támogatta a helyi védelmi ipar fejlesztésében, így utat nyitva számukra a transznacionális védelmi hálózatba [146, 156]. Az ágazatban bekövetkezett átalakulás egy olyan technológiai forradalmat indított be, melynek eredményeként a védelmi ipar vezetővé vált a KFI területén.

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, stratégiailag függetlenebb és erősebb nemzetközi politikai pozíciót képes fenntartani [42]. 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 [43, 49, 176, 178]. 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, 157, 179, 180]. Bár a szektorban még mindig jellemző az autarkiára való törekvés, azonban a nemzetek többsége korlátozott erőforrásokkal rendelkezik [181], 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, 169, 175, 179, 181]. Az autarkia a védelmi iparban 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 [182, 183]. Ezáltal 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 országhatárokon átnyúló együttműködéssel [45]. 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 [46].

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 [159, 184, 185]. Azok a szervezetek, amelyek elsőként tesznek lépéseket az új technológiák átvételére, amik később dominánssá vállnak, általában megőrzik versenyképességüket és sikeresek maradnak [186]. A nemzetek, melyek elsőként képesek rendszeresíteni az újdonságokat, jelentős stratégiai és taktikai előnyre képesek szert tenni [49].

Az elmúlt években a védelmi piac keresleti és kínálati oldala, a védelmi felszerelések gyártása és nemzetközi kereskedelme is dinamikus növekedést mutatott [54, 179, 187],

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 kémkedés problémakörének elméleti megalapozása

A fejezetben részletesen elemzem az ipari kémkedés jelenségét, bemutatva annak okait, folyamatát, típusait és módszereit. Ezt követően ismertetem a humán faktor ipari kémkedés területén betöltött szerepét, azon belső és külső, továbbá véletlen és szándékos megnyilvánulásain keresztül. Ezután áttekintem az ipari kémkedés fenyegetésének mérséklési lehetőségeit szociotechnikai megközelítésből, majd bemutatom az Ipar 4.0 által teremtett információbiztonsági kihívásokat.

Az **információbiztonság** olyan intézkedések összessége, melyek célja, hogy biztosítsák az információ biztonságát az egyén, a társadalom és az állam védelme érdekében [188]. A fogalom olyan információk tudatos megóvására terjed ki, amelyeket véletlen vagy szándékos, természeti vagy emberi tényezők elleni védelemmel látnak el, mert ezek sérülése nemcsak azok tulajdonosainak, hanem felhasználóinak és a támogató infrastruktúrának is kárt okozhat [188]. Az információbiztonság három alappillére, (1) hogy az adott információ pontos és sértetlen legyen, (2) hogy az arra felhatalmazott felhasználó mindig hozzáférjen, (3) továbbá, hogy csak az arra jogosult vagy felhatalmazott személy számára legyen elérhető [189]. Az **ipari kémkedés** olyan, az információbiztonságot károsító tevékenységek összessége, melyek közös vonása, hogy az információt jogtalanul megszerző/birtokló entitás azt a saját előnyére törekszik fordítani. Az értekezésben az ipari kémkedés az emberi tényező véletlen vagy szándékosan kárt okozó, az információhoz való hozzáférés szabályait sértő cselekedeteit öleli fel.

Az ipari 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 kémkedéssel összefüggésbe hozható incidensek gyakorisága, továbbá a nemzeti iparra, gazdaságra és a teljes nemzetbiztonságra gyakorolt negatív hatása az elérhető szekunder források alapján

globális szinten jelentős növekedést mutatott [14, 133, 134]. A végbemenő dinamikus technológiai fejlődés még több eszközt teremtett az információlopás elkövetésére, tovább fokozva a problémát, amely az egyik legsúlyosabb fenyegetéssé nőte ki magát az országok iparával és fenntartható fejlődésével szemben [190]. Az ipari kémkedés kiemelten fenyegeti azon szervezetek működését, mely feladatainak teljesítése a kritikus információ rendelkezésre állásától függ, melyek között az védelmi ipar az egyik legfenyegetettebb szektor [163, 191].

A 4. táblázat az ipari kémkedés elméleti megalapozása során érintett fő témaköröket foglalja össze.

Tényező	Probléma leírása	Szerző
KUTATÁSI PROBLÉMÁK[9]		
Nincs általánosan elfogadott definíció	Nem áll rendelkezésre szakirodalom a jelenség pontos meghatározására.	Carl (2017), Button (2020), Hou – Wang (2020)
Kevés a releváns tanulmány	A probléma nehezen kutatható terület, korlátozott tudományos figyelmet kap.	Brancik – Ghinita (2011), Omar (2015), Søilen (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 esteket, ami a statisztikák torzulásához vezet.	Crane (2005), Stadler (2012), Bedford – Van Der Laam (2016), Søilen (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 információlopás 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), Søilen (2016), Glitz – Meyersson (2020), Hou – Wang (2020), Ingesson (2023)
Ipari kémkedés módszerei	Az információlopás elkövetésére számos fizikai és információs technológiai módszer áll rendelkezésre, mely történhet belső szervezés, vagy külső kém megbízása során.	House (1995), Sinha (2012), Søilen (2016), Duckworth – De Silva (2019), Button (2020), Choi – Teresa (2020), Hou – Wang (2020), Lyan & Frenkel (2020), Kelemen-Erdős – Mészáros (2023)

[9] Az ipari kémkedés kutatási problémái az 1. Kutatási módszerek fejezetben kerülnek részletes bemutatásra.

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), Nasheri (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)
VÉDEKEZÉS SZOCIOTECHNIKAI MEGKÖZELÍTÉSBŐL		
Információbiztonsági kultúra	Magában foglal minden olyan intézkedést, melyek során az 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), Bedford – Van Der Laam (2016), Gheyas – Abdallah (2016), Elifoglu et al. (2018)
IPAR 4.0 INFORMÁCIÓBIZTONSÁGI KIHÍVÁSAI		
Innovatív megoldások, jövőbeni fenyegetések	Az információs technológia és mesterséges intelligencia alapú eszközök fejlődésével innovatív információvédelmi eszközök és ezzel párhuzamosan új fenyegetések jelennek meg.	Zīle – 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 kémkedés motivációi és megnyilvánulási formái

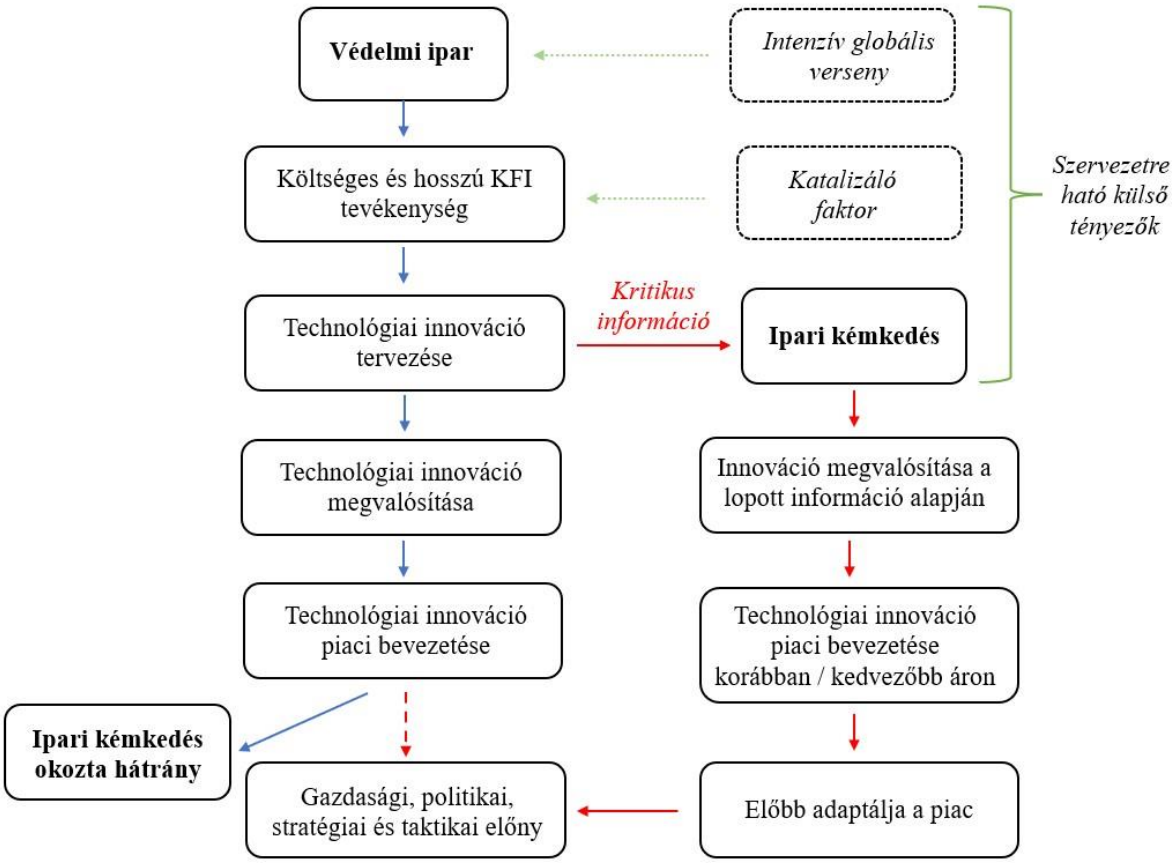
A védelmi iparban való működés feltétele a kritikus információ, melynek gyűjtése vagy előállítása hosszú és költséges folyamat, ami magában foglalja a külső környezet elemzését és a belső KFI tevékenységeket. Amennyiben a szervezet/állam sem belső, sem külső (nyílt) forrásból nem képes vagy hajlandó erőfeszítéseket tenni az igényelt technológiai innováció megvalósításához szükséges kritikus információ beszerzésére vagy előállítására, akkor merül fel az ipari kémkedés eszköztárának alkalmazása [192]. Jelen fejezet során elemzem az ipari kémkedés motivációit, folyamatát, megnyilvánulási formáit, a lehetséges elkövetők sajátosságait, valamit az általuk alkalmazott módszereket.

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 [17]. 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 piacvezetőkké válhatnak és lobbilehetőséget szerezhetnek kormányzati szerveknél, hogy befolyásolják az iparágukkal kapcsolatos gazdasági döntéseket [19].

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 [193]. Az információlopás fenyegetése nem csak abból következik, hogy a szervezetek nagy mennyiségű kritikus információt tárolnak elektronikusan vagy felhőben, közvetlenül a világhálóhoz csatlakozva, – amit kihasználnak a kiber-kémek, akiknek kiléte gyakran ismeretlen marad, [194] – hanem abból is, hogy a széles körben elterjedő technológiai újdonságok sok esetben fizikai érintkezés és egyéb nehézségek nélkül tettek hozzáférhetővé nagy mennyiségű kritikus információt [12]. Ezen átalakulások egyre több szervezetet bátorítanak fel arra, hogy kihasználják ezt a költség- és időhatékony információszerzési módszert [25].

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 területén kiemelkedő teljesítményt nyújtanak a kkv-k [3, 42, 48, 49, 50], mivel azonban nem rendelkeznek a nagyvállalatok pénzügyi, humán és technológiai erőforrásával, így jellemzőbb az ipari kémkedés [16, 75].



4. ábra: Ipari kémkedés folyamata

Forrás: saját szerkesztés

Témavezetőmmel folytatott [29] korábbi kutatásunk 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 feladatainak 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 résztét veszítheti el, hanem a KFI-be fektetett hatalmas költségeket, továbbá nem élvezheti a technológia elsőként való bemutatásával járó stratégiai és harcászati taktikai előnyöket. Emellett az illegálisan eltulajdonított információ felhasználása a piaci versenyt is torzítja.

