Vállalkozásfejlesztés a XXI. században 2020/1. kötet
A szervezetek reakciója és válaszai a jelen kor üzleti kihívásaira

A vállalati biztonságpolitika a stakeholder elmélet és a felelősségvállalás tükrében

Saáry Réka

Óbudai Egyetem, Keleti Károly Gazdasági Kar
Gazdaság- és Társadalomtudományi Intézet
saary.reka@kgk.uni-obuda.hu

A vállalati biztonságpolitika a közbiztonsággal, nemzetbiztonsággal, a szociális, gazdasági biztonsággal illetve magánbiztonsági ágazat kihívásaival foglalkozó szakirodalmakkal összevetve, elenyésző figyelmet kapott az utóbbi évtizedben. Mindez azért meglepő, mert ahogy a fent felsorolt területeken, úgy a vállalati szinten is komoly küzdelem és versenyfutás zajlik a turbulens környezet indukálta, újfajta biztonsági kihívásokkal. A biztonsági vezetőknek manapság a vállalatirányítási feladatoktól, az üzlet folytonossági tervezésen és információ védelmen keresztül, a hírnév- illetve válságmenedzsmentig számtalan területen kell helyt állniuk, miközben a biztonsági terület vállalaton belüli megítélése, elismertsége nem sokat változott az utóbbi években.(Briggs-Edwards, 2006)

Cikkemben arra vállalkozom, hogy feltárjam a vállalati biztonság új stakeholderekhez köthető aspektusait. Vizsgálom, hogy értelmezhető-e az alapvetően gazdasági érdekek mentén működő szervezetek biztonsági felelősségvállalása és ha igen, akkor milyen kritériumok mentén definiálható a fogalom. A téma jellegére tekintettel az információgyűjtés feltáró kutatási módszer segítségével történt. Az eredmények öt vállalati biztonságpolitikai vezetővel lebonyolított, szakértői mélyinterjú során elhangzott vélemények alapján születtek.

Kulcsszavak: vállalati biztonságpolitika, vállalati biztonsági felelősségvállalás (CSecR), grounded theory

Bevezetés

A Magyar Értelmező Kéziszótár meghatározása alapján a biztonság „veszélytől, bántódástól mentes, zavartalan állapot". A Magyar Nyelv Értelmező Szótára szerint pedig „a dolgoknak, életviszonyoknak olyan rendje, olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs vagy alig van lehetősége, amelyben nem kell ilyentől félni…Valakinek vagy valaminek (veszélytől, kártól, jogtalan beavatkozástól, bántódástól való) védett állapota, helyzete." A legáltalánosabb értelmezés szerint tehát a biztonság - negatív

definícióval - leginkább valaminek (veszély, kockázat, bántódás stb.) a hiányával írható le. (Király-Pataki, 2013)

Tökéletes biztonság ugyanakkor nem létezik, ezért a szakértők a zavar elfogadható mértékének elismerése mellett, kiemelten kezelik a védelem fogalmát, ami adott fenyegetettség mellett „a biztonság megteremtésére, szinten tartására, fejlesztésére irányuló tevékenység." (Muha, 2007), illetve „…a véd igével kifejezett cselekvés, valakinek vagy valaminek a megvédését, megoltalmazását" jelenti .(Munk, 2007) A biztonság tehát állapotként, míg a védelem tevékenységként értelmezhető.

A fogalom összetettsége okán jelentéstartalmát, a különböző szakterületek jellemzően minősítő jelzők segítségével konkretizálják. A jelzős szerkezetekben, kontextustól függően egyaránt találkozunk a biztonság illetve a védelem kifejezésekkel, például (a teljesség igénye nélkül) a nemzetbiztonság, nemzetvédelem; egészségbiztonság, egészségvédelem; környezetbiztonság, környezetvédelem; szociális biztonság, szociális védelem esetében. (Munk, 2007, Borzán et.al, 2011; Lentner et.al, 2011)

A biztonság értelmezése körül kiterjedt diskurzus zajlik. A vita leginkább a szűkebb (realista) katonai- és államközpontú szemlélet képviselői illetve az új, kiterjesztő komplex megközelítés szükségességét sürgető teoretikusok között bontakozott ki. A nemzetközi biztonság diszciplína kutatói szerint a fogalom kiterjesztett, neorealista megközelítésének, azaz tág értelmezésének elfogadása ma már elkerülhetetlennek tűnik. A korábbi, a mindenkori államhoz kötött biztonság fogalma mára oly mértékben megváltozott, hogy rendszerében egyre növekvő súllyal jelennek meg a nem állami szereplők), fokozatosan zajlik az üzleti szféra bevonása erre a területre.

Elfogadhatjuk tehát, hogy legyen szó bármilyen biztonságról, annak garantálása a továbbiakban nem kizárólagosan az államhatalom, vagy a mindenkori kormány feladata. A rendszerben érintettek köre egyre sokszínűbb, és a szereplők biztonsággal kapcsolatos elvárásai is komplexebbé válnak. Jelen tanulmány a továbbiakban az üzleti szféra, a vállalatok, szervezetek lehetséges szerepvállalását vizsgálja az érintettjeik (stakeholdereik) szubjektív biztonságérzetének megteremtésében.

1. Vállalati biztonság

A vállalati biztonság számtalan definíciója ismert, általánosan elfogadott, a környezet kihívásihoz igazodó meghatározással azonban nem találkozunk a

szakirodalomban. Induljunk ki abból, hogy a biztonság üzleti követelmény, a vállalati célkitűzések a biztonság garanciája nélkül nem teljesíthetők. (Vasvári et al, 2006) „A vállalati biztonságpolitika fő szempontja a legfontosabb termelési tényező: az emberi élet és egészség védelme,…a vállalat működőképessége és a szolgáltatási piacok megtartása" (Király-Pataki, 2013: 181 o.) A szervezet biztonsága kedvező állapot (a fenyegetettséget – biztonságérzékenységet figyelembe véve a szervezet számára elfogadható), amelynek megváltozása nem valószínű, de nem is kizárható. (Vasvári, 2009)

