HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 3. szám 113–134.
DOI: 10.32567/hm.2025.3.7

Pataki János Imre,[1] Sulányi Péter[2]

# Az autóipari vállalatok és beszállítók integrált biztonsági és védelmi stratégiája

## Security and Defence Strategy of Companies in the Automotive Industry

**Absztrakt**

*Napjaink biztonsági kihívásai világszerte jelentősen befolyásolják a multinacionális vállalatok biztonságos működését. Ezt a problémát a multinacionális vállalatok korán felismerték, ezért különböző elméletek és módszerek alkalmazásával alkották meg saját válságkezelő szabályaikat és folyamataikat. A különböző elgondolások alkalmazása több vállalatnál nem működött hatékonyan, ezért a nemzetközi szervezetek és intézmények megalkottak egy sor jogszabályt és ajánlást, amelyek válaszokat adnak a 21. század biztonsági kihívásaira, veszélyeire és kockázataira. A privát szektorban jelenleg két fontos nemzetközi/nemzeti jogszabály jelent meg, amelyek bevezetése és alkalmazása jelentős terhet jelent a vállalkozói szféra számára. A jelenlegi biztonsági helyzet a vállalatok számára integrált biztonsági és védelmi stratégia kidolgozását teszi szükségessé, amely figyelembe veszi az új jogszabályoknak való megfelelést.*

*Kulcsszavak: biztonsági stratégia, integrált biztonsági és védelmi koncepció, fizikai védelem, Helyzetelemző Központ*

[1] AUDI HUNGARIA Zrt., e-mail: janos.pataki@audi.hu
[2] Suprex Kft., e-mail: speter@suprex.hu

## Abstract

*Today's security challenges have significant impact on large enterprises worldwide. Multinational companies recognised this problem early on and used different theories and methods to create their own crisis management rules and processes. The application of different concepts has not worked well in many companies, so international organisations and institutions have created a series of laws and recommendations that respond to the security challenges, threats and risks of the twenty-first century. In the private sector, two important international/national laws have emerged at present, the introduction and operation of which represent a significant burden for the business sector. The current security situation makes it necessary for companies to develop a Security and Defence Strategy that takes into account compliance with the new legislation.*

*Keywords: security strategy, integrated security and defence system, physical security, Situation Centre*

„Élet és halál alapja, a túlélés vagy a megsemmisülés Útja (Tao).
Éppen ezért alapos vizsgálatot és mérlegelést kíván."
Szun-Ce[3]

## Bevezetés

A stratégiai gondolkodás a nagy földrajzi felfedezések és a haditechnikai eszközök fejlődésével[4] új korszakba lépett. Új katonai intézmények alakultak, amelyekben új eljárásokat és módszereket dolgoztak ki, amelyek máig hatást gyakorolnak a jelen kor stratégiai gondolkodóira. Viszont Montecuccoli[5] kijelentése, hogy a háborúhoz csak pénz, pénz, pénz szükséges, ez máig érvényes.

Napjainkban a geopolitikai helyzet változását a civilizációk közötti ellentétek generálják,[6] amelyek helyi szinten törésvonal-konfliktusokat[7] okoznak a különböző civilizációkat képviselő nemzetállamok között, illetve egy országon belül polgárháború[8] vagy konfliktus[9] törhet ki. Ez negatívan befolyásolja a globális gazdaság működését, ami működési zavarokat okoz a multinacionális vállalatoknál.[10]

2013 februárjában jelent meg Valerij Geraszimov tábornok cikke, amelyben a Varsói Szerződés totális háborús doktrínáit és taktikáját vette alapul, és ötvözte azokat a mai stratégiai katonai gondolkodással. Kidolgozta a modern hadviselés egy új elméletét. Ez az elmélet inkább egy ellenséges hatalom megdöntésére irányul és nem közvetlen támadásra. Azt írta: „A háború szabályai megváltoztak. A politikai és stratégiai célok

[3] Szun-Ce 2012: 17.
[4] A lovagvilág megszűnése, tűzfegyverek megjelenése.
[5] Paret 1986: 32–40.
[6] Huntington 2006: 343–346.
[7] Orosz–ukrán háború.
[8] Húszi felkelők Jemenben, évtizedes polgárháború, hajóforgalom támadása a Vörös-tengeren.
[9] Gázában: izraeli–palesztin konfliktus.
[10] Zavar az ellátási láncban, közvetlen és közvetett költségek növekedése.

elérésében a nem katonai eszközök szerepe megnőtt, és hatékonyságuk sok esetben meghaladta a fegyverek erejét. Mindezt rejtett katonai eszközök egészítik ki."[11] Oroszország 2014-ben megszállta a Krím félszigetet, és céljait a különleges erők,[12] a helyi fegyveres szereplők, a gazdasági befolyás, a dezinformáció és az ukrajnai társadalmi-politikai polarizáció kihasználásával érte el.

Az unió területén több kibertámadás történt az elmúlt években. A közműrendszerek és vállalkozások kiberbiztonsági sérülékenysége magas kockázati szintet jelent. A támadások elkövetőinek fő célja a közműrendszerek és a vállalkozások működésének akadályozása, amivel veszélyeztetik a lakosság és a fontosabb létesítmények ellátását, illetve működését. A támadásokkal az adott állam működőképességét is veszélyeztethetik.[13] 2024-ben világszerte megnőtt a vállalatok elleni kibertámadások száma, mert a támadások átlagos száma 44%-kal magasabb volt, mint 2023-ban. A támadások elleni védekezés jelentős költséggel jár a közüzemek és a vállalatok számára. Átlagosan 75 napot vesz igénybe, hogy egy szervezet visszanyerje működőképességét egy kiberincidens után.

A járműiparban kiemelt feladat a járművek IT-biztonsági szempontok alapján történő fejlesztése, gyártása, valamint az értékesített járművek folyamatos felügyelete. Az Automotive Security Management System (ASMS) előírásainak betartása kiemelt feladat a járművek intenzívebb adatforgalma miatt. Ez vonatkozik a *cyber security* (kiberbiztonság) és a *software update* (szoftverfrissítés) feladatokra is. A kibervédelmet a járművek teljes életciklusára ki kell terjeszteni.

A reziliencia kérdése mint új kihívás a 2016-os varsói NATO-csúcson[14] merült fel, ahol megfogalmazták az ezzel kapcsolatos feladatokat szövetségi és tagállami szinten. A kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (CER[15]), a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (NIS 2[16]), valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló módosított 2021. évi XCIII. törvény[17] megkövetelik a vállalatok biztonsági és védelemi rendszereinek felülvizsgálatát és a szükséges intézkedések bevezetését, valamint alkalmazását.

A 21. században a multinacionális vállalatok felismerték, hogy a biztonságos működés elengedhetetlen feltétele a biztonsági és védelmi intézkedések bevezetése és folyamatos működtetése. Ez viszont megnöveli a vállalatok működési költségeit, amit már nem terhelhetnek tovább a fogyasztókra, mert az már a piaci pozíciójukat veszélyeztetné. Mindez indokolja, hogy miért Montecuccoli gondolataival kezdtem a stratégiai gondolkodás jelentőségét. A jelenkor biztonsági kihívásainak kezelése a vállalatoktól egyre nagyobb anyagi ráfordítást követel meg.

[11] Hameleers 2025: 90–100.
[12] „Kicsi zöld emberek" jöttek és elfoglalták a félsziget stratégiai pontjait, majd biztosították a területet. Azonosító nélküli fegyveresek, akik egyértelműen orosz katonák voltak, de ezt hivatalosan nem tudták bizonyítani.
[13] Dénes–Kovács 2019: 52–84.
[14] NATO 2016.
[15] Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.
[16] Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).
[17] Továbbiakban Vbö.

A stratégiaalkotás nagyon fontos *vezetői funkció*.[18] Ezért fontos szempont a megfelelő vezető, módszer kiválasztása és alkalmazása, ami jelentősen befolyásolja az új stratégia bevezetését. A magyarországi nagyvállalatok biztonsági vezetői a velük folytatott informális beszélgetések során elmondták, hogy különböző szintű biztonsági szabályokkal, előírásokkal vagy szabályzatrendszerekkel rendelkeznek, de a biztonsági stratégiával mint témakörrel még nem foglalkoztak. A „Biztonsági stratégia és keretei" fejezetben ismertetjük azon feltételeket és követelményeket, amelyek mintaként szolgálhatnak az autóipari vállalatok saját stratégiájának kialakításához.