A védelmi piacon magas belépési korlát jellemző, ami jelentősen megnehezíti, sok esetben ellehetetleníti az új szereplők megjelenését [195]. 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 [25]. Az a szereplő, amely elsőként képes adaptálni egy új technológiát, anélkül, hogy jelentős erőforrást fordítana KFI tevékenységekre, potenciálisan globális előnyhöz juthat [196]. 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 [191].

Témavezetőmmel folytatott [197, 198, 199] korábbi kutatásaink során vizsgáltuk 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 [198]. 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 [199]. 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 [197].

Az ipari kémkedés legegyszerűbb formája, amikor egy szervezet kémkedik valamelyik versenytársa után. Más esetekben egy külföldi kormány vagy szervezet kémkedik egy belföldi vállalkozás vagy állami KFI program után [19]. A kormányok által szervezett ipari kémkedés elemezhető mikro- 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 [200]. 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 [200].

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 [73]. Ezzel szemben Ingesson (2023) [201] szerint a nagyfokú ipari kémkedést nem szabad automatikusan a nemzeti innovációsképességek 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 [18] – mivel felismerték a mikro- és makrogazdaságra gyakorolt pozitív következményeit [18, 19, 38, 62]. Más esetekben – példának okáért Európa szerte [12], Közel-Keleten, Észak-Afrikában és Ázsiában [202] – a kormányok kifejezetten ösztönzik a lokális vállalatokat az új technológiák kémkedés útján történő beszerzésére, a hazai védelmi képességek fejlesztése céljából [18, 19]. Kínát és Oroszországot számos kutató kiemelte [12, 13, 35, 62, 191] azon országok között, melyekben az ipari kémkedés az állam támogatásával történik. A listát mások többek között kiegészítették Németországgal [12, 35], Franciaországgal, Iránnal és Dél-Koreával [35]. 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 [112, 203]. Az ipari kémkedés globális fenyegetését csak súlyosbítja, hogy a kapitalista országok törvénykezése hajlamos elbagatellizálni a problémát, hogy a gazdasági/politikai hatalommal rendelkező,

bűncselekményt elkövető személyek el tudják kerülni a hivatalos büntetőeljárást és annak következményeit [63].

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 nemzetgazdaságuk újjáépítésére fordították [17], 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 [38, 196].

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 [29]. 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 [19]. Azonban más szervezeti érintettől származó adat is egyéb forrásból gyűjtött információkkal kombinálva értékes és átfogó tudást nyújthat egy elemző számára.

Az ipari kémkedés elkövetésének számtalan módszere áll rendelkezésre, amelynek az eszköztára az etikátlan viselkedéstől a bűncselekményekig terjed. (1) Gyakran az innovációt fejlesztő szervezet sincs 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 [204]. (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 [19]. (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 visszafejthetik a versenytárs fejlesztését, hogy betekintést nyerjenek az új technológiába [29, 204]. (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 [19]. (9) A szükséges kritikus információ megszerzése történhet a belső érintett megbízása, zsarolása, megvesztegetése vagy kényszerítése útján is [13, 19, 194].

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 [20]. Akár a szervezeten belülről, akár kívülről történik a kritikus információlopás, az a védelmi iparban súlyos következményeket vonhat maga után, így a probléma vizsgálata a humán faktor nézőpontjából elengedhetetlen a jelenség mélyebb megismeréséhez.

2.2.2. A humán faktor információbiztonsági fenyegetésének elemzése az ipari kémkedés szempontjából

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. Jelen fejezetben elemzem a humán faktor ipari kémkedésben betöltött szerepét annak külső és belső elkövetőin, továbbá a szándékos és véletlen megnyilvánulásain keresztül.

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 [37, 39, 71, 113, 205]. 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, ellopásához, jogosulatlan személy hozzáféréséhez és egyéb etikátlan vagy törvénysértő információkezelési cselekedethez vezethet [206]. 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 [36]. A kritikus információlopás történhet belső érintett megbízása, zsarolása, megvesztegetése, vagy kényszerítése útján [13, 194]. Más esetekben a jó szándékú alkalmazottak munkavégzés közben tudatukon kívül vállhatnak kémek célpontjává [115], vagy a szervezet belső érintettje kezdeményezi az ellopott információ értékesítését [207].

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 [33, 36, 71, 72, 208, 209]. 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 [206] ○ Illegális vagy etikátlan tevékenység az információk szisztematikus gyűjtésére, elemzésére és felhasználására [20] ○ Nem képes vagy hajlandó erőfeszítéseket tenni az igényelt információ beszerzésére vagy előállítására [192] ○ Bennfentes beépítése [36] ○ Belső személy megbízása, zsarolása, megvesztegetése, vagy kényszerítése [13, 194] ○ Versenytársak szakembereinek alkalmazása [13] ○ Külső személy megbízása [38, 196] ○ Szervezet illegális elektronikus megfigyelése [13] ○ IT innovációk biztonságossá tették [12], ami egyre több szervezetet bátorít fel [25] ○ Kibertámadás [19, 138]	○ Információ nyílt forráskódú platformokon való megosztása (kiállítások, közösségi média felületek, értékesítési ajánlatok vagy marketinganyagok) [204] ○ Konferenciák és kiállítások során értékes információ gyűjtése a másik szervezetről [12] ○ Több szervezetet magában foglaló együttműködés keretein belül végzett munka bizalmas információk megosztásához vezethet [19]
Belső	○ Jó kapcsolatokkal rendelkezik, és hozzáfér vagy hozzáférést biztosít az információhoz [207] ○ Belső fenyegetés információbiztonsági kockázati szintje magasabb, mint a külső támadásnál [70, 210] ○ Átfogó ismeretekkel, hozzáféréssel és ellenőrzési joggal rendelkezik és tisztában van a védelmi rendszerek hiányosságaival [210] ○ Elkövetheti a foglalkoztatása korai szakaszában [211], vagy nyugdíjazás előtt [12]. ○ Az elkövető lehet a szervezet belső biztonsági rendszerét jól ismerő, magasan képzett személy [39, 72] vagy tevékenységét rossz szándékkal végző alkalmazott [71]	○ Hanyagság vagy gondatlanság [33] ○ Munkavégzés közben elkövetett hibák [208] ○ Biztonságpolitika hiánya vagy nem betartása [72] ○ Nem megfelelő képzés vagy annak hiánya [72] ○ Stressz, munkavégzést támogató eszközök vagy okoseszközök elvesztése, ártatlan és naiv segíteni akarás a külső kérésekre vagy a zsarolás eszközeinek való kiszolgáltatottság [71] ○ Üzleti út során vállnak célponttá [204] ○ Új technológiák telepítése [208], alkalmazottak nem szívesen változtatnak a korábbi, szokásaikon [211]

5. táblázat: A szándékos és véletlen esetek jellemzői

Forrás: saját szerkesztés

A **véletlen** belső fenyegetést olyan belső vagy külső, jelenlegi vagy múltbéli szervezeti értintett testesít meg, aki engedélyezett hozzáféréssel rendelkezik vagy rendelkezett a szervezet információs rendszereihez, és rossz szándék nélküli cselekedete információszivárgáshoz vezet, amely kárt okoz az intézménynek [208]. Számos tevékenység vagy magatartás közvetlen vagy közvetett következménye vezethet véletlen információszivárogtatási incidensekhez. Az alkalmazottak hanyagsága vagy gondatlansága [33], munkavégzés közben elkövetett hibák [208], a biztonságpolitika hiánya vagy nem betartása, a nem megfelelő képzés vagy annak hiánya [72] mind olyan faktorok, melyek növelik a belső fenyegetés kockázatát, és hozzájárulhatnak a kritikus információ illetéktelen kezekbe való kerüléséhez. A stressz, a munkavégzést támogató eszközök vagy okoseszközök elvesztése, ártatlan és naiv segíteni akarás a kívülről érkező kérésekre vagy a zsarolás eszközeinek való kiszolgáltatottság [71] szintén súlyos szervezeti biztonsági résekhez vezethet. A munkavállalók fenntartásokkal kezelik az új, számukra ismeretlen technológiákat, mert nem szívesen változtatnak a korábbi, kényelmes munkavégzési szokásaikon [211], ebből kifolyólag az alkalmazott rendszereken végrehajtott változtatások növelik a véletlenül elkövetett esetek számát. Más esetekben üzleti útjuk során vállhatnak a vállalkozás érintettjei a kifinomult kémkedési módszerek célpontjává [204].

A **szándékos** belső fenyegetést a szervezet olyan korábbi vagy jelenlegi érintettje személyesíti meg, aki jogosult hozzáféréssel rendelkezik vagy rendelkezett az intézmény információs rendszeréhez, és hozzáférését tudatosan olyan módon használja fel, amely megkárosítja a szervezetet [208, 212]. 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 [207]. A szándékos bennfentes fenyegetés – a szervezet rendszereinek alapos ismerete következményeként – információbiztonsági kockázati szintje exponenciálisan magasabb a külső támadókénál [70, 113, 210]. 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 [114, 210]. A belső érintett elkövethet információlopást a foglalkoztatása korai szakaszában amikor egy külső entitás építi be és használja fel az információval való

visszaélésre [211], 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) [72], Brancik és Ghinita (2011) [39] 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) [71] 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 elkövezőt [12, 13], azonban hozzájárul a szervezettel szembeni lojalitás elvesztése, a szervezet iránti negatív attitűd, vagy felmerül egy jó alkalom az információlopásra 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 munkavállaói hűség csökkenését, és a szervezettel szembeni negatív érzelmek halmozódását, ami hajlandóságot ébreszt az intézmény megkárosítására [20, 213]. 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 hátterét és neveltetését [213]. A szervezet tudatos megkárosítása hátterében lehet pszichés egészségügyi probléma is, mint a depresszió vagy a személyiség zavar [206]. Más esetekben az elkövetők külső nyomás, zsarolás vagy megvesztegetés hatására folytatják káros tevékenységüket [13].

2.2.3. Az ipari kémkedés kockázatának csökkentése szociotechnikai megközelítésből

Elméletben a védelmi iparban minden vállalkozás rendelkezik szervezeti politikával az ipari kémkedés kezelésére, amely kiterjed valamennyi tevékenységre, azonban a gyakorlatban a hatékony útmutatás kidolgozása a legtöbb vállalkozás számára komoly kihívást jelent [19], és a biztonságpolitika megléte önmagában nem garantálja annak hatékonyságát. Ennek egyik oka, hogy a kockázatok valós üzleti folyamatoknak megfelelő értékelése, továbbá a biztonsági funkciók ezen üzleti folyamatokba való

integrálása nehézséget okoz a szervezeteknek, amelynek a gyakorlati hatékonyságát csak úgy lehet biztosítani, hogy a folyamat a belső érintettek aktív bevonásával történik [75]. Az alkalmazott biztonságpolitika hatékonyságának hiánya eredhet abból a tényezőből is, hogy a kritikus üzleti információk védelmét sok szervezet csak IT szempontból közelíti meg, elsősorban a külső támadások kivédésére fókuszálva, figyelmen kívül hagyva a szervezeti érintettek által megszemélyesített belső fenyegetést, mikor ez az egyik legnagyobb információbiztonsági probléma [31, 32, 114, 209]. A vállalkozásoknak a biztonságpolitika definiálása során a humán és a technológiai szempontokat is egyaránt figyelembe kell venni [114, 116], mivel az IT központú szemlélet kizárólagos hangsúlyozása hibákat és biztonsági réseket okozhat a rendszer tervezése és végrehajtása során. Ez a megközelítés rávilágít a felhasználók bevonásának fontosságára a kockázatelemzésbe, mert a gyakorlatban hozzájárul a hatékonyabb biztonsági intézkedésekhez [75, 136]. A következőkben az ipari kémkedés kockázatának csökkentési lehetőségeit mutatom be szociotechnikai megközelítésből, mely az emberek és a technológiai rendszerek integrációját helyezi előtérbe.