A vállalati biztonság a biztonságtudományok alkalmazott területe, feladatorientált megközelítésben célja az emberek, az információ illetve a vállalati vagyon védelme a szervezeten belül, a vállalati önvédelem biztosítása. A vállalati biztonságpolitika lehetővé teszi, hogy a szervezet ellenőrzött és szabályozott formában lépjen fel a biztonsági fenyegetésekkel szemben. (Ludbey et al., 2017)

Michelberger (2014) meghatározásában egyedi módon, nem kizárólag a szervezet védelmére koncentrál, hanem hangsúlyozza annak, a környezete biztonságának megteremtésében, fenntartásában vállalt szerepét. „A vállalatbiztonság olyan állapot, amelyben a gazdálkodó szervezet képes hosszútávon fenntartani a működőképességét és értékteremtő folyamatait… A biztonság további kritériuma, hogy a vállalat jövője a stratégiai tervei alapján saját kezében van, és a vállalat tevékenysége során nem veszélyezteti a környezetét, a külső és belső érintetteket."

A fenyegetettség napjainkban egyre sokrétűbb, ezért fontos egyidejűleg több, különböző védelmi mechanizmus kialakítása, szervezése, működtetése. Ugyanakkor az egyes rendszerek kölcsönös függősége, a hatékony védelem megvalósításával kapcsolatos elvárások szükségessé teszik ezen mechanizmusok összefésülését, integrálását. (Papp, 2006) Ennek outputjaként valósul meg az integrált vállalati biztonságpolitika, ami értelmezhető, a korábban szigetként működő biztonsági alrendszerek összehangolásaként vagy a logikai és a fizikai biztonság. (de Cora, dn.) A vállalati biztonság menedzsmentje a biztonsági szervezet feladata, és nem megvalósítható a vállalat vezetésének elkötelezettsége, illetve a munkavállalók tudatosságának fokozása nélkül. A sikeres biztonsági vezetők a hagyományos biztonság szervezési feladatok ellátásán túl, képesek a biztonsági kultúrát kialakítani a szervezetben. A biztonsági kultúráról beszélhetünk általános értelemben akkor, ha az emberek ismerik és érvényesítik jogaikat, tisztában vannak a biztonságot veszélyeztető tényezőkkel és oktatják, esetleg elmarasztalják a társadalom azon tagjait, akik tudatlanságból, feledékenységből vagy személyes gyengeségből nem biztonságos magatartást tanúsítanak. (Vasvári, 2009)

A fentieken túl a vállalati biztonságnak további haszonélvezői is lehetnek, személyek vagy szervezetek, amelyek nem csak a biztonság előnyeiből részesülnek, hanem befolyással lehetnek az általános vállalati biztonság alakítására is (pl. beszállító partnerek, ügyfelek, tulajdonosok, külső szabályozó szervek, közösségek stb.). A vállalat egyes érintettjei a biztonság különböző aspektusai tekintetében határoznak meg elvárásokat, esetleg valósítják meg hozzájárulásukat a vállalati biztonságpolitika számtalan területén.

2. Stakeholder szemlélet és a kapcsolódó elméletek bemutatása

Jelen publikációban nem törekszem a primer kutatást megalapozó elméletek széles körű bemutatására, ugyanakkor fontosnak gondolom az egyes teóriák alapvetéseinek ismertetését. Ennek megfelelően a tanulmány ezen fejezetében az érintetti elmélet, a vállalati társadalmi felelősségvállalás valamint a biztonsági felelősségvállalás alapjait tekintem át.

2.1 Stakeholder elmélet

A vállalati működés érintettek irányából történő megközelítése a hagyományos közgazdaságtani vállalatfelfogástól eltérően a szervezeteket a környezettel szoros interakcióban lévő entitásként határozza meg. (Málovics, 2009)

A stakeholder elmélet atyjaként aposztrofált Freeman több definíciót fogalmazott meg az évek során, az első, és egyben legelterjedtebb szerint „érintett/érdekgazda minden olyan szervezet vagy csoport, amely képes hatni egy vállalatra/szervezetre céljainak elérésében illetve/vagy a vállalat/szervezet céljai elérése során hat rá”. (Freeman, 1984) Később az érintettek definíciói vonatkozásában parázs vita bontakozott ki, amelyben a szakértők fent említett tág értelmezéstől, a legitim igényeken át, a legszűkebben vett, kockázatot vállaló szereplőkig, eltérő módon közelítették meg a kérdést.

Freeman a piaci szereplőket úgynevezett érintetti térképen ábrázolta, amelyen a szerző tizenegy érintettet tüntetett fel, a későbbi modellek általában hét stakeholdert jelölnek, ezek: a tulajdonsok/befektetők, alkalmazottak, beszállítók, versenytársak, ügyfelek/fogyasztók, a társadalmi környezet/közösségek valamint a kormányzat. (Fassin, 2009)

Az érintetti elmélet premisszáit a következőképpen foglalhatjuk össze: (Jones-Wicks, 1999) (Savage et al,, 1991)

- a szervezetek kapcsolatot létesítenek olyan egyénekkel illetve csoportokkal, amelyekkel kölcsönösen hatnak egymásra,
- a stakeholder elmélet ezen kapcsolatok természetére fókuszál, a folyamatok valamint az együttműködésből származtatható eredmények vizsgálatának tükrében,
- a legitim érintettek érdekei belső értékkel bírnak a szervezet számára és az elmélet azon az előfeltevésen alapul, hogy nem létezik egyetlen, a többi érdekkel szemben uralkodó érdek sem (ellentétben a korábbi shareholder/részvényesi szemlélettel)
- az elmélet a vezetői döntéshozatal szempontjaira összpontosít,
- az érintetti elmélet keresi a választ arra, hogy miként képesek az egyes érintettek befolyásolni a vállalati döntéshozatalt, hogy annak kimenete összhangban legyen saját szükségleteikkel, prioritásaikkal,
- az stakeholder elmélet alapvetése, hogy a szervezetek legfőbb feladata megismerni, megérteni az egyes szereplők érdekeit és megteremteni az egyensúlyt azok között. (Mainardes et al., 2012)

Noha Freeman szerint a stakeholder megközelítés több elmélet és irányzat eredményeit integrálja magába, mégis a mainstream menedzsment irodalom perifériájára szorult az elmúlt évtizedekben, és elsősorban a társadalmi felelősségvállalás kutatási vonulatában, mintsem a stratégiai menedzsment területén kapott megfelelő figyelmet.