## A tudományos probléma megfogalmazása

Kutatásunk során megállapítottuk, hogy nemzetközi és nemzeti szinten még nincs releváns szakirodalom, amely a két hipotézisben megfogalmazott stratégiai szintű kihívásokra és az összetett biztonsági kérdésekre választ adna. Kutatásunkban bemutatjuk azt, hogyan befolyásolja a stratégiai gondolkodás egy vállalkozás biztonságát, és milyen adminisztratív és technikai intézkedésekkel garantálható az üzletmenet folytonossága és az új jogszabályoknak való megfelelés.

### *Kutatási hipotézisek*

Kutatómunkánkban alapvetően két hipotézisben fogalmazhatjuk meg a felmerült kihívásokat.

- Biztonsági stratégiában szükséges rögzíteni azokat az iránymutatásokat, amelyek alkalmazásával a vállalkozások meg tudnak felelni napjaink biztonsági kihívásainak, illetve az új jogszabályi kereteknek.
- A költségek – köztük a védelmi költségek – csökkentése alapvető elvárás a jelen gazdasági környezetben. Ezért szükséges a biztonsági koncepciók újragondolása, ami magába foglalja a szervezeti keretek optimalizálását, valamint a biztonsági rendszerek és a beavatkozó erők létszámának felülvizsgálatát.

### *Kutatási módszerek*

A tanulmányunkban a már közzétett tudományos eredményekre hivatkozva (alkalmazott kutatás) dolgoztuk ki azokat a szabályokat és módszereket, amelyek a gyakorlatban már beváltak. A különböző biztonsági intézkedéseket interjúk és a kvantitatív statisztikai módszerek szabályai alapján vizsgáltuk. Ezen folyamatok és módszerek alkalmazásával fogalmaztuk meg hipotéziseinket, és ezeket elemeztük és hasonlítottuk össze más vállalatok biztonsági rendszereivel. A vállalatok biztonsági vezetői csak anonim módon nyilatkoztak.

[18] Turi–Resperger–Túri 2012: 8.

## Biztonsági stratégia és keretei

A biztonság fogalmát átfogóan kell értelmezni, mivel a biztonsági környezet is folyamatosan változik. Ma a globális kihívások, fenyegetések, veszélyek és kockázatok több szinten jelentkeznek, egyének, közösségek, államok és régiók szintjén.

A biztonsági stratégia kidolgozásánál figyelembe kell venni a Magyarország Nemzeti Biztonsági Stratégiájáról szóló kormányhatározatot.[19] A biztonság – vagy annak hiánya – közvetlen hatással van a vállalat teljes termelésére és működésére. Az összes üzleti egységre kiterjedő és átfogó biztonsági stratégia hiánya hatékonysági problémákat és erőforrás-pazarlást okozhat, ami sebezhetővé teszi a vállalatot a külső kihívásokkal és a belső fenyegetésekkel szemben. A vállalatot fenyegető veszélyek változó jellege miatt a vállalatbiztonság évente felülvizsgálja a biztonsági stratégiát. Erre azért kerül sor, hogy a terveket és tevékenységeket úgy igazítsák ki, hogy azok tükrözzék az új információkat és tanulságokat. A vállalatbiztonság jövőképe, küldetése és célja a stratégia hosszú távú elemeit alkotják. A vállalat felső vezetésének létre kell hoznia és meg kell bíznia egy vállalatbiztonsági tanácsadó csoportot (VTCS),[20] hogy tervezze meg, koordinálja és rangsorolja a vállalat biztonságával és védelmével kapcsolatos döntéseket, valamint hozzon létre és felügyelje a biztonsági szintet emelő projekteket, amelyek jelentősen csökkentik a vállalat biztonsággal kapcsolatos költségeit. A stratégia végrehajtása során új célkitűzéseket és kezdeményezéseket határoznak meg. A dokumentumban foglalt célkitűzések és kezdeményezések a vállalat általános stratégiájának egyik kiindulópontját képezik.

Ezen túlmenően a stratégia eredményeként szükség lehet a jelenlegi vállalati politikák és ágazati stratégiák megváltoztatására, és ez fordítva is igaz. Az új vállalati politikák megkövetelik a stratégiák finomítását és összehangolását. A vállalatbiztonság egyik fontos feladata, hogy évente vagy szükség esetén felülvizsgálja és módosítsa a stratégiát. A biztonsági stratégiát a vállalat felső vezetése hagyja jóvá.

### *Biztonsági vízió*

A vízió a biztonság kívánt végállapotának megfogalmazása. A jövőkép kihívást jelent a vállalat számára, és minden üzleti egység minden szintjét egyetlen átfogó eredményre összpontosítja, amely a biztonságos működés és zavartalan üzletmenet biztosítása. Ez a kockázatalapú biztonsági és védelmi intézkedések kidolgozását és megvalósítását jelenti a vállalatnál, figyelembe véve azokat a kihívásokat, fenyegetéseket és biztonsági sebezhetőségeket, amelyek a vállalat működését befolyásolják.

A jövőképnek több fontos összetevője van:

- a stratégiát alakító fenyegetési és kockázati környezet rendkívül dinamikus, és folyamatosan új fenyegetések jelennek meg;

[19] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

[20] Mátrixszervezet, tagjai olyan vezető beosztású személyek, akik olyan szervezeti egységet (osztályt) vezetnek, amely „biztonsági" funkcióval is rendelkezik (pl. egészségmenedzsment, rizikómenedzsment, *compliance,* munkavédelem, környezetvédelem, IT-biztonság stb.

- a jövőkép a kockázatértékelés során beazonosított fenyegetések és sebezhetőségek kezelésén alapul;
- a kihívások, fenyegetések és biztonsági rések csökkentése;
- a rendelkezésre álló eszközök[21] alkalmazása a vállalaton belül.

### *Küldetés*

A küldetés egyszerű magyarázat arra, hogy mit csinál a vállalatbiztonság. A küldetés magában foglalja a vállalatbiztonság tevékenységét, függetlenül attól, hogy melyik szint[22] hajtja végre.

A vállalatbiztonság partnerség és együttműködés révén integrálja és folyamatosan javítja a különböző kompetenciák[23] biztonsági szintjét tanácsadással, koordinációval és ellenőrzésekkel. A küldetés nem foglalja magában a kompetenciaterületek felügyeletét, az alapvető biztonsági funkciók adminisztrációját vagy a fenti küldetésben kifejezetten nem tükröződő egyéb tevékenységek teljesítményének irányítását. A vállalatbiztonság célja a Biztonsági stratégiában megfogalmazott követelmények megvalósítása, a feladatok azonosítása és azon konkrét intézkedések végrehajtása, amelyek javítják a vállalatbiztonság alaprendeltetéséből adódó funkcióit.

### *Fő célok*

A biztonsági stratégia célja, hogy az értékek és érdekek figyelembevételével, valamint a biztonsági környezet elemzésével meghatározza a vállalat biztonsági és védelmi céljait, feladatait és eszközeit, amelyek révén a vállalat garantálja az emberek életét és egészségét, valamint a vállalat biztonságos működését egy globalizált világban.

A vállalat vezetése két átfogó célt tűz ki a vállalat számára:

- közös biztonsági szabályok és rendszerek,
- védelmi költségek optimális meghatározása.

Közös biztonsági szabályok és rendszerek:

- szabványosítják a biztonsági funkciók szinergikus végrehajtását a működés javítása érdekében;
- ezeknek a funkcióknak a szabványosítása növeli a folyamatok hatékonyságát, és egyre zökkenőmentesebbé teszi a tevékenységek integrációját és szinkronizálását a vállalat üzleti egységei között.