Technikai szempontból az ipari kémkedés megelőzése és észlelése megköveteli a megfelelő fizikai és informatikai eszközök alkalmazását, az információbiztonsági szakértők felelősségeinek pontos meghatározását, továbbá a munkavállalók képzését és tevékenységük monitorozását [78]. A felsorolt intézkedések szükségességét igazolja, hogy a technológiai fejlődéssel a belső érintettek által elkövetett incidensek is egyre komplexebbé válnak [214], költséghatékony és egyszerű hozzáférést biztosítva a vállalkozás kritikus információjához [215].

A humán természet komplexitásának köszönhetően az információvédelem során az egyén a legösszetettebb faktor, és egyben a leggyengébb láncszem [33, 216]. A sokrétű bennfentes fenyegetés problémaköréről nem állnak rendelkezésre széleskörű tudományos eredmények, ami megnehezíti a hatékony védelmet nyújtó rendszer modellezését [210]. Az általuk elkövetetett 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 [217]. Ezenfelül a gyakorlatban is használható megállapítások megfogalmazásához a belső fenyegetések modellezése, az alkalmazottak sebezhetőségének értékelése és a szervezeten belüli biztonságtudatosság vizsgálata is fontos a kockázat mértékének azonosításához [39, 72, 218]. Azonban az elméleti keret

hiányában nem áll rendelkezésre hatékony adatgyűjtési módszer vagy mérési eszköz a kritikus információhoz hozzáféréssel rendelkező személyek megbízhatóságának vizsgálatára [210, 219], ennélfogva a valós idejű cselekvések nehezen megfigyelhetők, a gyanús viselkedések gyakran észrevétlenül maradnak és bizonyítékok nehezen gyűjthetők. 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 [211, 220], hanem holisztikus megközelítést igényel [36, 135]. Ez a megközelítés magában foglalja a technológiai és vállalatspecifikus tényezőket, a pszichológiai faktorokat és az üzleti folyamatokat egyaránt [75, 115, 117].

Az IT biztonsági megoldások és a szociotechnikai megközelítés együttes alkalmazása támogatja a probléma holisztikus természetéből eredő szakadékok áthidalását, és egy biztonságtudatosabb szervezeti kultúra kialakítását. 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 [221], amely magában foglalja a csoport információbiztonsággal kapcsolatos hiedelmeinek, elképzeléseinek és értékeinek tudatos alakítását [222]. A szervezeti kultúra újszerű megközelítésének célja az IT eszközökkel való emberi interakciók irányítása, és az érintettek tudatos viselkedésének ösztönzése az információbiztonság fenntartása érdekében [223]. 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 vállnak az információbiztonságra nézve kockázatot jelentő tevékenységek [218].

A szervezeti érintettek által elkövetett ipari kémkedés kockázata csökkenthető korai jelzőrendszerek alkalmazásával, amelyek felismerik az esetek bekövetkezésének valószínűségét, mielőtt az megtörténne [71, 224]. Az esetek korai észlelését támogatja, amennyiben a vállalkozás az alkalmazott stratégiát, a technológiát, az üzleti folyamatokat, továbbá az emberi erőforrást szinkronizálja, és összehangolva kezeli [37]. 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 sebezhetőség folyamatos felülvizsgálatát, továbbá az alkalmazottak tevékenységének nyomon követését, proaktívan védheti az információs infrastruktúrát a belső támadásoktól [72]. A munkavállalók magatartásának kisebb változásai is mutathatnak olyan mintákat, amelyeket érdemes szem előtt tartani [209], azonban a jelentősebb viselkedésbeli változások (mint verbális kirohanások, a biztonságpolitika szándékos megsértése, valamit az agresszív és konfrontatív magatartás) olyan figyelmeztető jelzések lehetnek, amelyek segíthetik egy szervezet ellen elkövetett incidens előrejelzését és prevencióját [206]. A belső érintettek közösségi média aktivitása is szolgáltathat adatokat az ipari kémkedés gyanújának korai észleléséhez [225, 226], mert az emberek sok kritikus információt osztanak meg magukról, mint a vállalkozások, amelyek foglalkoztatják őket, anélkül, hogy átgondolnák cselekedeteik lehetséges következményeit [227]. A munkavállaló büntetetlen előéletéről való megbizonyosodás is nagyban csökkentheti a kockázatot [228]. Azonban az intenzív megfigyelés zavarhatja a munkavégzést, bizalmatlanságot ébreszt, és hatékonyságcsökkenéshez vezethet [229]. A megelőzésre használt rendszerek eredményének megbízhatóságát megkérdőjelezi, hogy az emberi tényező mélyen beágyazódik az információbiztonsági incidensek prevenciójára tervezett különböző szoftverek és hardverek technikai kialakításába [38].

2.2.4. A negyedik ipari forradalom információbiztonsági kihívásai az ipari kémkedés szemszögéből

Az értekezésben vizsgált innovatív védelmi kkv-k az Ipar 4.0 által teremtett környezetben működnek, melynek jellemzője, hogy a fizikai infrastruktúrák és a digitális rendszerek közötti határ elmosódott. Azonban előnyei mellett a negyedik ipari forradalom számos új információbiztonsági fenyegetést is hozott, melyek még fontosabbá teszik a döntéshozók ipari kémkedés megelőzésére és észlelésére irányuló erőfeszítéseit. A fejezetben ezen kihívásokat elemzem.

A védelmi iparban az ipari kémkedés elleni védekezés részét képzi a létfontosságú infrastruktúra védelme [29], mert az olyan rendszerekből és eszközökből áll, melyek romlása káros hatással lehet az ipar kulcsfontosságú funkcióinak ellátására [214, 230]. Az értekezés szempontjából a kritikus infrastruktúrák elsősorban az új technológiák fejlesztéséhez és előállításához szükséges területeket, telephelyeket, továbbá a gyártáshoz szükséges berendezéseket és gépeket foglalják magukban. A létfontosságú létesítmények védelme még napjainkban is főként a véletlen balesetek és az ember által okozott fizikai

támadások megelőzésére irányul, azonban az értekezés szempontjából az informatikai rendszerek is releváns szerepet játszanak az új technológiák előállításához szükséges infrastruktúrák működésében, ezáltal a növekvő számú kiberfenyegetések kockázatát is figyelembe kell venni [230]. 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 is károsíthatják a speciális berendezéseket és megzavarhatják a létfontosságú folyamatokat [214].

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 [231]. A mesterséges intelligenciával támogatva ezek a kiber-fizikai rendszerek előreláthatólag sokkal kifinomultabb reakciókat lesznek képes létrehozni [231, 137]. 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 [137, 232, 233]. A fenyegetések fejlődése ellen a vállalkozásoknak szükséges lesz alkalmazni az újszerű védekezési lehetőségeket, – mint a mesterséges intelligencia és a blokklánc alapú platformok – melyek az ipari felhasználás során is növelhetik az általános kiberbiztonsági képességeket [234]. A mesterséges intelligencia algoritmusok lehetővé teszik a blokklánc hálózatok számára, hogy jelentős és komplex műveleteket hajtsanak végre, ami rendkívül hasznosnak bizonyulhat a gyártási feladatok automatizálásában [235].

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 [232]. Ezen adatbázis decentralizált modellje magas szintű rugalmasságot és a munkafolyamatok átláthatóságát biztosítja, ezenfelül a láncalapú adatszerkezet integritást és az adatvédelem legmagasabb szintjét képes nyújtani [234, 236, 237], mivel azonban új technológia, a szakirodalomban az értekezés írásának időpontjában nem áll rendelkezésre hatékony modell a blokklánc alkalmasságának értékelésére, és összehasonlítására a hagyományos rendszermegoldásokkal [232]. 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 [234, 235]. Ezen technológiák fontossága az értekezés szempontjából, hogy intelligens rendszereik révén nagyban képesek csökkenteni az emberi hibákból történő információszivárgási esetek kockázatát.

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 nehézségeket hozhatnak. Az Ipar 5.0, mely az ember és a robot közötti hatékony együttműködésen alapszik, lehetővé teszi, hogy a robotok monoton, ismétlődő műveletek végrehajtása helyett autonóm módon végezzék a feladatukat [238]. A kvantumszámítógépek még fejlesztés alatt állnak, azonban speciális területeken már most jelentős teljesítményjavulást mutatnak speciális feladatok elvégzésében, mint a korábban biztonságosnak gondolt titkosítási módszerek visszafejtése, ami potenciális veszélyt jelent az információbiztonság és az Ipar 4.0 szempontjából [239]. Az intelligens rendszerek integrálódása a vállalkozások hétköznapi működésébe, áthidalva a digitális és fizikai környezet közötti szakadékot, szintén növeli az ipari kémkedés kockázatát [137]. 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 [138]. Az újszerű fenyegetések elleni védekezés minden esetben rugalmasságot, gyors reakciót és célzott biztonsági frissítéseket igényel [240].

3. EREDMÉNYEK

Az ipari kémkedés egy olyan külső tényező, amely nagy mértékben befolyásolja a szervezet működését és stabilitását, így a kontingenciaelméleti megközelítésnek fontos szerepe van a minden szervezeti folyamatot magában foglaló, többrétegű információvédelmi rendszer kidolgozásában. A kontingenciaelmélet alapelvein nyugvó információbiztonsági stratégia segíthet az innovatív vállalkozásoknak a külső fenyegetésre való gyors és hatékony reagálásban. A 3. fejezetben a gyűjtött adatok elemzése alapján bemutatom a védelmi iparban tapasztalható ipari kémkedéssel összefüggésbe hozható esetek növekedése mögött azonosított külső és belső kontingenciatényezőket, továbbá ismertetem, hogy a döntéshozóknak milyen szempontokat szükséges figyelembe venni az információvédelmi rendszer kialakítása során. Ezenfelül az eredmények bepillantást nyújtanak, hogy várhatóan a közeljövőben milyen ipari kémkedési módszerekre kell felkészülni az innovatív védelmi vállalkozásoknak.

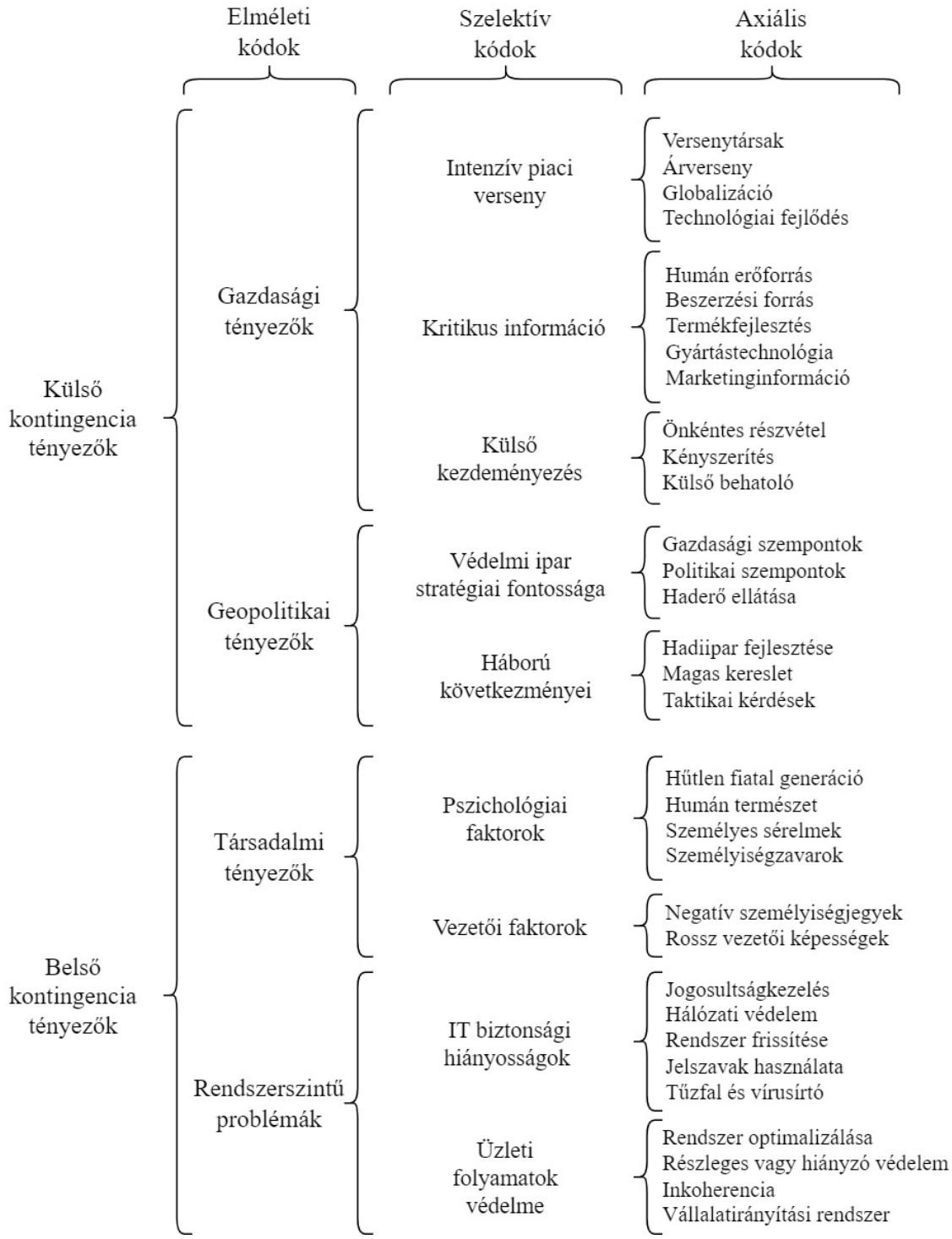
Jelen kutatás során az adatgyűjtés szakértői mélyinterjúk keretében valósult meg. Az interjúalanyok a védelmi kkv-ket fenyegető ipari kémkedésről alkotott véleménye és tapasztalatai feltárása volt a cél. Mivel az adatgyűjtés megkezdése után néhány héttel kitört az orosz-ukrán fegyveres konfliktus, ennek 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) [110] 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.