2.2 Vállalatok társadalmi felelősségvállalása

Kotler-Lee (2005) szerzőpáros szerint a „ vállalati társadalmi felelősségvállalás azt az elkötelezettséget jelenti, amely során a vállalat a közösség jóléténe érdekében folytat önkéntesen, szabadon választott üzleti gyakorlatot, amit erőforrásaival is támogat.”

Az Európai Unió Zöld könyve értelmében a társadalmi felelősségvállalás lényege az, hogy „a vállalatok önkéntesen szociális és környezeti szempontokat érvényesítenek üzleti tevékenységükben és a partnerekkel fenntartott kapcsolatokban.” idézi Lukács (2017)

A felelősségvállalás dimenzióit figyelembe véve azt mondhatjuk, hogy a CSR a gazdasági, társadalmi, környezeti tényezőket egyaránt figyelembe vevő önkéntes, etikus vállalati magatartás. (Málovics, 2009)

A CSR-nak nincs mindenki által egységesen elfogadott definíciója, eszközként, koncepcióként, sőt új üzleti modellként értelmezik az egyes teoretikusok, kiemelve, hogy megvalósítása gyökeres szemléletváltást igényel a vállalatoktól. (Lentner et al., 2015)

2.3 Politikai CSR

Scherer és Palazzo (2006) a vállalatok szándékolt társadalmi szerepvállalásának jelentőségét hangsúlyozzák. Post-pozitivista elméletekre alapozva, a szerzőpáros úgy gondolja, hogy nem definiálható az univerzális, mindenki által ismert/elismert üzleti morál normája, és mint ilyen nem egyértelműsíthető a vállalat társadalmi feladatköre sem. Felfogásuk szerint a vállalatok legitimációja csakis folyamatos, körültekintő a politikai szereplőkkel, civilekkel és egyéb stakeholderekkel folytatott diskurzus révén érhető el. (Ezen idea mentén bontakozott ki a politikai CSR kutatás vonulata. A politikai CSR (Seele-Lock, 2014) minden olyan vállalati aktivitást lefed, amelyeknek politikai vetülete lehet és hagyományosan állami, kormányzati feladatként értelmezünk (Petersen, 2013) (ilyenek nyilvánvalóan a biztonsággal kapcsolatos tradicionálisan államhoz rendelt feladatok is). Ez alapján a vállalati biztonságpolitika komplex értelmezése elkerülhetetlen.

2.4 Vállalatok biztonsági felelősségvállalása (CSecR)

Vitathatatlan, hogy a gazdasági szereplők esetenként fegyveres konfliktusokban is érintetté válnak. A konfliktushelyzetekben felmerülő morális felelősség fogalmának konceptualizációja céljából alkotta meg egy német kutatócsoport a vállalatok biztonsági felelősségvállalásának (Corprorate Security Responsability, CSecR) fogalmát. (Wenger-Möckli, 2003) A szerzők elismerik, hogy a tradicionális CSR-nak van implicit biztonsági vetülete konfliktushelyzetben is, hiszen egyebek mellett a gazdasági helyzet stabilizálása, a környezetbarát technológiák alkalmazása, a munkaerő piaci szerepvállalás egyaránt hozzájárulnak a béke megteremtéséhez, mindazonáltal fontosnak tartják, hogy a hagyományos gyűjtőfogalomtól elszakadva, a fenyegetettségtől terhes környezeti sajátosságokból adódó specifikus szerepvállalás új narratívaként, önálló kutatási irányzat formájában megjelenjen. (Wolf et al., 2007)

A szerzők tehát a vállalatok biztonsági felelősségvállalását elsősorban fenyegetettséghez kötik, ugyanakkor véleményem szerint, a vállalatok biztonsági felelősségének ilyetén megközelítése drasztikusan leszűkíti a fogalmat, hiszen egyrészt azt sugallja, hogy békés környezetben nincs ilyen jellegű szerepvállalása a szervezeteknek, továbbá mint a CSR részterületeként értelmezett felelősség (annak implicit következményeként való értelmezése), arra utalhat, hogy azon vállalatok esetében, amelyek nem működnek társadalmi felelősség irányelvei szerint, nem értelmezhető az biztonsággal kapcsolatos felelősségvállalás, ami nyilvánvalóan nem igaz.

3. A kutatás célja és az alkalmazott módszer bemutatása

Empirikus kutatásom megkezdése előtt az alábbi exploratív célokat határoztam meg.

A kutatások egyik premisszája a Michelberger-féle (2014) vállalati biztonság definíció , amely felveti a védelem külső aspektusát, amennyiben feladatként definiálja a külső környezet, valamint az vállalati érintettek védelmét, a belső jövedelemtermelő feladatok biztonságának megteremtése mellett. Ehhez kapcsolódik empirikus kutatásom első és második kutatási célja, azaz annak a vizsgálata, hogy a vállalati biztonságpolitika mennyire integrálódik a stratégiai tervezés rendszerében (C1), illetve annak feltárása, hogy hogyan jelenik meg a vállalati biztonság külső és belső aspektusa, az értintetti kapcsolatok viszonyrendszerében a vállalati gyakorlatban (C2).

A vállalatok biztonsági felelősségvállalásának (CSecR) fogalmát Wolf és szerzőtársai (2007) a hagyományos társadalmi felelősségvállalás alternatívájaként határozták meg. Szerintük a biztonsági felelősség kizárólag fegyveres konfliktusokkal terhelt környezetben értelmezhető, és ez az a jellemző, ami megkülönbözteti a fogalmat a tradicionális CSR-tól. Harmadik kutatási célként a vállalatok biztonsági felelősségvállalásának egy alternatív konceptualizációját határoztam meg.(C3)

Kvalitatív kutatásomban vállalati biztonságpolitikai vezetők véleményét vizsgáltam szakértői mélyinterjúk keretében. A mélyinterjúk alanyainak kiválasztása során igyekeztem több gazdasági szektor képviselőit megszólítani, figyelembe véve, hogy a vállalati biztonságpolitika erősen ágazat specifikus. A

mintát végül két távközlési szolgáltató, egy elektronikai termékek gyártásával foglalkozó multinacionális vállalat, egy energetikai szolgáltató valamint egy élelmiszer- és vegyipari termékek gyártásával foglalkozó cég illetékes szakértője alkotja.