Biztonsági funkciói fejlesztése érdekében a vállalatnak nagy hangsúlyt kell fektetnie küldetésére, jövőképére és céljaira. A vállalatbiztonsági tanácsadó csoport felelőssége a specifikus feladatok meghatározása, amelyek irányíthatják a napi tevékenységet. Minden ilyen feladat maximum 10 éves időtartamra fogalmaz meg célkitűzéseket,

[21] Az eszközök közé tartoznak az emberek, rendszerek, berendezések, létesítmények és információk.
[22] Munkatárs, vezető, szervezeti egység, üzleti egység.
[23] Biztonsági helyzetelemzés, információvédelem, *know-how* védelem, prototípus-védelem, utazásbiztonság, objektumvédelem, tűzvédelem, iparbiztonság, katasztrófavédelem, munkabiztonság, környezetvédelem, egészségmenedzsment stb.

amelyek célja, hogy mérhető kiindulási alapot biztosítsanak az üzleti egységek számára, és ez alapján a fejlesztések hatékonysága mérhetővé válik. Ahogy a biztonsági funkciók és feladatok végrehajtása javul, és a fejlesztések megvalósulnak, a vállalatbiztonsági tanácsadó csoport felülvizsgálja a vállalat biztonsági helyzetét a célokhoz képest, és szükség szerint módosítja a korábban meghatározott mérföldköveket. Az egységes szabály- és biztonságtechnikai rendszerek alkalmazásával a különböző üzleti egységek biztonsági személyzeti létszáma csökkenthető.

## A védelmi költségek közgazdasági elmélete és gyakorlata

A vállalatok biztonsági kérdéseivel foglalkozó menedzsment tagjainak és munkatársainak folyamatosan figyelemmel kell kísérniük a saját szakterületükön bekövetkezett változásokat. Ennek megfelelően új eljárásokat és módszereket kell kidolgozni és alkalmazni annak érdekében, hogy a vállalat felső vezetése időszerű és megfelelő információk birtokában tudja meghozni döntéseit.

Alapvetően azt kell mérlegelni, milyen költségeket kíván a vállalat ebben a témakörben *cash flow*[24] szinten internalizálni. Nyilvánvalóan felmerül az a kérdés, hogy egy konkrét kiadásnak van-e vállalatbiztonsági dimenziója, vagy nincs. Például, ha egy nagy kiterjedésű telephellyel rendelkező vállalat a telephelyen egy új utat épít vagy egy meglévőt kijavít, akkor ez például a beavatkozó egységek[25] elérési útvonalának optimalizálása révén védelmi költségnek minősül-e, avagy inkább a telephelyen belüli árumozgatás támogatása miatt logisztikai kiadás. Hasonló kérdés számos esetben felmerülhet, alapvető fontosságú tehát ezen kérdések gondos mérlegelése és a különböző költséghelyek, erőforrások és kivitelezések megfelelő csoportosítása, illetve hozzárendelése. A kellő gondossággal kimutatott védelmi költségek esetén a következő kérdés, hogy milyen védelmi dimenzióban szükséges a vállalatnak gondolkodnia ahhoz, hogy jól hasznosítható keretek között történjen az idevonatkozó elemzés.

A vállalat több tényezőhöz kötheti az általa szükségesnek ítélt védelmi képességeket, és ennek megfelelően biztosíthat ezek eléréséhez erőforrásokat. Ez a csoportosítás két dimenzióban összegezhető. Egyfelől meg kell határozni, hogy pontosan milyen képességeket igényel a vállalat, és utána meg kell határozni, hogy minden egyes képesség elfogadható szintű eléréséhez milyen időtávon és milyen erőforrások szükségesek. (Az időtáv már csak likviditási szempontokból is lényeges.) Ez a csoportosítás természetesen a megfelelő szintű, azaz igazgatóság általi jóváhagyást követően folyamatos nyomon követést igényel annak érdekében, hogy pontosan követhetők legyenek azok a lehetséges hatások, amelyek a vállalatot érik, illetve érhetik, valamint hasznosíthatók legyenek a vállalaton belüli szinergiahatások. A vállalatot érő hatások csoportosítása és elemzése annál bonyolultabb feladat, és annál magasabb szintű elemzőcsapatot igényel, minél nagyobb kiterjedésben dolgozik a vállalat. Könnyű belátni, hogy a világméretekben tevékenykedő nagyvállalat világméretű veszélyekkel kell hogy szembenézzen, vagy legalábbis az egész világon szóba jöhető veszélyek érinthetik

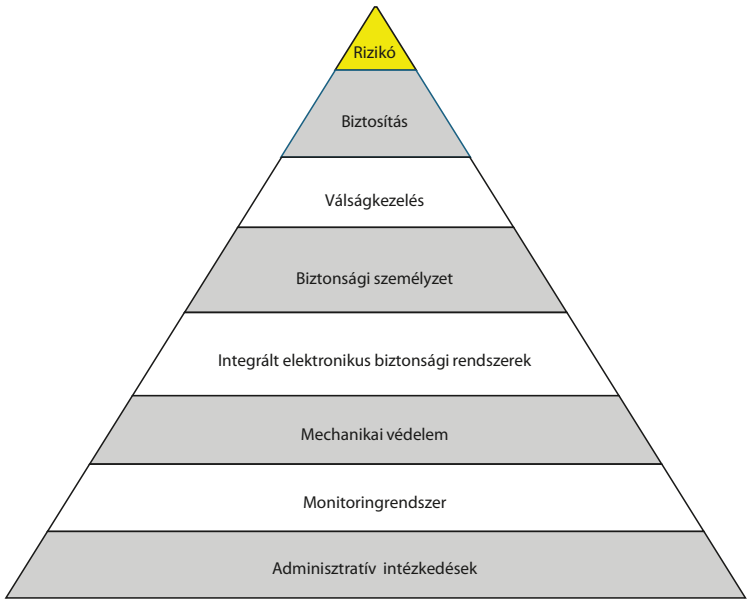
[24] Pénzügyi kimutatás, amely összefoglalja a készpénz és készpénzhez kapcsolódó eszközök mozgását.
[25] Létesítményi tűzoltóság, mentőszolgálat, járőrszolgálat.

tevékenységét. Ugyanakkor minél több ilyen veszélynek, illetve fenyegetettségnek kitett a vállalat, annál nagyobb a valószínűsége annak, hogy valamely telephelyén már merült fel olyan igény, illetve intézkedés, amely megkönnyíti más telephelyeken is a hasonló fenyegetettségekre való reagálást. Ezen tényezők statikus vizsgálata természetesen nem elégséges, azok folyamatos és dinamikus vizsgálatot igényelnek.[26]

A következő kérdés, hogy milyen időtávra próbál meg az elemzőcsapat előre tekinteni. Különböző és nagyon gondosan összeállított szempontok alapján kell meghatározni az elemzés célzott időtávját. Ennek során értelemszerűen nemcsak gazdasági, hanem politikai tényezőket is célszerű elemezni, amelyek különböző földrészek különböző országaiban, különböző telephelyeket közvetlenül érinthetnek. Ugyanilyen fontos kérdés lehet a lehetséges intézkedéseket, illetve felhasznált berendezéseket befolyásoló jogszabályi környezet változásának kérdése. Voltaképpen a kérdés úgy tehető fel összegzésképpen: a világ mely táján, mely hatások alapján létező, illetve várhatóan kialakuló, mely fenyegetésekkel szemben, milyen védelmi képességek alkalmazását, illetve kifejlesztését látja szükségesnek a nagyvállalat. Figyelembe kell venni ehhez természetesen saját termelési ciklusait is, valamint portfóliója folyamatos módosulását, ami szintén befolyásolhatja a biztonsági igényeket (lásd többcélú felhasználási termékek). Ha sikerült összeállítani a fenti igényeket, akkor nagyon gondosan össze kell állítani az ezek lefedéséhez szükséges költségstruktúrákat is. Amennyiben ez sikerült, úgy el kell fogadtatni a vállalat vezetésével az ehhez szükséges költségvetést. Adott esetben a költségeket persze csökkentheti a különböző együttműködési lehetőségek köre, de végső soron a kérdés az, hogyha lebontjuk a költségeket, akkor egy dolgozó biztonságos jelenlétének költségét kell meghatározni, egy termék biztonságos előállításához a nagyvállalat összes egyéb funkciójának biztonságos megvalósítása mellett. Ez természetesen az egyes tényező szintjére lebontva éppoly nehéz feladat, mint amikor a kérdés úgy merül fel, hány reklámforint, hány eladott terméket eredményez – amivel kapcsolatban óhatatlanul fel kell idézni azt a megközelítést, miszerint a reklámköltségek fele mindig felesleges, ugyanakkor aligha lehetséges meghatározni, hogy melyik fele. Voltaképpen egyfajta diszkontált nettó jelenérték-számítást célszerű elvégezni, ily módon szembe állítva egymással a biztonságot és a munkatársak számára biztonságos körülmények között zajló termelést. Innentől kezdve voltaképpen a két tervező-elemző csapatnak kell dinamikus kölcsönhatásban működnie: hogyan alakulnak a kölcsönösen meghatározott súlypontok eredőjeként meghatározott időtávok vonatkozásában a biztonságos körülmények által előidézett működésbeli, illetve termelékenységi előnyök egyfelől, illetve a kellő gondossággal és a mindenkori várható veszélyek elemzése kapcsán meghatározott képességek finanszírozását szolgáló költségek másfelől. Felmerül a kérdés, mi az, amit a vállalat elfogadhatónak tart, mi az, amit szükségesnek vél, mi az, amire már csak presztízsokokból is szüksége van, hogyan változik mindez napról napra, és a diszkontált nettó jelenértéken számított költségek, illetve forgalomnövekmények aránya milyen várható pontosság mellett, hogyan viszonyul egymáshoz.