A kutatás során törekszem egy olyan hatékony információvédelmi rendszer definiálására, amely a legtöbb olyan eszközt és tevékenységet felöleli, amellyel a vállalkozás képes az ipari kémkedés megelőzésére és észlelésére.

3.1. Az ipari kémkedési esetek növekedése mögött azonosított tényezők

Konopatsch (2020) [133], Shelupanov és szerzőtársai (2021) [134] kutatási eredményei alapján az elmúlt évek során a védelmi iparban az ipari kémkedéssel összefüggésbe hozható incidensek gyakorisága jelentős növekedést mutatott, továbbá Pellegrino (2015) [191], Kim és Kim (2021) [163] 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 vizsgáltam, hogy milyen kontingenciaváltozók 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. Az 5. ábra szemlélteti a témában azonosított eredmények kódfáját.

Az eredmények ismertetése során alkalmazott idézetek azáltal segítik a megértést, hogy bevonják az alanyok hangját az elemzésbe, ezért Sántha és Tódor (2022) [241] javasolja, hogy a kutatók használják ezt az eszközt magyarázatok nyújtására és az alanyok perspektíváinak illusztrálására.



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

Forrás: saját szerkesztés (n=42)

3.1.1. Külső kontingenciatényezők

Jelen empirikus kutatás során az ipari kémkedés gyakoriságának növekedő tendenciája mögött azonosított eredményeket a vállalkozások szempontjából külső és belső kontingenciatényezőként határoztam meg. 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 szakértők 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 gyűjtött kvalitatív adatok elemzése alapján az árverseny szintén olyan gazdasági kontingenciatényező, amely azonosítható az esetszámok emelkedésének 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 képességek 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 teszi 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 kkv-k vizsgálata során az azonosított szelektív kódok a humánerőforrás, a beszerzési források, a termékfejlesztési információk, a gyártástechnológia és a marketinginformációk axiális kódokból fejlődtek.

A humánerőforrás a vállalkozás által alkalmazott, speciális szaktudást igénylő pozíciót betöltő munkavállalók képességeire utal. Az interjúalanyok elmondása szerint a védelmi iparban foglalkozatott 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.

A gyűjtött empirikus adatok alapján 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 költséghatékonnyá 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”*. A kutatás eredményei alapján elmondható, hogy az ipar stratégiai jellegéből adódóan a fő vásárlók az állami szereplők, amelynek okán számos vállalkozásnak nehézséget okoz az új termék célpiacnak való bemutatása. A versenytárak marketinginformációi iránt szintén magas a kereslet a védelmi iparban. A kritikus információ szelektív kód szorosan kapcsolódik az intenzív piaci versenyhez és a geopolitikai tényezőkhöz.

Az ipari kémkedéshez fűződő esetszámok növekedésének okai közé kategorizáltam a **külső kezdeményezést**. Bár az értekezés keretei között primer kutatás során nem vizsgáltam az elkövetési módszereket, ez a kategória utal az információlopás végrehajtásának módjára is. A gyűjtött empirikus adatok 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 engedélyeztető hatóságok”* vagy „*auditáló szervezetek munkatársai”*. A külső kezdeményezés jelensége csak közvetve járul hozzá az ipari kémkedés gyakoriságának 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.

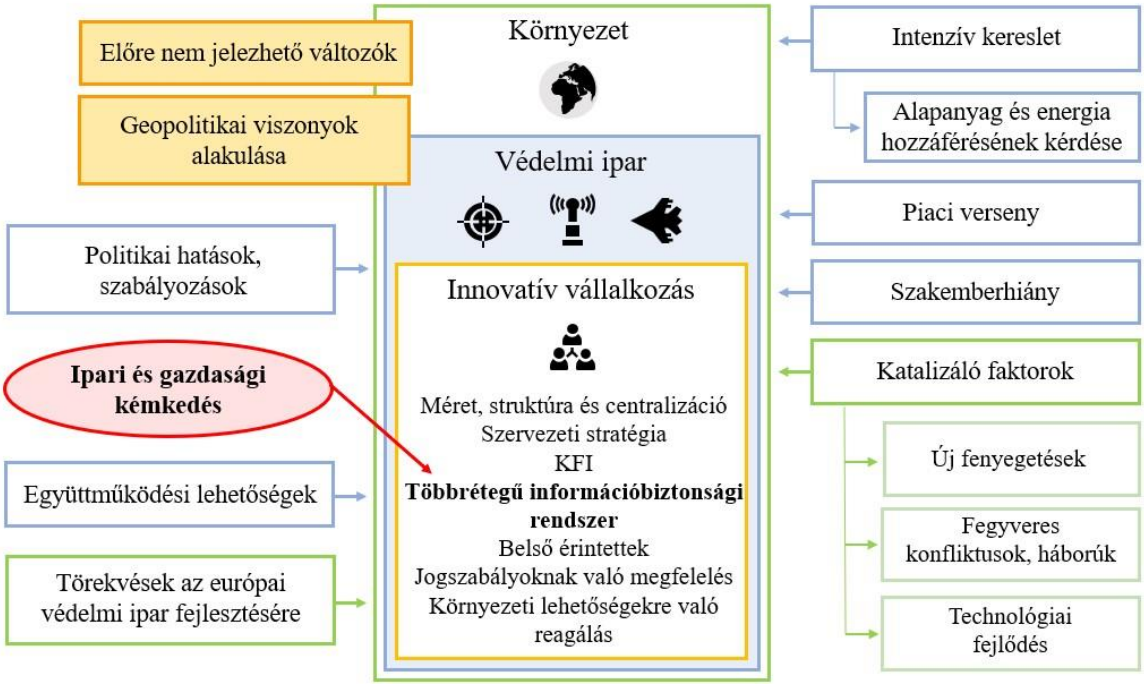
A **geopolitikai tényezők** elméleti kód a védelmi ipar stratégiai jelentősége és a háború következményei szelektív kódokból fejlődött. A kutatás eredményei szerint az esetszámok növekedésének szempontjából a probléma gyökere, hogy a **védelmi ipar stratégiai fontossággal** rendelkezik minden európai 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 kkv-k 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 elméleti 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 arról, 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.

Korábbi kutatómunkám során [42, 48] vizsgáltam az európai védelmi iparban működő kkv-kre ható kontingenciatényezőket, melyeket a 6. 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 kontingenciatényezőket. Azonban a jelen értekezés szempontjából legfontosabb kontingenciaváltozó 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.



6. ábra: A védelmi iparban működő szervezetre ható kontingenciatényezők

Forrás: saját szerkesztés korábbi kutatásom alapján [42, 48]

3.1.2. Belső kontingenciatényezők

A gyűjtött empirikus adatok alapján azonosítottam azon szervezeti belső tényezőket, melyek hozzájárulnak az ipari kémkedés gyakoriságának növekedéséhez. Ezek 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 esetekre 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.[10] Tapasztalataik szerint a fiatalabb generációk tagjai „*gyakran váltanak munkahelye*t", 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 a „*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 az 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

[10] Jelen empirikus kvalitatív kutatás az ipari kémkedéssel összefüggésbe hozható szituációkat vizsgálta, eredményei nem általánosíthatók a „*fiatal generációk*" összes tagjára.

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 empirikus 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 értekezés 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 kóddokkal, 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 problémákat** a belső kontingenciatényezők közé osztályoztam, mely az alkalmazott információvédelmi eszközök üzleti folyamatokba való integrációját 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. Ezen üzleti folyamatok során 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 arról, 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.

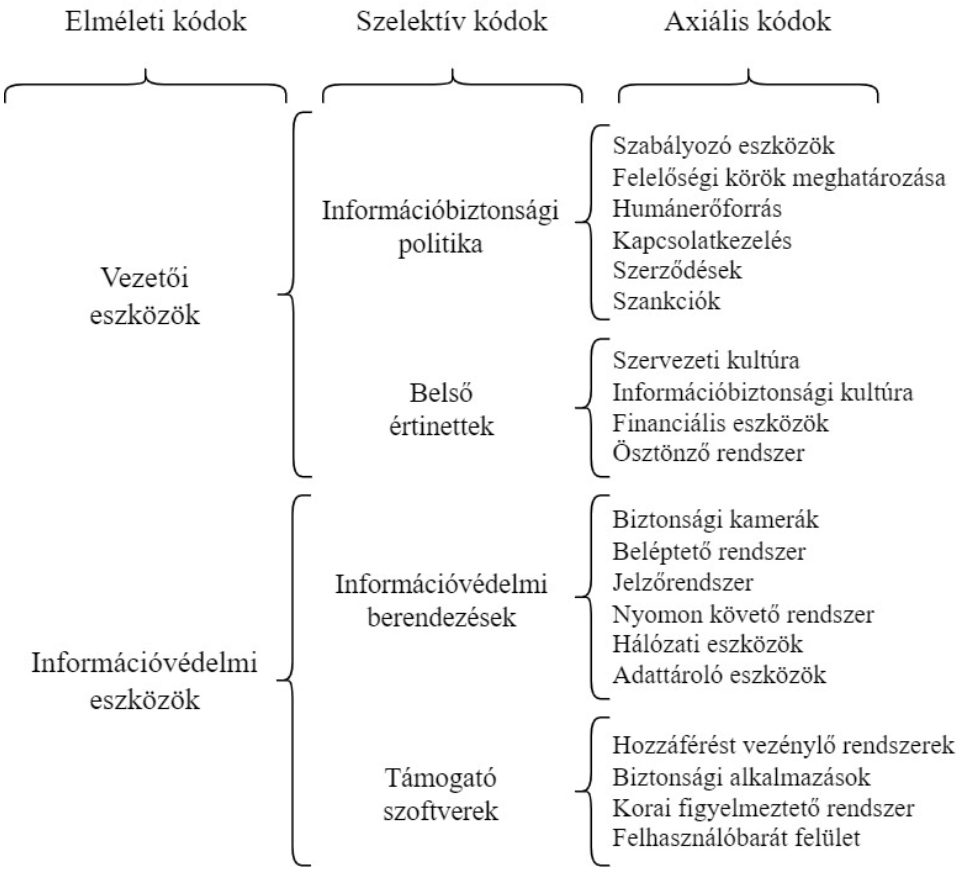
A determinizmus szerint a kutatások oksági megfogalmazásainál a legritkább esetben fordul elő, hogy egy változó feltétlenül és teljes egészében oka legyen a másiknak, így ezek többnyire több okváltozóval dolgoznak, továbbá a vizsgált jelenségek szükségszerűen összefüggenek egymással [64]. Ezt igazolja, hogy az empirikus kutatásom eredményeként az ipari kémkedés gyakoriságának növekedése mögött azonosított külső és belső kontingenciatényezők mind közvetlen vagy közvetett kölcsönhatásban állnak egymással, melyek megtekinthetők az 5. számú mellékletben.

A védelmi iparban tapasztalható ipari kémkedés gyakoriságának hátterében bemutatott tényezők feltárása és megértése nélkülözhetetlen része a fenyegetés elleni hatékony információvédelmi rendszer kialakításának. A következő fejezetben bemutatom, 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) [209], Homoliak és szerzőtársai (2020) [31], továbbá Saxena és szerzőtársai (2020) [32] véleménye szerint a vállalkozások által alkalmazott információbiztonsági rendszerek sok esetben csak IT 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) [220], továbbá Samy és szerzőtársai (2020) [211] 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) [72] szerint a megoldást egy olyan többrétegű 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 (7. ábra).



7. ábra: Az ipari kémkedés elleni védekezés és megelőzés tényezői, a grounded theory elemzés kódfája

Forrás: saját szerkesztés (n=42)

Az empirikus kutatás eredményei alapján a kérdésben a vezetői és az információvédelmi eszközök elméleti kódokat azonosítottam, melyek alapot biztosítanak a vállalkozásra optimalizált információbiztonsági rendszer kialakításához.

3.2.1. Vezetői módszerek és 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.

A kutatás eredményei alapján 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”*.

Az interjúalanyok 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 ügyiratkezelés, 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 munkavállaló alkalmazása előtt „*szükséges ellenőrizni, hogy részt vett-e korábban ipari kémkedésben, bűncselekményben”* vagy „*az ipar jellegéből adódóan van-e kapcsolata bármilyen szélsőséges csoporttal”*.

A kutatás eredményei alapján 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 egyezett 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 gyűjtött empirikus adatok alapján a védelmi iparban folytatott kereskedelmi tevékenységek vagy együttműködések során a vállalkozás titoktartási szerződéssel védheti a kritikus információt a külső érintettektől, továbbá titoktartási és versenytilalmi szerződésekkel kötelezheti a belső érintetteket az üzleti titkok védelmére. Azonban az interjúalanyok tapasztalta szerint sok esetben, – például „*külföldön”* vagy „*Európai Unión kívüli”* szerződésszegés esetén – nehéz szankcionálni ezen dokumentumok megszegését.

A szankciók azon eljárásokat jelentik, 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 „*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 financiális 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 képzik 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 képzi 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 financiális eszközök biztosítása, mint a versenyképes fizetés és egyéb juttatások, közvetlenül támogatják a munkavállaók 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 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

A kutatás eredményei alapján 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 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 estekben 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 beszámolói 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 ölelik 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”*.

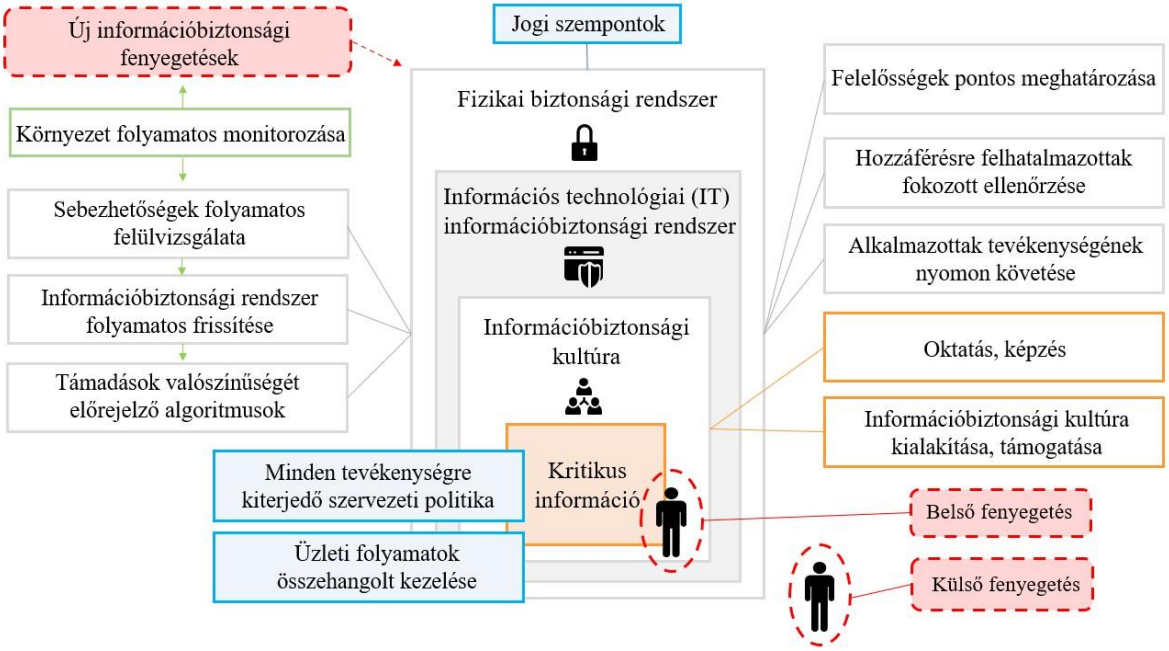
A mélyinterjúk során megkérdezett szakértők szerint a vállalkozásoknak lehetőségük van korai jezőrendszert (*early warning sign system)* alkalmazni, amely elsősorban a belső érintettek kamerákkal történő megfigyelésén alapszik. A válaszadók tapasztalatai alapján a módszer többek között „*növeli a biztonságot”*, lehetővé teszi az ipari kémkedéssel összefüggésbe hozható *„kísérletek időben való észlelését”*, „*figyelemmel kisérhető 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 8. ábra szemlélteti a holisztikus megközelítésű, többrétegű információbiztonsági rendszert, mely magában foglalja a fizikai elemeket, az IT megközelítést és az információbiztonsági kultúrát egyaránt.

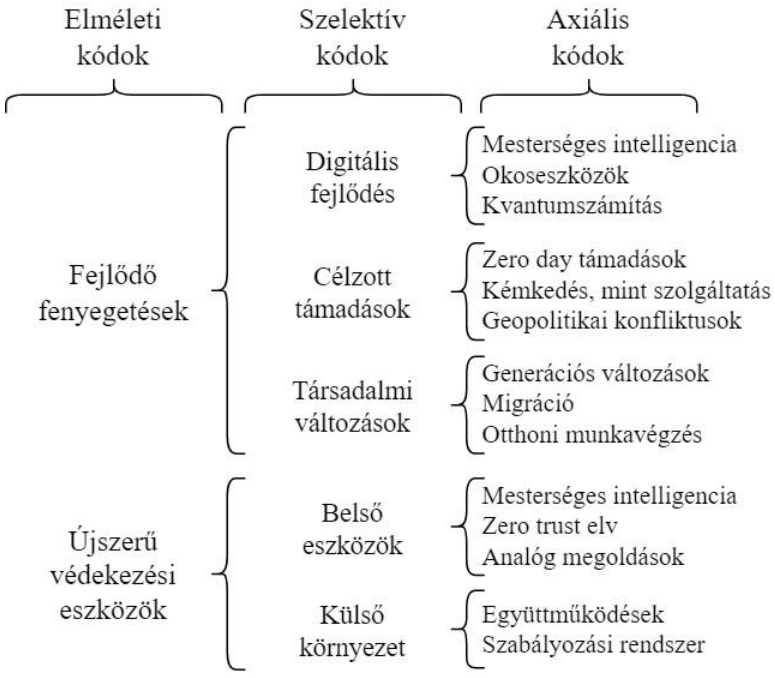


8. ábra: Többrétegű információbiztonsági rendszer

Forrás: saját szerkesztés (n=42)

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) [137] az ipari kémkedés növekedésének kockázatát az intelligens rendszerek üzleti folyamatokba való integrálásában látják. Wilson és Hingnikar (2023) [138] szerint az egyre különfélébb hackertámadások, továbbá az autonóm entitások és robotok megjelenése növeli a vállalkozások ellen elkövetett ipari kémkedés előfordulásának gyakoriságát. Bár az alanyok nem 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 (9. ábra).



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

Forrás: saját szerkesztés (n=42)

3.3.1. Fejlődő fenyegetések

A gyűjtött empirikus adatok elemzése során 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*" információlopást 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 vállnak 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 kémkedés 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 a jövőben várhatóan egyre több entitás fog a célzott információlopásra *„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 hátterű személyek munkaerőpiacra való belépése is változásokat hoz az információbiztonsági kultúra dinamikájában. A válaszadók 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 hátterüket 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 az otthoni 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 mestereséges 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, mely 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 téri a régi, analóg módszerekhez”*, mint a *„papír alapú megoldások”* és az *„információ személyes átadása”*. Azonban ennek hátránya, hogy a *„régi módszerek”* alkalmazásával vissza fognak térni a „*régi fenyegetések”* 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 vállalkozások próbálták az információvédelmi megoldásaikat eltitkolni”*. Azonban a jövőben ez nem megoldható, mert a rendszerek közötti inkoherencia biztonsági résekhez vezet és jelentősen növeli az ipari kémkedés kockázatát. Az interjúalanyok véleménye szerint egyre nagyobb szükség van az állami szintű lépésekre, a *„törvények és szabályozások elfogadásra”* az ipari kémkedés

szankcionálása érdekében, továbbá 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. A 10. ábra az grounded theory módszertan alkalmazásával feltárt elméletet, a kutatás legfőbb eredményeit mutatja be.

10. ábra: A grounded theory alkalmazásával definiált elmélet összefoglalása

Forrás: saját szerkesztés (n=42)

3.4. Diszkusszió

A fejezetben összefoglalom a kutatás eredményeit a definiált kérdések (**K1-K4**) sorrendjében és elfogadom vagy elvetem a megfogalmazott propozíciókat (**P1-P4**).

A megalapozott elmélet[11] összehasonlítása a témában rendelkezésre álló szakirodalommal a kvalitatív eredmények hitelességét, továbbá a kutatás deduktív jellegét biztosítja. A grounded theory módszertan 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 [87]. A kutatás során feltárt eredmények alátámasztják Button (2020) [13], Hou és Wang (2020) [38], továbbá Carl (2017) [69] 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)

Megelőző kutatásom [42] eredményei alapján 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 európai védelmi ipar fejlesztése fontossá vált, melyben a védelmi innovációs ökoszisztéma részeként meghatározó szerepet töltenek be a kkv-k. Ezen vállalkozásoknak az ipari kémkedés kockázatának hatékony mérsékléséhez fontos ismerni minden olyan kontingeciaváltozót, melyek közvetve vagy közvetlenül az esetek fokozódásához vezetnek.

A kutatás során vizsgáltam az ipari kémkedéshez fűződő esetszámok növekedésének mögöttes tényezőit, melyek között külső kontingenciatényezőként azonosítottam a gazdasági tényezőket. 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

[11] A grounded theory alkalmazása során nyert eredmények.

rendelkező entitások, amelyek szolgáltatásként kínálják a megrendelő által igényelt információ beszerzését.

A védelmi iparban zajló globalizációs folyamatok eredményeként a vállalkozások az országhatárokon túl is terjeszkedhetnek.[12] A külföldi, főként az Európai Unión kívüli tevékenység folyatása azért jelent kiemelt kockázatot, mert számos nemzet az ipari kémkedést a gazdasági tevékenységek legitim eszközének tartja [18, 19, 38, 62], továbbá a nemzetközi ügyletek során a szervezetek a saját kultúrájukban elfogadható információkezelési módszereket részesítik előnyben [112, 203]. Egy ilyen természetű információlopás esetén – példának okáért amikor egy kisvállalkozás indít eljárást egy külföldi állam ellen – a jogi folyamat rendkívül körülményes, költséges és sok esetben eredménytelen.

A védelmi technológiák és a kommunikációs eszközök gyorsütemű fejlődése szintén hozzájárulnak az esetszámok növekedéséhez. Heickerö (2019) [190], továbbá Szerb és szerzőtársai (2020) [193] 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 humánerőforrást, 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.

Empirikus eredményein alapján 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

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

kínálati oldala is dinamikus növekedést mutatott [3, 54, 187], 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 információlopás, hanem sok esetben azok rombolása.

A belső kontingenciatényezők közé sorolt 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 [31, 32, 114, 209, 211, 220].

A dinamikusan fejlődő fenyegetések korában az alkalmazott információvédelmi rendszerek és eszközök folyamatos fejlesztést igényelnek. Amennyiben ez megkövetei 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) [211], továbbá Williams és szerzőtársai (2019) [208] 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.

Az empirikus kutatásom eredményei alapján **az első propozíciót (P1) elfogadom**, mert egy innovatív védelmi kkv csak abban az esetben képes hatékonyan csökkenteni az ipari kémkedés fenyegetését, ha pontosan ismeri azon belső és külső kontingenciatényezők természetét, melyek más entitásokban igényt kelthetnek az általuk birtokolt információ iránt. A külső és belső környezet elemzésére számos modell létezik, mely keretrendszert nyújthat a vállalkozásoknak. Az előbbire alkalmas lehet többek között a PESTEL elemzés vagy Porter 5 erő modell, az utóbbira a McKinsey 7S modell.

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

A kutatás során a belső érintettek által elkövetett ipari kémkedés mögött – függetlenül annak szándékos vagy véletlen természetétől – számos különböző támogató változót sikerült feltárnom. 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 vezet információszivárgáshoz. Mindazonáltal az alkalmazottak ritkán követnek el ipari kémkedést pusztán rossz szándék által vezérelve, jellemzően az anyagi vagy egyéb jellegű kompenzáció motiválja őket.

Az eredmények alapján a leggyakoribb motiváló tényező az eltulajdonított információért cserébe kínált anyagi kompenzáció, ugyanerre az eredményre jutott Button (2020) [13] és Søilen (2016) [12] is. Bár a szakirodalom szerint [33, 36, 71, 72, 208, 209] 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 azonosítható pszichológiai faktorok (1) a 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. Laufer és szerzőtársai (2021) [227] a digitális térben történő információszivárogtatás kockázati tényezőit vizsgálták a humán faktor szempontjából, és a legkockázatosabb változók között azonosították (1) az erkölcsi problémákat, (2) az értékrendbeli eltéréseket, (3) a vállalkozással szembeni lojalitás hiányát, (4) a béremelés vagy előléptetés hiányából fakadóan elkövetett jogsértéseket, (5) az elkövető kedvezőtlen pénzügyi hátterét, (6) a társadalmi normáktól való rejtett eltéréseket (például vallási, szexuális vagy politikai), továbbá (7) a kritikus információkhoz való magasfokú hozzáférést.

Ezen változók gyakori előfordulása jelentős információbiztonsági kockázatot jelent az innovatív védelmi vállalkozásoknak. Vashisth és Kumar (2013) [213] korábbi kutatásuk során az incidensek mögött szintén feltártak a személyiséghez fűződő változókat, úgy, mint a kielégítetlen célok, ideológiai szerepvállalás és az elkövetett tettekért való felelősség hiánya. Noonan (2018) [206] 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 növekszik a versenypiaci nyomással, az iparágban jellemző képzett munkaerőhiánnyal (túlterhelt munkavállalók), a nem megfelelő vezetési gyakorlattal, továbbá a rosszul kialakított információs rendszerrel. Ashenden (2018) [33] az alkalmazottak hanyagságát és gondatlanságát, Omar (2015) [72] a biztonságpolitika be nem tartását, továbbá Elifoglu és szerzőtársai (2018) [71] a munkavállalói stresszt, a munkavégzést szolgáló okoseszközök elvesztését és a naivitást azonosította, melyek véletlen esetek elfordulásához vezetnek. A nem szándékos incidenseknél azonban felmerülhet a kérdés, hogy ténylegesen véletlenül 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 a vezetők nem mutatnak etikus viselkedést a munkavállalók felé, nem támogatják az információbiztonsági kultúra kialakulását hatékony oktatással, továbbá nem csoportosítanak erőforrásokat az információbiztonsági rendszer megfelelő kivitelezésére, úgy jelentős kockázatnak teszik ki a vállalkozást. Nasheri (2004) [20], továbbá Vashisth és Kumar (2013) [213] 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)

Kutatásom eredményei alapján a vezetőknek tisztában kell lennie az ipari kémkedés növekedésének globális trendjeivel, továbbá azon külső kontingenciatényezőkkel, amelyek ezeket okozzák. Feladataik közé tartozik a belső tényezők vizsgálata, a kockázatok értékelése, a sérülékeny pontok azonosítása, továbbá ezeket figyelembe véve az információbiztonsági politika definiálása és folyamatos aktualizálása. Tevékenységüket nagyban támogathatja az információbiztonsági kultúra, mely megvalósításának egyik fő eszköze a belső érintettek oktatása. Az információbiztonsági kultúra támogatásával a kritikus információk védelme az alkalmazottak tudatos és tudatalatti tevékenységének természetes részévé válhat. Fontos része a hatékony védekezésnek a komprehenzív információvédelmi rendszer, melynek részei az üzleti folyamatokra hangoltak, fizikai és digitális elemei megfelelően konfiguráltak, továbbá kialakításának és rendszeres felülvizsgálatának a döntéshozók fokozott felügyelete mellett kell történnie.

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 (1) a felelősségi körök meghatározását; (2) a humánerőforrás menedzselését; (3) a külső és belső kapcsolatok kezelését; (4) a szerződéses eszközöket; (5) és az incidensek szankcionálását.

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. Tick Andreával korábban (2021), a magyar szervezetek körében végzett kvantitatív kutatásaink eredményei alapján a vezetők tisztában vannak az ipari kémkedés jelentette kockázattal, azonban a belső érintettek által megtestesített fenyegetést nem tartják jelentősnek [242, 243].

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 módszerek és eszközök közé sorolható a versenyképes bérezés biztosítása, továbbá a motiváló és ösztönző rendszerek alkalmazása.

Empirikus kutatásom eredményei alapján 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) [224], továbbá Elifoglu és szerzőtársai (2018) [71] 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) [209] szerint már a kisebb magatartásbeli változások is mutathatnak olyan

mintákat, amiket érdemes szem előtt tartani, azonban Noonan (2018) [206] 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) [226], továbbá Carstens és szerzőtársai (2021) [225] eredményei alapján az alkalmazottak közösségi média aktivitásának analizálása is szolgáltathat adatokat az ipari kémkedés gyanújának korai felismerésére. A belső érintettek monitorozása támogatja az ipari kémkedés kísérletek időbeni észlelését és azonnali beavatkozást tesznek lehetővé, azonban a folyamatos megfigyelés negatív hatással lehet a munkavégzésre.

A kutatás eredményei szerint a mesterséges intelligencia alapú eszközöket egyre több döntéshozó tervezi beépíteni az alkalmazott információvédelmi rendszerbe, mivel azok képesek felismerni és automatikusan blokkolni a potenciális fenyegetéseket. Aoun és szerzőtársai (2021) [231], továbbá Williams és szerzőtársai (2023) [137] szerint a mesterséges intelligenciával támogatott rendszerek sokkal kifinomultabb reakciókat lesznek képesek létrehozni egy információbiztonsági támadás esetén. Mohanta és szerzőtársai (2019) [234], továbbá Fadi és szerzőtársai (2022) [235] 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 megosztott. 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 fejlődése, ha nem is teljes mértékben, de közelebb vihet az esetek feltárásához. Fadi és szerzőtársai (2022) [235] szerint a mesterséges intelligencia az innovatív iparágak területén alkalmazva a közeljövőben képes lehet az adatokból olyan tudást előállítani, amelynek segítségével az emberekhez hasonló döntéseket hozhat, bár ezzel az állítással a kutatásban részt vevő alanyok nem értettek egyet.

Együttműködések során a fenyegetés, illetve a kockázat csökkenthető a külső partner felülvizsgálatával, továbbá szerződések 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 mérsékelhetik az ipari kémkedés kockázatát az alkalmazott információbiztonsági eszközök összehangolásával. A 6. táblázat a 6. számú mellékletben összefoglalja a kutatás során feltárt megelőzési és észlelési eszközöket az elsődleges feladatuk alapján.

Empirikus kutatásom eredményei alapján **a második propozíciót (P2) elfogadom**, mert a vállalkozás külső és belső érintettjei által szándékosan vagy véletlen elkövetett ipari kémkedés kockázata egyaránt mérsékelhető a megfelelő intézkedések meghatározásával.

A kutatás során gyűjtött adatokból levont következtetések alapján **a harmadik propozíciót (P3) elfogadom**, mely szerint az információbiztonsági rendszer kialakítása során a védelmi kkv-k döntéshozói elsősorban a különböző üzleti folyamatokra hangolt IT eszközöket alkalmazzák, és nem alkalmaznak holisztikus megközelítést, továbbá a szociotechnikai szempontokat is csak részben veszik figyelembe.

3.4.4. Jövőbeni információbiztonsági fenyegetések várható természete (K4)

Bár a dinamikusan változó környezeti kontingenciatényezők mellett lehetetlen pontos hosszútávú előrejelzéseket készíteni, azonban az értekezés írásának időpontjában jellemző ipari kémkedési módszerekből és eszközökből rövidebb távra előre lehet vetíteni. A kutatás eredményei alapján a digitális fejlődéssel az információlopás elkövetésére is több eszköz fog rendelkezésre állni, (1) mint az okostelefonok, melyek lehallgatására egyre modernebb technológiák vállnak 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, az Ipar 5.0 az emberek és a robotok közötti együttműködést támogatja, melyek számos hatékonyságnövelő előnyeik mellett információbiztonsági kihívásokat is jelentenek a védelmi vállalkozások döntéshozóinak. Williams és szerzőtársai (2023) [137] 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 kiber-fizikai támadások növekedéséhez vezetett, ami új és jelentős globális fenyegetést jelent a védelmi vállalkozások számára.

Empirikus kutatásom eredményei szerint 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 feltételezhető, 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 munkavégzésnek annak ellenére, hogy az interjúalanyok nem támogatják a tevékenység folytatásának ezen formáját az információbiztonsági kockázatok miatt. Tóth és Csiszárik-Kocsir (2022) [244] 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 számos problémát okoz, hogy a belső érintettek megbíznak a digitális technológiákban, melyre megoldást kínál a *zero trust* elv alkalmazása, mely csökkenti a véletlen esetek kockázatát. A kritikus információk továbbítására számos megkérdezett 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 [45], így várhatóan a jövőben a kooperációk száma növekedni fog. A közös tevékenységet folytató vállalkozásoknak

szükséges az információvédelmi rendszerüket konfigurálni, az alkalmazott eszközök közötti biztonsági résekhez vezető inkoherencia elkerülésének érdekében.

Az évtizedek óta zajló technológiai fejlődés tagadhatatlan (például dróntechnológia), azonban ezek használta 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 kkv-k 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.

Az empirikus kutatásom eredményei alapján **a negyedik propozíciót (P4) teljeskörűen sem igazolni, sem elvetni nem tudom**, ezáltal vizsgálatát további kutatásra javaslom. Egyrészről az értekezés írásának időpontjában az internet és az okos eszközök telterjedése óta nem jelentek meg az ipari kémkedés elkövetésére alkalmas diszruptív innovációk vagy azok üzleti titok eltulajdonítására való alkalmazása nem életszerű. Másrészről a gyorsütemű fejlődés mellett bármikor megjelenhetnek olyan eszközök, melyek hatására a kkv-k teljesen átalakítani kényszerülnek a korábban alkalmazott információvédelmi módszerket.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A doktori értekezésben az ipari kémkedés jelentette fenyegetést vizsgáltam a védelmi iparban tevékenységet folytató kkv-kre fókuszálva, kvalitatív kutatási módszert alkalmazva. Célom 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 a külső környezeti fenyegetés kezelése, az átfogó információbiztonsági politika és a belső érintettek jelentette fenyegetés menedzselése.

A kontingenciaelméleti megközelítést alkalmazva nem törekszem egy univerzális, minden körülmények között és helyzetben jól működő információvédelmi rendszert definiálni, mivel minden vállalkozásra más külső és belső tényezők hatnak ugyanabban az időben, így ez nem megvalósítható. Azonban célom a döntéshozók számára 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.

A védelmi kis- és középvállalkozásokra ható külső környezeti kontingenciatényezők vizsgálata

A belső információbiztonsági rendszer tervezése és megvalósítása előtt az innovatív védelmi vállalkozások vezetőinek kiemelt fontosságú feladata a külső környezeti kontingenciatényezők 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 makrogazdasági feltételek, infláció, együttműködések, export lehetőségek, finanszírozási források, lehetséges célpiacok, piaci környezet, versenytársak tevékenysége és árpolitika.

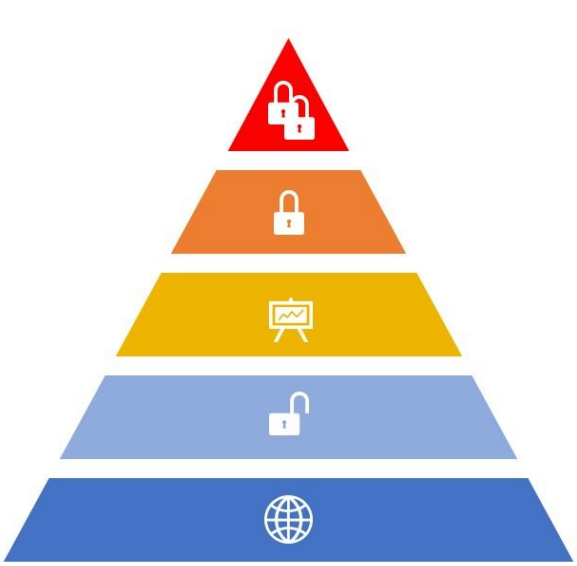
- **Politikai faktorok,** példának okáért jogszabályok és szabályozások, export szabályozások és nemzetközi szankciók, nemzeti stratégia, védelmi ipar fejlesztési stratégia, védelmi kiadások és finanszírozási források, beszerzési politika és tenderek, diplomáciai kapcsolatok és együttműködések.
- **Geopolitikai 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 információbiztonsági politika szerepe az ipari kémkedés kockázatának csökkentésében

Az információbiztonsági politika definiálása előtt azonosítani célszerű minden, a vállalkozás zavartalan működéséhez nélkülözhetetlen belső tevékenységet, továbbá azok folytatásához szükséges összes eszközt és információt, amelyeket védeni indokolt a fenyegetéstől. 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 általam fejlesztett információbiztonsági piramis modell, melynek során a piramis csúcsában kerülnek kategorizálásra a kritikus információk és azok titkos természete lefelé haladva csökken. A 11. ábra a teljesség igénye nélkül mutat be egy példát az információbiztonsági piramis modell alkalmazásáról.



Kritikus információk

Legmagasabb szinten titkosított információk, melyek kiszivárgása súlyos károkat okozhat a vállalkozásnak.
Pl.: termékfejlesztés dokumentációk, megrendelők

Nagyon fontos információk

Titkosított információk, melyek fontosak az üzleti folyamatok végrehajtásához, kiszivárgásuk közepes károkat okozhat.
Pl.: külső szerződött partnerek

Korlátozott hozzáférésű információk

A vállalkozáson belül korlátozott hozzáférésű információk, kiszivárgásuk nem okoz jelentős károkat.
Pl.: alapanyag beszállítók

Szabadon elérhető információk

Szabadon elérhető információk, nem szorulnak titkosításra.
Pl.: weboldal, termékleírás

Nyilvános információk

Azon információk, melyeket fontos a külső környezet felé kommunikálni.
Pl.: sajtóközlemények

11. ábra: Információbiztonsági piramis modell alkalmazása

Forrás: saját szerkesztés

Az üzleti folyamatokra vonatkozó információbiztonsági vizsgálat és a kockázatelemzés eredményeit fontos világosan kommunikálni valamennyi 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 képzi 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, amelyek magukban 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. A védelmi vállalkozásoknál indokolt 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 szükséges a vállalkozás azon területeinek és üzleti folyamatainak definiálása, melyek gyakori felülvizsgálatot igényelnek az információszivárgás 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, az alkalmazott szerződéseket (pl.: titoktartási és versenytilalmi szerződés vagy partnerségi megállapodás).

(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 szintúgy 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 a szervezeten belül jól működő információbiztonsági kultúra. Ezen ideális szervezeti kultúrára jellemző, hogy tagjai lojálisak és tisztelik a vállalkozást, tisztában vannak az ipari kémkedés kockázatával és negatív következményeivel, ezáltal az információ védelme a mindennapi munkavégzésük természetes részévé 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 (ügyiratkezelés, 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 képzi 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 jelentős 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 zeró 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.

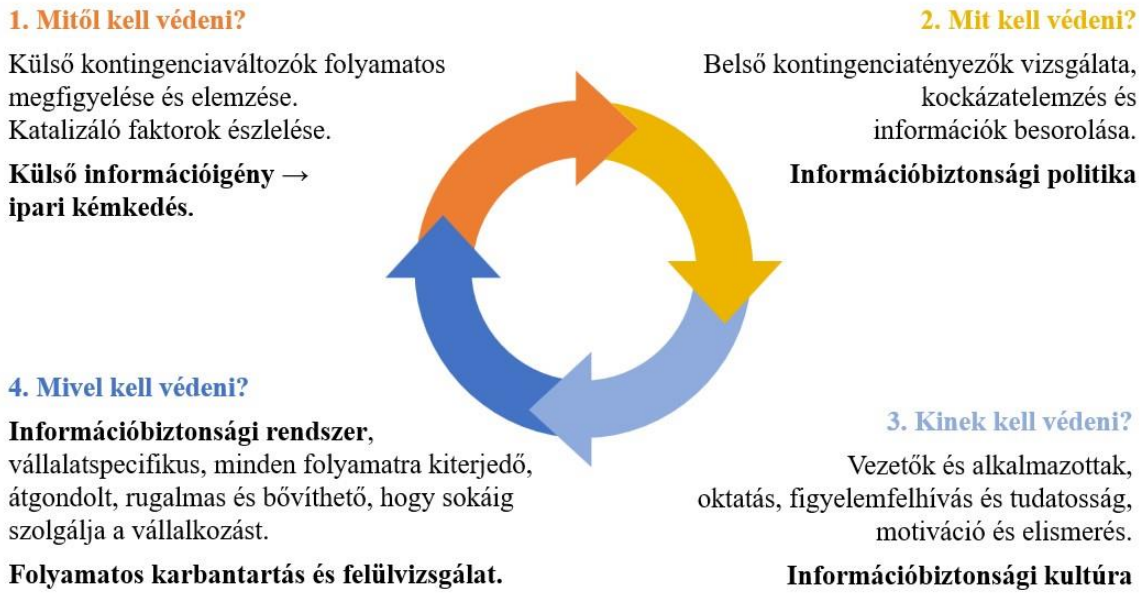
Az innovatív védelmi kis- és középvállalkozásoknál kialakítható információbiztonsági rendszer sajátosságai

Az információbiztonsági rendszer tervezése egy rendkívül komplex folyamat, melynek során az értekezésben bemutatott vállalati külső és belső kontingenciatényezők 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 az értekezésben 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 kkv-k nem mindig rendelkeznek az ehhez 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 szerződések alkalmazása.

A vezetőknek törekednie 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 diszkrét módon kezelni. A nyilvános felelősségre vonás semmilyen körülmények között sem javasolt, mert következményképp a belső érintett a vállalkozás ellen fordulhat.

A 12. ábra szemlélteti az információbiztonsági rendszer kialakításának folyamatát.



12. ábra: Információbiztonsági rendszer kialakítása.

Forrás: saját szerkesztés

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 kémkedhetnek 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 kkv-knek 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 financiális terheit.

Sokan feltételezik, hogy a mesterséges intelligencia gépi tanulással támogatva nagy előrelépést hoz az információbiztonság területén, ugyanis képes lesz észlelni és időben beavatkozni az általa gyanúsnak vélt események esetén. Azonban véleményem szerint a mesterséges intelligencia nem lesz képes 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 kutatásom eredményeként definiált téziseket. A témában releváns szakirodalom feldolgozása az értekezés elméleti keretének kialakításában nyújtott segítséget. A kvalitatív empirikus kutatás során célkitűzésem azon eredmények feltárása volt, melyek a tudományos és gyakorlati alkalmazás során támogatják az innovatív védelmi kkv-k vezetőit az üzleti titkok ipari kémkedéstől való védelmében.

Tézis 1.

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

(Lásd: 3. ábra, 35. oldal; 5. ábra, 58. oldal; 6. ábra, 63. oldal; 10. ábra, 80. oldal; 12. ábra, 98. oldal. Kapcsolódó publikációk: **P2** (*MTA besorolás szerint B*), **P5** (*Q3*), **P6** (*MTA besorolás szerint A*), **P7**, **P8**)

Tézis 2.

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

(Lásd: 7. ábra, 68. oldal; 8. ábra, 75. oldal; 10. ábra, 80. oldal; 12. ábra, 98. oldal; 6. táblázat 141. oldal. Kapcsolódó publikációk: **P1** (*Q2*), **P3**, **P4**, **P6** (*MTA besorolás szerint A*))

Tézis 3.

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

(Lásd: 5. ábra, 58. oldal; 10. ábra, 80. oldal; 5. táblázat, 48. oldal. Kapcsolódó publikációk: **P1**(*Q2*), **P3**, **P4**)

Tézis 4.

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

(Lásd: 10. ábra, 80. oldal; 12. ábra, 98. oldal. Kapcsolódó publikációk: **P1** (*Q2*), **P2** (*MTA besorolás szerint B*), **P3**, **P4**)

Tézis 5.

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

(Kapcsolódó publikációk: **P5** (*Q3*))

Az eredmények elméleti hasznosíthatósága

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

A kutatás során kontingenciaelméleti megközelítésből vizsgáltam a védelmi ipar területén tevékenységet folytató innovatív kkv-ket 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. A kutatás során levontam a következtetést, hogy a kontingenciaelmélet a napjaink dinamikusan változó környezetében is aktuális és releváns megközelítés. Az értekezés azon külső és belső kontingenciatényezőkkel egészíti ki a problémát vizsgáló szakirodalmat, melyek globális szinten hozzájárulnak az ipari kémkedéshez fűződő esetszámok növekedéséhez (Tézis 1., 2.). A kutatómunka során az orosz-ukrán fegyveres konfliktust is a védelmi iparban működő kkv-kre ható kontingenciaváltozóként

azonosítottam, amely probléma területén akadémiai megközelítésből szintén elméleti hiányosság azonosítható.

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

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

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

A kutatás eredményei hozzájárulnak a menedzsment tudományok fejlesztéséhez a gazdasági és ipari kémkedés kockázatának csökkentésére alkalmazható, empirikus adatokon alapuló gyakorlatok definiálásával (Tézis 4.), továbbá az ipari kémkedés elkövetésére alkalmas eszközök és módszerek közeljövőben várható természetének bemutatásával (Tézis 5.), alapot biztosítva a kutatóknak a téma mélyebb kifejtésére. Bár a digitalizáció szempontjából elérhetők tudományos publikációk a jövőbeni információbiztonsági fenyegetésekről [137, 138, 240], azonban ezen megközelítések mellett jelen értekezés társadalmi és pszichológiai szempontból is érinti az ipari kémkedés várható körülményeit, amely szintén kevésbé kutatott terület.

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

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

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 keretében fontosnak érzem, hogy a definiált elmélet a tudományos körök mellett azon döntéshozók számára is elérhető legyen, akiknek a mindennapi üzleti gyakorlatára lehet jelentős hatással (Tézis 4.). A célom olyan empirikus – kiemelkedő ágazati ismeretekkel rendelkező interjúalanyok tapasztalatain alapuló – eredmények feltárása volt, melyek a gyakorlatban alkalmazva hatékonyabb információbiztonsági intézkedések tervezését és végrehajtását teszik lehetővé.

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

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

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

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

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

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

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 a 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, 37, 75]. Szintén torzíthatja az eredményeket, hogy az információlopás nem jár azonnal észrevehető, kézzel fogható veszteséggel, így előfordul, hogy a vállalkozás egyáltalán nem, vagy csak hosszabb idő után szembesül a történtekkel [75]. 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, 38, 69], a terminológiahasználat nem konzisztens, kevés az elérhető releváns tanulmány [34, 69], és a tudományos probléma vizsgálata interdiszciplinárisam elkülönülve történik [38].

Jelen kutatás limitációja, hogy az értekezés írásának időpontjában nem volt elérhető pontos és releváns statisztikai adat az ipari kémkedés gyakoriságának növekedéséről, továbbá a védelmi iparban való gyakoriságáról és következményeiről, így az ezekre utaló kijelentéseket szekunder forrásokkal támasztottam alá.

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 az értekezés 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 értekezés 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 kkv-k 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, az Ipar 5.0 az emberek és a robotok együtt történő munkavégzését támogatja, melyek számos új információbiztonsági kihívást jelentenek a védelmi vállalkozásoknak.

A környezetben végbemenő társadalmi átalakulások is hozhatnak 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 kutatási terület, amely számos tudományág, többek között a műszaki, pszichológiai és a tárdadalomtudományok szempontjából történő vizsgálatot igényel, melyet a jelen innovatív technológiai környezetben 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 tudományterületek fejlődését, miközben arra ösztönzik a kutatókat, hogy további mélyreható elemzéseket folytassanak az ipari kémkedés területén. Az empirikus eredmények segítik az innovatív védelmi kkv-k vezetőit a probléma megértésében és az ipari kémkedés jelentette információbiztonsági kihívások elleni hatékony védelmi

stratégiák kifejlesztésében. Az értekezés 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 az ipari kémkedés elleni globális erőfeszítésekben, miközben megerősítik a vállalkozások védekezőképességét a 21. század információbiztonsági kihívásaival szemben.

Kutatás lezárásának időpontja: 2024. február 1.

AZ ÉRTEKEZÉS TÉMÁJÁHOZ KAPCSOLÓDÓ PUBLIKÁCIÓK

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] BARRACHINA, A. – TAUMAN, Y. – URBANO, A.: Entry with two Correlated Signals: the Case of Industrial Espionage and its Positive Competitive Effects; International Journal of Game Theory 50. (2021) pp. 241–278. DOI: https://doi.org/10.1007/s00182-020-00748-8

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

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

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

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

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

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

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

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

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

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

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

[37] BEDFORD, J. – VAN DER LAAM, L.: Organizational Vulnerability to Insider Threat. In: STEPHANIDIS, C. /szerk./: HCI International 2016 – Posters' Extended Abstracts. HCI 2016. Communications in Computer and Information Science 617. 2016., pp. 465–470. DOI: https://doi.org/10.1007/978-3-319-40548-3_77

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[101] GRANEHEIM, U. H. – LUNDMAN, B.: Qualitative Contentanalysis in Nursing Research: Concepts, Procedures and Measuresto Achieve Trustworthiness; Nurse Education Today 24. 2. (2004) pp. 105–112. DOI: https://doi.org/10.1016/j.nedt.2003.10.001

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[151] BREZNITZ, D.: Industrial R&D as a National Policy: Horizontal Technology Policies and Industry-state Co-evolution in the Growth of the Israeli Software Industry; Research Policy 36. 9. (2007) pp. 1465–1482. DOI: https://doi.org/10.1016/j.respol.2007.06.006

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

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

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

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

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

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

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

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

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

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

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

[163] KIM, S. Y. – KIM, Y. H.: A Study on the Understanding of the Analysis of the Future Operational Environment for Smart Defense Innovation and the Application of the ROK MND, 스마트 국방혁신을 위한 미래 작전환경 분석의 이해와 군 적용방안에 대한 고찰; Journal of Information Technology Services (한국IT서비스학회지) 20. 1. (2021) pp. 55–65. DOI: https://doi.org/10.9716/KITS.2021.20.1.055

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

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

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

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

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

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

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

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

[172] MARTINS, D. M. – FARIA, A. C. – PREARO, L. C. – ARRUDA, A. G.: The Level of Influence of Trust, Commitment, Cooperation, and Power in the Interorganizational Relationships of Brazilian Credit Cooperatives; Strategy &

Bussiness Economics - Revista de Administração 52. 1. (2017) pp. 47–58. DOI: https://doi.org/10.1016/j.rausp.2016.09.003

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GLOSSZÁRIUM

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

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

1. számú melléklet: 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 környezetedben történt? (*El tudja mondani a részleteket*?)

4. Véleménye szerint milyen tényezők vezetnek egy vállalatnál az információ biztoság 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*)

2. számú melléklet: 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)*

3. számú melléklet: 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?

4. számú melléklet: 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?

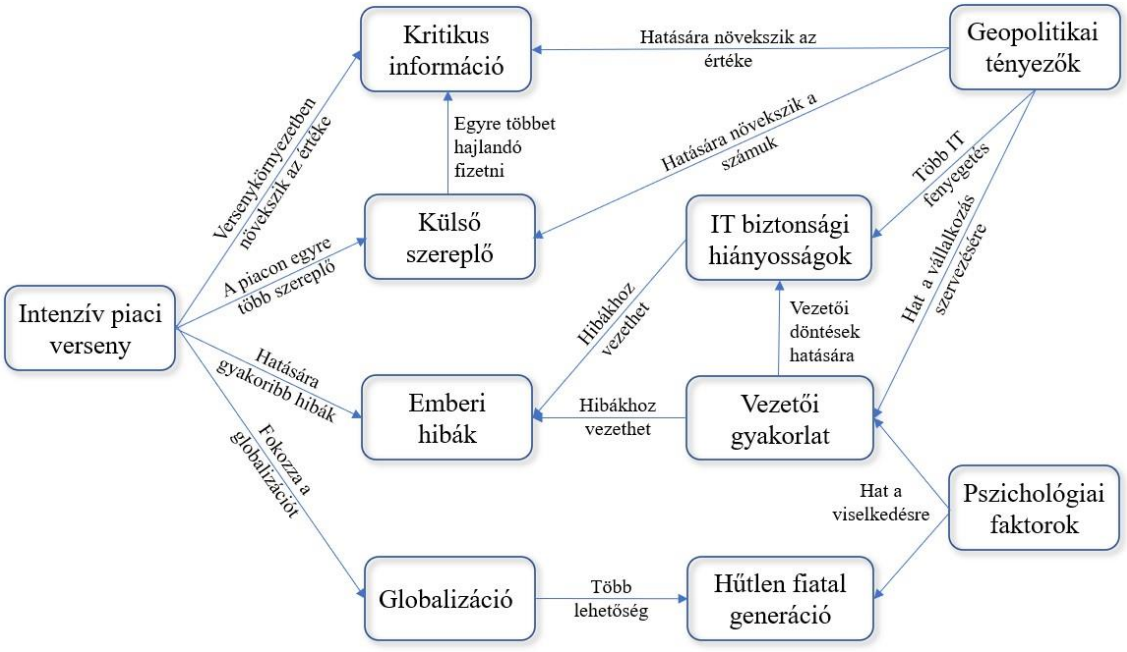
    a. How can these threats be anticipated based on certain factors?
    b. How can they defend against these threats?

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?

5. számú melléklet: A növekedés tényezői közötti hipotetikus összefüggések

Az ipari kémkedés gyakoriságának növekedése mögött azonosított külső és belső kontingenciatényezők mind közvetlen vagy közvetett kölcsönhatásban állnak egymással, melyeket a 13. ábra szemléltet. A védelmi piacon tapasztalható intenzív verseny hatására növekszik a kritikus információ értéke; a piaci szereplők száma, akik jelentős összeget hajlandók fizetni az információért; a munkavállalókra gyakorolt nyomás, melynek hatására gyakrabban követnek el hibát; továbbá fokozódnak a globalizációs folyamatok. A geopolitikai tényezők hatására szintén növekszik a kritikus információ értéke; a piaci szereplők száma; az IT fenyegetések száma, továbbá befolyással van a védelmi kkv-k szervezésére. A vezetői döntések befolyással vannak az IT rendszer kialakítására, mely hiányosságai platformot teremtenek a munkavállalói hibáknak. A globalizáció számos, akár külföldi munkalehetőséget biztosít a fiatal munkavállalók számára, akik gyakran élnek a lehetőséggel. A pszichológiai tényezők a vezetők és a munkavállalók viselkedésében is negatív változásokat eredményezhetnek.



13. ábra: A növekedés tényezői közötti hipotetikus összefüggések

Forrás: saját szerkesztés (n=42)

6. számú melléklet: Az ipari kémkedés megelőzésének és észlelésének eszközei

Megelőzés eszközei	Észlelés eszközei
Minden üzleti folyamatra kiterjedő információbiztonsági politika	
○ Szabályozó eszközök ○ Felelősségi körök meghatározása ○ Humánerőforrás menedzsment ○ Kapcsolatkezelés ○ Szerződések ○ Kritikus információ kiemelt védelme [72] ○ Belső sebezhetőségek folyamatos felülvizsgálata [72]	○ Szankciók ○ Jogi lehetőségek [78]
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 [71, 224]	○ Blokklánc [232, 236, 234] ○ Gépi tanulás és mesterséges intelligencia [234, 235]
Belső érintettek	
○ Belső érintettek hűségének növelése ○ Szervezeti kultúra ○ Információbiztonsági kultúra ○ Versenyképes bérezés ○ Ösztönző rendszer ○ Munkavállalók előéletének ellenőrzése [228]	○ Belső érintettek monitorozása ○ Korai figyelmeztető rendszer ○ Tevékenység nyomon követése [72, 78] ○ Közösségi média aktivitás megfigyelése [225, 226]

6. táblázat: Az ipari kémkedés megelőzésének és észlelésének eszközei

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

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, bíztatott és hitt bennem. Anikó doktori értekezése példaként szolgált számomra a munkám során.

Szeretném őszinte hálámat kifejezni Prof. Dr. Berek Lajosnak a segítségért és támogatásért, amelyet az értekezésem befejezése során nyújtott, akinek az ösztönzése és iránymutatása nélkülözhetetlen volt számomra abban az időszakban.

Köszönöm Szabó Richardnak az önzetlen támogatást és azt a rengeteg értékes gondolatot, valamint ajánlást, amelyekkel hozzájárult az értekezésem sikeréhez.

Ezúton szeretném megköszönni Prof. Dr. habil. Tick Andreának, hogy doktori tanulmányaim során kiemelkedő segítséget nyújtott a statisztikai módszerek megértésében és alkalmazásában.

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