A félig strukturált interjú főbb témakörei:

- a vállalati biztonságpolitika vállalaton belüli helyzetének feltárása
- a vállalatok biztonsági felelősségvállalásának értelmezése
- a vállalati biztonság külső és belső aspektusainak áttekintése stakeholder szempontok alapján

Az adatok, elhangzott információk feldolgozása során jellemzően egyszerű tartalomelemzést alkalmaztam, ugyanakkor a biztonsági felelősségvállalás konceptualizációja kapcsán úgy gondoltam, célszerű egy kifejezetten elméletalkotásra létrehozott módszertan használata. A grounded theory olyan megismerési, kutatási irányzat, amelyet jellemzően – de nem kizárólag kvalitatív vizsgáltatok során alkalmaznak. A módszertan legfontosabb jellemzője, hogy hidat képez az elmélet és az empirikus kutatás között, célja, hogy a kutató egyedi esetek vizsgálata és megértése révén, induktív megközelítéssel, szisztematikus módszertani lépésekkel eljusson az elméletalkotásig. (Bernschütz, 2009)

A grounded theory alkalmazása során a kutatás jól körülhatárolt probléma helyett általános felvetéssel indul, amely a kutatási eredmények függvényében fejlődik, alakul át, konkretizálódik. Flick meghatározása szerint a grounded theory az állandó összehasonlítás elvén alapul, ami az adatok, információk folyamatos vizsgálatát, fő és alkategóriák kialakítását, a kategóriák és tartalmaik integrálását, az elmélet körvonalainak kialakítását, majd azok konkretizálását jelenti mindaddig, amíg össze nem áll a „big picture”, az elméleti keret. (Mitev, 2012)

A kódolási mechanizmusok tekintetében a Strauss-Corbin féle irányzat nyitott, szelektív és axiális kódolást javasol. Míg a nyílt kódolás szakaszában az információegységeket fogalmakká és kategóriákká rendezzük, addig az axiális kódolásban kapcsolatokat keresünk a kategóriák között. (Bernschütz, 2009)Az axiális kódolás során tehát összehasonlító elemzéssel a korábban létrehozott kategóriák közötti kapcsolatokat, összefüggéseket feltárva kirajzolódnak a főbb csomópontok és alapkategóriák, így a szelektív kódolás előtt elkerülhető az információk túlburjánzása. (Mitev, 2012) (Kelemenné, 2014) A szelektív kódolás gyakorlatilag az alapkategóriák (core) kiemelését jelenti. (Bernschütz, 2009)

4. Eredmények

A kutatás eredményeinek bemutatását a szakirodalmi megalapozás során kirajzolódott prioritások áttekintésével kezdem, ezen belül a vállalati biztonságpolitika stratégiai beágyazódottsága tekintetében megfogalmazott szakértői véleményeket mutatom be. A vállalatok biztonsági felelősségvállalása kapcsán elhangzottakat grounded theory módszertanával elemzem, és tekintve, hogy az elméletalkotásom célja a vállalati biztonságot új megvilágításba helyezése, a kódolás során részben figyelemben veszem a témakör elméleti előzményeit. (Wolf et al., 2007) Végezetül a stakeholderek és a vállalati biztonságpolitika összefüggéseit tekintem át.

4.1 A vállalati biztonság helyzete a stratégiai tervezésben

A szakirodalmi előzmények alapján úgy gondolom, hogy noha a biztonság megítélése tekintetében elmozdulás tapasztalható, a biztonságszervezést a mai napig elsősorban operatív menedzsment feladatként tartják számon a vállalaton belül.

A vállalati biztonság szervezeten belüli megítélése kapcsán, egységes álláspont, csak annak több tényezőtől való függőségét illetően rajzolódott ki a mélyinterjúk tanúsága szerint. Az interjúalanyok kivétel nélkül úgy látják, hogy noha tapasztalható némi pozitív elmozdulás a terület presztízsét illetően, a biztonsági vezetőknek folyamatosan tennie kell a biztonsági szervezet, a biztonsági irányelvek elfogadottságáért. A kutatásban résztvevők mindannyian kiemelték a vállalatvezetés elköteleződésének jelentőségét (amit erősen személyiségfüggőnek gondolnak), illetve a biztonsági szakértő személyének, meggyőző erejének fontosságát.

A biztonság szervezeten belüli elismertsége egyértelműen visszatükröződik a vezető szervezeti hierarchiában elfoglalt pozíciójában. Ezt támasztja alá az, ami az egyik interjúalany (V3) megfogalmazásában így hangzott *„ahogy nő a legfelsőbb vezetés és a biztonsági vezető közötti szintek száma, úgy csökken a biztonságszervezés hatékonysága."* A kutatásban képviselt vállalatok közül négy esetben a biztonsági vezető a legfelsőbb vezetőnek közvetlen beosztottja, igaz volt olyan cég (V5), amelyben ez egy alig több, mint egy éves szervezeti struktúraváltás okán alakult így. Az átszervezés esetükben ugyanakkor nem pusztán ebből a szempontból volt fontos, hanem az egyes területek (létesítmény, információs biztonság, complience, hatósági adatszolgáltatás) integrációját is jelentette, ami egy rendkívül komplex kompetenciaközpont létrejöttét

eredményezte. A fennmaradó egy esetben, a biztonsági funkciók zöme, az ágazati sajátosságából fakadóan jelentős operatív területhez, az supply chain (ellátási lánc) szervezethez tartozik. Mindazonáltal, a szakértő véleménye alapján, ebben az esetben is elmondható, hogy a cég felismerte a biztonság fokozott jelentőségét, és egyre inkább kiemelten kezelik ezt a területet.