[26] „Tényezők statikus vizsgálata" a már rendelkezésre álló adatok (jogszabályok, bekövetkezett események és statisztikák) elemzése. A „dinamikus vizsgálatok" egy konkrét esemény elemzését jelenti, amelyet a SitCen (lásd Security and Situation Centre fejezet) hajt végre. Ezen információk alapján van lehetőség a biztonsági előírások felülvizsgálatára.

Védelmi rendszer kiépítésénél és üzemeltetése során figyelembe kell venni a biztonsági rendszer elemeinek fontossági sorrendjét. Az elemek egymásra épülnek, és kiegészítik egymást. Az *integrált biztonsági és védelmi koncepció*[27] tartalmazza az összes elemet.




| |
|---|
| Kockázat |
| Biztosítások, felelősségbiztosítások |
| SitCen, Válságkezelő Központ, egyéb ügyeleti szolgálatok |
| Létesítményi tűzoltók, vagyonőrök, mentőorvosok, mentőápolók |
| Tűzjelzők, betörésjelző, beléptető, videómegfigyelő rendszerek |
| Tűzgátló anyagok, kapuk, ajtók, kerítések, rácsok, biztonsági fóliák |
| SitCen: térinformatikai rendszerek alkalmazása, szakértők, ügyeleti rendszer |
| Jogszabályok, szabványok, hatósági előírások, rizikóanalízis alapján (SWOT, Bartlett-modell…), belső előírások készítése |

*1. ábra: Integrált biztonsági és védelmi koncepció*
*Forrás: a szerzők szerkesztése* PATAKI *2019a alapján*

Ebben határozzák meg a különböző szakterületek és üzleti egységek feladatát és kötelezettségeit, valamint az alkalmazott biztonsági rendszerek teljes körű integrációját:[28]

[27] PATAKI 2021: 151–152.
[28] PATAKI–SULÁNYI 2011.

- a vállalatbiztonságra fordított erőforrások és befektetések megtérülésének bizonyítása;
- értékalapú irányítási rendszert alkalmazunk, amelynek relatív mutatója a befektetés megtérülése (roi);[29]
- érték-hozzájárulás és értékmutatók alkalmazása.[30]

A biztonsági költségek üzleti titkoknak minősülnek. Így nehéz megfelelő adatok hiányában pontos adatokat publikálni, de informális beszélgetések alapján kijelenthetjük, hogy Magyarországon ma a vállalatok döntő többségénél ez pontosan ellentétes a szakmailag elvárt arányokkal. Jelentős projekteket kell indítani a vállalatoknál, hogy a szakmailag elfogadott optimális költségeloszlás valósuljon meg. Az új jogszabályok (NIS 2 és CER) és az ISO 27000-es sorozatok „rákényszerítik" az érintett vállalatokat, hogy a törvényi elvárásoknak megfeleljenek úgy, hogy a működési költségeik se nőjenek. Ezt csak az integrált biztonsági koncepcióval tudják megvalósítani. Ezen belül is az „Adminisztratív intézkedések", „Monitoring" és „Biztonságtechnikai rendszerek" elemek erősítésével, annak érdekében, hogy a „beavatkozó erők" létszáma csökkenthető legyen. Így a biztonsági költségek is jelentősen csökkenthetők.

A koncepció „Biztosítás" elemének szerepét is át kell gondolni, mert jelentős költségeket jelent. Az utóbbi években a biztosítási költségek többszörösükre emelkedtek.[31] A tapasztalatok alapján csak a közvetlen károk térülnek meg teljesen, a közvetett károk összegét a biztosítók már nem tudják teljes egészében megtéríteni.

Meg kell gondolni, hogy a biztosításokat úgy kössék meg a cégek, hogy a közvetlen károkat teljes egészében fizesse ki a biztosító, a közvetett károkat nem fogják tudni, mert ha történik egy olyan esemény, amely több multinacionális vállalatot érint, akkor több cég is benyújtja a számláit, így a biztosítók képtelenek kifizetni a teljes összegeket.

A vállalatbiztonság feladata egy sor eredményorientált intézkedés és kapcsolódó mérőszám[32] kidolgozása kell hogy legyen, amelyek:

- segítik a felső vezetést a biztonsággal kapcsolatos kockázatok megértésében és a kockázattűrés paramétereinek kialakításában;
- biztosítják, hogy a pontok hatékonyan kapcsolódjanak egymáshoz a kockázati kitettség megbízható képe érdekében;
- nyomon követési ajánlásokat és intézkedéseket tesznek lehetővé;
- lehetővé teszik a kockázatcsökkentési tevékenységek eredményeinek nyomon követését; valamint
- keretet biztosítanak a biztonság értékének értékeléséhez mint az üzleti stratégia központi eleméhez egy egyre kockázatosabb világban.

[29] *Return on Investment* – beruházások megtérülése.
[30] Nemessályi 2005.
[31] European Insurance and Occupational Pensions Authority 2024.
[32] Teljesítménymutató (*performance indicator*, PI) a kitűzött cél elért eredményét objektíven, számokkal írja le. Ez a tömörített információ lehetővé teszi a terv/tényértékek összehasonlítását. Ezt az adott vállalat biztonsági stratégiájából kell levezetni, kidolgozni és követni. Ezek alapul szolgálnak az üzleti és szervezeti egységek céljainak meghatározásához. Minden biztonsággal kapcsolatos teljesítménymutatót az adott vállalat felső vezetése hagyja jóvá, de a vállalatbiztonság készíti el.

## A munkaerő technológiával való felváltása

A nagyvállalati szegmens valószínűleg gyors ütemben fog növekedni a globális fizikai biztonsági piacon. Az üzleti egységeket olyan tényezők vezérlik, mint az új EU-irányelvek bevezetése, valamint a megnövekedett védelmi infrastruktúra, az érzékeny információk védelme és a megnövekedett befektetési költségek.

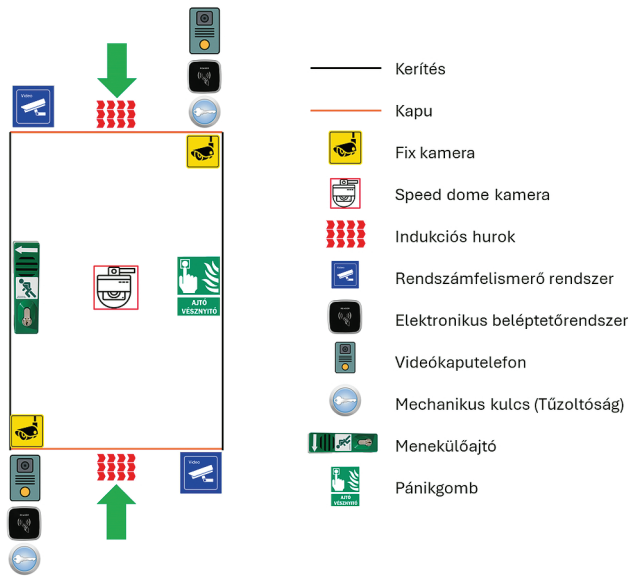
A költséghatékonyság egyik fő ösztönzője az új technológiák alkalmazása tekintetében az, hogy a biztosítási és védelmi feladatok elvégzéséhez szükséges személyzet létszámának csökkentésével mérsékelhetik a személyzeti költségeket. A hatékonyság ugyanakkor javítható: kamerák vagy drónok figyelhetik a nehezen vagy költségesen hozzáférhető területeket. A telefonok, az AI[33] -alapú videómegfigyelés vagy más érzékelők által gyűjtött és a mesterséges intelligencia által feldolgozott adatok képesek azonosítani és felismerni azokat a mintákat, amelyekre az emberek nem képesek. A technológia a biztonsági alkalmazottak biztonságérzetét is javíthatja, mivel kevesebb kockázatnak teszi ki őket azáltal, hogy lehetővé teszi azok távoli értékelését és javítja a munkahelyi kommunikációt. Jó példa erre a CCTV és a drónok közös használata nagy területek megfigyelésére vagy az incidens bejelentését követő helyzet gyors felmérésére. A fejlődő technológiák és a változó biztonsági igények miatt a szervezetek és az egyének folyamatosan értékelik eszközeik védelmének legjobb módjait. Az egyes biztonsági megoldások árnyalatainak megismerése során szem előtt kell tartani annak fontosságát, hogy a választást az egyedi biztonsági igényekhez és célokhoz igazítsák.[34]

Az objektumok/épületek az elmúlt években folyamatosan fejlődtek, és az „egyszerű" riasztástól eljutottunk a mesterséges intelligencia alkalmazásáig. Az integrált biztonsági rendszerek alkalmazása költséghatékonyabb, mert egy biztonsági rendszer folyamatosan és stabilan működik – a megfelelő karbantartás mellett –, és ezzel a biztonsági személyzet létszáma csökkenthető. Viszont a rendszereknek is vannak korlátai, ezért fontos az egyensúly megteremtése a technológia és az ember között. Egy tökéletesen kiépített és működtetett integrált biztonsági rendszer nem tud úgy gondolkodni, mint egy ember. Egy rendszer csak azokat az eseményeket tudja detektálni és kezelni, amelyekre programozták, ha ettől eltérő esetet derít fel, akkor „összezavarodhat", és riasztást generál, ha nincs is valós veszély, illetve figyelmen kívül hagyja az alattomos fenyegetéseket, amelyeket csak egy ember tud észlelni. Ha az emberek egy biztonsági őrt látnak, nagyobb biztonságban érzik magukat. A biztonsági személyzet sokkal többet tesz annál, mint hogy csak figyel a veszélyre. Azért is ott vannak, hogy segítsenek a látogatóknak, útbaigazítást vagy segítséget nyújtsanak, amire egy biztonsági rendszer nem képes. Ezt az integrált biztonsági rendszerek nem tudják garantálni. Az emberi tényező előnye, hogy képes értelmezni az összetett és bonyolult helyzeteket, döntéseket hozni, és szükség esetén azonnali beavatkozást végrehajtani.[35]

[33] *Artificial intelligence* – mesterséges intelligencia.
[34] Husseini 2019.
[35] Tóth 2018: 35–39.

*Befektetésarányos megtérülés számítása*

A járműforgalom ellenőrzésénél fontos szempont a „négy szem elv”,[36] vagyis a gépjárművek ellenőrzését két vagyonőrnek kell végrehajtania. Ezt a feladatot automatizálhatjuk egy automata zsilipkapurendszer kiépítésével. Ezzel az egyszeri befektetéssel az élőerős őrzés kiváltható. Ha a vállalat már rendelkezik videómegfigyelő rendszerrel, illetve rendszámfelismerő rendszerrel, valamint elektronikus beléptetőrendszerrel, akkor csak a meglévő biztonságtechnikai rendszereink bővítéséről beszélünk. A zsilipkapurendszer létesítésénél a következő szempontokat kell figyelembe venni:




*2. ábra: Automata zsilipkapu blokkvázlata*
*Forrás: a szerzők szerkesztése*

Biztonságtechnikai rendszerek és felszerelések, valamint minimumkövetelmények:

- minimális kerítés/kapu magasság 2 m;
- vészhelyzetek kezeléséhez szükséges a mechanikus kulcs telepítése, párhuzamos zárással (tűzoltóság);
- „Tűzoltókapu” felirat szükséges, Megállni tilos tábla (KRESZ szerint);
- közlekedési lámpák;
- infravörös fotocellák és elektromos biztonsági érintkezőléc;
- vészajtó vagy biztonsági kézi vészkioldó;
- beléptetőrendszer;videómegfigyelés (fix, dóm és rendszámfelismerő kamera);
- videókaputelefon (segélyhívás opció);
- biztonsági központ: a vészhelyzetek kezelése és a rendszer felügyelete.

[36] A „négy szem elve” olyan ellenőrzési módszer, amelynek alkalmazásával egy adott feladatot, egy feladat/esemény szabályszerűségét két, egymástól függetlenül eljáró személy teljeskörűen vizsgál.

*3. ábra: Automata zsiliprendszer járműforgalom számára*
*Forrás: a szerzők szerkesztése*

A meglévő biztonságtechnikai rendszerek alkalmazásával építünk ki egy, a nap 24 órájában működő kaput, amely egysávos és kétirányú forgalmat biztosít. Ha egy rendelkező kaput telepítünk, a ROI-érték meghatározása a következő: ha egy vagyonőr óradíját 4000 forintban határozzuk meg, akkor két fő vagyonőr éves költsége 70 080 000 forint. Az automata zsilipkapurendszer összköltsége a beérkezett árajánlatok alapján 66 800 000 forint. Tehát az őrzés költségét elosztjuk a befektetés összköltségével, majd megszorozzuk 100-zal, és megkapjuk a befektetés ROI-mutatóját, így 105,98%-os ROI-val számolhatunk, vagyis jövedelmező lesz a befektetés már az első évben. A későbbi időszakban költségként már csak a karbantartási és javítási költségekkel kell számolnunk.

## Gördülő tervezés

A gördülő tervezés[37] alkalmazásával a stratégia bevezetésének alapkövét jelenti a *pénzügyi mutatók* transzparenssé tétele.

Az első években fix biztonsági költséggel kell számolnunk, amely tartalmazza a humán, a karbantartás és első alkalommal a beruházás költségeit. Az új elemként megjelenő beruházási költségeket belső átcsoportosítással teremthetjük meg, de ez megköveteli – egyidejűleg – a humán költségek csökkentését, amit az egységes adminisztratív intézkedések bevezetése tesz lehetővé. A stratégiában meghatározott

[37] *Rolling wave planning,* bizonyos elemeit alkalmazva a hosszú távú terveket a legmagasabb szinten határozzák meg. Ez folyamatos célkövetést igényel, és ezzel megvalósul a projekt kontrollingfolyamata is. A stratégiai tervezés pénzügyi céljait, amikor még kevesebb információ áll rendelkezésre, a munkacsomagokat csak az ismert szintig bontják. Amint több ismeret válik tudottá a közeljövő eseményeiről, a munkacsomagokat tevékenységekre bontják.

időszakban el kell érni a kívánt 50-50%-os arányt, és így a jövőben már három költségnemmel kell számolni:

- humán,
- karbantartás,
- beruházás.

A tervezés során a létszám optimalizált legyen és ne a fűnyíró elvet alkalmazzuk. Az első lépés a már meglévő folyamatok felülvizsgálata és a nem működő vagy felesleges folyamatok megszüntetése. Így a bürokrácia csökkentésével más költségeket is csökkenthetünk, és a maradó alkalmazottak munkavégzése is hatékonyabbá válik. A létszám-optimalizálás során előállhat olyan helyzet, hogy egy új szervezeti egységet (osztályt) kell megalakítani. Ez első hallásra antagonisztikus kijelentésnek tűnhet, de ha megvizsgáljuk az így létrehozandó új szervezeti kereteket, akkor bebizonyosodik, hogy az új szervezeti egységgel a biztonsági szervezet összlétszáma csökken. Természetesen a különböző kompetenciaterületeknek továbbra is működnie kell, de ha az azt végző alkalmazottat leépítettük, akkor meglévő munkatársaknak kell továbbképzést szervezni, hogy *multitaskingban*[38] képesek legyenek további kompetenciaterületen érvényesülni.

A régi és az új biztonságtechnikai és IT-biztonsági rendszereknek meg kell felelni a CER és NIS 2 jogszabályokban megfogalmazott elvárásoknak. A már meglévő biztonságtechnikai rendszereket az új biztonsági kihívásokhoz kell igazítani. Kiemelt feladat, hogy az új rendszerek kiválasztásánál figyelembe kell venni a kompatibilitást a már meglévő rendszerekkel, mert a megfelelő kommunikáció nélkül az integrált biztonsági koncepció működésképtelen lesz. Automatizáljunk, szüntessük meg és/vagy szervezzük ki a felesleges folyamatokat!