Annak megítélését illetően, hogy mennyire érvényesülnek a biztonsági szempontok a stratégiai tervezés folyamatában, heterogén véleményekkel szembesültem. A biztonság nehezem megfogható, leginkább a hiánya manifesztálódik a különböző incidensek során. Pontosan emiatt a biztonsági szervezetek, sok esetben reaktívan lépnek fel, a felkészülés, proaktivitás ugyanis jellemzően komoly költségekkel jár. Azt mondhatjuk, hogy a mai vállalatvezetők *számára „a biztonság fontos, de nem eléggé”* (V3) ahhoz, hogy ne utólagosan foglalkozzanak ezzel a területtel.

Az elhangzottak alapján, az inkább csak utópia, hogy a biztonság minden esetben, már a tervezési fázisokban, a folyamatokba integráltan jelen legyen („security as design”). A törekvések ugyanakkor ebbe az irányba mutatnak, hiszen számtalan esetben bebizonyosodott, hogy a prevenció kevesebbe kerül, mint az utólagos kármentesítés. (V5)

Noha volt olyan interjúalany (V1), aki úgy gondolja, hogy a vállalatvezetők megfelelő mértékben figyelembe veszik a biztonsági szempontokat a stratégiai tervezés során, ennek ellentmondani látszik az a közös nevező, amely a biztonságszervezési büdzsé meghatározását illetően alakult ki a kutatásban résztvevők között. Egyetértés volt tehát a tekintetben, hogy a biztonsági szervezet költségtervezése során egyértelműen operatív szempontok érvényesülnek a vállalatoknál. Ebből az aspektusból ismét kiemelten fontossá válik a biztonsági vezető személye, aki ráfordítás/megtakarítás – esetleg árbevétel - szemlélettel támaszthatja alá az egyes kiadások indokoltságát. *„…az üzlet szinte minden esetben elsőbbséget élvez”* (V1) A folyamatot ugyanakkor nyilvánvalóan megnehezíti számtalan tényező, amelyek nem csak a nem, vagy nehezen monetizálható tételek miatt adódnak, hanem a helyzetelemzés, kockázatelemzés kapcsán felmerülő információhiányból is.

Szintén egyetértettek a megkérdezettek abban a kérdésben, hogy a biztonság érték *„a biztonság és a minőség nem megkérdőjelezhető”* (V1), a biztonságszervezés tehát *„értékteremtő folyamat”* (V2), *„produktív terület”*(V3) *„mozgatóerő”* (V4), amely közelebb viszi a vállalatok az üzleti célok teljesítéséhez. Mi több, az egyik vállalatnál a biztonsági szervezeten belül működik *„profit center”* (V5), ahol a „security as a service” elv alapján értékesítik a biztonsági szolgáltatásokat.

4.2 A vállalatok biztonsági felelősségvállalása

Következő kutatási célom a vállalati biztonsági felelősségvállalás fogalmi keretének kibővítése volt. Úgy gondolom, hogy a vállalati biztonságnak értelmezhető egy, az általános társadalmi felelősségvállalástól függetlenül érvényes külső/belső aspektusa, amely az egyes stakeholder érdekek mentén pontosan megragadható, és mint ilyen a vállalati biztonságpolitika új dimenziójaként definiálható.

A vállalatok biztonsági felelősségvállalásának értelmezése során az interjúalanyok elsőként egyöntetűen az alkalmazottak irányában felmerülő kötelességekre, törődésre, szerepvállalásra, a biztonságos munkakörnyezet megteremtésére asszociáltak. A fogalom boncolgatását követően került elő, másodsorban a biztonságos termék, az adat és információbiztonság, a biztonságos létesítmények, a biztonságos ellátási lánc kérdésköre, továbbá a terrorellenes előírásoknak való megfelelés. A vezetők közül többen hangsúlyozták, hogy a vállalati biztonságpolitika minden esetben a jogi környezet, szabályozások, rendeletek, törvényi előírások keretei között valósul meg, így ebben a tekintetben is szolgálja az általános, komplex biztonságot, ugyanakkor ennek okán semmiképpen tekinthető önkéntes tevékenységnek.

Visszautalva a hagyományos társadalmi felelősségvállalás definíciókból kirajzolódó dimenziókra (Dahlsrud, 2008) – társadalmi-, gazdasági-, környezeti pillér, stakeholder fókusz, önkéntes tevékenység – úgy gondolom, hogy a társadalmi tényező beemelhető a biztonsági felelősségvállalás fogalmi körébe. A gazdasági és környezeti pillér említés szintjén ugyan megjelent a diskurzusban, de véleményem szerint ezen dimenziók bevonása csökkentené a fogalom konzisztenciáját.

Iniciális nyitott kód - Idézet (forrás)	Tematizált nyitott	Axiális kód	Szelektív kód
"...törődés az alkalmazottakkal, ami megváltoztatja a viselkedésüket" (V2)	Alkalmazotti attitűd alakítása	Biztonságtudatosság, alkalmazotti fókusz	Implicit társadalmi dimenzió
"A vállalat dolgozói folyamatosan kapnak oktatást, látják hogyan működnek a dolgok bent, ez mindenképpen hat a társadalomra is" (V3)	Biztonsági képzés, biztonságtudatosság	Biztonságtudatosság	
A felelősség leegyszerűsítve minden érdekelttel szemben (stakeholders), elsősorban a saját munkavállalók fontosak" (V1)	Alkalmazottak kiemelése	Alkalmazotti fókusz	
"Biztonsági értelemben a céges biztonságtudatossági kultúra kiterjesztése az otthoni környezetbe" (V4)	Biztonsági kultúra kiterjesztése	Biztonsági kultúra	
"Biztonságos termékek, szolgáltatások kialakítása révén…" (V1)	Term.- és szolg, biztonság	Biztonságos output	Implicit fizikai biztonság dimenzió
"Azáltal, hogy biztonságos létesítményeket hoz létre, azáltal hozzájárul a komplex biztonsághoz" (V3)	Infrastruktúra biztonsága	Infrastruktúra fizikai védelme	
biztonságos épületbe jönnek be, ahol biztonságban érezhetik maguk, nem csak munkavédelmi és egészségvédelmi szempontból. (V5)	Alkalmazotti fókusz Infrastruktúra védelem	Infrastruktúra fizikai és információs védelme	
"...céges infrastruktúra ne lehessen érintett illegális tevékenységben és az ezekkel szembeni ellenállóképességgel rendelkezzen" (V1)	Infrastruktúra védelme	Infrastruktúra fizikai védelme	
amelyeknél nem kell félni az információszivárgástól, adatokkal való visszaéléstől." (V5)	Adatvédelem	Információk védelme	Implicit információs biztonság dimenzió
"…adatokkal való visszaélések elleni küzdelem" (V4)	Adatvédelem	Információk védelme	

1. táblázat:Kódolás folyamata, részlet

Forrás: saját szerkesztés primer kutatás alapján

Noha az interjúk kis száma okán, a keletkezett szövegtörzs mérete nem indokolta volna, az elhangzott információkat többször átkódolva (1. táblázat), a vállalatok biztonsági felelősségvállalását illetően az alábbi dimenziók rajzolódtak ki:

Az interjúk során elhangzottak alapján, az alkalmazottak biztonsági képzése, a biztonsági kultúra fejlesztése és annak otthoni környezetre, illetve a mindennapi viselkedésre történő kiterjesztése egyben az általános társadalmi szintű biztonságtudatosság kialakulásának egy fontos építő eleme lehet.

- A biztonságos termékek és szolgáltatások előállítása és forgalmazása, a védett létesítmények létrehozása, az ellátási lánc biztonságának garantálása révén a vállalatok hozzájárulhatnak a komplexen értelmezett, általános biztonsághoz. Ezek az elsősorban, de nem kizárólagosan fizikai védelemhez köthető tényezők, a vállalatok alaptevékenységét támogató funkcióként értelmezett biztonságszervezés járulékos hozadékaiként értelmezhetők.
- A fentieken túl, noha jellemzően csak ágazat specifikusan, de kirajzolódott egy az adatok védelméhez köthető információs biztonsági pillér, ami azoknál a vezetőknél jelent meg, ahol integrált biztonságpolitika valósul meg a szervezet szintjén is.
- Fontos kiemelni a fent leírt dimenziók implicit jellegét. Míg a társadalmi felelősségvállalás vonatkozásában az önkéntesség körül zajlik a diskurzus, az interjúk alapján úgy tűnik, hogy ez a kérdés a biztonsági felelősségvállalást illetően fel sem merül, azaz, ha értelmezhető is a fogalom, semmiképpen nem írható le a profitcéloktól független, szándékolt, tervezett folyamatok összességeként, sokkal inkább jellemezhető úgy, mint az egyébként megvalósuló, a vállalat belső biztonságos működését szolgáló intézkedések jótékony vagy szükséges velejárója.

Van tehát biztonsági felelősségvállalása a vállalatoknak, de ahogyan egyik interjúalanyom megfogalmazta *„…igen, inkább kényszer hatására és gazdaságossági okokból, semmint saját elhatározásból.”* (V1)

4.3 A stakeholder szerepek a vállalati biztonság vonatkozásában

Az egyes stakeholderek vállalti biztonsághoz köthető hozzájárulásait illetve elvárásait illetően, elsősorban a belső érintettek kiemelt szerepe rajzolódott ki az interjúk során.

A tulajdonosok, befektetők, részvényesek szavazati jogukon keresztül, elsősorban a források allokációja tekintetében vállalnak szerepet, a vállalati biztonsági büdzsétervezés vonatkozásában, elvárásaik pedig pusztán a menedzsment beszámoltatása, motiválása formájában manifesztálódik.

A már korábban ismertetett eredmények tükrében is egyértelmű, hogy a munkatársaknak kiemelt szerepe van a vállalati biztonságpolitikai célok elérésében, mi több a vállalatok biztonsági felelősségvállalását illetően is, miközben nyilvánvaló elvárásuk a lét- és szociális biztonságot illetően, kiegészül a biztonságos munkakörnyezet az egészségvédelem iránti igényekkel. Fontos körülmény ugyanakkor, hogy a munkavállalók követeléseinek legitimációja a jogi környezet garanciáin nyugszik, elvárásaik érvényesítéséhez, hatékony eszközök csak korlátozottan állnak rendelkezésükre.

Biztonsági kérdésekben a külső stakeholderek szerepvállalása kevésbé tűnik esszenciálisnak a biztonság hatékonyságát, teljesítményét illetően.

A vevők, üzleti partnerek hozzájárulása nem értelmezhető az interjúalanyok véleménye alapján, elvárásaik pedig a szolgáltatás- illetve termékbiztonság vonatkozásában ragadhatók meg. A biztonság ezen dimenziója tekintetében fontossá válik a felelősségek megosztása, az átadás átvételi pontok pontos definiálása, ahol nem pusztán a termékek, de a biztonsághoz köthető felelősség is átterhelődhet a másik félre.

Utóbbi megállapodások jelentősége a beszállítókkal való együttműködés tekintetében is fokozottan igaz. Az ellátási lánc biztonsága közös felelősség, ahol a partnerségen túl, a folyamatos auditoknak való megfelelés, a vállalat biztonsági előírásainak figyelembe vétele, az ezekhez való igazodás alapvető elvárás, a biztonsági vezetők véleménye alapján. Az interjúalanyok mindegyike feladataként jelölte meg a beszállító partnerek ellenőrzését, auditálását, ami véleményük szerint szintén a vállalati biztonságpolitika implicit hatásaként a biztonsági kultúra kiterjesztését eredményezhető.