A stábfunkcióval rendelkező személyi állomány[39] jelentősen csökkenthető, ha a központban szolgálatot teljesítő alkalmazottak magasabb szintű szakmai végzettséggel rendelkeznek, és minden kompetenciaterületen képesek döntéseket hozni.[40]

## Security and Situation Centre (SitCen)

A SitCen[41] központi irányító egységként szolgál a különböző beavatkozó egységekkel együtt. A SitCen folyamatosan felügyeli a vállalat biztonsági helyzetét, és az elvárt kockázati szinten tartja azt. A SitCen a vállalatbiztonság szervezetének része és két funkcióval rendelkezik.

[38] *Multitasking:* egyszerre több feladatot képes elvégezni a munkatárs.
[39] Saját mérnöki és/vagy adminisztratív munkatársak.
[40] Biztonságtechnikai mérnök (Tűzvédelem/Vagyonvédelem/Munkavédelem) + Környezetvédelmi technikus – OKJ-tanfolyamok.
[41] Pataki 2019a.

### *Biztonságtechnikai és IT-biztonsági rendszerek felügyelete és a beavatkozó erők irányítása*

Felügyeli, feldolgozza, kiértékeli és dokumentálja a vállalat területén üzemeltetett biztonsági rendszerek jelzéseit, amelyekre a megfelelő intézkedéseket kiadja. Irányítja a beavatkozó egységek[42] munkáját, koordinálja és támogatja egy adott esemény felszámolása során. Intézkedik a biztonsági rendszerekkel kapcsolatos hibák kijavításáról.[43]

A SitCen-ben alkalmazott biztonságtechnikai rendszerekben sokféle hardver és szoftver üzemel. Ezeknek képeseknek kell lenni arra, hogy önállóan is működjenek, illetve egy integrált rendszerben legyenek felügyelve. Az egymásra épülésükből kialakított rendszer az integrált felügyeleti rendszer. Feladatai a jelzést adó alközpontok jelzéseinek vétele, értelmezése, megjelenítése, mentése (naplózás).[44] A lehetőség szerinti magas integráció lehetővé teszi a különféle releváns telepített biztonsági rendszerek vezérlését is. A megjelenítésnél mindig prioritást kapnak az életvédelmi rendszerek (például tűzjelző). Az egyes riasztási típusokhoz tartozó tevékenységi rend a háttérben jelenik meg. Ez esetben fontos az épületek és helyiségek grafikus megjelenítése (a riasztás helye, oka, a kamerák helyzete, a helyiségek, az ott-tartózkodó személyek létszáma, a veszélyforrások, például tárolt veszélyes anyagok). A kiértesítési terv közvetlen összeköttetésben van a riasztási tervvel, de manuálisan is elérhető.

### *Helyzetelemző funkció*

Információ gyűjtése, információk kezelése, médiafigyelés, elemzés, várható kihatások felmérése, szakértők bevonása, döntés-előkészítés, koordináció, kapcsolattartás, szakértők és érintett vezetők informálása. A SitCen időben való tájékoztatása nélkül – vagy hiányában – a válságkezelő szervezetek nem tudják tevékenységüket megkezdeni és a válságot megoldani. A válságkezelés feladatait a SitCen-ből irányítják, amelynek működési alapját az információk gyűjtése, elemzése, értékelése és terjesztése, a döntések meghozatala, a feladatok meghatározása és a végrehajtás eredményeinek értékelése jelenti.

### *Válságkezelés*

Ezen alapvetések szerint a vállalatnak rendelkeznie kell a kor színvonalán álló válságkezelő szervezetekkel és módszerekkel, amelyek a menedzsmentfolyamatok fontos részét képezik.

[42] Létesítményi tűzoltóság, vagyonvédelmi szolgáltató, mentőszolgálat.
[43] Helyzetelemző és Biztonsági Központ – Security and Situation Centre.
[44] Berek 2014: 9–11.

DIADAL válságkezelési módszer

A módszert a konfliktuskezelés egyes szakaszainak kezdőbetűi alapján nevezték el DIADAL-nak.[45]

A válságkezelés első lépése mindig a *diagnózis* megállapítása, amely a vállalat SitCen szervezeti egységének feladata. Az első azonnali feladat a kialakult helyzettel kapcsolatos információk gyűjtése, majd végre kell hajtani az elsődleges elemzést. A következő 2–4 órában az időszámvetés a legfontosabb: mit tudunk azonnal cselekedni, valamint az azonnal alkalmazandó rendszabályok, első intézkedések, utasítások, korlátozások bevezetése.

A válságkezelés második lépése a kríziskezelés *irányának* meghatározása. Ez a vállalati válságstáb és a vállalati felső vezetés feladata, és ezt a válság kitörését követő 3-4, maximum 5 órán belül kell megtenniük. Először közösen kell megfogalmazni a stratégiai célokat, beleértve a válságkezelés pozitív céljainak meghatározását (azaz az elérendő eredményeket); a negatív céljaink meghatározását (azaz az elkerülni kívánt eseményeket és következményeket) és az elkerülhetetlen következmények meghatározását. A stratégiai célokat követően meg kell határoznunk a válságkezelés fókuszát és fontosabb területeit. Az irány meghatározásának utolsó feladatai közé tartozik a médiakapcsolatok felkeresése: előzetes nyilatkozat kiadása, sajtótájékoztató megtartása, valamint egy szóvivő kijelölése a média folyamatos tájékoztatására.

A válságstáb feladata továbbá, hogy a válságot követő 12–24 órán belül kidolgozza a cselekvési lehetőségeket és *alternatívákat.* Ekkor a válságstáb kidolgozza a krízis lefolyásának legjobb, legrosszabb és legvalószínűbb változatait, felvázolja a válság valószínűsíthető irányait, előnyeit és hátrányait, valamint indokolja a feltételezéseket. Ezt követően a SWOT-módszerrel[46] értékeli a kidolgozott alternatívákat.

A negyedik lépésben arról kell dönteni, hogy a javasolt cselekvési irányok közül melyiket érdemes végrehajtani és részletesen *kidolgozni.* A választás során a döntéshozó a döntési mátrix (normál, súlyozott) alapján hozza meg döntését, figyelembe véve az adott lehetőségek előnyeit és hátrányait, a szükséges időt és a költségeket. A döntést a válság bekövetkezését követő 13–27 órán belül meg kell hozni.

Az ötödik lépés az *alkalmazás:* az érintett szervezeti egységek kidolgozzák és beterjesztik a kiválasztott cselekvési változat részletes feladattervét.

A válságkezelési folyamat *lezárása* a vállalati felső vezetőség feladata, amely magába foglalja a válságstáb és a beavatkozó erők ellenőrzését a cselekvés teljesítése során, továbbá a válságkezelésben részt vevők tapasztalatainak, benyomásainak és javaslatainak összegyűjtését.

[45] Resperger 2018: 16–20.

[46] SWOT-elemzés egy stratégiai tervezési eszköz: *strengths* (erősségek), *weaknesses* (gyengeségek), *opportunities* (lehetőségek), *threats* (veszélyek).

Biztonsági kockázatok meghatározása

- A biztonsági kockázatértékelések[47] átfogó értékelést nyújtanak a vállalatról (GRC).[48]
- A biztonsági kockázatértékelési jelentés azonosítja a megfelelően biztonságos rendszereket és azokat, amelyek nem megfelelően működnek. Ezen rendszereket felül kell vizsgálni, valamint új biztonsági szabályokat és konkrét technikai ajánlásokat kell megfogalmazni.

A jóváhagyott biztosítási és védelmi tervekkel a kidolgozott szcenáriók alapján kell a válsághelyzetet kezelni a térinformatikai/biztonsági rendszerek alkalmazásával. Így az előre nem látható események időben felderíthetők, ami lehetővé teszi a válságkezelő szervezetek és a beavatkozó erők előzetes figyelmeztetését és riasztását.