A közvetett érintetteket illetően a közgondolkodás, a biztonságtudatosság, a biztonsággal kapcsolatos attitűdök jelentőségét emelte ki az egyik interjúalanyom (V1). Amennyibe a szabályozó szervek támogató környezetet teremtenek, akkor a gazdasági szféra minden szereplőjétől elvárhatóvá válik a fokozott teljesítmény a vállalati biztonság területén, mindezt pedig növelheti a közösségek biztonsággal kapcsolatos ismereteit, elvárásait, ami a társadalom biztonsághoz való viszonyulása tekintetében is elmozdulást eredményezhet. (pl. minősített termékek vásárlása)

A biztonsággal kapcsolatos kommunikáció nyilvánvalóan fontos feladat egy biztonsági vezető számára, noha ennek mértékével (mennyiségével, minőségével) nem feltétlenül vannak megelégedve a kutatásban résztvevők. Az alkalmazott eszközök említése során, figyelemre méltó eredmény, hogy az interjúalanyok többsége (négyen) csak a belső információáramlás formáira, csatornáira,

felületeire koncentrált. Álljon itt az egyik vezető (V1) ebben a kérdésben megfogalmazott rendkívül hasznos és tanulságos megállapítását.

„Sajnos a biztonsági területen van egy krónikus félelem a nyilvánosságtól (security by obscurity). Igyekszünk ez ellen tenni, a terület láthatóságának javításával, biztonságtudatossági kampány, előadás, körüzenetek révén, de a visszamérések szerint még mindig vannak, akik szerint mi a kamerákkal foglalkozunk. Többet kell tehát tenni, ennek kulcsa szerintem a rendszeres kommunikáció…” (V1)

Van ugyanakkor figyelemre méltó, jó gyakorlat is a biztonsággal kapcsolatos információáramoltatás tekintetében. A kutatásban vizsgált egyik vállalat (V5) esetében a „látható biztonság” koncepció jegyében mind belső, mind külső kommunikációs csatornákon keresztül rendszeresen osztanak meg információkat, a biztonsági ügyek kapcsolatban, a biztonsági kultúrát pedig kreatív eszközökkel (pl. információbiztonsági ismeretekre építő szabadulószoba) építik a szervezeten kívül és belül egyaránt.

Összefoglalás

Az interjúk összegzéseként megállapítható, hogy a kutatásban résztvevő biztonsági vezetők véleménye alapján, a biztonság megítélését illetően jelentős változás nem feltétlenül érhető tetten az utóbbi években, noha több mint egy évtizede volt egy jelentősebb fordulat a digitalizáció és a globalizációs nyomás kapcsán.

Az is egyértelműnek tűnik, hogy a terület vállalaton belüli jelentőségét és megítélését kevésbé a külső trendek, mint inkább a biztonsági vezető személyisége, alku ereje, fellépése, szemléletmódja határozza meg. A biztonsági szempontok jellemzően nem a stratégiai tervezés során válnak megfontolás tárgyává. Az interjúalanyok egyöntetű tapasztalata, hogy vállalati biztonsági szervezetet továbbra is elsősorban költséghelyként kezelik a vállalatvezetők, annak ellenére, hogy a szakemberek egyöntetűen hangsúlyozzák a terület értékteremtő képességét.

Az interjúkban elhangzottak alapján meghatározható a vállalatok biztonsági felelősségvállalásának egy lehetséges, kiterjesztő koncepciója, amelynek egyik fontos jellemzője – a szakértői vélemények alapján -, hogy a felelősségvállalás a vállalati biztonsági intézkedések implicit hatásaként manifesztálódik, tehát kijelenthető, hogy szándékos, tudatos, egyéb vállalati céloktól független felelősségvállalás a biztonság területén nem értelmezhető a mai vállalati gyakorlatban.

A kutatás során sikerült a vállalati biztonságpolitika dimenzióit az egyes stakeholderek érdekekhez, hozzájárulásokhoz kötni, ezen belül is elsősorban a belső érintettek meghatározó szerepvállalását feltárni, ugyanakkor úgy tűnik, ez nem jelent alapjaiban új megközelítést a szakemberek számára. A szakértők nem feltétlenül látják az új aspektusban rejlő lehetőségeket, nem érzékelik jelentőségét az integrált kockázatok feltárását, a biztonságszervezés folyamatának esetleges átalakítását illetően.

Az eredmények értelmezése során mindazonáltal, figyelembe kell vennünk azt a tényt, hogy az ezen a területen tevékenykedő szakemberek számára, a területen való jártasság, a mindennapos problémamegoldás, a tevőleges részvétel a folyamatokban megnehezíti az elvonatkoztatást, illetve azt, hogy az éppen zajló trendeket külső szemlélőként értékeljék.

Fontosnak tartom kiemelni, hogy sajnálatos az interjúk során tetten érhető, a biztonsági vezetőkre jellemző, belső fókuszú, tradicionális gondolkodásmód (igaz ezt a vállalati biztonságpolitika ma uralkodó értelmezése előre is vetíti). Azt gondolom, hogy a stakeholder szemlélet integrálása, és annak hozadékaként a külső érintettek igényeinek fokozottabb megjelenése, érvényesítése a vállalati biztonságpolitika területén, nem csak abban segítene, hogy könnyebben átlátható, elemezhető legyen ez az egyre komplexebbé váló terület, hanem egyben katalizátora lehetne (ágazattól és egyéb belső tényezőktől, alkupozíciótól függetlenül) a biztonság stratégiai szintre emelésének is.

Hivatkozások

[1.] Bernschütz M. (2009): Kvalitatív kutatás a magyarországi integrált marketingkommunikáció-alkalmazás feltételeiről Vezetéstudomány, 40. évf., 9. sz., 29–40. o.
[2.] Borzán, A. – Lentner, Cs. – Szigeti, C. (2011): A pénzügyi vállalkozások felelősségvállalásának új dimenziói, ECONOMICA (SZOLNOK) 4, 22-30.p.
[3.] Briggs, R., Edwards, C. (2006): The business of resilience : Corporate security for the 21st century, Demos: Londres DOI: 10.3917/sestr.006.0076
[4.] de Cora, R. R. (dn): Systemic Approach Safety-Security: The Future Safety and Security Research in Europe, European Forum http://www.s2rforum.es/wp-content/uploads/2017/01/5.BTextoCompleto_CalsSystemic-Approach-for-Safety-SecurityV2.pdf
[5.] Freeman, R. E. (1984): Strategic management: A stakeholder approach. Boston, Massachusetts: Pitman Publishing.

[6.] Gelencsér, K. (2003): Grounded theory, Szociológiai Szemle, 2003/1
[7.] Jones, T., Wicks, A. (1999): Convergent Stakeholder Theory. The Academy of Management Review, 24(2), 206-221. from www.jstor.org/stable/259075
[8.] Lentner, Cs. – Szigeti, C. – Borzán, A. (2011): New Dimensions of Banks Social Responsibility, In: Szente, Viktória; Szendrő, Katalin; Varga, Ákos; Barna, Róbert (szerk.) Sustainable economics, community strategies : abstracts of the 3rd International Conference of Economic Sciences, Kaposvár, Magyarország : Kaposvár University, Faculty of Economic Science, 29-48. p.
[9.] Kelemenné Erdős A, (2014) A közforgalmú közlekedési szolgáltatás és piac vizsgálata marketing és fenntarthatósági nézőpontból, Doktori (PhD) értekezés, Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és Társadalomtudományi Kar Gazdálkodás- és Szervezéstudományi Doktori Iskola
[10.] Király, L., Pataki, J. (2013): Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz, Hadtudomány: A Magyar Hadtudományi Társaság Folyóírata 23: (E 1) pp. 173-187. http://mhtt.eu/hadtudomany/2013_e_Kiraly_Laszlo_ Pataki_Janos.pdf
[11.] Kotler, P., Lee, N. (2005). Corporate Social Responsibility: Doing the Most Good for Your Company and Your Cause. Hoboken, New Jersey: John Wiley &Sons, Inc.
[12.] Lentner, Cs., Szegedi, K., Tatay, T. (2015). Társadalmi felelősségvállalás a bankszektorban. Public finance quarterly. 60. 96-104. https://www.researchgate.net/publication/312057054_Tarsadalmi_felelossegvallalas_a_bankszektorban
[13.] Lock, I, Seele, P. (2018): Politicized CSR : How corporate political activity (mis-)uses political CSR. J Public Affairs.; 18:e1667. https://doi.org/10.1002/pa.1667
[14.] Ludbey, C., Brooks, D., Coole, M. (2017): Corporate Security: Identifying and Understanding the Levels of Security Work in an Organisation. Asian Journal of Criminology. DOI: 10.1007/s11417-017-9261-x. https://www.researchgate.net/publication/320676038_Corporate_Security_Identifying_and_Understanding_the_Levels_of_Security_Work_in_an_Organisation/citations
[15.] Lukács, R. (2017): A társadalmi felelősségvállalás és a vállalati reputáció érintetti szempontú vizsgálata Doktori (PhD) értekezés, Budapesti Corvinus Egyetem, Gazdálkodástani Doktori Iskola. DOI 10.14267/phd.2017031L

[16.] Mainardes, E., Alves, H., Raposo, M. (2012): A model for stakeholder classification and stakeholder relationships. Management Decision. 50. 10.1108/00251741211279648.
[17.] Málovics, Gy. (2009): A vállalati fenntarthatóság érintettközpontú vizsgálata Doktori (PhD) értekezés, Pécsi Tudományegyetem Közgazdaságtudományi Kar Regionális Politika és Gazdaságtan Doktori Iskola https://www.yumpu.com/hu/document/view/34521631/doktori-disszertacio-pecsi-tudomanyegyetem-
[18.] Michelberger, P. (2014). Információbiztonság és üzleti bizalom, Habilitációs tézisfüzet, Óbudai Egyetem Biztonságtudományi Doktori Iskola https://bdi.uni-obuda.hu/sites/default/files/tezisfuzet-MP.pdf
[19.] Mitev A. Z. (2012): Grounded theory, a kvalitatív kutatás klasszikus mérföldköve. Vezetéstudomány,43/1, pp. 17–30.
[20.] Muha, L. (2007): A magyar köztársaság kritikus információs infrastruktúráinak védelme, Doktori disszertáció, Zrínyi Miklós Nemzetvédelmi Egyetem http://real-phd.mtak.hu/74/1/1228916.pdf
[21.] Munk, S. (2007): Információbiztonság vs. informatikai biztonság, Hadmérnök, különszám, http://www.hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf
[22.] Papp, A. (2006): Biztonsági megoldások integrációja Robothadviselés 6. Tudományos Szakmai Konferencia http://hadmernok.hu/kulonszamok/robothadviseles6/papp_rw6.html
[23.] Petersen, K.L. (2013) 'The Corporate Security Professional: A Hybrid Agent Between Corporate and National Security.' Security Journal 26/3: 222–235.
[24.] Petersen, K. (2014): The Politics of Corporate Security and the Translation of National Security. 10.1057/9781137346070_5.
[25.] Sántha, K (2011): Abdukció a kvalitatív kutatásban, Eötvös József kiadó, Budapest
[26.] Savage, G. T., Nix, T. W., Whitehead, C. J., Blair, J. D. (1991): Strategies for assessing and managing organizational stakeholders. Academy of Management Executive, 5. pp. 61-75.
[27.] Scherer, A., Palazzo, G. (2006): Toward a Political Conception of Corporate Responsibility: Business and Society Seen From a Habermasian Perspective. Academy of Management Review. 32. 10.5465/AMR.2007.26585837.
[28.] Seele, P., Lock, I. (2014): Instrumental and/or Deliberative? A Typology of CSR Communication Tools. Journal of Business Ethics. 131. 401-414. 10.1007/s10551-014-2282-9.
[29.] Vasvári, Gy., Lengyel, Cs., Valádi, Z. (2006): Vállalati biztonság keretrendszere, Vagyonbiztonság, Üzembiztonság, Informatikai Biztonság

Ajánlás 6.0 változat–Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, ISBN nélkül

[30.] Vasvári, Gy (2009): A társadalmi és szervezeti (vállalati) biztonsági kultúra Ad Librum Kiadó, Budapest

[31.] Wenger, .A., Möckli, D. (2003): Conflict Prevention: The Untapped Potential of the Business Sector. Boulder, CO: Lynne Rienner.

[32.] Wolf, K. D., Deitelhoff, N., Engert, S. (2007): Corporate Security Responsibility: Towards a Conceptual Framework for a Comparative Research Agenda. Cooperation and Conflict, 42(3), 294–320. https://doi.org/10.1177/0010836707079934