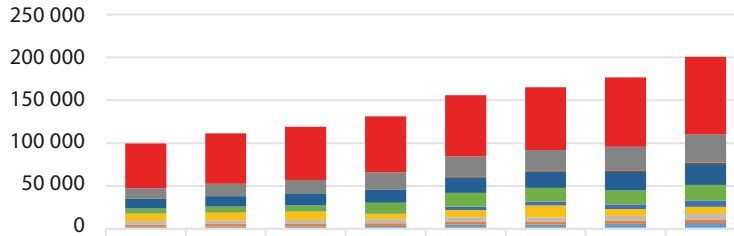
## CER, NIS 2 és a módosított Vbö.-nek való megfelelés

A tanulmányunk első részében a globalizáció hatásait már vizsgáltuk, és megállapítottuk, hogy a legnagyobb problémát a törésvonal-konfliktusok okozzák. Ezek az ellentétek államok közötti szembenálláshoz, konfliktusok kialakulásához vezethetnek, amelyek során az államok a negyedik generációs hadviselés[49] módszereit alkalmazhatják egymással szemben. Ezért egységes fellépésre van szükség a nemzetközi szervezetekkel és intézményekkel közösen a kritikus területeken.[50]

Az IT-technológia gyors fejlődésével a vállalatok egyre komplexebb biztonsági fenyegetésekkel szembesülnek mind a fizikai védelem kompetenciaterületen, mind a virtuális térben. Nagyon sok vállalatnál a fizikai biztonság és az IT-biztonság külön szervezeti egységek kompetenciaterületei, annak ellenére, hogy sok szálon kapcsolódnak egymáshoz. Ezeket egyedül az ISO 27000 szabványsorozatban kezelik egy egészként. A fizikai biztonság és az IT-biztonság közötti határok egyre inkább elmosódnak. Ezért véleményünk szerint a biztonsági stratégiának mindkettővel egyenrangú szinten kell foglalkoznia.

„Az IFSEC Global tanulmánya bizonyítja, hogy 2023-ban az informatikai és biztonsági szakemberek 36%-a tervez befektetni a fizikai biztonság fokozását célzó biztonsági rendszerekbe. Ezen adatok alapján kijelenthetjük, hogy a biztonsági infrastruktúra nagymértékben függ a hálózattól, valamint azt, hogy a »fizikai« és IT-biztonsági szakemberek hagyományos szétválasztása már nem hatékony."[51]

47 CER, NIS 2, Vbö. szerinti kockázatok.
48 *Governance, risk and compliance.*
49 A háborút továbbra is hagyományos és aszimmetrikus katonai eszközökkel vívják meg, kiegészítve irreguláris erőkkel és más nem katonai szereplőkkel és eszközökkel, például hackertámadásokkal, terrortámadásokkal, médiafölénnyel, nyomásgyakorlással üzleti körökre, kiszivárogtatásokkal és álhírekkel.
50 Pataki 2019b.
51 Moore 2023.




| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|
| Biztonsági szolgálat | 52 315 | 58 920 | 61 979 | 65 070 | 71 081 | 73 394 | 80 835 | 89 997 |
| Infrastruktúra-védelem | 12 583 | 14 106 | 16 520 | 20 462 | 24 109 | 24 089 | 28 359 | 33 319 |
| Adatvédelem | | | | | 1140 | 1192 | 1338 | 1667 |
| Hálózatbiztonság | 10 911 | 12 427 | 13 387 | 15 262 | 17 558 | 18 932 | 21 383 | 24 360 |
| Felhasználóazonosítás | 5948 | 6395 | 6699 | 12 036 | 15 865 | 15 900 | 16 169 | 18 556 |
| Felhőalapú tárhely védelme | 185 | 304 | 439 | 595 | 4323 | 4487 | 5616 | 7000 |
| Felhasználóbiztonsági szoftver | 8823 | 9043 | 9837 | 6507 | 8103 | 13 944 | 7901 | 8406 |
| Integrált rizikómenedzsment | 3949 | 4347 | 4555 | 4859 | 5647 | 5157 | 5687 | 6277 |
| Adatbiztonság | 2563 | 3063 | 2662 | 2981 | 3000 | 3073 | 3692 | 4333 |
| Alkalmazásvédelem | 2434 | 2742 | 3095 | 3383 | 4963 | 5048 | 5765 | 6670 |

*4. ábra: Információvédelmi költségek 2017–2024*
*Forrás: a szerzők szerkesztése Statista 2024 alapján*

A biztonsági szektor költségeinek meghatározásánál csak az IT-biztonsági költségekről találtunk statisztikai adatokat, amelyek tartalmazzák az *általános* és fizikai biztonság költségeit is. Megfigyelhető, hogy 2017 és 2024 között a biztonsági költségek megduplázódtak. A költségek elemzése során megállapítottuk, hogy a fizikai biztonság költségei 2017-ben a biztonsági költségek 52,4%-át tették ki, ami 2024-re 44,4%-ra csökkent. Ez a biztonsági rendszerek integrálásának és a mesterséges intelligencia alkalmazásának tudható be. Nagyon kevés biztonsági szervezet rendelkezik az összes biztonsággal kapcsolatos kompetenciaterülettel egy szervezeti egységen belül. A jövő a biztonsági kérdések integrált megközelítése, mert a *fizikai biztonság* és az *információbiztonság* összekapcsolódik, a konvergencia a jelenlegi tendencia. Az *integrált biztonsági rendszer* egyre népszerűbb fogalom, azonban még mindig túl kevesen alkalmazzák, és a fogalom ki is zárja a biztonsági kompetenciák számos elemét, amelyek a vállalat védelme szempontjából alapvetők, mint például:

- hatékony, logikus kapcsolat az IT-biztonsági rendszerek és a fizikai biztonságot adó rendszerek között;
- valós kockázatot jelent, ha a biztonsági auditot egy olyan *nem minősített külső szolgáltató*[52] végzi, aki érzékeny információkhoz vagy folyamatokhoz fér hozzá;
- a biztonsági stratégia, amelyben fontos szerepe van az alkalmazottak és a vezetők biztonságtudatának, nagyobb valószínűséggel csökkenti a bűncselekményeket

[52] Lásd NIS 2 törvény, TISAX, ISO 2700 sorozat.

és kötelességszegéseket, és így gyorsabb reakció várható el a biztonsági személyzettől;
- az információbiztonsági kockázatok megelőzése kulcsfontosságú a vállalat üzletmenet-folytonosság- és hírnévvesztéssel járó eseményeinek kezelésében;
- a pénzügyi veszteséggel járó események kivizsgálása lehetőséget kínál az ismert sebezhetőségek azonosítására vagy kiküszöbölésére, amelyeket a jövőbeli kockázatok elkerülése érdekében le kell zárni;
- a különböző biztosított kockázatoknak megfelelő megelőző védelemi képességek hozzájárulnak az alacsonyabb biztosítási díjakhoz;
- a beléptető és behatolásjelző, illetve más fizikai biztonsági rendszerek közvetlenül hozzájárulnak a kockázatok korai azonosításához.[53]

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 4.) MK rendelet a 2. számú mellékletének 12. pontjában határozza meg a Fizikai és környezeti védelemmel kapcsolatos követelményeket, de a melléklet több ponton is kapcsolódik ehhez, és a vállalatbiztonság több kompetenciaterülete is érintett/együttműködő (például válságkezelés, információvédelem) a következő feladatokban:
- üzletmenet-folytonossági terv kidolgozása;[54]
- biztonsági események kezelése;
- azonosítás és hitelesítés;[55]
- személyek háttérellenőrzése;
- adathordozók védelme;[56]
- karbantartás (TISAX[57]).

A CER, NIS 2 és Vbö. törvényeknek megfelelő biztosítási és védelmi rendszert és tervet a már meglévő biztonsági előírásokra alapozva célszerű kidolgoznia a következő lépésekben:
1. biztonsági kihívások, veszélyek és rizikók azonosítása;
2. érvényben lévő biztonsági előírások felülvizsgálata;
3. új biztonsági szabályok, folyamatok kidolgozása és beillesztése a már meglévő biztonsági rendszerbe.

Ezt azért tartjuk jó megoldásnak, mert a változtatás nem az egész rendszert érinti, hanem annak csak bizonyos elemeit.

[53] Campbell 2014: 31–39.
[54] Válságkezelés, krízismenedzsment, SitCen.
[55] Többfaktoros hitelesítés és azonosítás (pl. gyári belépőkártya: intelligens kártya és RFID-kódolás).
[56] A fizikai biztonságon túl, az üzleti utak során betartandó szabályok, *home office*.
[57] Trusted Information Security Assessment Exchange – német autóipari beszállítók részére kidolgozott IT-biztonsági követelményrendszer.

## Összegzés, következtetések

A geopolitikai változások, valamint az új EU tanácsi irányelvek hatálybalépése miatt egy új biztonsági stratégiát szükséges megalkotni, amelyben meghatározzák a nagyvállalat biztonsági vízióit és küldetését, valamint a védelmi célokat. Ezen stratégiát mindig az adott vállalat legmagasabb döntéshozatali szervezete vagy vezetője hagyja jóvá.

Bizonyítottuk, hogy egy multinacionális vállalat biztonsági szabályainak, előírásainak és biztonsági szervezetének kidolgozásakor teljes mértékben figyelembe kell venni az ország nemzetbiztonsági stratégiáját, illetve meghatároztuk a biztonsági stratégia alapvető elemeit. A biztonsági és védelmi rendszerekkel és azok működtetésével kapcsolatban kidolgozott stratégiák olyan alapvető dokumentumok, amelyek meghatározzák a vállalat felső vezetése számára a hosszú távú biztonsági célokat és elvárásokat.

A biztonsági projektek (NIS 2, CER, Vbö.) kölcsönösen függenek egymástól, és ez nagyon fontos szempont a stratégiai tervezésnél, amelyet egy közös projektben lehet eredményesen teljesíteni, illetve a költségeket is így optimalizálhatjuk. Ezen tény meggyőzően bizonyítja, hogy egy szervezeti egységeken átnyúló, a beazonosított kockázatoknak megfelelő kompetenciaterületekkel rendelkező „vállalatbiztonság" szervezet megalakítására van szükség. Napjainkban a megszokott biztonsági modellekkel ezért szükséges egy mátrix szervezeti egységet kialakítani, amelyben a különböző szervezeti egységek (IT-biztonság és vállalatbiztonság) önállósága és felelőssége nem vész el. Ezzel a modellel lehet eredményesen és hatékonyan kezelni a jelen biztonsági kihívásait. Természetesen a jogszabályokban meghatározott biztonsági auditokat a hatóságok vagy az általuk megbízott vállalkozások egymástól függetlenül hajtják végre.

Igazoltuk, hogy a NIS 2 és CER törvények miatt új biztonsági stratégia kidolgozása szükséges, amely figyelembe veszi a jogszabályi keretek változását, a világszerte jelentkező új kihívásokat, veszélyeket és kockázatokat, valamint a vállalatok vezetőségének és a biztonsággal közvetlenül érintett szervezeti egységeknek nyomon kell követniük a saját szakterületükön jelentkező a multinacionális vállalat működését alapvetően befolyásoló tényezőket. Ennek megfelelően új eljárásokat és módszereket kell kidolgozni és alkalmazni, hogy a vállalat felső vezetése megfelelő információk birtokában, kellő időben tudjon döntéseket hozni.

Vizsgálataink alapján igazoltuk, hogy a SitCen meghatározó szerepet tölt be a vállalatok biztonsági helyzetének megítélésében, tervezésében és működtetésében, valamint a kialakult válsághelyzetek kezelésében. Ehhez magas képzettséggel rendelkező alkalmazottakra lesz szükség, akik folyamatos munkarendben képesek lesznek a megfelelő szakemberek, illetve előre definiált mátrixszervezetek alkalmazásával a különböző válsághelyzeteket kezelni. A biztonsági rendszerek az elmúlt években folyamatosan fejlődtek, és az „egyszerű" riasztástól eljutottunk a mesterséges intelligencia használatáig. Az integrált rendszerek alkalmazása költséghatékony, mert egy biztonsági rendszer folyamatosan és stabilan működik – a megfelelő karbantartás mellett –, és ezzel a biztonsági személyzet létszáma csökkenthető.

Elemzéseink és következtetéseink alapján rámutattatunk, hogy a NIS 2 és a CER előírásai miatt a legtöbb vállalkozás esetében gondot jelentenek a megfelelés pénzügyi hatásai. Az irányelvek jelentősen kibővítik a szigorú biztonsági és védelmi intézkedések

betartására kötelezett iparágak és vállalkozások körét. Ezért a vállalatoknak erőforrásokat kell elkülöníteni a megfelelőség biztosítása érdekében. A biztonsági költségek növekednek, az előrejelzések szerint a vállalkozásoknak 10-20%-os költségnövekedéssel kell számolniuk.

## Felhasznált irodalom


Berek Lajos (2014): *Biztonságtechnika.* Budapest: Nemzeti Közszolgálati Egyetem. Online: https://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf

Campbell, George K. (2014): *Measures and Metrics in Corporate Security.* Waltham, USA: Elsevier.

European Insurance and Occupational Pensions Authority (2024): *European Insurance Overview 2024*. Online: https://nexteuropa-multisites.s3.eu-west-1.amazonaws.com/www.eiopa.europa.eu/assets/insurance-overview-report/European_Insurance_Overview_2024.html

Dénes Kálmán – Kovács Zoltán (2019): Létesítmények közműrendszereinek robbantásos cselekmények általi veszélyeztetettsége és védelme. *Hadtudományi Szemle,* 12(Különszám), 82–84. Online: https://doi.org/10.32563/hsz.2019.1.ksz.5

Hameleers, Michael (2025): The Visual Nature of Information Warfare: The Construction of Partisan Claims on Truth and Evidence in the Context of Wars in Ukraine and Israel/Palestine. *Journal of Communication,* 75(2), 90 – 100. Online: https://doi.org/10.1093/joc/jqae045

Huntington, Samuel P. (2006): *A civilizációk összecsapása és a világrend átalakulása*. Budapest: Európa.

Husseini, Talal (2019): Ai In The Sky: Can Drone Surveillance Technology Replace CCTV? *Army Technology,* 2019. július 10. Online: www.army-technology.com/features/ai-drone-surveillance-cctv/

Moore, James (2023): *Editor's Viewpoint: 2023 Technology Trends Ahead for the Physical Security Industry.* Online: www.ifsecglobal.com/physical-security/editors-viewpoint-2023-technology-trends-ahead-for-the-physical-security-industry/

North Atlantic Treaty Organisation (2016): *Commitment to Enhance Resilience*. Online: www.nato.int/cps/en/natohq/official_texts_133180.htm

Nemessályi Zsolt (2005): Jövedelem, jövedelmezőség, versenyképesség a hatékonyság rendszerében. In *A mezőgazdaság tőkeszükséglete és hatékonysága: Pfau Ernő professzor 70. születésnapja tiszteletére megrendezett tudományos ülés. 2005. május 26.* Debrecen: Debreceni Egyetem Agrártudományi Centrum, 199–208. Online: https://real.mtak.hu/6738/1/1190849.pdf

Paret, Peter (1986): *Makers of Modern Strategy from Machiavelli to the Nuclear Age.* Princeton, New Jersey: Princeton University Press. Online: https://doi.org/10.1515/9781400835461

Pataki János (2019a): Situation Centre in the Private Sector. *Nemzetbiztonsági Szemle,* 7(3), 18–27. Online: https://doi.org/10.32561/nsz.2019.3.2

PATAKI, János (2019b): NATO in 2030 and What the Future Will Bring „Essential Security, Dynamic Engagement". *Nemzetbiztonsági Szemle,* 7(4), 61–70. Online: https://doi.org/10.32561/nsz.2019.4.5

PATAKI János (2021): *A terrorizmus mint biztonsági probléma, a kritikus infrastruktúra védelmi szabályainak tükrében.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2021.014

PATAKI, János – SULÁNYI, Péter (2011): Lage- und Analysezentrum bei einem internationalen Unternehmen. *Hadmérnök,* 6(3), 161–168. Online: http://hadmernok.hu/2011_3_pataki_sulanyi.pdf

RESPERGER István (2018): *A válságkezelés és a hibrid hadviselés* [ePub]. Budapest: Dialóg Campus. Online: https://bit.ly/3NxwVNG

Statista (2024): *Information Security Spending Worldwide from 2017 to 2024, by Segment.* Online: www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/

Szun-Ce (2012): *A hadviselés tudománya*. Budapest: Göncöl.

TÓTH Levente (2018): A komplex objektumvédelem kihívásai napjainkban. *Bolyai Szemle,* 1, 35–39. Online: www.szakmaikamara.hu/files/images/Orszagos/Szakmai_Kollegium/publikaciok/Bolyai_Szemle_2018_01_toth-levente.pdf

TURI Laura Tamara – RESPERGER István – TÚRI Viktória (2012): *Stratégiaalkotás, stratégiai módszerek* [ePub]. Közigazgatási Vezetői Akadémia. Online: www.scribd.com/document/577246519/438

## *Jogi források*

Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról