DOKTORI (PhD) ÉRTEKEZÉS

BALOGH PÉTER

2026

NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Balogh Péter

TECHNOLÓGIAI REZILIENCIA A DIGITÁLIS ÉS KRITIKUS INFRASTRUKTÚRÁK VÉDELMÉBEN

Elméleti modell, mérési keretrendszer és stratégiai alkalmazás

Doktori (PhD) értekezés tervezet

Témavezető

Dr. Kovács László vezérőrnagy, DSc.

Budapest, 2026

TARTALOMJEGYZÉK

BEVEZETÉS

A kutatás bemutatása

A téma fontossága és időszerűsége

A 21. század biztonsági, gazdasági és technológiai környezetének egyik meghatározó sajátossága, hogy az államok, a társadalmak és a fegyveres erők működése egyre nagyobb mértékben egymással összekapcsolt, digitalizált és részben globális technológiai rendszerektől függ. Az energiaellátás, a közlekedés és logisztika, az elektronikus hírközlés, a felhő- és adatközponti szolgáltatások, a műholdas kommunikáció és helymeghatározás, valamint a katonai vezetési és irányítási rendszerek ma már nem önálló infrastruktúrákként működnek. Kölcsönös függőségeik olyan szocio-technikai rendszert alkotnak, amelyben egy lokális technikai, szervezeti vagy szabályozási zavar más ágazatokban is működési következményeket válthat ki.

A digitalizáció biztonsági és hadtudományi szempontból kettős hatást gyakorol a társadalmi, gazdasági és katonai működőképességre. Egyfelől növeli a rendszerek hatékonyságát, gyorsítja az információáramlást és a döntéshozatalt, támogatja az automatizálást, valamint olyan új képességeket hoz létre, amelyek a fegyveres erők esetében közvetlenül befolyásolják a vezetés és irányítás, a felderítés, a logisztika, a precíziós képességek és a többdoménes műveletek eredményességét. Másfelől ugyanez a digitalizáció növeli a technológiai rendszerek komplexitását, támadási felületét és kölcsönös függőségét, valamint fokozza a civil infrastruktúráktól, kereskedelmi szolgáltatóktól és globális technológiai ellátási láncoktól való függést. Biztonsági szempontból ez azt jelenti, hogy egy technológiai zavar, kibertámadás, elektronikai hadviselési tevékenység, fizikai károkozás vagy kritikus szolgáltatás kiesése a közvetlenül érintett rendszeren túlmutató, kaszkádszerű következményeket idézhet elő.

Hadtudományi szempontból ennek jelentősége abban áll, hogy a technológiai sérülékenység közvetlenül befolyásolhatja a katonai vezetés folytonosságát, a döntéshozatal sebességét, a műveleti tempó fenntartását, az erők alkalmazhatóságát és végső soron a katonai művelet eredményességét. A technológiai fejlődés ezért önmagában nem azonos a nagyobb biztonsággal vagy katonai képességgel: a technológia csak akkor jelent tartós képességnövekedést, ha annak működőképessége békében, válságban és fegyveres konfliktusban, illetve szándékos ellenséges behatás és nem szándékos zavar esetén egyaránt fenntartható. A technológiai reziliencia ebből a megközelítésből nem pusztán

műszaki vagy kiberbiztonsági kérdés, hanem a nemzeti ellenálló képesség, a katonai műveleti képesség és a hiteles elrettentés egyik technológiai előfeltétele.

Hadtudományi megközelítésben a kutatás központi problémája ezért annak vizsgálata, hogy a technológiai rendszerek növekvő összekapcsoltsága és függősége miként befolyásolja a katonai képességek rendelkezésre állását, a műveleti folytonosságot és a döntési szabadság fenntarthatóságát. A technológiai reziliencia ebben az értelemben összekapcsolja a kritikus infrastruktúrák védelmét a katonai műveletek technológiai feltételrendszerével: azt vizsgálja, hogy a fegyveres erők és az azokat támogató civil rendszerek milyen mértékben képesek ellenséges, műszaki vagy környezeti zavarok mellett is biztosítani a katonai feladat végrehajtásához nélkülözhetetlen funkciókat.

A disszertáció 1. fejezete ennek elméleti alapjait és fogalmi evolúcióját tárja fel, a 2. fejezet a rezilienciát alakító technológiai, szervezeti, szabályozási és stratégiai kihívásokat elemzi, a 3. fejezet a saját háromdimenziós modell és annak mérési logikája felé lép tovább, míg a 4. fejezet a modell ágazati validációját, gyakorlati alkalmazhatóságát és stratégiai kiterjesztését vizsgálja.

A kutatás aktualitását tovább növeli, hogy a kritikus infrastruktúrák működése és a katonai műveleti képesség között egyre közvetlenebb kapcsolat áll fenn. A vezetés és irányítás, a logisztika, a kommunikáció, a helymeghatározás, az energiaellátás és az adatfeldolgozás jelentős része olyan civil vagy kettős felhasználású infrastruktúrákra támaszkodik, amelyek békeidőben gazdasági szolgáltatásokat biztosítanak, válság vagy fegyveres konfliktus esetén azonban a nemzeti ellenálló képesség és a katonai műveletek előfeltételeivé válnak. A civil és katonai technológiai reziliencia ezért nem kezelhető két elkülönült rendszerként.

A technológiai reziliencia mint szocio-technikai és stratégiai probléma

Az 1. fejezetben bemutatott elméleti fejlődési ív alapján a reziliencia fogalma az ökológiai rendszerek stabilitásának és alkalmazkodásának vizsgálatától a mérnöki, szervezeti, kiberbiztonsági és kritikusinfrastruktúra-megközelítésekig jutott el. E fejlődés közös tanulsága, hogy a reziliencia nem azonos a robusztussággal. A robusztusság elsősorban az ellenállás képességét fejezi ki, míg a reziliencia időbeli és adaptív dimenziót is tartalmaz: azt vizsgálja, hogy a rendszer a zavar bekövetkezése előtt, alatt és után miként képes alapvető funkcióit megőrizni, helyreállítani, illetve szükség esetén működését átalakítani.

A technológiai reziliencia ebből következően szocio-technikai tulajdonság. Egy rendszer akkor sem tekinthető reziliensnek, ha műszaki komponensei magas rendelkezésre állásúak, de a szervezet nem képes gyors döntést hozni, nincs megfelelő információáramlás, a személyi állomány nem felkészült, vagy a szabályozási környezet merev és kizárólag statikus megfelelőségi követelmények teljesítésére épül. Ugyanígy a jó szervezeti kultúra sem képes kompenzálni a kritikus technológiai egyedi hibapontokat, az elégtelen redundanciát vagy az átláthatatlan beszállítói függőségeket.

E felismerés vezeti el a kutatást a háromdimenziós értelmezéshez. A technológiai dimenzió a rendszer architektúráját, modularitását, redundanciáját, monitorozását, kiberbiztonsági kontrolljait és adaptív technológiai képességeit foglalja magában. A szervezeti dimenzió a vezetést, a döntéshozatalt, a tanulást, a képzést, a gyakorlatokat, a kultúrát és az alkalmazkodóképességet vizsgálja. A szabályozási–irányítási dimenzió a governance, a felelősségi rendszer, a stratégiai tervezés, a szabályozás, a standardizáció és a köz- és magánszféra közötti koordináció szerepét értékeli. A disszertáció alapállítása szerint a technológiai reziliencia e három dimenzió kölcsönhatásából jön létre, ezért egyik dimenzió sem vizsgálható önmagában.

A 2. fejezetben vizsgált környezeti kihívások ezt a szocio-technikai értelmezést tovább erősítik. A technológiai függőségek rétegei az alkalmazásoktól és kritikus funkcióktól a felhő-, kommunikációs és PNT[1]-szolgáltatásokon, a számítási kapacitáson és energiaellátáson keresztül a félvezetőkig, nyersanyagokig, beszállítói hálózatokig és geopolitikai környezetig terjednek. A függőség önmagában nem feltétlenül jelent sérülékenységet; stratégiai kockázattá akkor válik, ha koncentrált, nem átlátható, nem helyettesíthető vagy válsághelyzetben nem kezelhető.

Technológiai szuverenitás, függőségek és civil–katonai összekapcsoltság

A technológiai szuverenitás a disszertációban nem azt jelenti, hogy egy államnak minden technológiát és technológiai komponenst saját maga kell előállítania, vagy teljesen függetlenné kell válnia a külső beszállítóktól és partnerektől. A reziliencia szempontjából ezért a függőségek ismerete, diverzifikálása, helyettesíthetősége, a kritikus készletek és kompetenciák fenntartása, valamint a partneri kapcsolatok megbízhatósága egyaránt jelentős.

[1] PNT: Positioning Navigation and Timing, helymeghatározás, navigáció és pontos időszolgáltatás

A civil–katonai összekapcsoltság különös jelentőséggel bír. A katonai műveleti képesség és a C2[2]-rendszerek működése energia-, közlekedési, digitális, felhő-, űr/PNT- és ellátásilánc-szolgáltatásokra támaszkodik, amelyek jelentős része civil tulajdonban vagy civil üzemeltetésben van. A technológiai reziliencia ezért nem kizárólag védelmi ágazati feladat, hanem összkormányzati, gazdasági és társadalmi koordinációt igénylő kérdés. A szabályozás, az ipar, a kutatás-fejlesztés, a nemzetközi partnerek és a kritikus szolgáltatók együtt alkotják azt a külső környezetet, amelyben a katonai és civil rendszerek rezilienciája kialakul.

Ebből következik a kutatás governance-szemlélete is. A megfelelőség szükséges, de önmagában nem elégséges. A statikus követelmény–audit–megfelelés ciklust adaptív reziliencia-governance-nak kell kiegészítenie, amelyben a folyamatos monitorozás, a gyakorlatok és valós incidensek tapasztalatai, az értékelés, a szabályok és eljárások módosítása, majd az újratesztelés egymást követő és ismétlődő lépések. Ez a logika a 3. és 4. fejezet mérési, validációs és stratégiai kiterjesztési megközelítésében is megjelenik.

A kutatás alapproblémája

A disszertáció alapproblémája annak vizsgálata, hogy **miként tehetők a** magas fokú digitalizáltsággal, összekapcsoltsággal és külső függőségekkel jellemezhető **technológiai rendszerek úgy reziliensebbé**, hogy **közben megőrizzék működési hatékonyságukat, innovációs képességüket és interoperabilitásukat**. A probléma nem oldható meg kizárólag technológiai eszközökkel, mert a sérülékenység és az alkalmazkodóképesség egyaránt a technológiai architektúra, a szervezeti működés és a szabályozási–irányítási környezet kölcsönhatásából ered.

A hagyományos kockázatkezelési és szabályozási megfelelőség (compliance)-megközelítések jellemzően az ismert veszélyek azonosítására, valószínűségük és következményeik értékelésére, majd kontrollok kialakítására épülnek. Ez szükséges, de a komplex adaptív rendszerekben nem minden zavar jelezhető előre. **A reziliencia ezért kiegészíti a kockázatkezelést**: nemcsak azt kérdezi, hogyan előzhető meg egy meghibásodás vagy támadás, hanem azt is, hogyan marad működőképes a rendszer akkor, amikor a megelőzés nem volt teljesen sikeres.

A kutatási probléma további eleme a technológiai reziliencia mérhetősége és összehasonlítható értékelhetősége. Ennek lényege annak meghatározása, hogy egy vizsgált

[2] C2: Command and Control: vezetés és irányítás

technológiai rendszer milyen mértékben képes kritikus funkcióinak fenntartására, a zavarok elnyelésére, a működés stabilizálására és helyreállítására, valamint a tapasztalatok alapján történő alkalmazkodásra. **A mérhetőség problémája ezért nem egyetlen technikai teljesítménymutató meghatározását jelenti, hanem annak vizsgálatát, hogy a technológiai, szervezeti és szabályozási–irányítási tényezők állapota és kölcsönhatása miként tehető strukturáltan értékelhetővé.** A reziliencia absztrakt stratégiai fogalom marad, ha nem kapcsolható olyan értékelhető dimenziókhoz, indikátorokhoz és érettségi szintekhez, amelyek segítségével azonosíthatók a kritikus hiányosságok, a kapcsolati szűk keresztmetszetek és a fejlesztési prioritások.

A **mérhetőség hadtudományi jelentősége abban áll, hogy lehetővé teszi annak értékelését, milyen mértékben képes egy katonai vagy a katonai működést támogató technológiai rendszer a műveleti szempontból kritikus funkciókat zavarás, támadás vagy részleges kiesés mellett fenntartani**. Így a technológiai reziliencia értékelése közvetlenül összekapcsolható a hadrafoghatóság, a műveleti folytonosság és a döntési képesség fenntarthatóságának vizsgálatával.

A probléma stratégiai szinten abban foglalható össze, hogy **az ágazati reziliencia önmagában nem biztosít nemzeti technológiai rezilienciát.** A kritikus infrastruktúrák közötti függőségek, a civil és katonai rendszerek kapcsolatai, a technológiai beszállítói láncok és a szabályozási kompetenciák széttagoltsága olyan koordinációs igényt teremt, amely túlmutat az egyes szervezetek vagy ágazatok felelősségi körén.

Kutatási kérdések

K1: Hogyan értelmezhető a technológiai reziliencia olyan integrált szocio-technikai rendszertulajdonságként, amely egyidejűleg képes megragadni a technológiai, szervezeti és szabályozási–irányítási tényezők hatását?

K2: Milyen környezeti, technológiai, szervezeti, kiberbiztonsági, ellátásilánc- és governance-tényezők alakítják a digitális és kritikus infrastruktúrák rezilienciáját, és ezek között milyen kölcsönös függőségek azonosíthatók?

K3: Milyen dimenziók, indikátorok és érettségi szintek segítségével tehető a technológiai reziliencia összehasonlíthatóan értékelhetővé anélkül, hogy a fogalom komplexitása egyetlen technikai mutatóra redukálódna?

K4: A kidolgozott háromdimenziós modell és érettségi megközelítés mennyiben alkalmazható eltérő kritikus infrastruktúra-ágazatok vizsgálatára, és milyen közös, illetve ágazatspecifikus reziliencia-követelmények tárhatók fel?

K5: Milyen stratégiai és intézményi irányítási keret szükséges ahhoz, hogy az ágazati, civil–katonai és technológiai függőségek nemzeti szinten összehangolt rezilienciafejlesztéssé alakíthatók legyenek?

Kutatási célok

A kutatás átfogó célja egy olyan tudományosan megalapozott, ugyanakkor gyakorlati felhasználásra alkalmas technológiai reziliencia-értelmezési és értékelési rendszer kialakítása, amely összekapcsolja az elméleti fogalomalkotást, a környezeti kihívások elemzését, a mérhetőséget, az ágazati validációt és a stratégiai irányítást.

C1: A technológiai reziliencia fogalmának elméleti tisztázása és elhatárolása a robusztusság, redundancia, helyreállítás, üzletmenet-folytonosság, kiberreziliencia és antifragilitás kapcsolódó fogalmaitól.

C2: A technológiai rezilienciát alakító 21. századi kihívások és függőségek rendszerezése, különös tekintettel a digitalizációra, kiber- és hibrid fenyegetésekre, IT/OT[3]-konvergenciára, felhő- és PNT-függőségre, ellátási láncokra, humán tényezőkre és szabályozási környezetre.

C3: Egy integrált, háromdimenziós technológiai reziliencia modell kialakítása, amely a technológiai, szervezeti és szabályozási–irányítási dimenziókat egységes szocio-technikai rendszerként kezeli.

C4: A modell mérhetővé és értékelhetővé tétele érettségi szintek és indikátorok segítségével annak érdekében, hogy a technológiai reziliencia ne csak leíró fogalom, hanem értékelhető és fejleszthető képesség legyen.

C5: A modell ágazati alkalmazhatóságának összehasonlító szakági validációja kiválasztott kritikus infrastruktúra-rendszerek és releváns szakági követelmények alapján.

C6: A validáció eredményeire építve egy nemzeti szintű technológiai reziliencia-irányítási logika megfogalmazása, amely támogatja az ágazatközi, civil–katonai, szabályozási, ipari és innovációs koordinációt.

Hipotézisek

A kutatási kérdések és célok alapján a következő hipotéziseket fogalmaztam meg[4]**:**

[3] IT/OT- Information Technology/Operational Technology: információtechnológiai és műveleti/üzemirányítási technológiai rendszerek

[4] Így a hipotézisek közvetlenül kapcsolhatók a disszertáció saját modelljéhez, mérési rendszeréhez és validációjához.

H1: A technológiai rendszerek rezilienciája nem írható le kielégítően kizárólag technikai vagy kiberbiztonsági mutatókkal; a reziliencia szintjét a technológiai, szervezeti és szabályozási–irányítási dimenziók együttes állapota és kölcsönhatása határozza meg.

H2: A technológiai reziliencia összehasonlíthatóan értékelhető, ha a három dimenzióhoz egységes értelmezési logika szerint kialakított indikátorok és egymásra épülő érettségi szintek kapcsolódnak.

H3: Az eltérő kritikus infrastruktúra-ágazatokban a konkrét technológiai kitettségek különböznek, ugyanakkor a reziliencia alapvető szerkezete – technológiai ellenálló és helyreállítási képesség, szervezeti adaptáció, valamint szabályozási–irányítási koordináció – közös mintázatot mutat.

H4: A magas fokú technológiai interdependencia miatt egy ágazat rezilienciája nem értékelhető kizárólag saját belső képességei alapján; a kapcsolódó energia-, kommunikációs, digitális, közlekedési, PNT-, felhő- és ellátásilánc-függőségek érdemben befolyásolják a működőképességet és a kaszkádhatások kockázatát.

H5: A statikus megfelelőségorientált irányítás önmagában nem biztosít megfelelő technológiai rezilienciát; magasabb rezilienciaszint ott érhető el, ahol a governance folyamatos monitorozásra, gyakorlatokra és incidensekre, értékelésre, szervezeti tanulásra, módosításra és újratesztelésre épül.

H6: Az ágazati reziliencia fejlesztések nemzeti szintű hatékonysága növelhető olyan integrált technológiai reziliencia-irányítási kerettel, amely összekapcsolja a kritikus infrastruktúrák, a védelmi szféra, a szabályozás, az ipar, a kutatás-fejlesztés és a nemzetközi együttműködés szereplőit.

A kutatás módszertani megközelítése

A disszertáció módszertana egymásra épülő kutatási lépésekből áll. A módszertani logika nem egyetlen kvantitatív vagy kvalitatív eljárás alkalmazására épül, hanem az elméleti szintézis, a modellalkotás, az indikátoralapú mérhetővé és értékelhetővé tétel és az összehasonlító szakági validáció összekapcsolására.

1. Elméleti és fogalmi elemzés. Az 1. fejezet interdiszciplináris szakirodalmi szintézisben vizsgálja a reziliencia ökológiai, mérnöki, szervezeti, kiberbiztonsági és kritikusinfrastruktúra-előzményeit. A cél azoknak a fogalmi elemeknek az azonosítása, amelyek a technológiai rendszerekre átvihetők.

2. Környezeti és stratégiai elemzés. A 2. fejezet a technológiai rezilienciát alakító fenyegetéseket, függőségeket és intézményi kihívásokat rendszerezi. A vizsgálat külön

kezeli a technológiai architektúrák, a kiberbiztonság, az ellátási láncok, az emberi és szervezeti tényezők, valamint a szabályozás és governance hatását, majd ezek kölcsönhatását elemzi.

3. Koncepcionális modellalkotás és mérhetővé és értékelhetővé tétel. A 3. fejezetben az elméleti és környezeti eredmények szintéziséből létrejön a háromdimenziós technológiai rezilienciamodell. A modellhez kapcsolódó érettségi megközelítés a technológiai, szervezeti és szabályozási–irányítási dimenziók értékelését indikátorokhoz és fejlettségi szintekhez kapcsolja.

4. Összehasonlító ágazati validáció. A 4. fejezet a modell alkalmazhatóságát kiválasztott kritikus infrastruktúra-területek szakági dokumentumai, követelményei és működési sajátosságai alapján vizsgálja. A validáció célja nem pusztán a modell megerősítése, hanem annak feltárása is, hogy mely elemek tekinthetők általánosnak és melyek igényelnek ágazati adaptációt.

5. Stratégiai szintézis. A validáció eredményei alapján a kutatás a szervezeti és ágazati szint fölé emeli a technológiai reziliencia kérdését, és nemzeti irányítási keretben kapcsolja össze a kritikus infrastruktúrák, a digitális transzformáció, a kiberbiztonság, az innováció és a nemzeti ellenálló képesség szempontjait.

A kutatás tehát elsősorban kvalitatív, konceptuális és összehasonlító módszertanra épül, amelyet strukturált indikátoralapú értékelési logika egészít ki. Nem cél nagymintás statisztikai általánosítás vagy valamennyi kritikus infrastruktúra teljes körű kvantitatív modellezése. A módszertani cél olyan egységes, reprodukálhatóságra törekvő értékelési keret létrehozása, amely különböző ágazatokban azonos logika szerint alkalmazható, miközben lehetőséget biztosít az ágazatspecifikus sajátosságok figyelembevételére.

Szakirodalom-kiválasztási protokoll

A kutatás szakirodalmi megalapozása narratív, kritikai szakirodalmi áttekintésre épült, amelynek célja nem teljes körű szisztematikus review készítése, hanem a technológiai reziliencia eltérő tudományterületi megközelítéseinek azonosítása, összevetése és integrált értelmezése volt. A források feltárása elsősorban a **Scopus, Web of Science és Google Scholar** adatbázisokban történt, kiegészítve a NATO, az Európai Unió, az ENISA[5], a NIST[6],

[5] ENISA-European Union Agency for Cyber Security: Az Európai Unió Kiberbiztonsági Ügynöksége

[6] NIST- National Institute of Standards and Technology: az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete

az OECD[7], valamint releváns szabványügyi szervezetek hivatalos dokumentumaival. A keresés során többek között a *technological resilience*, *resilience engineering*, *organizational resilience*, *cyber resilience*, *critical infrastructure resilience*, *critical infrastructure interdependencies*, *socio-technical systems*, *resilience measurement*, *maturity model*, *supply chain resilience*, *technological sovereignty* és *resilience governance* keresőkifejezések, illetve ezek logikai kombinációi kerültek alkalmazásra[8].

A szakirodalmi feltárás időbeli kerete alapvetően a **rezilienciaelmélet klasszikus alapműveitől – elsősorban az 1970-es évektől – 2026-ig** terjedt. A klasszikus szerzők és modellek bevonása azért volt szükséges, mert ezek képezik a reziliencia fogalmi fejlődésének elméleti alapját, míg a 2015–2026 közötti publikációk kiemelt súlyt kaptak a digitális infrastruktúrák, kiberreziliencia, IT/OT-konvergencia, technológiai függőségek és rezilienciamérés aktuális megközelítéseinek feltárásában[9].

A **beválasztási kritériumok** közé tartoztak azok a lektorált tudományos közlemények, monográfiák, szabványok, valamint NATO-, EU-, ENISA- és NIST-dokumentumok, amelyek közvetlenül hozzájárultak a reziliencia fogalmi meghatározásához, mérhetőségéhez, szocio-technikai értelmezéséhez, kritikusinfrastruktúra-alkalmazásához vagy szabályozási–irányítási dimenziójához. Előnyt élveztek azok a források, amelyek többdimenziós, rendszerszintű vagy adaptív megközelítést alkalmaztak. A **kizárási kritériumok** közé kerültek a kizárólag egyedi technológiai termékeket tárgyaló, elméleti vagy módszertani hozzáadott értéket nem tartalmazó anyagok, a nem ellenőrizhető eredetű internetes források, valamint azok a

[7] OECD- Organisation for Economic Co-operation and Development: Gazdasági Együttműködési és Fejlesztési Szervezet

[8] Az angol nyelvű keresőkifejezések alkalmazását az indokolta, hogy a vizsgált témakör nemzetközi szakirodalmának meghatározó része angol nyelven jelenik meg, továbbá a Scopus és a Web of Science bibliográfiai adatbázisokban az angol nyelvű címek, absztraktok és kulcsszavak biztosítják a különböző országokból és tudományterületekről származó publikációk egységes visszakereshetőségét. A keresőkifejezések a technológiai reziliencia vizsgálatához kapcsolódó fő fogalmi dimenziókat fedték le, és igazodtak a nemzetközi szakirodalomban, valamint a NATO, az EU, az ENISA, a NIST és az OECD dokumentumaiban alkalmazott terminológiához. Az angol keresőkifejezések használata így nem a magyar szakirodalom kizárását, hanem a nemzetközi forrásbázis összehasonlítható és reprodukálható feltárását szolgálta; a magyar nyelvű releváns szakirodalom feltárása ezt kiegészítő keresésekkel történt.

[9] Az 1970-es évek kiemelése nem azt jelenti, hogy a rezilienciához kapcsolódó rendszerszemléletű kutatások ekkor kezdődtek. A technológiai reziliencia későbbi értelmezéséhez fontos szocio-technikai előzmények már az 1950-es években megjelentek, mindenekelőtt Eric L. Trist és Ken W. Bamforth munkájában, akik a technikai és társadalmi alrendszerek kölcsönös függőségét vizsgálták. Az 1970-es évek azért jelentenek külön elméleti fordulópontot, mert C. S. Holling 1973-ban megjelent *Resilience and Stability of Ecological Systems* című tanulmánya a rezilienciát explicit elemzési fogalomként vezette be a komplex rendszerek stabilitásának és alkalmazkodóképességének vizsgálatába. A szakirodalmi feltárás ezért megkülönbözteti a rezilienciagondolkodás korábbi szocio-technikai előzményeit és a reziliencia önálló elméleti fogalmának 1970-es évektől kibontakozó fejlődését.

publikációk, amelyek a rezilienciát kizárólag metaforikus vagy a kutatás tárgyához nem kapcsolható értelemben alkalmazták.

A kutatás módszertanának önálló elemét képezte a **technológiai rezilienciához kapcsolódó meghatározó tudományos modellek kritikai összehasonlító elemzése**. Ennek során nem pusztán az egyes megközelítések fogalmi tartalmát és fejlődését vizsgáltam, hanem egységes elemzési szempontok alapján értékeltem azok vizsgálati fókuszát, elemzési szintjét, erősségeit, korlátait, valamint a technológiai, szervezeti és szabályozási–irányítási tényezők kezelésének módját. **Külön figyelmet fordítottam** arra, hogy az egyes modellek **mennyiben alkalmasak a komplex szocio-technikai rendszerek, a kritikus infrastruktúrák és a katonai működőképességet támogató technológiai rendszerek dinamikus rezilienciájának értelmezésére és értékelésére.** A kritikai összehasonlítás célja nem az egyes modellek általános érvényességének megkérdőjelezése volt, hanem alkalmazhatósági határaik és a közöttük fennálló elméleti kapcsolatok feltárása. **Az elemzés eredményei alapján azonosítottam azt a kutatási rést,** amely indokolttá tette a technológiai, szervezeti és szabályozási–irányítási dimenziókat egységes rendszerben kezelő saját technológiai rezilienciamodell kialakítását. (BATR[10], TRI[11]–TRMM[12] keretrendszer kidolgozása)

A téma lehatárolása

Tárgyi lehatárolás

A disszertáció a **technológiai rezilienciát a digitálisan támogatott kritikus infrastruktúrák és a védelmi–biztonsági alkalmazások összefüggésében** vizsgálja. Nem cél a reziliencia pszichológiai, közösségi vagy ökológiai értelmezésének önálló, teljes körű feldolgozása; ezek csak annyiban jelennek meg, amennyiben elméleti elemeik hozzájárulnak a technológiai reziliencia fogalmának kialakításához.

A **kutatás nem vállalkozik valamennyi kritikus infrastruktúra** azonos mélységű ágazati elemzésére. A kiválasztott rendszerek a modell validációs terepei: céljuk annak vizsgálata, hogy a háromdimenziós értelmezés és az érettségi logika eltérő technológiai és intézményi környezetben is alkalmazható-e.

[10] BATR- Balogh Adaptive Technological Resilience Cycle: Balogh féle (a szerző modellje) Adaptív Technológiai Reziliencia Ciklus

[11] TRI-Technological Resilience Index: Technológia Reziliencia Index

[12] TRMM-Technological Resilience Maturity Modell: Technológia Érettségi Modell

Földrajzi és intézményi lehatárolás

A kutatás **globális technológiai és fenyegetési folyamatokat vesz figyelembe**, de elsődleges intézményi referenciakerete az **euroatlanti térség, különösen az Európai Unió, a NATO és a magyar kritikus infrastruktúra-** és védelmi környezet. A nemzetközi kitekintés célja az összehasonlíthatóság és a stratégiai összefüggések feltárása, nem pedig egy teljes nemzetközi kapcsolatelméleti elemzés.

Időbeli lehatárolás

A vizsgálat súlypontja a **21. század első negyedének technológiai és biztonsági folyamataira** esik. A korábbi elméletek és történeti példák az 1. fejezetben a fogalom fejlődésének megértését szolgálják, míg a 2–4. fejezet a digitalizáció, a kiberfenyegetések, a kritikus technológiai függőségek, az ellátási láncok és az adaptív governance jelenlegi problémáira koncentrál.

Módszertani lehatárolás

A disszertáció **nem tekinti céljának egy univerzális, minden technológiai rendszerre** azonos súlyokkal alkalmazható matematikai reziliencia-index megalkotását. A modell **célja** ehelyett egy **strukturált, többdimenziós értékelési keret kialakítása**, amely támogatja a hiányosságok azonosítását, az érettségi szint meghatározását, az ágazatok közötti összehasonlítást és a fejlesztési prioritások kijelölését.

A disszertáció tudományos hozzájárulása

A kutatás tudományos hozzájárulása **nem egyetlen új indikátor vagy technológiai megoldás bevezetésében áll**, hanem abban, hogy a technológiai rezilienciát az elmélettől a mérésen és validáción át a stratégiai irányításig egységes logikai rendszerben kezeli.

1. A **technológiai reziliencia integrált szocio-technikai értelmezésének megalapozása**, amely a rezilienciát a technológiai, szervezeti és szabályozási–irányítási dimenzió kölcsönhatásából származtatja.

2. A szerző által megfogalmazott **Adaptív Technológiai Reziliencia Ciklus** (BATR), valamint a **TRI–TRMM értékelési és érettségi keret** kidolgozása, amelyek a

háromdimenziós modell dinamikus működésének és strukturált mérhetővé és értékelhetővé tételének módszertani alapját biztosítják.

3. A modell **kritikus infrastruktúra-ágazatokon történő összehasonlító validálása**, amely empirikus-szakági alapon vizsgálja az általánosítható és az ágazatspecifikus reziliencia-követelményeket.

4. A **Nemzeti Technológiai Reziliencia Irányítási Keretrendszer koncepciójának kialakítása**, amely a technológiai rezilienciát az ágazati szintről a nemzeti stratégiai irányítás szintjére emeli, és összekapcsolja a kritikus infrastruktúrák, a digitális transzformáció, a kiberbiztonság, az innováció, a védelmi igények és a nemzeti ellenálló képesség területeit.

A disszertáció felépítése

Az **1. fejezet** a reziliencia fogalmának tudományos evolúcióját és a technológiai reziliencia elméleti megalapozását mutatja be. Az ökológiai, mérnöki, szervezeti, kiberbiztonsági és kritikusinfrastruktúra-megközelítések összehasonlításával azonosítja azokat a közös elemeket, amelyek a technológiai reziliencia integrált értelmezéséhez szükségesek. A fejezet a technológiai rezilienciát szocio-technikai rendszerkörnyezetben helyezi el, és megalapozza a háromdimenziós modell elméleti logikáját.

A **2. fejezet** a technológiai rezilienciát alakító 21. századi környezeti kihívásokat elemzi. A technológiai gyorsulás, a hiperösszekapcsoltság, a kiber- és hibrid fenyegetések, az IT/OT-konvergencia, a felhő-, kommunikációs és PNT-függőségek, az energia- és ellátásilánc-kitettségek, valamint a humán, szervezeti és szabályozási tényezők együttes vizsgálatából vezeti le a reziliencia-követelményeket. Külön hangsúlyt kap a statikus compliance és az adaptív reziliencia-governance közötti különbség, valamint a civil és katonai technológiai rendszerek összekapcsoltsága.

A **3. fejezet** a kutatás saját modellalkotó része. Az elméleti és környezeti elemzés eredményeire építve kidolgozza a technológiai, szervezeti és szabályozási–irányítási dimenzióból álló integrált technológiai reziliencia modellt. A fejezet a modell kapcsolati és dinamikus logikáját, valamint a technológiai reziliencia mérhetőségét és érettségi szintjeit is meghatározza, ezzel a fogalmi keretet gyakorlati értékelési eszközzé alakítja.

A **4. fejezet** a modell alkalmazását, validálását és stratégiai kiterjesztését végzi el. A kiválasztott kritikus infrastruktúra-területek szakági követelményeinek összehasonlító elemzésével vizsgálja a háromdimenziós modell alkalmazhatóságát, majd a validáció eredményeiből kiindulva megfogalmazza a Nemzeti Technológiai Reziliencia Irányítási

Keretrendszer architektúráját és működési logikáját. A fejezet egyben összegzi a kutatás tudományos eredményeit és azok gyakorlati, stratégiai alkalmazhatóságát.

Az 5-6. fejezet összegzi a kutatás eredményeit, megválaszolja a kutatási kérdéseket, értékeli a hipotéziseket, tételesen megfogalmazza az új tudományos eredményeket, valamint meghatározza a gyakorlati alkalmazás és a további kutatás irányait.

A bevezetés összegzése

A technológiai reziliencia a disszertáció értelmezésében nem egy újabb, a kiberbiztonság vagy a kritikus infrastruktúra-védelem mellé helyezett részterület, hanem olyan integráló szemlélet, amely a technológiai rendszerek működőképességét a zavarok előtti felkészülés, a zavar alatti funkciófenntartás, a helyreállítás, az adaptáció és a tanulás teljes ciklusában vizsgálja. A technológiai, szervezeti és szabályozási–irányítási dimenziók egymástól nem választhatók el; a reziliencia a köztük kialakuló kölcsönhatás eredménye.

A disszertáció logikai íve ennek megfelelően az elméleti megalapozástól a környezeti kihívásokon és saját modellalkotáson át az ágazati validációig és a nemzeti stratégiai irányításig vezet. Ez biztosítja, hogy a kutatás fogalomhasználata, hipotézisei, módszertana és tudományos eredményei egymással, valamint az 1–4. fejezet tartalmával közvetlenül összhangban álljanak.

1. fejezet A technológiai reziliencia elméleti alapjai és fogalmi fejlődése

1.1 A fejezet célja és kutatási megközelítése

A technológiai reziliencia fogalmának tudományos megalapozása csak akkor lehet koherens, ha a **rezilienciát** nem a digitális korszak önálló termékeként, **hanem több tudományterületen végbement fogalmi fejlődés eredményeként értelmezzük**. A reziliencia az ökológiai rendszerek stabilitásának vizsgálatából indult, majd a pszichológiai és szervezeti kutatásokon, a komplex rendszerek elméletén és a reziliencia-mérnökségen keresztül fokozatosan olyan rendszerszintű kategóriává vált, amely a technológiai infrastruktúrák, a működtető szervezetek és az intézményi-szabályozási környezet együttes alkalmazkodóképességének leírására is alkalmas. E fejlődési ív megértése azért szükséges, mert a doktori kutatás későbbi fejezeteiben alkalmazott technológiai reziliencia fogalom nem egyetlen korábbi iskola átvétele, hanem azok kritikai szintézisére épül.

A fejezet célja kettős. **Egyrészt rekonstruálja a reziliencia fogalmának** tudományos evolúcióját, és azonosítja azokat az elméleti elemeket, amelyek a modern technológiai rendszerek vizsgálatában továbbra is érvényesek. **Másrészt elhatárolja egymástól** a megbízhatóság, a robusztusság, a biztonság, a kiberbiztonság és a reziliencia fogalmait, majd megmutatja, hogy a digitalizáció, a hálózatosodás és a kritikus infrastruktúrák kölcsönös függősége miért teszi szükségessé a technológiai reziliencia tágabb, szocio-technikai értelmezését. A fejezet nem saját mérési modellt vagy értékelési keretrendszert dolgoz ki; e feladat a 3. fejezethez tartozik. Ugyancsak nem az aktuális fenyegetési környezet részletes elemzésére vállalkozik, amelyet a 2. fejezet végez el. Feladata az a fogalmi és elméleti alapozás, amelyre a későbbi modellalkotás és validáció építhető.

A **vizsgálat kritikai szakirodalmi szintézisre** épül. Az elemzés kiindulópontját a reziliencia klasszikus ökológiai, pszichológiai és szervezeti megközelítései adják, ezt követi a komplex adaptív rendszerek, a szocio-technikai rendszerek és a reziliencia-mérnökség elméleti hozzájárulásainak áttekintése. A fejezet ezután a kiberreziliencia és a kritikus infrastruktúrák szakirodalmán keresztül vizsgálja a fogalom technológiai újraértelmezését, végül bemutatja a reziliencia stratégiai és szabályozási intézményesülését. A magyar szakirodalmi kontextus külön hangsúlyt kap annak érdekében, hogy a technológiai reziliencia ne kizárólag nemzetközi elméleti kategóriaként, hanem a hazai kiberbiztonsági és kritikusinfrastruktúra-védelmi gondolkodásba illeszkedő fogalomként is értelmezhető legyen.

A fejezet logikai felépítése ennek megfelelően az elméleti gyökerektől a technológiai és stratégiai újraértelmezés felé halad. A cél nem a különböző reziliencia elméletek egymás mellé helyezése, hanem annak feltárása, hogy mely fogalmi elemek maradnak állandók a tudományterületek közötti átmenet során. Ilyen állandó elem az alapvető funkciók fenntartása, a zavarások elnyelése, az alkalmazkodás, a tanulás, a helyreállítás és a megváltozott környezethez történő újrakonfigurálás. A technológiai reziliencia későbbi munkadefiníciója ezeknek az elemeknek a komplex szocio-technikai rendszerekre történő kiterjesztéséből vezethető le.

A reziliencia elméletek hadtudományi relevanciája abból következik, hogy a katonai szervezetek és képességek maguk is komplex szocio-technikai rendszerekként működnek. A korszerű katonai műveletek eredményességét nem kizárólag a fegyverrendszerek technikai teljesítménye határozza meg, hanem a vezetési, kommunikációs, felderítési, logisztikai, energetikai és információs rendszerek együttes rendelkezésre állása, valamint az ezeket működtető szervezet alkalmazkodóképessége. A technológiai reziliencia elméleti vizsgálata ezért hadtudományi szempontból a katonai képesség fenntartásának és a technológiai zavarok mellett történő feladat-végrehajtásnak az értelmezési keretét is jelenti.

1.2 A reziliencia fogalmának tudományos evolúciója

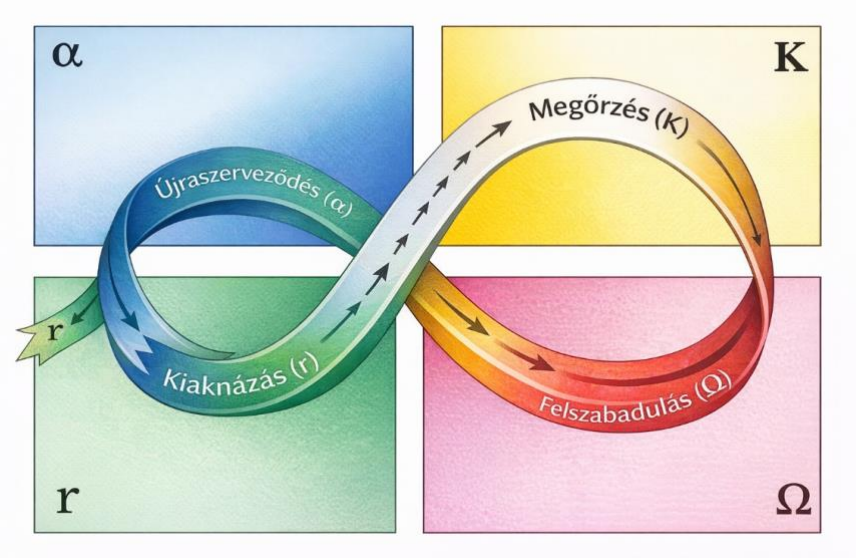
1.2.1 Az ökológiai reziliencia: a stabilitástól az adaptív változásig

A reziliencia modern tudományos diskurzusának meghatározó kiindulópontja **C. S. Holling 1973-ban megjelent tanulmánya** [1]. Holling elméleti hozzájárulása e kutatás szempontjából elsősorban abban ragadható meg, hogy megkülönböztette az egyensúlyi állapot helyreállításának gyorsaságát attól a képességtől, amellyel a rendszer jelentős zavarások mellett is megőrzi alapvető működési karakterét. E megkülönböztetés teszi lehetővé, hogy a rezilienciát ne egyszerű helyreállításként, hanem a változó körülmények között fenntartott működőképességként értelmezzem. Ez a szemléletváltás a **későbbi adaptív és szocio-technikai megközelítések** egyik fontos elméleti előzményévé vált [1], [99].

1.1. ábra: A reziliencia fogalmának elméleti fejlődési íve (saját szerkesztés)

Az ökológiai megközelítés egyik legfontosabb következménye, hogy a zavar nem feltétlenül rendellenesség, hanem a komplex rendszer működésének természetes része. A reziliens rendszer nem azért életképes, mert képes kizárni valamennyi külső vagy belső változást, hanem azért, mert bizonyos határok között képes azokat elnyelni, feldolgozni, illetve működését újraszervezni. Ez a gondolat közvetlenül átvihető a technológiai rendszerekre is. Egy modern informatikai vagy kiberfizikai rendszerben a frissítések, komponenscserék, hálózati átrendeződések, incidensek és technológiai migrációk nem kivételes események, hanem a normál működéshez tartozó változások.

Holling későbbi munkáihoz kapcsolódva az adaptív ciklus logikája a növekedés, a konszolidáció, a felszabadulás és az újraszerveződés ismétlődő dinamikáját írja le. E szemlélet fontos tanulsága, hogy a nagyfokú optimalizáltság és kapcsoltság nem szükségszerűen azonos a magas rezilienciával. [1] Egy rendszer működése rövid távon rendkívül hatékony lehet, miközben a redundanciák csökkenése, a túlzott specializáció vagy a függőségek sűrűsödése miatt sérülékenyebbé válik. A technológiai reziliencia szempontjából ez arra figyelmeztet, hogy a kizárólag hatékonyságra optimalizált architektúrákban a tartalék kapacitások, az alternatív működési utak és az újrakonfigurálhatóság hiánya rendszerszintű kockázatot teremthet.



1.2. ábra: Gunderson és Holling adaptív ciklusának vizualizációja (saját szerkesztés Gunderson és Holling [99] alapján)

Az ökológiai reziliencia technológiai alkalmazásának ugyanakkor vannak korlátai. A technológiai rendszerek nem önszerveződő ökoszisztémák a szó szoros értelmében: működésüket tudatos emberi tervezés, szervezeti döntéshozatal, jogi szabályozás és gazdasági ösztönzők alakítják. Az ökológiai elmélet ezért nem ad közvetlen magyarázatot arra, hogyan hat a vezetés, a szervezeti kultúra, a felelősségi rend vagy a szabályozás a rendszer alkalmazkodóképességére. Mégis innen származik a technológiai reziliencia egyik alapvető tétele: a tartós működőképesség nem az állandóság, hanem a változások közepette fenntartott funkcionális identitás kérdése.

1.2.2 Pszichológiai reziliencia: adaptáció, erőforrások és tanulás

A reziliencia fogalmának következő jelentős kiterjesztése a pszichológiai és fejlődéslélektani kutatásokban történt meg. **Masten** [2] **„ordinary magic" koncepciója arra hívja fel a figyelmet**, hogy a kedvezőtlen körülményekhez történő alkalmazkodás nem feltétlenül rendkívüli képességekből, hanem a rendszerben már meglévő erőforrások, kapcsolatok és tanulási mechanizmusok mozgósításából ered. A technológiai reziliencia szempontjából e gondolatot nem közvetlen modellként veszem át, hanem az adaptáció, az erőforrás-mobilizáció és a tanulás szerepének elméleti előzményeként értelmezem.

A technológiai reziliencia szempontjából a pszichológiai megközelítés két eleme különösen fontos. Az első az, hogy az adaptáció nem kizárólag az objektív környezeti feltételektől, hanem azok értelmezésétől és a rendelkezésre álló erőforrások mozgósításától is függ. A második a tanulás szerepe: egy zavar akkor válik reziliencia fejlesztő tapasztalattá,

ha annak következményei beépülnek a későbbi működésbe. E gondolat a technológiai rendszereket működtető szervezetekre is alkalmazható, mivel incidensek, meghibásodások és válságok során az emberi helyzetértékelés, a döntéshozatal és a tapasztalatfeldolgozás közvetlenül befolyásolja a technológiai képességek tényleges hasznosulását.

A pszichológiai reziliencia ugyanakkor nem ad megfelelő magyarázatot a nagy technológiai rendszerek strukturális tulajdonságaira. Nem képes leírni a redundancia, az architekturális modularitás, a hálózati függőségek vagy a szabályozási környezet hatását. Jelentősége ezért nem abban áll, hogy közvetlen technológiai modellt kínál, hanem abban, hogy a reziliencia fogalmába beemeli az aktív alkalmazkodás, a tanulás és az erőforrás-mobilizáció elemeit. Ezzel megalapozza a szervezeti reziliencia későbbi megközelítéseit.

1.2.3 Szervezeti reziliencia: dinamikus képesség és intézményesített tanulás

A szervezeti reziliencia kutatása a fogalmat az egyéni alkalmazkodás szintjéről a kollektív működés és stratégiai menedzsment szintjére emelte. **Lengnick-Hall, Beck és Lengnick-Hall szerint a szervezeti reziliencia olyan képességkészlet**, amely lehetővé teszi, hogy a szervezet a váratlan eseményekhez ne pusztán reaktívan alkalmazkodjon, hanem a változó környezetben új működési lehetőségeket is kialakítson [3]. A megközelítés középpontjában a kognitív, viselkedési és kontextuális képességek állnak, amelyek a vezetés, a tudás, a humán erőforrás és a szervezeti kapcsolatok szintjén teremtik meg az alkalmazkodás feltételeit.

Duchek [4] a szervezeti rezilienciát három egymáshoz kapcsolódó képességcsoport – az eseményt megelőző anticipáció, az esemény alatti megküzdés (coping), valamint az azt követő adaptáció – segítségével írja le. A jelen kutatás e modellt nem veszi át technológiai reziliencia modellként, hanem annak időbeli és tanulási logikáját használja fel a későbbi saját dinamikus modell elméleti megalapozásához. A megközelítés azért releváns, mert a rezilienciát nem egyszeri reakcióként, hanem időben kiterjesztett, fejleszthető szervezeti képességként kezeli.

Boin és van Eeten a reziliens szervezet kapcsán arra hívják fel a figyelmet, hogy a megbízható és alkalmazkodó működés nem vezethető le egyszerűen a formális szabályok vagy technikai kontrollok meglétéből [5]. A kritikus szolgáltatásokat biztosító szervezeteknek egyszerre kell stabil működési rutinokat fenntartaniuk és képesnek lenniük azok gyors felülvizsgálatára, amikor a környezet megváltozik. Ez a kettősség a technológiai szervezetekben különösen élesen jelenik meg: a standardizáció és biztonsági kontrollok

nélkülözhetetlenek, ugyanakkor túlzott merevségük válsághelyzetben lassíthatja az adaptációt.

A szervezeti reziliencia kutatásának fő hozzájárulása tehát az, hogy a rezilienciát a vezetéshez, a kultúrához, a döntési struktúrákhoz, az információáramláshoz és a tanulási folyamatokhoz kapcsolja. Egy korszerű technológiai rendszer képességei csak akkor eredményeznek tényleges rezilienciát, ha a működtető szervezet képes a rendelkezésre álló információt értelmezni, megfelelő döntést hozni, az erőforrásokat átcsoportosítani és az új működési módot intézményesíteni. A szervezeti megközelítés korlátja ugyanakkor, hogy a technológiai architektúrát gyakran adottságként kezeli; ezért a technológiai reziliencia átfogó értelmezéséhez ezt a nézőpontot a rendszerelméleti és mérnöki megközelítésekkel kell összekapcsolni. [89].

1.3 Komplex rendszerek és a szocio-technikai rendszermegközelítés

1.3.1 Komplexitás, emergencia és adaptív rendszerek

A technológiai reziliencia fogalmi fejlődésének következő lépcsője a komplex rendszerek elmélete. A modern digitális és kritikus infrastruktúrák nagyszámú komponensből, többszintű függőségekből és dinamikus kapcsolatokból épülnek fel. Viselkedésük ezért nem vezethető le egyszerűen az egyes elemek tulajdonságainak összegzéséből. A komplex adaptív rendszerek elmélete szerint a rendszer egészében olyan, az egyes elemek kölcsönhatásából kialakuló tulajdonságok jelenhetnek meg, amelyek az egyes komponensek önálló vizsgálatából nem vezethetők le. **Holland munkái** e rendszerek alkalmazkodását, visszacsatolásait és önszerveződő mintázatait hangsúlyozzák [6], míg **Mitchell a nemlineáris kölcsönhatások és a kialakuló viselkedés** központi szerepét emeli ki [7].

Ez a nézőpont a technológiai reziliencia szempontjából alapvető jelentőségű. Egy rendszer rezilienciája nem azonos a komponensek egyedi megbízhatóságának összegével. Lehetséges, hogy valamennyi elem magas technikai minőséget képvisel, mégis sérülékeny rendszerszintű konfiguráció alakul ki, ha a függőségek túl szorosak, a döntési mechanizmusok lassúak vagy az információáramlás elégtelen. Ezzel szemben közepes teljesítményű komponensekből is kialakítható magasabb rezilienciájú rendszer, ha a működés modularizált, a hibák lokalizálhatók, a szervezet gyorsan reagál, és alternatív működési módok állnak rendelkezésre.

A komplexitás tehát nem pusztán a komponensek számát jelenti. A technológiai reziliencia szempontjából legalább ilyen fontos a kapcsolatok sűrűsége, a csatoltság mértéke, a függőségek iránya, a közös erőforrásokra támaszkodás, valamint a visszacsatolási hurkok. A digitális infrastruktúrákban a szolgáltatások közötti API[13]-kapcsolatok, identitáskezelési szolgáltatások, felhőplatformok, adatkapcsolatok és harmadik fél által biztosított komponensek olyan rejtett összefüggéseket hozhatnak létre, amelyek normál működés során hatékonyságnövelők, zavar esetén azonban hibaterjedési útvonallá válhatnak.

A komplex rendszerelméleti szemlélet egyik legfontosabb következménye, hogy a rezilienciát a kapcsolatok és nem kizárólag az elemek szintjén is vizsgálni kell. Ez a gondolat később közvetlenül hozzájárulhat a technológiai, szervezeti és szabályozási tényezők közötti kapcsolatok elemzéséhez, de e fejezetben még nem saját modellként, hanem az elméleti megalapozás részeként jelenik meg. A rendszer szintű viselkedés megértése teremti meg azt az átmenetet, amelyen keresztül az ökológiai és szervezeti reziliencia technológiai rendszerekre alkalmazhatóvá válik.

1.3.2 A „normális balesetek” és a szoros csatoltság problémája

Charles Perrow „normal accidents” elmélete a komplex, szorosan csatolt rendszerek egyik alapvető kockázati sajátosságára mutat rá: bizonyos rendszerekben a meghibásodások teljes kizárása nem reális cél, mert a komponensek közötti összetett és gyakran előre nem látható kölcsönhatások maguk is új hibalehetőségeket hoznak létre [8]. A „normális” jelző nem azt jelenti, hogy a baleset elfogadható vagy gyakori, hanem azt, hogy a rendszer szerkezetéből következően bizonyos hibakombinációk elkerülhetetlenül bekövetkezhetnek.

A digitális infrastruktúrák e logika szempontjából különösen érzékenyek. A nagyfokú összekapcsoltság, az automatizáció, a szoftveres függőségek és a valós idejű működés rövid reakcióidőt és gyors hibaterjedést eredményezhet. Egy kezdetben lokális probléma – például hibás frissítés, identitásszolgáltatás-kiesés vagy hálózati konfigurációs hiba – több szolgáltatáson keresztül láncreakciót indíthat el. A technológiai reziliencia ebből következően nem épülhet kizárólag a meghibásodások megelőzésére. Szükséges a hibák detektálásának, izolálásának, kontrollált degradációjának és a szolgáltatás alternatív módon történő fenntartásának képessége is.

13 API: Application Programming Interface; magyarul: alkalmazásprogramozási felület.

A szoros csatoltság problémáját tovább erősíti a technikai adósság. **Kruchten, Nord és Ozkaya a technikai adósságot olyan felhalmozódó strukturális költségként írják le**, amely a rövid távú fejlesztési kompromisszumok későbbi karbantartási és működési kockázataiban jelenik meg [9]. A technológiai reziliencia szempontjából a technikai adósság azért kritikus, mert csökkenti a rendszer átláthatóságát, növeli a függőségek számát és korlátozza a gyors újrakonfigurálás lehetőségét. Az örökölt komponensek, nem dokumentált interfészek és ideiglenes megoldások hosszú távon olyan rejtett sérülékenységeket halmozhatnak fel, amelyek válsághelyzetben egyszerre aktiválódnak.

E megközelítésből a reziliencia a kontrollált komplexitás menedzsmentjeként is értelmezhető. A cél nem minden kapcsolat megszüntetése, hiszen a hálózatos működésből származik a modern digitális rendszerek jelentős funkcionális előnye. A cél inkább az, hogy a kritikus függőségek azonosíthatók, a hibaterjedési útvonalak korlátozhatók, a komponensek szükség esetén izolálhatók, és a rendszer rendelkezzen alternatív működési konfigurációkkal.

1.3.3 A szocio-technikai rendszerek: technológia, ember és intézmény egysége

A technológiai reziliencia szempontjából a szocio-technikai rendszerelmélet teremti meg a legközvetlenebb átmenetet a technikai és szervezeti nézőpont között. **Trist és Bamforth klasszikus munkája** arra mutatott rá, hogy a technológiai és társadalmi alrendszerek teljesítménye kölcsönösen függ egymástól [10]. A későbbi rendszerfejlesztési szakirodalom ezt azzal egészítette ki, hogy a technológia tervezése és működtetése nem választható el a szervezeti folyamatoktól, a felhasználói szerepektől és az intézményi környezettől [11], [103].

A digitális infrastruktúrákban e kölcsönös függőség tovább erősödött. A szoftverarchitektúra meghatározza a szervezet döntési lehetőségeit és munkafolyamatait, miközben a szervezeti követelmények, szabályozási elvárások és humán kompetenciák visszahatnak a technológia kialakítására. Egy kiberbiztonsági rendszer például nem tekinthető önmagában reziliensnek pusztán azért, mert fejlett észlelési technológiát alkalmaz. Az észlelt esemény értékeléséhez szakértelem, döntési jogosultság, kommunikációs eljárás, vezetői támogatás és megfelelő incidenskezelési folyamat szükséges.

A szocio-technikai megközelítés ezért a rezilienciát nem egyetlen komponens tulajdonságaként, hanem a rendszer elemei közötti együttműködés eredményeként kezeli. E szemlélet fontos előnye, hogy lehetővé teszi a technikai és humán hibák mesterséges

szétválasztásának meghaladását. A legtöbb súlyos technológiai incidensben a kiváltó ok és a következmények több szinten oszlanak meg: technikai sérülékenység, szervezeti döntési hiba, hiányos szabályozás, elégtelen képzés vagy beszállítói függőség egyszerre lehet jelen.

A szocio-technikai keret ugyanakkor csak akkor válik a technológiai reziliencia megfelelő elméleti alapjává, ha a társadalmi komponens alatt nem kizárólag a közvetlen felhasználókat értjük. A modern kritikus infrastruktúrák működését állami szabályozók, beszállítók, felhőszolgáltatók, auditáló szervezetek, nemzetközi szabványok és biztonságpolitikai követelmények is alakítják. A technológiai reziliencia ezért a klasszikus ember–gép kapcsolaton túl intézményi és governance-dimenziót is feltételez.

1.3. Ábra: A technológiai reziliencia szocio-technikai rendszerkörnyezete (saját szerkesztés)

1.3.4 Interdependencia, kialakuló sérülékenység és a rendszerek rendszere szemlélet

A komplexitáselméleti és szocio-technikai megközelítés összekapcsolásának egyik legfontosabb következménye, hogy a technológiai reziliencia elemzési egysége nem szükségszerűen egyetlen szervezet vagy infrastruktúra, hanem gyakran több, egymással kölcsönös függőségben álló rendszer együttese. A kritikus infrastruktúrák kutatásában **Rinaldi, Peerenboom és Kelly az interdependenciát olyan kétirányú kapcsolatként** írják le, amelyben az egyik infrastruktúra állapota befolyásolja egy másik infrastruktúra működését, miközben a visszahatás ugyancsak módosítja az első rendszer működési feltételeit [30]. E megközelítés elméleti jelentősége abban áll, hogy a rezilienciát nem lehet

kizárólag az egyes komponensek megbízhatóságának összegeként kezelni. Egy lokálisan jól védett rendszer is sérülékennyé válhat, ha olyan külső szolgáltatástól, energiaellátástól, kommunikációs kapcsolattól vagy adatforrástól függ, amelynek kiesése az adott szervezet kontrollján kívül esik.

Az interdependencia több formában jelenhet meg. Fizikai függőség áll fenn, amikor az egyik infrastruktúra működéséhez a másik által előállított anyag, energia vagy szolgáltatás szükséges. Kiberfüggőség esetén az információs és irányítási rendszerek kapcsolódása közvetíti a hatást; tipikus példa, amikor az energiaelosztás működése telekommunikációs és digitális vezérlőrendszerektől függ. Földrajzi függőség akkor alakul ki, ha több infrastruktúra ugyanazon fizikai térben koncentrálódik, míg logikai függőség esetén szervezeti, szabályozási, pénzügyi vagy döntési mechanizmusok kapcsolják össze a rendszereket [30]. **Ouyang későbbi áttekintése arra mutat rá**, hogy e függőségek modellezése azért különösen nehéz, mert a hálózatok kölcsönhatása nemlineáris, és a zavarások következményeit gyakran időbeli késleltetések, visszacsatolások és másodlagos hatások módosítják [31].

A technológiai reziliencia szempontjából ebből az következik, hogy a sérülékenység forrása nem feltétlenül ott található, ahol a működési zavar megjelenik. Egy adatközponti szolgáltatás kiesése mögött lehet energiaellátási hiba, egy közlekedési rendszer működésképtelensége mögött kommunikációs vagy műholdas navigációs zavar, egy szervezet döntési bénultsága mögött pedig olyan adatminőségi vagy jogosultsági probléma, amely technikailag egy másik rendszerhez tartozik. Ez a kialakuló sérülékenység fogalmához vezet: a rendszer egészének kitettsége olyan kölcsönhatásokból is származhat, amelyek egyik alrendszer izolált elemzéséből sem lennének azonosíthatók. A technológiai reziliencia ezért szükségképpen kapcsolat-orientált fogalom, amelyben az interfészek, függőségek és visszacsatolások legalább olyan fontosak, mint az önálló komponensek belső robusztussága [6][7][30][31],[86].

A **rendszerek rendszere (system of systems) szemlélet** tovább erősíti ezt az értelmezést. Ilyen környezetben az alrendszerek önálló tulajdonossal, célrendszerrel, irányítási logikával és életciklussal rendelkezhetnek, miközben egy magasabb szintű funkció csak összehangolt működésük révén valósul meg. A kritikus infrastruktúrák és a digitális ökoszisztémák tipikusan ilyen struktúrák. A technológiai reziliencia fejlesztése ezért nem korlátozható egy szervezeten belüli beruházásra: szükségessé válik az interoperabilitás, a függőségi térképezés, a közös incidenskezelés, a kölcsönös tájékoztatás és a több szereplőt átfogó gyakoroltatás. E logika később közvetlenül kapcsolódik a 3. fejezetben kidolgozott

interdimenzionális kapcsolatokhoz és a 4. fejezet ágazatok közötti összehasonlító validációjához.

Az **interdependencia elmélete egyben a hatékonyság és a reziliencia** közötti feszültséget is új megvilágításba helyezi. A digitalizáció és a szolgáltatások koncentrációja gazdasági és működési szempontból gyakran racionalizálja az erőforrás-felhasználást, ugyanakkor csökkentheti a rendszerben rendelkezésre álló alternatívákat. Ha több szervezet ugyanazon felhőszolgáltatóra, azonos kommunikációs gerincre, közös szoftverplatformra vagy egyetlen stratégiai beszállítóra támaszkodik, akkor az egyedi szervezeti redundancia ellenére rendszerszintű koncentrációs kockázat alakulhat ki. A reziliencia szempontjából ezért a redundancia fogalmát is tágabban kell értelmezni: nemcsak komponensszintű tartalékot, hanem funkcionális, szolgáltatói és szervezeti alternatívákat is jelent [19][30][31].

1.4 Reziliencia-mérnökség, technológiai és kiberreziliencia

1.4.1 A reziliencia-mérnökség hozzájárulása

A reziliencia-mérnökség a nagy kockázatú rendszerek működésének vizsgálatából fejlődött ki, és alapvetően szakított azzal a feltételezéssel, hogy a biztonság kizárólag a hibák számának csökkentésével növelhető. **Hollnagel, Woods és Leveson megközelítése a rendszer változó körülmények közötti sikeres teljesítményére**, az alkalmazkodó működésre és az ember–technológia együttműködésére irányította a figyelmet [12], [14], [57], [103]. A reziliencia ebben a felfogásban azt jelenti, hogy a rendszer képes előre jelezni, monitorozni, reagálni és tanulni.

Woods későbbi elemzése rámutatott arra, hogy a rezilienciát több eltérő módon lehet értelmezni: visszapattanásként, robusztusságként, kiterjeszthető alkalmazkodóképességként vagy olyan képességként, amely megakadályozza, hogy a rendszer teljesítménye egy kritikus határ alá essen [13]. Ez a differenciálás különösen fontos a technológiai rendszerek vizsgálatakor. Egy szolgáltatás nem feltétlenül tér vissza az eredeti konfigurációhoz; a sikeres adaptáció eredménye lehet egy tartósan megváltozott architektúra vagy működési folyamat is.

Madni és Jackson a reziliencia-mérnökséget olyan koncepcionális keretként értelmezik, amelyben a rendszer képes a váratlan zavarásokra reagálni, működését fenntartani és megfelelő időn belül helyreállni [14]. A technológiai reziliencia számára e megközelítésből három elem emelhető ki: a funkcióközpontúság, a kontrollált degradáció elfogadása és az újrakonfigurálhatóság. A rendszer célja nem feltétlenül az összes

szolgáltatás változatlan minőségű fenntartása, hanem a kritikus funkciók prioritásos megőrzése.

A reziliencia-mérnökség korlátja, hogy hagyományosan elsősorban operatív és rendszerbiztonsági kérdésekre koncentrál. A nemzeti szabályozás, a stratégiai irányítás és a kritikus beszállítói ökoszisztéma jellemzően háttérfeltétel marad. A technológiai reziliencia tágabb értelmezése ezért megtartja a reziliencia-mérnökség adaptív működési logikáját, de azt szervezeti és intézményi szinttel egészíti ki.

1.4.2 A kiberreziliencia: a védelemtől a működésfenntartásig

A kiberreziliencia fogalma abból a felismerésből fejlődött ki, hogy a teljes kiberbiztonság nem reális állapot. A hálózatba kapcsolt rendszerek folyamatosan változó fenyegetési környezetben működnek, ezért a védelem mellett arra is fel kell készülniük, hogy sikeres támadás vagy technikai kompromittálódás esetén is fenntartsák alapvető funkcióikat. **Linkov és Kott a kiberrezilienciát** a rendszer azon képességeként értelmezik, amely a kibertérben bekövetkező kedvezőtlen események során is fenntartja vagy gyorsan helyreállítja a kritikus funkciókat [15].

A **NIST Cybersecurity Framework a kiberkockázatok kezelését az azonosítás**, védelem, észlelés, reagálás és helyreállítás funkcionális logikájába rendezi [16]. Bár a keretrendszer elsődlegesen kiberbiztonsági célú, szerkezete világosan mutatja a reaktív védelem és a reziliens működés közötti átmenetet. A helyreállítás nem különálló technikai lépés, hanem a teljes életciklus része, és a tapasztalatok visszacsatolásával a későbbi működés javításához is kapcsolódik. [104]

A kiberreziliencia technológiai rezilienciába történő integrálásakor ugyanakkor kerülni kell a két fogalom azonosítását. A kiberreziliencia a digitális komponensek, adatok, hálózatok és kiberfenyegetések kezelésére összpontosít. A technológiai reziliencia ennél tágabb: magában foglalja a fizikai infrastruktúrát, az energiaellátást, az üzemeltetési technológiákat, a szervezeti döntéshozatalt, a beszállítói láncokat és a szabályozási környezetet is. Különösen a kiber-fizikai rendszerek esetében válik nyilvánvalóvá, hogy egy digitális kompromittálódás fizikai szolgáltatás-kiesést, biztonsági eseményt vagy társadalmi zavart eredményezhet.

A **kiberreziliencia ezért a technológiai reziliencia egyik meghatározó, de nem kizárólagos részterülete**. A kettő közötti kapcsolat úgy írható le, hogy a kiberreziliencia a digitális működés folyamatos fenntartásának és helyreállításának képességét biztosítja, míg

a technológiai reziliencia ezt a képességet a teljes szocio-technikai rendszer szintjén értelmezi.

1.4.3 A reziliens technológiai architektúra alapelvei

A reziliens technológiai architektúra kialakítása több egymást kiegészítő tervezési elvre épül. A modularitás lehetővé teszi a komponensek elkülönítését és cseréjét; a redundancia alternatív működési útvonalakat biztosít; a diverzitás csökkentheti a közös hibamódok kockázatát; a monitorozhatóság támogatja a korai észlelést; a hibatűrés pedig biztosítja, hogy részleges meghibásodás esetén a rendszer ne veszítse el azonnal valamennyi kritikus funkcióját. E tulajdonságok a reziliencia-mérnökségben és a kritikus infrastruktúrák kutatásában visszatérően megjelennek. [14][17], [82], [100]

A technológiai reziliencia azonban nem azonos e technikai tulajdonságok egyszerű összegével. A redundáns komponens csak akkor jelent valódi rezilienciát, ha a szervezet tudja, mikor és hogyan kell átváltani rá; a monitorozás csak akkor értékes, ha az észlelt jel információvá és döntéssé alakul; a modularitás pedig csak akkor segíti az alkalmazkodást, ha a változtatáshoz szükséges jogosultságok, kompetenciák és beszállítói erőforrások rendelkezésre állnak. A technológiai architektúra ezért a reziliencia szükséges, de önmagában nem elégséges feltétele.

A modern technológiai rendszerekben külön kérdés a kontrollált degradáció. Bizonyos válsághelyzetekben a teljes szolgáltatási szint fenntartása nem reális, ugyanakkor a kritikus funkciók alacsonyabb teljesítményszinten tovább működtethetők. A reziliens architektúra ennek megfelelően nemcsak failover-mechanizmusokat[14], hanem prioritásokat, vészüzemi módokat és manuális vagy részben automatizált tartalék eljárásokat is feltételez. Ez az elv különösen fontos az energetikai, közlekedési, egészségügyi és katonai rendszerek esetében. [82][83]

Fogalom	Elsődleges cél	Időbeliség	Változáshoz való viszony	Technológiai reziliencia kapcsolata
Megbízhatóság	Előírt funkció hibamentes teljesítése	Normál működés	A változást lehetőség szerint minimalizálja	Alapfeltétel, de nem kezeli teljesen az adaptációt
Robusztusság	Zavar elviselése teljesítményromlás nélkül	Zavar alatt	Ellenáll a változásnak	A reziliencia egyik technikai összetevője

[14] A technológiai reziliencia növelésének egyik eszköze a redundáns architektúrák és az automatikus tartalékra váltási (failover) mechanizmusok alkalmazása, amelyek egy komponens kiesése esetén lehetővé teszik a kritikus funkciók folytonosságának fenntartását vagy elfogadható szintű, csökkentett működését

Fogalom	Elsődleges cél	Időbeliség	Változáshoz való viszony	Technológiai reziliencia kapcsolata
Biztonság/kiberbiztonság	Kockázatok és káros események megelőzése, kezelése	Megelőzés + eseménykezelés	Kontrollálja a fenyegetést	Nélkülözhetetlen, de nem azonos a rezilienciával
Reziliencia	Kritikus funkciók fenntartása, adaptáció és helyreállítás	Zavar előtt, alatt és után	Integrálja a változást és tanul belőle	Rendszerszintű, többdimenziós képesség

1.1. táblázat. A megbízhatóság, robusztusság, biztonság és reziliencia fogalmi elhatárolása (saját szerkesztés)

1.4.4 Safety-I, Safety-II és az adaptív teljesítmény értelmezése

A reziliencia-mérnökség tudományos fejlődésének egyik fontos fordulata a biztonság klasszikus és adaptív értelmezésének szétválasztása. A hagyományos, úgynevezett Safety-I szemlélet abból indul ki, hogy a biztonság elsődleges célja a hibák, eltérések és nem kívánt események számának minimalizálása. E logikában a rendszer akkor tekinthető biztonságosnak, ha működése az előírt tartományon belül marad, az eltérések okai azonosíthatók, a hibás komponensek kijavíthatók, és a jövőbeni hasonló események megfelelő kontrollokkal megelőzhetők. A modern komplex rendszerekben azonban a mindennapi sikeres működés és a rendkívüli helyzetek kezelése gyakran ugyanazon adaptív mechanizmusokra támaszkodik. **Hollnagel és munkatársai** ezért a reziliencia-mérnökségben a működés variabilitását nem kizárólag hibaforrásként, hanem a rendszer alkalmazkodóképességének alapjaként is értelmezik [12].

Hollnagel Safety-II megközelítése [12] a biztonsági elemzés fókuszát a meghibásodások kizárólagos vizsgálatáról a normál működés sikerességét fenntartó adaptív mechanizmusokra is kiterjeszti. A jelen kutatás számára ebből nem maga a Safety-II modell átvétele lényeges, hanem az a felismerés, hogy a változó körülmények közötti sikeres működés értelmezéséhez a rendszer teljesítményvariabilitását és alkalmazkodóképességét is vizsgálni szükséges. Ez különösen releváns gyorsan változó technológiai és műveleti környezetben, ahol a formális eljárások nem képesek valamennyi lehetséges helyzetet előre lefedni [12], [13].

Woods [13] **több, egymást kiegészítő nézőpontot különít el** a reziliencia értelmezésére. E tipológia részletes reprodukálása helyett a jelen kutatás szempontjából azt az adaptív megközelítést emelem ki, amely szerint a rendszernek a korábban nem kezelt vagy váratlan helyzetekre is képesnek kell lennie új válaszok kialakítására. Ez a technológiai reziliencia szempontjából azért meghatározó, mert a digitális környezetben a zavarok

gyakran új függőségek, technológiai kombinációk vagy gyorsan változó támadási módszerek eredményei, így a kizárólag korábbi eseményekre optimalizált kontrollrendszer szükségképpen korlátozott.

Az adaptív teljesítmény értelmezése ugyanakkor nem jelentheti a formalizált szabályok, szabványok vagy ellenőrzési mechanizmusok elutasítását. A technológiai reziliencia egyik alapvető irányítási dilemmája éppen a standardizáció és az adaptáció közötti egyensúly. A túl alacsony szabályozottság kiszámíthatatlan és személyfüggő működéshez vezethet, a túlzott merevség viszont akadályozhatja a gyors reagálást. A reziliens szervezet ezért olyan kereteket alakít ki, amelyek világosan meghatározzák a célokat, felelősségeket és biztonsági korlátokat, ugyanakkor megfelelő döntési mozgásteret biztosítanak a helyzethez igazodó végrehajtáshoz. Ez a gondolat összeköti a reziliencia-mérnökséget a szervezeti reziliencia, az adaptív vezetés és a governance későbbi kérdéseivel [4][5][12][13].

A szervezeti alkalmazkodás kutatása ezt a működési nézőpontot további mechanizmusokkal egészíti ki. **Weick és Sutcliffe a nagy megbízhatóságú szervezetek** esetében a gyenge jelek iránti érzékenységet, a leegyszerűsítő magyarázatok kerülését, a működés közelségének fenntartását és a szakértelemhez igazodó döntési autoritást emelik ki [32], [108]. **Teece dinamikus képességek elmélete** arra mutat rá, hogy a tartós alkalmazkodóképesség nem a meglévő erőforrások puszta birtoklásából, hanem azok érzékelési, megragadási és újrakonfigurálási képességéből származik [33]. **Argyris és Schön szervezeti tanulásról alkotott megközelítése** szerint a valódi adaptációhoz nem elegendő a hibák egyszerű korrekciója; szükség lehet a működést meghatározó alapfeltevések és döntési rutinok felülvizsgálatára is [34]. **Nonaka és Takeuchi tudásteremtési modellje** pedig azt emeli ki, hogy a tapasztalati és explicit tudás közötti átalakítás, megosztás és intézményesítés a szervezeti megújulás fontos feltétele [35]. E négy megközelítés együtt azt támasztja alá, hogy a technológiai reziliencia szervezeti oldala nem redukálható incidenskezelési eljárásokra: a döntési struktúra, a tanulási mechanizmus, a tudásáramlás és az erőforrások újrakonfigurálásának képessége egyaránt meghatározza, hogy a technológiai lehetőségek ténylegesen adaptív teljesítménnyé alakulnak-e.

A **Safety-II logika további tudományos értéke**, hogy a tanulás forrását is kiszélesíti. A hagyományos incidensvizsgálat elsősorban a kudarcokból tanul, miközben a reziliencia szempontjából ugyanolyan fontos annak megértése, hogy a rendszer miként képes nap mint nap sikeresen kompenzálni a hiányos információt, a korlátozott erőforrásokat és a változó feltételeket. Az ilyen sikeres adaptációk feltárása lehetőséget teremt a rejtett

szervezeti és technológiai képességek azonosítására. A későbbi mérési keretrendszer szempontjából ez azért lényeges, mert a reziliencia nem mérhető kizárólag kiesési idővel vagy incidensszámmal; vizsgálni kell az anticipáció, az észlelés, az adaptáció, a stabilizáció és a tanulás minőségét is.

1.5 Kritikus infrastruktúrák, interdependencia és technológiai függőségek

1.5.1 A kritikus infrastruktúrák, mint kölcsönösen függő rendszerek

A kritikus infrastruktúrák technológiai rezilienciájának vizsgálata azért különösen fontos, mert e rendszerek működése közvetlenül kapcsolódik az állam, a gazdaság és a társadalom alapvető funkcióihoz. A kritikus infrastruktúrák ugyanakkor nem izolált rendszerek. Energiaellátás, elektronikus hírközlés, közlekedés, pénzügyi szolgáltatások, egészségügy és kormányzati rendszerek kölcsönösen támaszkodnak egymás szolgáltatásaira. A hálózati megközelítés szerint a rendszer ellenálló képessége ezért nem kizárólag az egyes csomópontok robusztusságától, hanem a kapcsolati struktúrától és a függőségek eloszlásától is függ [18].

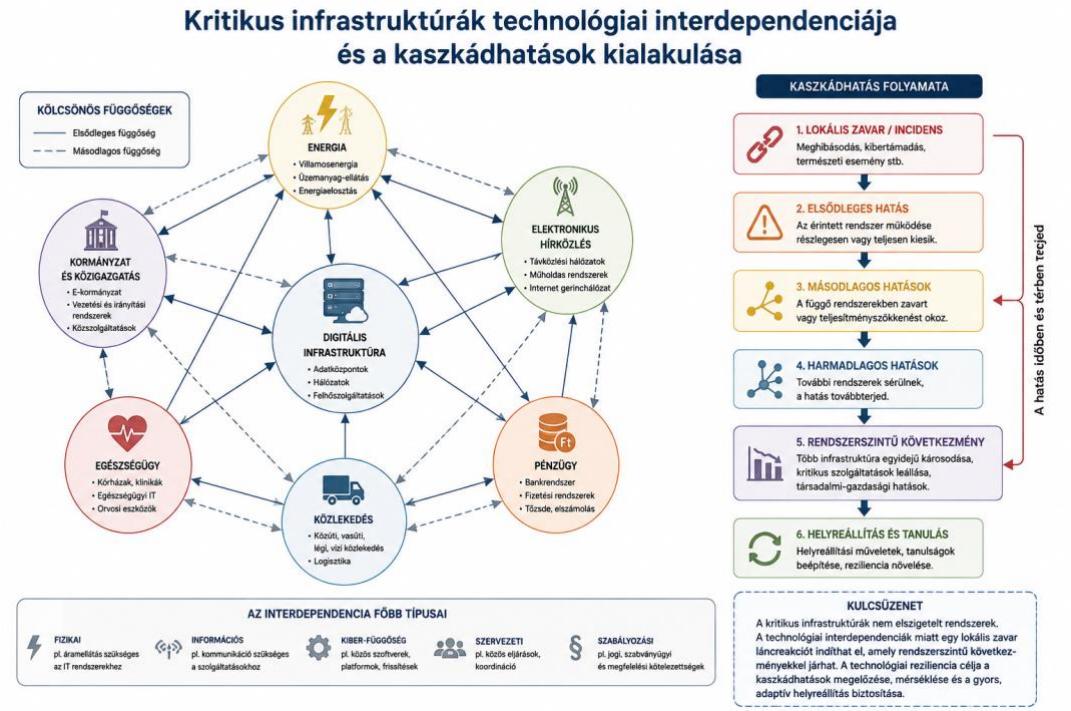
A digitális transzformáció e függőségeket tovább mélyítette. Korábban fizikailag elkülönülő infrastruktúrák közös telekommunikációs hálózatokra, felhőszolgáltatásokra, GNSS[15]-időszinkronizációra, adatközpontokra vagy azonos identitás- és hozzáféréskezelési szolgáltatásokra támaszkodhatnak. E közös szolgáltatások hatékonyságot és interoperabilitást teremtenek, ugyanakkor koncentrációs kockázatot is növelnek. Egy közös függőség meghibásodása több ágazatban egyidejű működési zavart idézhet elő.

A technológiai reziliencia szempontjából ezért a **kritikus infrastruktúra védelme nem értelmezhető kizárólag eszközvédelemként**. Szükséges a függőségi térkép, a kritikus szolgáltatások, a kölcsönös erőforrás-függések és a láncreakciós hatások vizsgálata. A rendszerkockázat sok esetben nem ott jelentkezik, ahol a legerősebb fenyegetés vagy a leggyengébb komponens található, hanem ott, ahol egy látszólag kis jelentőségű kapcsolat több kritikus folyamat közös előfeltételévé válik. [84]

A **kritikus infrastruktúrák hálózatosodása emellett megváltoztatja a védelem felelősségi logikáját** is. Ha egy infrastruktúra működése más ágazatok szolgáltatásaitól függ, akkor saját rezilienciáját részben olyan szervezetek és technológiai rendszerek határozzák meg, amelyek felett nincs közvetlen irányítási joga. Ez a probléma egyértelműen

[15] GNSS: Global Navigation Satellite System: globális műholdas navigációs rendszer.

túlmutat a hagyományos szervezeti kockázatkezelésen, és koordinációs, szabályozási, valamint közpolitikai kérdéssé válik.



1.4. ábra: Kritikus infrastruktúrák technológiai interdependenciája és a kaszkádhatások kialakulása (saját szerkesztés)

1.5.2 Ellátási láncok, platformfüggőség és koncentrációs kockázat

A technológiai rendszerek működése egyre nagyobb mértékben külső beszállítókra és szolgáltatói ökoszisztémákra épül. A beszállítói reziliencia szakirodalma rámutat, hogy a vállalati vagy intézményi működés ellenálló képességét nemcsak a belső erőforrások, hanem a kritikus partnerek rendelkezésre állása, helyettesíthetősége és adaptációs képessége is meghatározza [19]. A diverzifikáció, a beszállítói láthatóság és az alternatív beszerzési útvonalak ezért technológiai reziliencia-képességként értelmezhetők.

A digitális szolgáltatások esetében a függőség gyakran nem hagyományos ellátási láncként jelenik meg. Felhőplatformok, hyperscaler szolgáltatók, szoftverkönyvtárak, identitásszolgáltatások és külső menedzselt biztonsági szolgáltatók olyan alapvető komponensekké válhatnak, amelyek kiesése vagy kompromittálódása több, egymástól egyébként független szervezetet érint. A megosztott felelősségi modellek ráadásul elmoshatják a döntési és felelősségi határokat: a technikai kontrollok egy része a szolgáltatónál, más része az ügyfélnél, a kockázati felelősség pedig a teljes ökoszisztémában oszlik meg.

A koncentrációs kockázat szempontjából a technológiai szuverenitás fogalma is relevánssá válik, de e kérdés részletes geopolitikai vizsgálata a 2. fejezet feladata. Az 1. fejezet elméleti szintjén annyi rögzíthető, hogy a reziliencia és a függőség nem egymást kizáró fogalmak. A modern technológiai rendszerek szükségszerűen egymásra támaszkodnak; a reziliencia célja ezért nem az autarkia, hanem a kritikus függőségek ismerete, kontrollja, diverzifikálása és szükség esetén helyettesíthetősége.

A beszállítói és platformfüggőségek továbbá azt is megmutatják, hogy a reziliencia időhorizontja nem korlátozható az incidensreagálás időszakára. A kritikus komponensek elérhetősége, az alkatrész-utánpótlás, a gyártói támogatás, a szoftverfrissítések és a kompetenciák fenntarthatósága többéves életciklusban értelmezhető. A technológiai reziliencia tehát a működésfenntartás mellett technológiai életciklus- és függőségmenedzsmentet is feltételez. [96], [97].

1.5.3 Hazai kritikus információs infrastruktúra- és kiberbiztonsági gondolkodás

A technológiai reziliencia magyar szakmai kontextusának kialakításában meghatározó szerepet játszott a kiberbiztonság stratégiai dimenzióinak, valamint a kritikus és kritikus információs infrastruktúrák fogalmi rendszerének hazai feldolgozása. **Kovács László munkái a kiberbiztonságot nem kizárólag informatikai, hanem stratégiai és nemzetbiztonsági kérdésként értelmezik**, hangsúlyozva az állami felelősség, a szervezeti védelem és a kibertérben megjelenő függőségek kapcsolatát [20]. Ez a megközelítés közvetlenül kapcsolódik a technológiai reziliencia tágabb értelmezéséhez, mivel a digitális működőképességet az állami és társadalmi működés feltételévé emeli.

Haig Zsolt és Kovács László kritikus információs infrastruktúrákkal foglalkozó munkái arra mutatnak rá, hogy a fizikai és információs infrastruktúrák közötti határ fokozatosan elmosódik, és a kritikus szolgáltatások egyre nagyobb mértékben digitális vezérlésre, kommunikációra és információfeldolgozásra támaszkodnak [21]. A kritikus információs infrastruktúra fogalma ebben az értelemben nem egyszerűen informatikai rendszereket jelöl, hanem azokat az információs és kommunikációs komponenseket, amelyek más kritikus társadalmi funkciók működésének előfeltételei.

A **hazai szakirodalom stratégiai szemléletét** jól illusztrálja a **„Digitális Mohács" forgatókönyv,** amely a komplex kibertámadások nemzeti működőképességre gyakorolt lehetséges hatásait rendszerszinten értelmezte [22]. A forgatókönyv jelentősége nem annak konkrét technikai részleteiben, hanem abban áll, hogy korán rámutatott: a kibertámadás

következménye nem feltétlenül marad az informatikai rendszerek szintjén, hanem kiterjedhet kritikus szolgáltatásokra, intézményi működésre és társadalmi stabilitásra.

E hazai megközelítések a technológiai rezilienciát előkészítő fogalmi elemeket hordoznak: a technológiai függőségek stratégiai jelentőségét, a kritikus információs infrastruktúrák rendszerszerepét, az állami és szervezeti felelősség összekapcsolását, valamint a komplex kiberesemények nemzeti szintű következményeinek vizsgálatát. A doktori kutatás számára e szakirodalmi vonal azért fontos, mert bizonyítja, hogy a technológiai reziliencia integrált szemlélete nem idegen a magyar biztonságtudományi gondolkodástól, ugyanakkor a különálló technológiai, szervezeti és szabályozási tényezők egységes modellbe rendezése továbbra is kutatási feladat.

1.5.4 Függőségi láncok, ellátási ökoszisztémák és technológiai szuverenitás

A kritikus infrastruktúrák rezilienciájának vizsgálata a digitalizációval párhuzamosan fokozatosan kiterjedt az ellátási és szolgáltatási ökoszisztémákra is. A technológiai rendszer működőképessége ma már gyakran olyan komponensektől függ, amelyek felett a végfelhasználó szervezet nem rendelkezik közvetlen ellenőrzéssel: külső szoftverkönyvtárak, felhő- és adatközponti szolgáltatások, távközlési infrastruktúrák, beszállítói firmware-ek, licenc- és frissítési szolgáltatások, valamint globális hardver- és félvezető-ellátási láncok egyaránt a működés feltételeivé váltak. A reziliencia ezért a szervezeti határokon túlnyúló képességként értelmezendő, amelynek egyik kulcskérdése a kritikus függőségek láthatósága és kezelhetősége [19][20][21].

A beszállítói láncok sérülékenysége többféle mechanizmuson keresztül hat a technológiai rezilienciára. Egyrészt fizikai ellátási zavar következhet be, amikor egy kritikus alkatrész, eszköz vagy nyersanyag nem áll rendelkezésre. Másrészt digitális ellátásilánc-kockázat jelenhet meg, amikor egy külső komponens vagy szolgáltatás sérülékenysége közvetlenül beépül a felhasználó rendszerébe. Harmadrészt stratégiai függőség alakulhat ki, amikor a működés hosszú távon egyetlen technológiai ökoszisztémához, gyártóhoz vagy platformhoz kötődik. **Sheffi és Rice a reziliens vállalat szempontjából már korán hangsúlyozták** a rugalmasság, a beszállítói diverzitás és az ellátási lánc láthatóságának jelentőségét [19]. A digitális gazdaságban e logika kiegészül a szoftveres és szolgáltatási függőségekkel.

A technológiai szuverenitás fogalma e problémakör stratégiai kiterjesztéseként értelmezhető. A szuverenitás ebben az összefüggésben nem teljes technológiai önellátást vagy autarkiát jelent, hanem annak képességét, hogy egy szervezet vagy állam ismerje

kritikus függőségeit, képes legyen azok kockázatait értékelni, és szükség esetén alternatív működési lehetőségeket fenntartani. A technológiai reziliencia tehát nem a függőségek megszüntetésére, hanem azok tudatos, kockázatalapú irányítására törekszik. Ehhez szükséges a kritikus szolgáltatások és beszállítók azonosítása, a helyettesíthetőség vizsgálata, a szerződéses és technikai kilépési lehetőségek biztosítása, valamint az alternatív működési módok rendszeres tesztelése [20][24][25][26].

A platformfüggőség különösen összetett formája a koncentrációs kockázat. A felhőszolgáltatások, identitáskezelési rendszerek, vállalati szoftverplatformok és globális kommunikációs szolgáltatások gazdaságossága természetes módon ösztönzi a konszolidációt. Ugyanakkor, ha számos kritikus szervezet azonos technológiai szolgáltatóra támaszkodik, egyetlen szolgáltatói hiba vagy támadás több ágazatban egyidejű zavarokat okozhat. A szervezeti szinten megfelelőnek tűnő kockázatkezelés ezért rendszerszinten elégtelenné válhat. Ez az ellentmondás ismét azt támasztja alá, hogy a technológiai rezilienciát a szervezet, az infrastruktúra és az ökoszisztéma egymásba ágyazott szintjein kell értelmezni [30][31].

A technológiai függőségek kezelése a magyar és európai kritikusinfrastruktúra-védelmi gondolkodásban is egyre nagyobb hangsúlyt kap. A NIS2 [16] a beszállítói és szolgáltatói kockázatokat a kiberkockázat-kezelés részévé teszi, míg a CER [17] a kritikus szervezetek működési rezilienciáját szélesebb, fizikai és szervezeti kitettségeket is magában foglaló megközelítésben kezeli [25][26]. A két szabályozási logika együtt arra utal, hogy a technológiai reziliencia intézményesülése egyre kevésbé szervezetközpontú, és egyre inkább hálózati, ellátási és interdependencia-szemléletű.

1.6 A reziliencia stratégiai és szabályozási intézményesülése

1.6.1 A reziliencia mint stratégiai képesség

A reziliencia fogalmának fejlődésében minőségi változást jelentett, amikor a fogalom a szervezeti és mérnöki szakirodalomból a nemzeti biztonsági és közpolitikai dokumentumokba is beépült. Ettől kezdve a reziliencia már nem csupán azt a kérdést írta le, hogy egy rendszer vagy szervezet miként reagál a zavarokra, hanem azt is, hogy az állam

[16] NIS2 – Network and Information Systems Directive 2; a hálózati és információs rendszerek biztonságáról szóló (EU) 2022/2555 irányelv.

[17] CER – Critical Entities Resilience Directive: a kritikus szervezetek rezilienciájáról szóló (EU) 2022/2557 irányelv.

milyen módon képes fenntartani alapvető funkcióit, kritikus szolgáltatásait és döntéshozatali képességét tartós, összetett válsághelyzetekben.

A **NATO 2022-es Stratégiai Koncepciója** a rezilienciát a kollektív védelem, a kritikus infrastruktúrák biztonsága és a társadalmak ellenálló képessége szempontjából is kiemelt jelentőségűnek tekinti [23]. A stratégiai szintű megközelítés lényege, hogy a katonai képességek önmagukban nem elegendők, ha az azokat támogató energiaellátás, kommunikáció, közlekedés, gazdasági infrastruktúra vagy civil intézményrendszer nem képes működését fenntartani. A technológiai reziliencia ilyen értelemben a nemzeti reziliencia technológiai alaprétegeként értelmezhető.

Az **OECD infrastruktúra-rezilienciával foglalkozó munkái** hasonló irányba mutatnak: a kritikus infrastruktúrák megbízhatósága mellett a kockázatok előrelátását, a rendszerszintű függőségek kezelését, az életciklus-szemléletet és az intézményi koordinációt hangsúlyozzák [24]. A reziliencia ezzel közpolitikai képességgé válik, amelyet tervezni, finanszírozni, értékelni és folyamatosan fejleszteni szükséges.

A stratégiai intézményesülés fontos következménye, hogy a reziliencia többé nem kizárólag egyes üzemeltetők belső döntése. A kritikus infrastruktúrák működése olyan közérdekű szolgáltatásokat érint, amelyek kiesése más ágazatokra és a nemzeti működőképességre is hatással van. Ez indokolja a szabályozási minimumkövetelményeket, az állami koordinációt, a jelentési kötelezettségeket, a gyakorlatokat és a felügyeleti mechanizmusokat.

1.6.2 Az Európai Unió reziliencia- és kiberbiztonsági szabályozási logikája

Az **Európai Unió szabályozása** jól szemlélteti a reziliencia intézményesülését. A NIS2 [25] jelentősége a jelen kutatás szempontjából abban áll, hogy a kiberbiztonsági kockázatok kezelését már nem kizárólag technikai feladatként kezeli, hanem a vezetői felelősséghez, az üzletmenet fenntartásához, az incidenskezeléshez és a beszállítói kapcsolatok kezeléséhez is köti. Ez jól szemlélteti a technológiai és szervezeti dimenziók szabályozási összekapcsolódását.

A kritikus szervezetek rezilienciájáról szóló **CER irányelv** a fizikai és működési reziliencia oldaláról egészíti ki ezt a logikát [26]. A két szabályozási terület együtt azt mutatja, hogy a kritikus szolgáltatások ellenálló képessége nem osztható fel egyszerűen fizikai és digitális biztonságra. A kritikus szervezetnek egyszerre kell kezelnie a fizikai, technológiai, humán, beszállítói és szervezeti kockázatokat, valamint biztosítania a működés folytonosságát.

A **Cyber Resilience Act** [27] a digitális elemeket tartalmazó termékek biztonságát a fejlesztéstől az üzemeltetési támogatásig terjedő felelősségi rendszerben kezeli. A technológiai reziliencia szempontjából ennek fő következménye, hogy az üzemeltető szervezet működőképessége részben a beszállító sérülékenység-kezelési, frissítési és támogatási képességétől is függ. A termékbiztonság ezért a tágabb technológiai és szervezeti reziliencia egyik külső feltételévé válik.

Az európai szabályozási logika három irányban tágítja a reziliencia értelmezését: a technikai kontrolloktól a vezetői és szervezeti felelősség felé; az egyedi rendszerektől az ellátási lánc és a termék-életciklus felé; valamint a kiberbiztonságtól a kritikus funkciók teljes működési rezilienciája felé. A megfelelőség ugyanakkor önmagában nem jelent rezilienciát. Egy szervezet teljesítheti a formális követelményeket, miközben döntési sebessége, tanulási képessége vagy tényleges adaptációja alacsony marad. A szabályozás ezért a reziliencia minimumfeltételeit teremti meg, de nem helyettesíti a rendszer valós alkalmazkodóképességét.

1.6.3 Magyar kiberstratégiai és szabályozási kontextus

A **hazai kiberbiztonsági gondolkodásban** a stratégiai megközelítés már a digitális függőségek gyors növekedésének korai szakaszában megjelent. **Kovács László a nemzeti kiberbiztonsági stratégia kialakításának kérdését** olyan keretben tárgyalja, amelyben a technológiai kitettség, az állami működés, a társadalmi függőség és a biztonságpolitikai érdek egymással összekapcsolódik [28]. Ez a megközelítés közel áll a technológiai reziliencia logikájához, mivel a kibertér biztonságát nem egyetlen szervezet technikai ügyeként, hanem nemzeti szintű koordinációs problémaként kezeli.

Krasznay Csaba munkái a magyar kiberbiztonsági és digitális átalakulási környezet kapcsán szintén hangsúlyozzák, hogy a technológiai fejlődés szervezeti, szabályozási és humán alkalmazkodást követel meg [29]. A reziliencia szempontjából e felismerés azért lényeges, mert a technológiai innováció és a szabályozási adaptáció közötti időbeli különbség önmagában kockázati tényező lehet. Ha a szervezeti és intézményi környezet lassabban változik, mint a technológia, az új képességek nem feltétlenül hasznosulnak biztonságosan és hatékonyan.

A **magyar kontextusban a kritikus információs infrastruktúrák kijelölése és védelme**, a kiberbiztonsági felelősségi rendszer, valamint az állami és szolgáltatói együttműködés olyan intézményi alapokat jelent, amelyekre a technológiai reziliencia későbbi, integrált értelmezése építhet. A jelen kutatás szempontjából azonban fontos

elhatárolni a jogszabályi megfelelést a tudományos modelltől. A szabályozás konkrét kötelezettségeket és intézményi felelősségeket határoz meg; a technológiai reziliencia elméleti modelljének viszont azt kell megmagyaráznia, hogy e technológiai, szervezeti és szabályozási tényezők miként hatnak egymásra és hogyan alakítják a rendszer tényleges alkalmazkodóképességét.

1.6.4 A megfelelőségtől a tényleges rezilienciáig: governance és adaptív szabályozás

A reziliencia szabályozási intézményesülése szükségszerűen felveti a megfelelőség és a tényleges alkalmazkodóképesség kapcsolatának kérdését. A szabályozás olyan minimumkövetelményeket, felelősségi rendet és ellenőrzési mechanizmusokat hoz létre, amelyek nélkül a kritikus rendszerek védelme esetleges és szervezetfüggő maradna. Ugyanakkor a megfelelőség önmagában nem azonos a rezilienciával. Egy szervezet formálisan teljesítheti a dokumentációs, audit- vagy kontrollkövetelményeket úgy is, hogy valós válsághelyzetben lassú döntéshozatal, rossz információáramlás, nem tesztelt helyreállítási folyamat vagy beszállítói függőség miatt működése mégis sérülékeny marad [4][5][25][26].

A compliance és a resilience közötti különbség elsősorban időbeliségükben és funkciójukban ragadható meg. A megfelelőség azt vizsgálja, hogy egy adott időpontban vagy auditciklusban fennállnak-e az előírt kontrollok és folyamatok. A reziliencia ezzel szemben azt vizsgálja, hogy a rendszer változó körülmények között képes-e ezeket a képességeket ténylegesen működésbe hozni, összehangolni és szükség esetén módosítani. Egy incidenskezelési terv megléte megfelelőségi szempontból értékelhető; annak gyorsasága, döntési minősége, a technikai és szervezeti reakció összehangoltsága, valamint a tanulságok beépítése már reziliencia-kérdés. Ezért a technológiai reziliencia governance-a nem pusztán kontrollok létrehozását, hanem azok dinamikus működtetését is megköveteli.

A modern szabályozási környezetben ezért egyre nagyobb jelentőséget kap a kockázatalapú és adaptív irányítás. A NIS2, a CER és a Cyber Resilience Act eltérő tárgyi hatállyal, de közös irányba mozdul: a biztonságot nem kizárólag egyszeri megfelelőségi állapotként, hanem életcikluson át fenntartandó irányítási felelősségként kezelik [25][26][27]. Ez a megközelítés közelíti egymáshoz a jogi-szabályozási és a reziliencia elméleti logikát. A szervezetnek folyamatosan értékelnie kell kockázatait, incidenseit, függőségeit és képességeit, majd ezek alapján módosítania kell technológiai és szervezeti működését.

A **NATO rezilienciafelfogása** hasonlóan a folyamatos felkészültséget és a civil képességek fenntartását helyezi előtérbe. A **2021-es Strengthened Resilience Commitment** a rezilienciát a kollektív védelem és a hiteles elrettentés alapvető elemének tekinti, és hangsúlyozza a nemzeti felelősség, a kormányzati koordináció, a kritikus infrastruktúrák és a társadalmi működőképesség összekapcsolását [36]. A 2022-es NATO Strategic Concept e gondolatot már a stratégiai verseny, a technológiai változás és a hibrid fenyegetések környezetében helyezi el [23]. A technológiai reziliencia ebből következően olyan governance-képességként is értelmezhető, amely összeköti a technikai biztonságot a szervezeti és nemzeti döntéshozatallal.

A szabályozás adaptivitása ugyanakkor önálló kihívás. A technológiai innováció üteme sok esetben gyorsabb a jogalkotási és intézményi alkalmazkodásnál. A túl lassú szabályozási reakció biztonsági rést teremthet, a túl merev vagy túl korai szabályozás viszont korlátozhatja a szükséges innovációt. A technológiai reziliencia ezért olyan szabályozási környezetet feltételez, amely egyszerre biztosít stabil alapkövetelményeket és lehetőséget a kockázatokhoz igazodó módosításra. Ebből a szempontból a governance nem külső korlát, hanem a rendszer adaptív működésének egyik konstitutív eleme.

1.5. ábra: A technológiai reziliencia stratégiai és szabályozási intézményesülése (saját szerkesztés)

1.7 A technológiai reziliencia fogalmi szintézise és a kutatási rés

1.7.1 A technológiai reziliencia elhatárolása és munkadefiníciója

Az előző alfejezetek alapján megállapítható, hogy a **reziliencia fogalma a különböző tudományterületeken eltérő hangsúlyokat kapott, de közös magja jól azonosítható**. Az ökológiai megközelítés a funkcionális identitás fennmaradását és az adaptív változást; a pszichológiai megközelítés az erőforrások mozgósítását és a tanulást; a szervezeti kutatás az anticipációt, döntéshozatalt és intézményesített adaptációt; a reziliencia-mérnökség a kritikus funkciók fenntartását és kontrollált helyreállítást; a kiberreziliencia pedig a digitális kompromittálódás mellett is fenntartott működést emeli ki.

E közös elemek alapján a technológiai reziliencia nem azonos a technológiai megbízhatósággal. A megbízhatóság azt mutatja meg, hogy egy rendszer előírt körülmények között milyen valószínűséggel teljesíti funkcióját. A reziliencia ezzel szemben kifejezetten a változó, bizonytalan vagy kedvezőtlen körülmények közötti működésre irányul. Nem azonos a robusztussággal sem, mert a robusztusság elsődlegesen a változással szembeni ellenállást jelenti, míg a reziliencia az adaptív átalakulást is magában foglalja. A kiberbiztonság pedig a technológiai reziliencia nélkülözhetetlen részterülete, de nem fedi le a fizikai, szervezeti, beszállítói és szabályozási függőségeket. [101], [109], [110]

Hadtudományi értelmezésben a technológiai reziliencia ennek megfelelően a katonai képesség egyik feltételrendszere: annak képessége, hogy a katonai feladat végrehajtását támogató technológiai, szervezeti és intézményi rendszer ellenséges vagy nem szándékos zavarások mellett is fenntartsa a művelet szempontjából kritikus funkciókat, szükség esetén csökkentett működési szinten folytassa a feladat-végrehajtást, majd helyreállítsa és a tapasztalatok alapján adaptálja működését. E képesség nem vezethető vissza kizárólag az alkalmazott technológiára, mert tényleges eredményességét a működtető szervezet és az intézményi-szabályozási környezet is alakítja.

Ez a munkadefiníció szándékosan nem tartalmaz még formális dimenzióstruktúrát, indikátorokat vagy érettségi szinteket. Ezek kidolgozása a 3. fejezet saját tudományos feladata. Az 1. fejezet eredménye az a fogalmi premissza, hogy a technológiai reziliencia integrált szocio-technikai rendszerképességként értelmezendő, amelynek technikai, szervezeti és intézményi feltételei egymástól nem választhatók el.

1.7.2 A szakirodalmi fragmentáció mint kutatási probléma

A szakirodalom kritikai áttekintése ugyanakkor arra is rámutat, hogy a technológiai rezilienciához kapcsolódó tudományos eredmények jelentős része diszciplinárisan fragmentált. [88]. Az ökológiai és komplexitáselméleti megközelítések [1], [6], [7], [99] erős rendszerdinamikai alapot biztosítanak, de a technológiai governance kevésbé jelenik meg bennük. A szervezeti reziliencia szakirodalma [3]–[5] részletesen tárgyalja a vezetést, tanulást és alkalmazkodást, miközben a technológiai architektúrát jellemzően nem tekinti elsődleges elemzési egységnek. A reziliencia-mérnökség [12],[13],[103] a működési adaptációra és a rendszer viselkedésére helyezi a hangsúlyt, míg a kiberbiztonsági és szabályozási keretek elsősorban normatív és mérhetővé és értékelhetővé tehető követelményeket biztosítanak.

A fragmentáció problémája a gyakorlatban is megjelenik. Egy szervezet külön kezelheti az üzletmenet-folytonosságot, a kiberbiztonságot, a fizikai biztonságot, a beszállítói kockázatokat, a technológiai életciklust és a szabályozási megfelelést, miközben ugyanazon kritikus funkció működőképességét valamennyi terület egyidejűleg befolyásolja. E szakterületek különálló fejlesztése ezért nem garantál rendszerszintű rezilienciát.

A doktori kutatás első elméleti kutatási rése ebből vezethető le: a nemzetközi és hazai szakirodalomban a technológiai, szervezeti és szabályozási rezilienciaelemek egyaránt jelen vannak, de integrált kapcsolatuk és kölcsönhatásuk nem kellően mérhető és értékelhető. **A szakirodalom jelentős része vagy egy domináns elemzési szintet választ, vagy normatív követelményeket fogalmaz meg anélkül, hogy egységes magyarázó keretet teremtene a dimenziók közötti kapcsolatok vizsgálatára.**

A kutatás további fejezetei erre a résre épülnek. A 2. fejezet azt vizsgálja, hogy a XXI. század technikai, társadalmi és geopolitikai környezete milyen konkrét kihívásokat támaszt a rezilienciával szemben. A 3. fejezet ezekre az elméleti és környezeti megállapításokra támaszkodva dolgozza ki a technológiai reziliencia saját integrált modelljét és mérhetővé és értékelhetővé tételi keretét. A 4. fejezet pedig eltérő kritikus infrastruktúrák vizsgálatán keresztül értékeli a kialakított modell gyakorlati alkalmazhatóságát és stratégiai kiterjesztését.

Tudományterület	Meghatározó szerző/irányzat	Központi kérdés	Hozzájárulás a technológiai reziliencia értelmezéséhez
Ökológia	Holling	Hogyan marad fenn a rendszer zavarás után?	Adaptáció, több stabil állapot
Komplex rendszerek	Simon, Holland, Mitchell	Hogyan alakul ki rendszerszintű viselkedés?	Emergencia, nemlinearitás

Tudományterület	Meghatározó szerző/irányzat	Központi kérdés	Hozzájárulás a technológiai reziliencia értelmezéséhez
Szocio-technikai elmélet	Trist–Bamforth	Hogyan hat egymásra ember és technológia?	Technológiai és társadalmi alrendszerek integrációja
Reziliencia-mérnökség	Hollnagel, Woods, Leveson	Hogyan tartható fenn a működés változó körülmények között?	Adaptív működés
Szervezeti reziliencia	Lengnick-Hall, Duchek	Hogyan alkalmazkodik a szervezet?	Tanulás, vezetés, adaptáció
Kiberreziliencia	NIST, ENISA	Hogyan tartható fenn a digitális működés támadás esetén?	Ellenállás, helyreállítás, adaptáció
Kritikus infrastruktúrák	EU, NATO	Hogyan tarthatók fenn a kritikus társadalmi funkciók?	Interdependencia, szolgáltatásfolytonosság
Technológiai reziliencia	jelen kutatás	Hogyan integrálhatók ezek a megközelítések?	Átvezetés az integrált modellhez

1.2. táblázat. A technológiai rezilienciához kapcsolódó fő tudományos irányzatok és az azonosított kutatási rés (saját szerkesztés)

1.7.3 A fogalmi szintézis tudományos következményei és a kutatási kérdés mérhetővé és értékelhetővé tétele

A bemutatott tudományos fejlődési ív alapján a **technológiai reziliencia nem vezethető le egyetlen korábbi reziliencia elmélet közvetlen kiterjesztéséből**. Az ökológiai megközelítés a funkcionális fennmaradás és az adaptív változás logikáját adja [1]; a pszichológiai és szervezeti kutatások a tanulást, az erőforrások mobilizálását, az anticipációt és az adaptív döntéshozatalt emelik be [2][3][4]; a komplex rendszerek elmélete a kölcsönhatások és emergencia jelentőségét mutatja meg [6][7]; a reziliencia-mérnökség a működési variabilitás és adaptív teljesítmény elemzését teszi lehetővé [12][13]; a kritikus infrastruktúrák szakirodalma pedig az interdependenciákat és a rendszerek rendszere jellegét helyezi előtérbe [30][31]. E részmegközelítések együttesen olyan fogalmi teret hoznak létre, amelyben a technológiai reziliencia integrált rendszerképességként értelmezhető.

A **fogalmi szintézis második következménye**, hogy a technológiai reziliencia nem azonosítható egyetlen teljesítménymutatóval. A rendelkezésre állás, a helyreállítási idő, az incidensszám, a redundancia vagy a szabályozási megfelelőség önmagukban fontos indikátorok, de egyik sem képes megragadni a rendszer alkalmazkodóképességének teljességét. A reziliencia több rétegben jelenik meg: strukturális képességként a technológiai architektúrában; szervezeti képességként a döntéshozatalban és tanulásban; governance-képességként a felelősségi, szabályozási és stratégiai keretekben; valamint kapcsolati képességként az e rétegek közötti együttműködésben. Ez a felismerés módszertani indokot teremt a 3. fejezetben kialakított többdimenziós értékelési megközelítés számára.

Harmadik következményként a reziliencia elemzésében meg kell különböztetni a képességek meglétét és működésbe hozását. Egy szervezet rendelkezhet korszerű technológiával, képzett személyzettel és megfelelő szabályozási környezettel, mégis alacsony rezilienciát mutathat, ha e képességek között nincs megfelelő információáramlás, döntési kapcsolat vagy koordináció. A technológiai reziliencia ezért nem csupán erőforrás-, hanem kapcsolati probléma is. E megállapítás elméleti alapot ad annak a későbbi kutatási feltevésnek, hogy a rendszer teljes rezilienciáját gyakran nem a leggyengébb önálló dimenzió, hanem a dimenziók közötti elégtelen kapcsolat korlátozza.

Negyedik következményként a technológiai rezilienciát időben változó képességként kell kezelni. Az adaptációs sebesség, az új fenyegetések felismerése, a működési állapot stabilizálása és a tanulás intézményesítése legalább olyan fontos, mint a kiinduló rendszerállapot. A statikus megfelelőségi vagy megbízhatósági értékelés ezért csak részleges képet ad. A reziliencia dinamikus vizsgálata azt követeli meg, hogy az elemzés figyelembe vegye a zavar előtti anticipációt, a zavar alatti reagálást, a helyreállítást és az azt követő szervezeti-technológiai változást [4][12][13].

Ez teremti meg az elméleti átmenetet a később részletesen bemutatott BATR-ciklushoz, amely a technológiai rezilienciát négy, egymással összekapcsolódó és ciklikusan ismétlődő működési szakaszban értelmezi: felkészülés (Build), elnyelés (Absorb), átalakulás (Transform) és helyreállítás (Recover). A modell lényege, hogy a reziliencia nem egy egyszer elérhető statikus rendszerállapot, hanem folyamatos alkalmazkodási képesség: a rendszer a zavarokra való felkészüléstől azok hatásának elnyelésén és a szükséges működési átalakuláson keresztül jut el a helyreállításig, miközben az egyes ciklusok tapasztalatai visszacsatolódnak a következő felkészülési szakaszba. A BATR-ciklus ezért a technológiai reziliencia időbeli dinamikájának és adaptív jellegének mérhetővé és értékelhetővé tételára szolgál**.**

Mindezek alapján a **doktori kutatás elméleti kérdése pontosabban úgy fogalmazható meg, hogy milyen strukturális, szervezeti és irányítási feltételek együttese teszi lehetővé a komplex technológiai rendszerek számára alapvető funkcióik fenntartását, alkalmazkodó megújítását és hosszú távú fejlődőképességének megőrzését zavarások és gyors technológiai változások közepette**. A kérdés megválaszolásához nem elegendő az egyes részterületek külön vizsgálata; szükség van egy olyan integrált modellre, amely azonos fogalmi keretben képes kezelni a technológiai, szervezeti és szabályozási tényezőket, azok interdependenciáit és időbeli adaptációját. Az 1. fejezet ezzel kijelöli azt az elméleti problémateret, amelyet a 2. fejezet a stratégiai környezet

elemzésével konkretizál, a 3. fejezet modellként mérhetővé és értékelhetővé tesz, a 4. fejezet pedig empirikus-ágazati alkalmazással vizsgál.

1.8 Fejezetösszegzés

Az 1. fejezet a **technológiai reziliencia elméleti alapjait a reziliencia fogalmának tudományos evolúcióján keresztül rekonstruálta**. Az elemzés alapján a reziliencia jelentése fokozatosan mozdult el a stabilitás és helyreállítás kérdésétől az adaptív, tanuló és rendszerszintű működés irányába. Holling ökológiai rezilienciája a funkcionális identitás fennmaradását és a változás elnyelését állította középpontba; a pszichológiai és szervezeti megközelítések ehhez a tanulást, az erőforrás-mobilizációt, az anticipációt és az adaptív döntéshozatalt kapcsolták; a komplex rendszerelmélet pedig rámutatott arra, hogy a reziliencia kialakuló tulajdonságként a kapcsolatokból és visszacsatolásokból is származhat. [1]

A **szocio-technikai rendszerek és a reziliencia-mérnökség elmélete tette lehetővé** e felismerések közvetlen technológiai alkalmazását. A modern technológiai rendszerek működése nem választható el az emberi döntéshozataltól és a szervezeti folyamattól, miközben a komplex és szorosan csatolt architektúrákban a meghibásodások teljes kizárása nem reális. A kiberreziliencia ebből a szempontból fontos részterület, de a technológiai reziliencia ennél szélesebb fogalom, mert a digitális komponensek mellett a fizikai infrastruktúrákat, a szervezeti működést, a beszállítói ökoszisztémát és a szabályozási környezetet is magában foglalja.

A kritikus infrastruktúrák és a hazai kiberbiztonsági **szakirodalom vizsgálata megerősítette**, hogy a digitális függőségek és a kritikus információs infrastruktúrák védelme nem szűkíthető technikai kérdésre. A **magyar szakmai gondolkodásban** is korán megjelent a kiberbiztonság stratégiai, nemzetbiztonsági és infrastruktúra-szintű értelmezése. **A NATO és az Európai Unió szabályozási fejlődése** ezt az irányt intézményesítette: a rezilienciát a vezetői felelősséggel, kockázatkezeléssel, ellátási lánccal, üzletmenet-folytonossággal és kritikus funkciókkal kapcsolta össze. [23][25][26][36]

A **fejezet legfontosabb elméleti következtetése**, hogy a technológiai reziliencia integrált szocio-technikai rendszerképességként értelmezendő. A technikai robusztusság, a kiberbiztonság, a szervezeti tanulás és a szabályozási megfelelőség önmagukban nem biztosítanak magas rezilienciát. A tényleges ellenálló és alkalmazkodó képesség e tényezők összehangolt működéséből jön létre. E felismerés kijelöli a kutatási rést és megteremti a 2. fejezethez vezető átmenetet: a következő lépés annak vizsgálata, hogy a XXI. század

technológiai, társadalmi és stratégiai környezete milyen feltételek között teszi szükségessé e rendszerképesség tudatos fejlesztését.

2. fejezet. A XXI. század technikai, társadalmi és stratégiai kihívásai a technológiai reziliencia környezetében

2.1 A fejezet célja és kutatási megközelítése

Az 1. fejezetben rekonstruált elméleti fejlődési ív alapján a technológiai reziliencia nem statikus állapot, hanem a komplex szocio-technikai rendszerek azon képessége, amely lehetővé teszi a zavarások előzetes érzékelését, hatásuk elnyelését vagy korlátozását, a kritikus funkciók fenntartását, a működés szükség szerinti újrakonfigurálását és a tapasztalatok visszacsatolását. A jelen fejezet ennek az elméleti premisszának a környezeti feltételeit vizsgálja. A cél nem újabb reziliencia-definíció megalkotása, hanem annak feltárása, hogy a XXI. század technológiai, társadalmi, gazdasági és biztonsági folyamatai milyen módon változtatják meg a reziliens működés követelményeit. A fejezet ezért az elméleti alapozás és a 3. fejezetben végrehajtott modellalkotás közötti közvetítő szerepet tölti be.

A vizsgálat stratégiai környezet-elemzésre és kritikai dokumentumszintézisre épül. Elsődleges forrásként a **NATO Strategic Foresight Analysis 2023** dokumentumát alkalmazom, amely a 2040-ig tartó időszak biztonsági környezetének fő változóit és egymással összefüggő trendjeit rendszerezi [37]. E keretet egészíti ki a NATO 2022 Strategic Concept, amely a szövetségi biztonsági környezetet a stratégiai versengés, a hibrid fenyegetések, a kibertér, az űr és a kritikus infrastruktúrák oldaláról értelmezi [23], valamint a **NATO Warfighting Capstone Concept**, amely a jövő műveleti környezetében a többdoménes működést, az információs fölényt és a döntési előnyt hangsúlyozza [38]. A technológiai fejlődés hosszabb távú értelmezéséhez a **NATO Science and Technology Organization 2023–2043 közötti technológiai trendjelentése** is kapcsolódik [39].

A fejezet elemzési logikája abból indul ki, hogy a technológiai rezilienciát alakító kihívások nem különálló kockázatok. A mesterséges intelligencia például egyszerre jelent technológiai gyorsulást, új támadási felületet, humán kompetenciakihívást, szabályozási problémát és stratégiai függőséget. Ugyanez igaz a felhőszolgáltatásokra, a félvezetőkre, a műholdas szolgáltatásokra vagy az autonóm rendszerekre is. A vizsgálat ezért nem technológiai katalógust készít, hanem azokat a kölcsönhatásokat keresi, amelyekben egy technológiai változás szervezeti, társadalmi vagy szabályozási következményen keresztül rendszerszintű sérülékenységgé, illetve megfelelő irányítás esetén reziliencia-erősítő képességgé válhat.

A fejezet szerkezete ennek megfelelően négy elemzési szintet kapcsol össze. Elsőként a stratégiai környezet fő karakterjegyeit – a tartós versengést, a technológiai gyorsulást, a hiperösszekapcsoltságot és a bizonytalanságot – azonosítja. Ezt követően a technológiai kihívások, majd a társadalmi és szervezeti alkalmazkodás problémái kerülnek elemzésre. Harmadik szinten a szabályozási és governance-környezetet vizsgálom, végül pedig a kritikus infrastruktúrák, a védelem és a nemzeti reziliencia szempontjából foglalom össze a következményeket. A fejezet végén kialakított stratégiai szintézis már közvetlenül előkészíti a 3. fejezet saját modelljének dimenzióit, de még nem mérhetővé és értékelhetővé teszi azokat.

2.1. Ábra: A 2. fejezet elemzési logikája: környezeti kihívásoktól a reziliencia-követelményekig (saját szerkesztés)

2.2 A XXI. századi stratégiai környezet reziliencia-szempontú karaktere

2.2.1 Tartós versengés és a béke–válság–konfliktus határainak elmosódása

A technológiai reziliencia stratégiai jelentőségét alapvetően növeli, hogy a biztonsági környezetben egyre kevésbé választható szét élesen a béke, a válság és a fegyveres konfliktus

időszaka. A NATO SFA[18] 2023 a tartós versengést olyan állapotként írja le, amelyben az állami és nem állami szereplők folyamatosan próbálják befolyásolni egymás döntési szabadságát, technológiai lehetőségeit és társadalmi stabilitását [37]. E versengés jelentős része a hagyományos fegyveres küszöb alatt zajlik: kiberakciók, gazdasági nyomásgyakorlás, technológiai korlátozások, információs műveletek, ellátási láncok manipulációja és jogi-szabályozási eszközök egyaránt alkalmazhatók. A reziliencia ebből következően nem kizárólag válságkezelési képesség, hanem a mindennapi működésbe beépített stratégiai ellenálló képesség.

A 2022-es NATO Strategic Concept a hibrid eszközök, a kibertámadások, a rosszindulatú technológiai befolyásolás, valamint az energia- és más stratégiai függőségek szerepét a szövetségi biztonság szempontjából is kiemeli [23]. Ez a megközelítés a technológiai rendszerek üzemeltetését stratégiai térbe helyezi. Egy kommunikációs platform, felhőszolgáltatás vagy ipari irányítórendszer kiválasztása ezért nem kizárólag műszaki és gazdasági döntés, hanem hosszú távú függőségi viszonyt is létrehozhat. A technológiai reziliencia feladata ebben a környezetben a kritikus függőségek láthatóvá tétele, a stratégiai kitettségek csökkentése és olyan alternatív működési módok fenntartása, amelyek politikai vagy geopolitikai nyomás alatt is lehetővé teszik a kritikus funkciók biztosítását.

A tartós versengés másik következménye, hogy a támadó és védő fél közötti innovációs ciklus felgyorsul. A sérülékenységek, exploitok, mesterségesintelligencia-modellek, dezinformációs technikák vagy drónrendszerek gyorsan adaptálhatók az ellenfél reakcióihoz. A statikus biztonsági kontroll ezért rövid idő alatt elveszítheti hatékonyságát. A technológiai reziliencia stratégiai értéke pontosan abban áll, hogy a működési képességet nem egyetlen konfiguráció védelméhez köti, hanem lehetővé teszi a fenyegetési környezet változásához igazodó újrakonfigurálást. A reziliens rendszer tehát nem a változatlanságot védi, hanem a kritikus funkció fennmaradását biztosítja változó technológiai és stratégiai feltételek között.

2.2.2 Technológiai gyorsulás és konvergencia

A **stratégiai környezet második alapvető jellemzője a technológiai fejlődés gyorsulása és a korábban elkülönülő technológiai területek konvergenciája**. A NATO

[18] SFA: Strategic Foresight Analysis; A NATO kétévente kiadott stratégiai elemzése.

STO[19] a mesterséges intelligenciát, az autonóm rendszereket, a kvantumtechnológiát, a biotechnológiát, a világűrhöz kapcsolódó technológiákat, a fejlett anyagokat és az új generációs kommunikációt egymást erősítő fejlődési pályákként kezeli [39]. A konvergencia következtében egyetlen technológiai áttörés több ágazatban és több műveleti doménben is gyorsan megjelenhet. Ez növeli az innováció hasznát, ugyanakkor lerövidíti azt az időt, amely a szervezetek és szabályozók rendelkezésére áll az új kockázatok megértésére és kezelésére.

A **technológiai gyorsulás a reziliencia szempontjából időbeli problémát teremt**. A hardver- és szoftveréletciklusok, a szervezeti képzési ciklusok, a beszerzési eljárások és a jogalkotás sebessége eltér egymástól. Egy szervezet technológiai architektúrája akár hónapok alatt jelentősen változhat, miközben a kompetenciarendszer és a szabályozási környezet csak évek alatt alkalmazkodik. A reziliencia egyik kritikus pontja ezért az eltérő alkalmazkodási sebességek összehangolása. Ha a technológiai változás gyorsabb a szervezeti tanulásnál, a rendszer kihasználatlan képességeket és új hibamódokat halmoz fel; ha a szabályozás nem tud lépést tartani, bizonytalan felelősségi és kockázati tér alakul ki.

A gyorsulás egyben növeli a technikai adósság és az örökölt rendszerek jelentőségét. **Kruchten, Nord és Ozkaya szerint a rövid távú fejlesztési kompromisszumok** később strukturális költségként és karbantartási kockázatként jelennek meg [9]. Kritikus infrastruktúrák esetében a legacy-rendszerek gyakran évtizedekig működnek, miközben környezetük, kommunikációs kapcsolataik és fenyegetettségük gyökeresen megváltozik. A technológiai reziliencia ezért nem az új technológia minél gyorsabb átvételét jelenti, hanem a technológiai portfólió olyan életciklus-menedzsmentjét, amely az innováció mellett a kompatibilitást, a visszaállíthatóságot, a karbantarthatóságot és a hosszú távú támogatást is figyelembe veszi.

2.2.3 Hiperösszekapcsoltság, komplexitás és bizonytalanság

A **digitalizáció harmadik meghatározó következménye** a rendszerek korábban nem tapasztalt mértékű összekapcsoltsága. A felhőszolgáltatások, az API-alapú integráció, az IoT[20] és ipari IoT, a közös identitáskezelési rendszerek, az adatmegosztási platformok és a műholdas szolgáltatások olyan funkcionális hálózatokat hoztak létre, amelyekben az egyes

[19] STO: Science and Technology Organization; magyarul: NATO Tudományos és Technológiai Szervezete.

[20] IoT: Internet of Things; magyarul: dolgok internete.

szervezetek saját működése jelentős részben külső infrastruktúráktól függ. **Rinaldi, Peerenboom és Kelly klasszikus interdependencia-modellje** szerint a kritikus infrastruktúrák fizikai, kiber-, földrajzi és logikai függőségeken keresztül kölcsönösen befolyásolják egymást [30]. A digitális transzformáció ezt a kapcsolatstruktúrát tovább sűrítette.

Ouyang áttekintése rámutat, hogy az interdependens infrastruktúrák viselkedése nemlineáris, és a zavarások hatása időbeli késleltetéseken, visszacsatolásokon és másodlagos következményeken keresztül erősödhet fel [31]. Ez a reziliencia szempontjából alapvető: a működési zavar forrása és megjelenési helye gyakran eltér egymástól. Egy kommunikációs kiesés mögött energiaellátási probléma, egy pénzügyi szolgáltatás fennakadása mögött felhő- vagy identitásszolgáltatási hiba, egy közlekedési rendszer degradációja mögött GNSS- vagy adatkapcsolati probléma állhat. A rezilienciaelemzésnek ezért a komponensek mellett a kapcsolatokat és a közös függőségeket is vizsgálnia kell.

A komplexitás ugyanakkor nem csupán technikai tulajdonság. A rendszerben részt vevő szervezetek eltérő célokkal, felelősségekkel, jogi kötelezettségekkel és döntési ciklusokkal rendelkeznek. Ez különösen a kritikus infrastruktúrák és a civil-katonai ökoszisztémák esetében fontos, ahol a magasabb szintű funkció több, részben autonóm rendszer együttműködéséből áll elő. A technológiai reziliencia ilyen környezetben rendszer-a-rendszerekben képesség: interoperabilitást, közös helyzetértékelést, függőségtérképezést, incidens-koordinációt és rendszeres több szereplős gyakoroltatást igényel.

Stratégiai környezeti jellemző	Fő mechanizmus	Tipikus sérülékenység	Reziliencia-követelmény	Kapcsolódó forrás
Tartós versengés	Küszöb alatti és hibrid nyomásgyakorlás	Függőségek politikai kihasználása	Alternatív működés, diverzifikáció, gyors adaptáció	[37][23]
Technológiai gyorsulás	Rövidülő innovációs és támadás-védelem ciklus	Szervezeti és szabályozási lemaradás	Életciklus-menedzsment, gyors tanulás	[39][9]
Hiperösszekapcsoltság	Fizikai, digitális és szolgáltatási interdependencia	Kaszkád- és koncentrációs kockázat	Függőségtérkép, modularitás, alternatív útvonalak	[30][31]
Bizonytalanság	Nemlineáris, nehezen előrejelezhető hatások	Statikus tervek elégtelensége	Forgatókönyv-alapú felkészülés, adaptív governance	[37][38]

2.1. táblázat: a XXI. századi stratégiai környezet fő jellemzői és reziliencia-következményei (saját szerkesztés)

2.2.4 Stratégiai meglepetés, bizonytalanság és a forgatókönyv-alapú felkészülés

A XXI. századi stratégiai környezet egyik meghatározó sajátossága, hogy a **nagy hatású zavarok egy része nem jelezhető előre megfelelő pontossággal**. A technológiai reziliencia szempontjából **ezért veszélyes az a tervezési logika, amely kizárólag a korábban már bekövetkezett incidensek megismétlődésére készül**. Az összekapcsolt rendszerekben új technológiák, új szereplők és új függőségek olyan eseménykombinációkat hozhatnak létre, amelyeknek nincs közvetlen történeti analógiája. A reziliens rendszernek ezért nem minden lehetséges eseményre kell részletes tervvel rendelkeznie, hanem olyan általános adaptív képességekkel, amelyek ismeretlen vagy részben ismert helyzetben is működésbe hozhatók.

A **forgatókönyv-alapú tervezés ebben a környezetben nem jövőjóslás**, hanem a döntési és technológiai feltételezések tesztelése. A forgatókönyvek segítségével feltárható, hogy milyen függőségek válnak kritikussá egyidejű energia-, kommunikációs és beszállítói zavar esetén, mely döntésekhez hiányzik megfelelő információ, és hol nincs alternatív működési útvonal. A NATO stratégiai előretekintési megközelítése [37] éppen ezért a trendek egyszerű extrapolációja helyett alternatív jövőképek és bizonytalanságok vizsgálatára épül. A technológiai reziliencia számára a forgatókönyv értéke abban áll, hogy még a zavar előtt láthatóvá teszi a rendszer rejtett feltételezéseit.

A stratégiai meglepetés kezelése szervezeti szempontból is fontos. A túl részletes, egyetlen eseménysorra optimalizált terv hamis biztonságérzetet teremthet, ha a tényleges helyzet eltér a feltételezettől. A reziliens szervezet ezért a konkrét eljárások mellett döntési elveket, prioritásokat és küszöbértékeket is meghatároz: mely funkciókat kell minden körülmények között fenntartani, milyen feltételekkel fogadható el degradált működés, mikor kell alternatív architektúrára áttérni, és mely döntések delegálhatók. Ezzel a bizonytalanság nem megszüntetendő anomáliává, hanem a tervezés állandó paraméterévé válik.

2.3 Technológiai kihívások a konvergens és adatvezérelt rendszerek korában

2.3.1 Kiberreziliencia és az IT/OT konvergencia

Hadtudományi szempontból az alábbi technológiai kihívások jelentőségét nem önmagukban, hanem a katonai képességekre gyakorolt hatásuk alapján szükséges értékelni. A kiber-, kommunikációs, PNT-, energia-, felhő- vagy ellátásilánc-függőség akkor válik katonai jelentőségű sérülékenységgé, ha annak kihasználása vagy kiesése

korlátozza a vezetést és irányítást, csökkenti a helyzetismeretet, lassítja a döntéshozatalt, akadályozza az erők mozgatását és ellátását, vagy más módon csökkenti a műveleti feladat végrehajthatóságát. A technológiai reziliencia ezért a jelen fejezetben a műveleti szabadság fenntartásának egyik feltételeként jelenik meg.

A **kiberfenyegetések a technológiai reziliencia legközvetlenebb, de nem kizárólagos kihívásai**. A hálózatba kapcsolt digitális rendszerek esetében a támadó számára nem szükséges az infrastruktúra fizikai megsemmisítése; elegendő lehet az adatok integritásának, a hozzáférésnek, az időszinkronizációnak vagy az irányítási folyamatnak a megzavarása. A NIST Cybersecurity Framework 2.0 a kiberkockázat-kezelést a Govern, Identify, Protect, Detect, Respond és Recover funkciók egységes rendszerében kezeli [40], [107]. A Govern funkció kiemelése különösen fontos a technológiai reziliencia számára, mert a kiberbiztonságot vezetői és szervezeti felelősséggel kapcsolja össze.

A **jelen kutatás a NIST CSF[21] funkcionális struktúráját** nem technológiai rezilienciamodellként veszi át, hanem annak példájaként értelmezi, hogy a korszerű kiberbiztonsági keretekben a technikai kontrollok és a governance egyre szorosabban összekapcsolódnak.

Az **ENISA fenyegetési jelentései azt mutatják**, hogy a zsarolóvírusok, a szolgáltatásmegtagadási támadások, a social engineering, az ellátási lánc kompromittálása és az adatokkal kapcsolatos fenyegetések továbbra is jelentős kockázatot jelentenek [41]. Kritikus infrastruktúrákban azonban az informatikai és üzemeltetési technológiai rendszerek konvergenciája miatt a kiberesemény fizikai következményekkel is járhat. Az OT-rendszerek hosszú életciklusa, a korlátozott frissíthetőség, a folyamatos rendelkezésre állási követelmény és a gyártói függőség olyan sajátosságok, amelyek miatt a hagyományos IT-biztonsági logika önmagában nem elegendő.

A reaktív incidenskezelés mellett ezért egyre nagyobb jelentősége van a proaktív fenyegetésfelderítésnek. **Gyebnár Gergő szakmai és kutatási munkáiban** a threat hunting, a technikai fenyegetési intelligencia és a detekciós képességek gyakorlati oldalát vizsgálja; **Magyar Sándorral közös munkájuk a technikai threat intelligence indikátorok** felhasználását elemzi [78]. Ez a megközelítés jól illeszkedik a technológiai reziliencia anticipációs logikájához: a szervezet nem kizárólag bekövetkezett incidensekre reagál, hanem aktívan keresi a kompromittálódás, az anomáliák és az ellenérdekelt jelenlét korai jeleit.

[21] CSF: Cybersecurity Framework; kiberbiztonsági keretrendszer.

A reziliens kiber- és OT-architektúra ezért a megelőző védelem mellett a kompromittálódás feltételezésére épül. E szemlélet része a szegmentáció, a minimális jogosultság, a folyamatos monitorozás, a biztonságos mentés, a helyreállíthatóság rendszeres tesztelése, az alternatív üzemmódok és a manuális beavatkozási lehetőség. A threat hunting logikája ebből a szempontból nem egyszerűen kibervédelmi technika, hanem rezilienciafilozófia: abból indul ki, hogy a kompromittálódás lehetősége reális, ezért a szervezetnek aktívan kell keresnie a rejtett jelenlét és a rendellenes működés jeleit.

A hazai kiberbiztonsági és hadtudományi szakirodalom ugyanezt a problémát több, egymást kiegészítő nézőpontból tárgyalja. **Kovács László a kiberbiztonság stratégiai értelmezésében, majd a kiberműveleti képességek vizsgálatában hangsúlyozza**, hogy a kibertér biztonsága szabályozási, szervezeti és műveleti tevékenységek összehangolt rendszerét igényli [20][48]. **Haig Zsolt az információs műveletek kibertéri értelmezésével tovább tágítja** ezt a megközelítést: a kibertér fizikai, információs és kognitív rétegei közötti kapcsolat miatt a technikai védelem nem választható el az információs és döntési folyamatok védelmétől [49][50]. E hazai megközelítések közvetlenül támogatják a jelen kutatás azon állítását, hogy a technológiai reziliencia nem szűkíthető le informatikai rendelkezésre állásra vagy preventív kiberbiztonsági kontrollokra.

2.3.2 Mesterséges intelligencia, automatizáció és autonóm rendszerek

A mesterséges intelligencia a technológiai reziliencia szempontjából kettős természetű technológia. Egyrészt jelentősen javíthatja az észlelés, az előrejelzés és a döntéstámogatás képességét: nagy adatmennyiségek elemzésével korábban nem látható mintázatokat, rendellenességeket vagy meghibásodási trendeket azonosíthat. Másrészt az AI új függőségeket hoz létre az adatok, a modellek, a számítási kapacitás és a külső szolgáltatások irányába. A **NIST AI Risk Management Framework** az AI-rendszerek megbízhatóságát, biztonságát, átláthatóságát és kockázatkezelését teljes életciklusban értelmezi [42].

Az autonóm rendszerek esetében a reziliencia további kérdése a döntési autoritás és a degradált működés. Egy autonóm jármű, logisztikai UGV, drónrendszer vagy ipari automatizálási megoldás akkor tekinthető reziliensnek, ha kommunikációs zavar, GNSS-kiesés, szenzorhiba vagy részleges adatvesztés mellett is képes biztonságos, előre meghatározott korlátok közötti működésre. Ez szükségessé teszi a több szenzorra épülő navigációt, a lokális döntési képességet, a manuális felülbírálhatóságot, valamint a fail-safe és fail-operational megoldások tudatos szétválasztását.

Az AI-alapú rendszerek új kockázata az, hogy a hiba nem feltétlenül reprodukálható egyszerűen vagy közvetlenül visszavezethető egyetlen komponensre. A modelltorzítás, az adatminőségi probléma, az ellenséges szándékú manipuláció és a nem várt környezeti helyzet olyan viselkedést eredményezhet, amely csak a teljes rendszerkörnyezet vizsgálatával érthető meg. A technológiai reziliencia ezért az AI-t nem önálló képességként, hanem ember–gép–adat–szervezet rendszerként kezeli. A döntési felelősség, a modellfelügyelet és a működési korlátok meghatározása legalább olyan fontos, mint az algoritmus technikai teljesítménye.

2.3.3 Felhő, edge, 5G[22]/6G és digitális platformfüggőség

A felhőalapú infrastruktúrák jelentősen növelik a skálázhatóságot, a gyors telepíthetőséget és a szolgáltatások rugalmasságát, ugyanakkor koncentrációs kockázatot teremthetnek. Ha több kritikus szervezet ugyanazon felhőplatformra, identitáskezelési szolgáltatásra vagy szoftver-ökoszisztémára támaszkodik, egy szolgáltatói hiba, hibás frissítés vagy célzott támadás több ágazatban egyidejű zavart idézhet elő. A szervezeti szinten redundánsnak tűnő rendszer ezért rendszerszinten közös hibamóddal rendelkezhet. A reziliencia szempontjából a multi-cloud önmagában sem megoldás, ha az alkalmazásarchitektúra, az adatformátum vagy az üzemeltetési kompetencia továbbra is egyetlen szolgáltatóhoz kötődik.

Az edge computing és az új generációs mobilhálózatok ezzel párhuzamosan decentralizálják a számítási és kommunikációs kapacitást. Ez lehetőséget teremt arra, hogy a kritikus funkciók részben lokálisan akkor is működjenek, ha a központi szolgáltatás elérhetetlenné válik. Ugyanakkor a végpontok számának növekedése, a szoftveralapú hálózati funkciók és a dinamikus szolgáltatásláncok új konfigurációs és biztonsági kockázatokat hoznak létre. A technológiai reziliencia ezért a centralizáció és decentralizáció közötti optimális egyensúlyt keresi, nem valamelyik megoldást tekinti önmagában kívánatosnak.

A hálózati és felhőfüggőségek kezelésének kulcsa az exit-képesség. Egy reziliens szervezetnek nem feltétlenül kell minden kritikus technológiát saját maga üzemeltetnie, de ismernie kell azt a pontot, ahol a szolgáltatóváltás, az adatmigráció vagy a degradált helyi működés technikailag és szervezetileg végrehajtható. A szerződéses rendelkezésre állási mutatók ezért nem helyettesítik a valódi helyreállítási és migrációs próbákat. A reziliencia

[22] 5G: Fifth Generation Mobile Network; ötödik generációs mobilhálózat.

ebben az értelemben a technológiai függőség tudatos, tesztelt és visszafordítható menedzsmentje.

2.3.4 Űr-, PNT- és kommunikációs függőségek

A **modern infrastruktúrák jelentős része közvetlenül vagy közvetetten függ** az űralapú szolgáltatásoktól. A helymeghatározás, navigáció és pontos időszolgáltatás – PNT – nemcsak a közlekedés, hanem a pénzügyi rendszerek, a távközlés, az energetikai hálózatok és a katonai vezetés számára is kritikus. A műholdas kommunikáció és földmegfigyelés további függőségeket hoz létre. Az űr ezért nem különálló technológiai szektor, hanem több földi infrastruktúra rejtett háttérrétege. A reziliencia tervezésnek számolnia kell a zavarás, megtévesztés, szolgáltatás-kiesés és fizikai űrkörnyezeti események következményeivel.

A **PNT-reziliencia jó példája annak**, miért szükséges funkcióalapú és nem eszközalapú megközelítés. A cél nem egy konkrét műholdas rendszer mindenáron történő fenntartása, hanem a pontos hely-, navigációs és időinformáció biztosítása. Ennek alternatív forrásai lehetnek inerciális rendszerek, földi rádiónavigáció, hálózati időforrások, lokális térképezés vagy több szenzor adatainak fúziója. A technológiai reziliencia tehát a kritikus funkcióhoz több, lehetőség szerint eltérő hibamódú technológiai megoldást rendel.

Az **űr- és kommunikációs függőségek civil-katonai jellege** különös governance-kihívást jelent. Ugyanaz a kereskedelmi műholdas vagy távközlési szolgáltatás civil, állami és katonai feladatokat egyaránt támogathat. Válsághelyzetben a kapacitás prioritása, a hozzáférés, a szerződéses jogok és a fizikai védelem olyan kérdéssé válik, amelyet békeidőben kell rendezni. Ez a civil-katonai technológiai ökoszisztéma a későbbi védelmi alkalmazások szempontjából a technológiai reziliencia egyik legfontosabb kutatási területe.

2.3.5 Energia, számítási kapacitás és kritikus nyersanyagok

A **digitalizáció gyakran láthatatlanná teszi az energiafüggőséget**. Adatközpontok, AI-infrastruktúrák, telekommunikációs hálózatok és ipari automatizálási rendszerek csak stabil villamosenergia-ellátás mellett képesek működni. A technológiai reziliencia ezért nem választható el az energetikai rezilienciától. A helyi tartalék energiaforrás, a mikrogrid, az energiatárolás, a több betáplálási pont és az energiaigény dinamikus menedzsmentje digitális infrastruktúrában is közvetlenül a rendelkezésre állást befolyásolja. A villamosenergia-rendszer digitalizációja ugyanakkor kiberfüggőséget is teremt, így az energia és a digitális infrastruktúra kölcsönösen egymás rezilienciájának feltétele.

A technológiai függőség nem ér véget az üzemeltetésnél. A félvezetők, akkumulátorok, ritkaföldfémek és más kritikus nyersanyagok ellátása a technológiai képességek hosszú távú fenntarthatóságát határozza meg. Az **Európai Unió Critical Raw Materials Act[23]-ja kifejezetten** a biztonságos, reziliens és fenntartható nyersanyagellátás megerősítését célozza [43]. A kritikus nyersanyagok koncentrált kitermelése és feldolgozása miatt a technológiai reziliencia stratégiai beszállítói kérdéssé válik: a rendszer akkor is sérülékeny lehet, ha a pillanatnyi működése stabil, de hosszú távú alkatrész- vagy anyagellátása nem biztosítható.

A számítási kapacitás szintén stratégiai erőforrássá válik. A nagy AI-modellek fejlesztése és futtatása koncentrált adatközponti, chip- és energia-infrastruktúrát igényel. Ez új függőségi viszonyokat hoz létre a technológiai szolgáltatók, félvezetőgyártók, adatközponti kapacitások és villamosenergia-rendszerek között. A reziliencia szempontjából a számítási kapacitás rendelkezésre állása, földrajzi diverzitása és prioritáskezelése egyre inkább hasonló jelentőségű lehet, mint a hagyományos stratégiai készleteké.

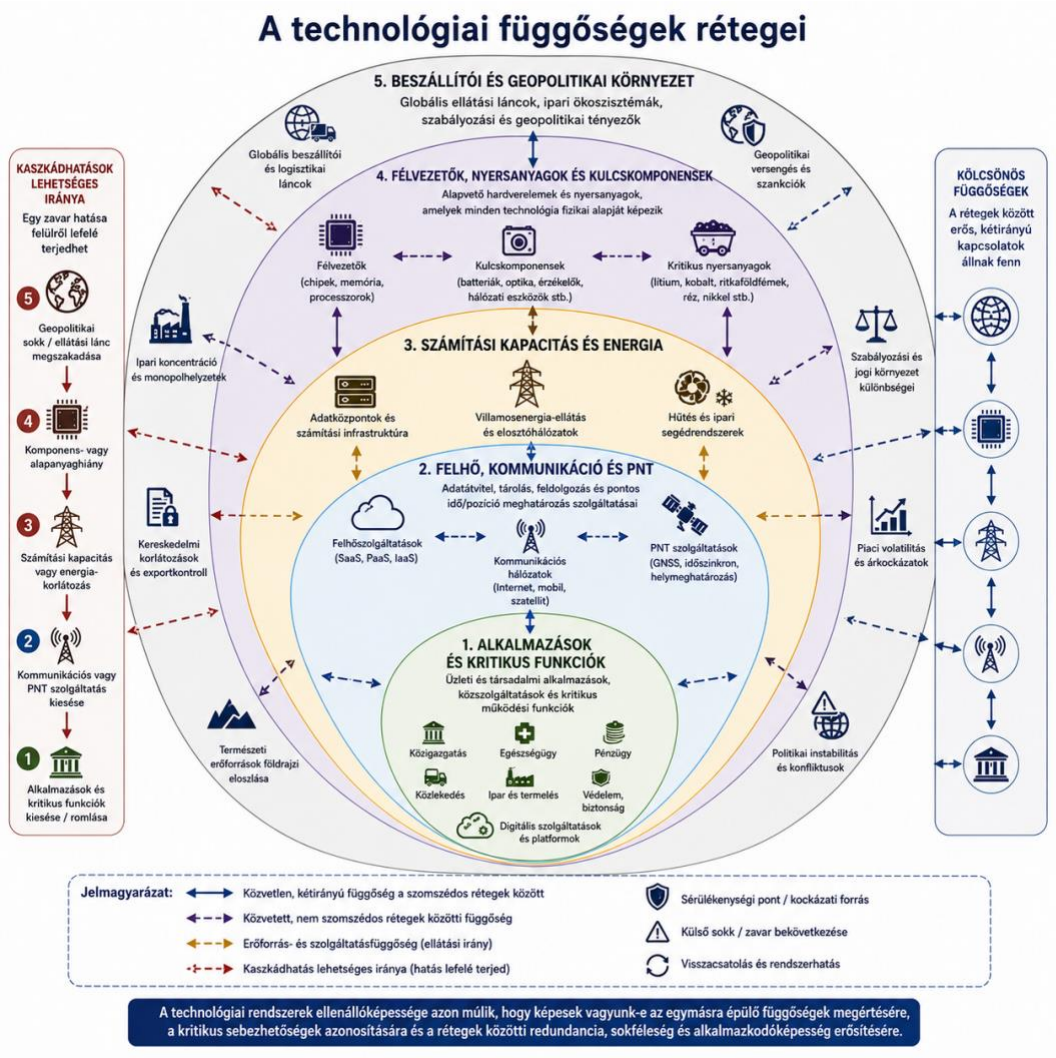
2.3.6 Ellátási láncok és technológiai szuverenitás

A technológiai ellátási láncok globális jellege egyszerre teremt hatékonyságot és sérülékenységet. **Sheffi és Rice már a 2000-es évek közepén hangsúlyozták** a beszállítói láthatóság, a rugalmasság és a diverzifikáció szerepét a reziliens vállalatban [19]. A digitális korszakban azonban az ellátási lánc fogalma kiterjed a szoftverkomponensekre, felhőszolgáltatásokra, firmware-ekre, frissítési mechanizmusokra, licencrendszerekre és távoli karbantartásra is. A fizikai és digitális ellátási lánc egyre kevésbé választható szét.

A technológiai szuverenitás ebben a kontextusban nem teljes önellátást jelent. A komplex technológiai rendszerekben az autarkia gazdaságilag és műszakilag is irreális lenne. A stratégiai cél sokkal inkább az, hogy a kritikus függőségek ismertek, értékeltek és szükség esetén helyettesíthetők legyenek. A reziliens függőség három követelményt foglal magában: láthatóságot, diverzitást és cselekvési szabadságot. Ez utóbbi azt jelenti, hogy válsághelyzetben legyen technikai, szerződéses és szervezeti lehetőség alternatív megoldásra áttérni.

[23] Critical Raw Materials Act (CRMA) – a kritikus fontosságú nyersanyagokról szóló európai uniós rendelet, hivatalosan az Európai Parlament és a Tanács (EU) 2024/1252 rendelete. Célja az EU kritikus és stratégiai nyersanyagokhoz való biztonságos, reziliens és fenntartható hozzáférésének erősítése, különösen az ellátási függőségek csökkentése, a beszerzési források diverzifikálása, valamint az európai kitermelési, feldolgozási és újrahasznosítási kapacitások növelése révén.

Az **Európai Unió gazdasági biztonsági stratégiája a kritikus függőségek**, a technológiai kockázatok és a gazdasági biztonság kapcsolatát stratégiai szinten kezeli [44]. A technológiai reziliencia ebből a nézőpontból gazdaságbiztonsági képesség is: a technológiai ökoszisztéma akkor reziliens, ha a külső sokkok, exportkorlátozások, ellátási zavarok vagy politikai nyomás ellenére képes a kritikus szolgáltatások és képességek fenntartására. Ez közvetlen átvezetést képez a nemzeti reziliencia és a védelmi ipari képességek kérdéséhez. [19][96][97][98]



2.2 ábra: A technológiai függőségek rétegei (saját szerkesztés)

2.3.7 Klímaváltozás, szélsőséges időjárás és fizikai környezeti stressz

A **technológiai reziliencia stratégiai környezetét nem kizárólag digitális és geopolitikai folyamatok** alakítják. A klímaváltozás, a gyakoribbá váló szélsőséges időjárási események, a hőhullámok, árvizek, aszályok és erdőtüzek közvetlenül érinthetik az energia-, közlekedési és kommunikációs infrastruktúrák működését. A fizikai környezeti stressz

különösen azért fontos, mert gyakran több infrastruktúrát egyszerre érint: egy hőhullám növeli az energiaigényt és csökkentheti egyes erőművek vagy adatközpontok hűtési hatékonyságát, miközben ugyanabban az időszakban a kommunikációs és egészségügyi rendszerek terhelése is nő. A reziliencia ezért nem egyetlen veszélyre optimalizált védelem, hanem több, egyidejűleg jelentkező stresszor kezelésének képessége.

A **fizikai és digitális kockázatok összekapcsolódása új típusú kaszkádhatásokat** eredményezhet. Egy szélsőséges időjárási esemény energiaellátási hibát okozhat, amely kommunikációs szolgáltatások és adatközpontok kiesésén keresztül már digitális szolgáltatási problémává válik. Fordított irányban is kialakulhat függőség: a digitális vezérlés, a távfelügyelet vagy a meteorológiai és szenzoradatok kiesése csökkentheti a fizikai infrastruktúra képességét a környezeti stressz kezelésére. A technológiai rezilienciát ezért több veszélyforrást együttesen kezelő (multihazard) megközelítésű logikában célszerű értelmezni, amelyben a kiber-, fizikai és természeti kockázatok nem különálló forgatókönyveket jelentenek, hanem közös rendszerhatásokat hozhatnak létre.

A hosszú távú környezeti változások az infrastruktúra-tervezési alapértékeket is módosíthatják. Egy rendszer, amelyet korábbi hőmérsékleti, csapadék- vagy vízhozam-adatok alapján terveztek, a jövőben olyan működési tartományba kerülhet, amelyre eredetileg nem optimalizálták. A technológiai reziliencia ezért nem korlátozható az incidensek utáni helyreállításra; része az alkalmazkodó tervezés, a tartalék kapacitások újraértékelése és a beruházási prioritások rendszeres felülvizsgálata is. E szemlélet összhangban áll a rezilienciának az 1. fejezetben bemutatott dinamikus értelmezésével, amely a rendszer funkcionális fennmaradását nem változatlan környezethez, hanem alkalmazkodóképességhez köti.

A **fizikai környezeti stressz különösen a katonai és kritikus infrastruktúrák kettős felhasználása esetén jelent kihívást**. Egy közlekedési útvonal, energiahálózat vagy kommunikációs rendszer békeidőben elegendő kapacitással rendelkezhet, válsághelyzetben azonban a katonai mobilitás, a lakossági igények és a helyreállítási feladatok egyidejű terhelése kapacitáshiányt okozhat. A reziliens tervezésnek ezért nemcsak a normál üzem átlagos terhelését, hanem a szélsőséges és összetett igénybevételt is figyelembe kell vennie. Ez a kapacitás- és prioritáskezelés a későbbi modellben a technológiai és szervezeti dimenzió közötti kapcsolat egyik fontos indikátora lehet.

2.3.8 Szoftver-ellátási láncok, technikai adósság és frissítési függőség

A **digitális infrastruktúrák egyre nagyobb része külső fejlesztésű** szoftverkomponensekre, nyílt forráskódú könyvtárakra, konténerekre, API-kra és felhőszolgáltatásokra épül. A szoftver-ellátási lánc ezért önálló reziliencia kérdéssé vált. Egyetlen széles körben használt komponens sérülékenysége vagy kompromittálódása egyszerre nagyszámú szervezetet érinthet, miközben az érintett felhasználók sok esetben nem is rendelkeznek teljes körű képpel arról, hogy az adott komponens hol és milyen függőségi láncban található. A technológiai reziliencia szempontjából ezért a szoftver-összetevők átláthatósága, a verzió- és függőségkezelés, valamint a frissítési útvonalak is kritikus képességek.

A **frissítés paradox módon egyszerre biztonsági kontroll és potenciális zavarforrás**. A gyors patch-elés csökkentheti a kihasználható sérülékenységek kockázatát, ugyanakkor kritikus rendszerekben egy hibás vagy inkompatibilis frissítés széles körű működési zavart okozhat. A reziliens frissítési stratégia ezért tesztkörnyezetet, fokozatos telepítést, visszaállítási lehetőséget és egyértelmű változáskezelést igényel. A cél nem a frissítések lassítása, hanem annak biztosítása, hogy a változtatás kontrolláltan, megfigyelhetően és szükség esetén visszafordíthatóan történjen. Ez a logika a technológiai modularitást közvetlenül összekapcsolja a szervezeti változáskezeléssel.

A technikai adósság [9] különösen a szoftver-ellátási láncokban válik kockázatossá. Az elavult függőségek, nem támogatott verziók, egyedi módosítások és dokumentálatlan integrációk olyan állapotot eredményezhetnek, amelyben a rendszer ugyan működik, de gyorsan nem frissíthető vagy migrálható. Válsághelyzetben ez jelentősen csökkenti az újrakonfigurálási képességet. A technológiai reziliencia ezért a technikai adósságot nem kizárólag fejlesztési minőségi kérdésként, hanem stratégiai mozgástérként kezeli: minél kisebb a rendszerben felhalmozott, nehezen módosítható örökség, annál nagyobb az adaptáció lehetősége.

A szoftver-ellátási lánc biztonsága szabályozási szinten is egyre hangsúlyosabb, amit a **NIS2** [25] és a **Cyber Resilience Act** [27] életciklus- és beszállítói logikája is tükröz. A reziliencia szempontjából azonban a formális termékbiztonság mellett azt is vizsgálni kell, hogy a beszállító mennyire képes válsághelyzetben gyors javítást, alternatív konfigurációt vagy támogatást biztosítani. A beszállítói értékelés ezért a biztonsági követelmények mellett helyreállítási, támogatási és exit-képességi szempontokat is tartalmazzon.

2.4 Társadalmi, humán és szervezeti kihívások

2.4.1 Digitális megosztottság és hozzáférési aszimmetriák

A technológiai reziliencia **társadalmi feltételei gyakran csak akkor válnak láthatóvá**, amikor a technológiai szolgáltatások válsághelyzetben elsődleges működési csatornává válnak. A digitális közigazgatás, távoli egészségügyi szolgáltatások, online oktatás, elektronikus fizetés és digitális válságkommunikáció azok számára teremtenek magasabb alkalmazkodási képességet, akik megfelelő eszközzel, kapcsolattal és kompetenciával rendelkeznek. A digitális megosztottság ezért nem pusztán társadalompolitikai kérdés, hanem a reziliencia egyenlőtlen eloszlása. Ha egy társadalom bizonyos csoportjai nem férnek hozzá a kritikus digitális szolgáltatásokhoz, a technológiai infrastruktúra formális rendelkezésre állása nem eredményez teljes társadalmi működőképességet.

A **hozzáférési egyenlőtlenségek területi és generációs dimenzióval is rendelkeznek**. A nagyvárosi infrastruktúra, a magas sávszélesség és a digitális szolgáltatások koncentrációja növelheti a központok hatékonyságát, miközben a periférikus térségekben kisebb lehet az alternatív hozzáférési lehetőség. Ugyanez igaz az idősebb vagy alacsonyabb digitális kompetenciával rendelkező csoportokra. A reziliencia tervezésének ezért a technológiai redundancia mellett hozzáférési redundanciával is számolnia kell: alternatív kommunikációs, ügyintézési és szolgáltatási csatornákra van szükség.

A **társadalmi inkluzivitás technológiai szempontból** is releváns. A túlzottan egycsatornás digitális szolgáltatás optimalizálhatja a normál működést, de válsághelyzetben kizárhatja azokat a felhasználókat, akik nem rendelkeznek megfelelő eszközzel vagy azonosítási lehetőséggel. A reziliens szolgáltatástervezés ezért nem a maximális digitalizációt, hanem a kritikus funkcióhoz szükséges többféle hozzáférési mód fenntartását tekinti célnak.

2.4.2 Humán tőke, készséghiány és technológiai függőség

A **technológiai rendszerek összetettségének növekedése felértékeli a humán kompetenciát**. A modern infrastruktúrák üzemeltetéséhez egyre több terület – kiberbiztonság, felhő, adat, AI, OT, rendszerintegráció és biztonságtechnika – együttes ismerete szükséges. A készséghiány ezért közvetlen reziliencia kockázat. Egy technológiai rendszer lehet magas műszaki színvonalú, ha azonban csak néhány szakértő képes

működtetni vagy helyreállítani, szervezeti szinten sérülékeny marad. A tudáskoncentráció egyfajta humán single point of failure.

A humán tényező jelentőségét a magyar kiberbiztonsági szakirodalom is hangsúlyosan kezeli. **Krasznay Csaba a közszolgálati kiberbiztonsági képességek vizsgálatakor arra mutat rá**, hogy a kibertéri kihívások jelentős része nem kizárólag műszaki természetű, ezért a reagáláshoz stratégiai szemlélettel és megfelelő kompetenciákkal rendelkező szakemberek szükségesek [51]. **Magyar Sándor információbiztonsági és kiberbiztonsági oktatási-szakmai tevékenysége** szintén az emberi tényező, a tudás és az attitűd fejlesztésének fontosságát helyezi előtérbe. Ez a megközelítés a technológiai reziliencia szervezeti dimenziója számára azért releváns, mert a technikai kontrollok hatékonysága végső soron a felhasználók, üzemeltetők és döntéshozók felkészültségén is múlik [52].

A szervezeti reziliencia szakirodalma az anticipációt, a megküzdést és az adaptációt fejleszthető képességként kezeli. **Duchek modellje alapján a szervezet rezilienciáját nem kizárólag a rendelkezésre álló erőforrások**, hanem azok mobilizálásának és a tapasztalatok intézményesítésének képessége határozza meg [4]. A technológiai reziliencia ezért képzési és tudásmenedzsment-rendszert igényel, amely nemcsak a normál üzemeltetéshez szükséges tudást, hanem a degradált és válságüzemhez szükséges kompetenciát is fenntartja.

A kritikus tudás dokumentálása és megosztása különösen fontos a hosszú életciklusú rendszereknél. A **legacy-platformok esetében gyakran nem a technikai dokumentáció**, hanem az évtizedek alatt kialakult tacit tudás teszi lehetővé a gyors hibaelhárítást. A személyi állomány cserélődése, kiszervezés vagy szervezeti átalakítás ezt a tudást rövid idő alatt elveszítheti. A reziliencia tervezésnek ezért a technológiai eszközállomány mellett a kritikus kompetenciák életciklusát is kezelnie kell.

2.4.3 Információs tér, dezinformáció és intézményi bizalom

A technológiai infrastruktúra társadalmi működőképessége a bizalomtól is függ. Egy digitális szolgáltatás akkor képes betölteni kritikus funkcióját, ha felhasználói hitelesnek, biztonságosnak és legitimnek tekintik. A hibrid és információs műveletek ezért nemcsak politikai véleményeket célozhatnak, hanem a technológiai rendszerekbe vetett bizalom gyengítését is. A kritikus infrastruktúrával kapcsolatos hamis információ, manipulált incidenskommunikáció vagy pánikkeltés növelheti egy valós vagy vélt technikai zavar társadalmi következményeit.

A hazai hadtudományi gondolkodásban **Haig Zsolt különösen részletesen elemzi a kibertéri kognitív befolyásolás és az információs műveletek** kapcsolatát. Megközelítése szerint a hálózatos technológia nem csupán információt továbbít, hanem a kognitív hatásgyakorlás infrastruktúráját is biztosítja, és a kognitív képességek technikai kibertéri képességekkel összehangoltan alkalmazhatók [50]. A technológiai reziliencia szempontjából ebből az következik, hogy a rendszer ellenálló képességének értékelésekor nem elegendő az adat és a szolgáltatás technikai integritását mérni; vizsgálni kell azt is, hogy a technológiai környezet milyen mértékben támogatja vagy veszélyezteti a hiteles helyzetértékelést és a döntéshozatalt.

A **reziliencia szempontjából az információs tér kétirányú kapcsolatban áll** a technológiai rendszerrel. Egyrészt a kommunikációs infrastruktúra teszi lehetővé az információ terjedését; másrészt az infrastruktúra működéséről kialakuló társadalmi kép befolyásolja a felhasználói viselkedést. Egy banki vagy üzemanyag-ellátási zavar például rövid idő alatt önmagát erősítő keresleti vagy bizalmi válsággá válhat, ha a kommunikáció nem hiteles és koordinált. A technológiai reziliencia ezért válságkommunikációs és információs integritási képességet is feltételez.

A **technikai és kommunikációs reagálás összehangolása különösen fontos** állami és kritikus szolgáltatói környezetben. A szervezetnek egyszerre kell pontos technikai helyzetképet kialakítania, vezetői döntést hoznia és a nyilvánosság számára érthető információt közölnie. Ha e három folyamat nincs összekapcsolva, a kommunikáció lemaradhat az események mögött, vagy ellentmondhat a technikai helyzetnek. A reziliens működés ezért nemcsak gyors, hanem konzisztens információáramlást követel meg.

2.4.4 Szervezeti tehetetlenség, döntési sebesség és adaptív kultúra

A **technológiai gyorsulás egyik legnagyobb kockázata nem maga** a technológia, hanem a szervezeti reakció lassúsága. A bürokratikus, silószerű és erősen centralizált rendszerek normál körülmények között magas fokú kontrollt biztosíthatnak, de gyorsan változó helyzetben a döntési késedelem önálló sérülékenységgé válik. Weick és Sutcliffe a nagy megbízhatóságú szervezeteknél a működéshez való közelséget, a gyenge jelek iránti érzékenységet és a szakértelemhez igazodó döntési autoritást emelik ki [32].

A technológiai reziliencia szempontjából **az adaptív kultúra nem szabálytalanságot** jelent. A cél olyan irányítási keret kialakítása, amely világosan meghatározza a kritikus korlátokat és felelősségeket, ugyanakkor a végrehajtás szintjén elegendő mozgásteret hagy a helyzethez igazodó döntésekhez. A túlzott centralizáció az

információs és döntési ciklust hosszabbítja; a kontroll nélküli decentralizáció viszont koordinációs hibát okozhat. A reziliens szervezet ezért a centralizált cél- és prioritásmeghatározást decentralizált helyzetadaptációval kapcsolja össze.

Teece dinamikus képességek elmélete alapján az alkalmazkodó szervezet képes érzékelni a változást, megragadni a lehetőséget és újrakonfigurálni erőforrásait [33]. Ez a technológiai reziliencia szervezeti oldalának jó leírása: nem elegendő a kockázat észlelése, ha a szervezet nem képes a technológiai architektúrát, a szerződéseket, a személyi erőforrást vagy a döntési struktúrát módosítani. A reziliencia ebben az értelemben végrehajtási képesség, nem pusztán tudatosság.

Társadalmi/szervezeti kihívás	Rezilienciahatás	Kritikus erőforrás	Tipikus válasz	Későbbi modellkapcsolat
Digitális megosztottság	A szolgáltatás társadalmi hasznosulása egyenetlen	Hozzáférés, kompetencia	Többcsatornás szolgáltatás, inkluzív tervezés	Szervezeti + szabályozási
Készséghiány	Humán single point of failure	Szakértelem, tudás	Képzés, utánpótlás, tudásmegosztás	Szervezeti
Bizalom és dezinformáció	Technikai zavar társadalmi hatása felerősödik	Hiteles információ, kommunikáció	Koordinált válságkommunikáció	Szervezeti + szabályozási
Szervezeti tehetetlenség	Lassú reagálás és újrakonfigurálás	Döntési autoritás, kultúra	Adaptív governance, decentralizált végrehajtás	Szervezeti

2.2. táblázat. A társadalmi és szervezeti kihívások reziliencia-hatásai (saját szerkesztés)

2.4.5 Ember–gép együttműködés, kognitív terhelés és döntési megbízhatóság

Az automatizáció és a mesterséges intelligencia elterjedésével a technológiai reziliencia egyre kevésbé írható le tisztán emberi vagy gépi képességként. A kritikus rendszerekben az ember–gép együttműködés minősége válik meghatározóvá. A túl alacsony automatizáció felesleges kognitív terhelést helyez az operátorokra, a túl magas vagy nem átlátható automatizáció viszont csökkentheti a helyzetértést és az emberi beavatkozás képességét. A reziliens rendszer ezért nem egyszerűen automatizál, hanem tudatosan osztja meg az érzékelési, elemzési és döntési feladatokat az ember és a gép között.

A **kognitív terhelés válsághelyzetben különösen** kritikus. Nagyszámú riasztás, bizonytalan információ, időnyomás és egymásnak ellentmondó adatok mellett az operátor döntési teljesítménye romolhat. A technológiai reziliencia ezért információs architektúrát is jelent: a rendszernek a releváns információt prioritás szerint kell megjelenítenie, támogatnia kell a gyors helyzetértékelést, és el kell kerülnie, hogy a monitorozás maga váljon túlterhelési forrássá. Az AI itt hasznos szűrő és döntéstámogató lehet, de a döntési felelősség és a bizonytalanság kommunikálása nélkül új kockázatot hozhat létre.

A gyakorlati reziliencia szempontjából fontos kérdés az automatizációból történő visszalépés képessége. Ha egy rendszer normál működésben magas fokú automatizációra épül, az operátorok készségei fokozatosan leépülhetnek, így meghibásodás esetén a manuális üzem nem feltétlenül állítható vissza. A rezilienciatervezésnek ezért nem elegendő manuális tartalék eljárást dokumentálnia; annak rendszeres gyakorlását és a szükséges kompetencia fenntartását is biztosítani kell. Ez különösen a katonai, energetikai és közlekedési rendszerek esetében kritikus.

Az ember–gép együttműködés a felelősség és elszámoltathatóság kérdését is felveti. Egy AI által javasolt döntés végrehajtásakor világosnak kell lennie, hogy ki jogosult annak elfogadására, milyen feltételek mellett kell felülvizsgálni, és milyen esemény esetén szükséges emberi kontrollra visszatérni. Az **AI Act** [45] emberi felügyeleti követelményei ebbe az irányba mutatnak. A technológiai reziliencia azonban ezen túlmenően azt is megköveteli, hogy a felügyeleti mechanizmus válsághelyzetben, információhiány mellett és degradált kommunikációban is működőképes legyen.

2.5 Szabályozási és governance-kihívások

2.5.1 Az uniós szabályozási környezet reziliencia-logikája

Az **Európai Unió szabályozási fejlődése jól szemlélteti**, hogy a kiberbiztonság és a kritikus infrastruktúrák védelme fokozatosan a reziliencia irányába mozdult el. A NIS2 [25] a technikai kontrollokat vezetői, szervezeti és ellátásilánc-felelősségekkel kapcsolja össze. A jelen kutatás szempontjából ez azért lényeges, mert megerősíti azt a tételt, hogy a kiberbiztonsági képesség önmagában nem választható el a szervezeti döntéshozataltól és a governance minőségétől.

A **CER** [26] **a kritikus szolgáltatások fenntartását szélesebb, nem kizárólag digitális fenyegetési környezetben** értelmezi. A **NIS2-vel együtt vizsgálva ezért a jelen kutatás számára azt támasztja alá**, hogy a technológiai reziliencia elemzési egysége nem lehet kizárólag az informatikai rendszer, hanem a kritikus funkciót biztosító teljes szocio-technikai rendszer. A fizikai, digitális, humán és ellátási zavarok közös következménye a kritikus funkció sérülése lehet, ezért az értékelésnek is e funkció fenntarthatóságára kell irányulnia.

A **Cyber Resilience Act** [27] a **digitális elemeket tartalmazó termékek biztonságát a teljes termékéletciklushoz kapcsolódó fejlesztői és gyártói felelősségek rendszerében kezeli**. A technológiai reziliencia szempontjából ennek fő következménye,

hogy az üzemeltető szervezet működőképessége részben a beszállító sérülékenység-kezelési és frissítési képességétől is függ. A termékreziliencia és a szervezeti reziliencia ezért egymást kölcsönösen meghatározó tényezőkké válhat.

Az **AI Act** [45] **a magas kockázatú mesterségesintelligencia-rendszerek működését olyan irányítási és felügyeleti követelményekhez köti**, amelyek a technológiai teljesítmény mellett az adatkezelésre, az emberi kontrollra és a rendszer robusztusságára is kiterjednek. A technológiai reziliencia számára ez új governance-réteget jelent: kritikus funkciókban alkalmazott AI esetében nemcsak a rendelkezésre állást, hanem a felügyelhetőséget, a hibás döntések kontrollját és a biztonságos degradáció lehetőségét is értékelni kell.

2.5.2 Compliance és tényleges reziliencia

A **szabályozás alapvető előnye, hogy minimumkövetelményeket, felelősségi rendet és ellenőrizhető kontrollokat teremt**. A compliance azonban nem azonos a rezilienciával. Egy szervezet rendelkezhet megfelelő szabályzatokkal, tanúsítványokkal és dokumentált eljárásokkal, miközben egy valós incidensben a döntéshozatal lassú, a mentések nem állíthatók vissza, a beszállítói függőség nem ismert vagy a személyi állomány nem képes a vészüzemi eljárások végrehajtására. A reziliencia ezért a formális kontrollok működésbe hozásának képességét vizsgálja.

A megfelelőség jellemzően pillanatfelvételt ad: azt mutatja meg, hogy egy adott időpontban fennállnak-e az előírt követelmények. A reziliencia ezzel szemben időben változó képesség. A rendszernek a zavar előtt anticipálnia, a zavar alatt reagálnia, utána helyreállnia és a tapasztalatok alapján változnia kell. Ez indokolja a rendszeres gyakorlatokat, stressztesztek és helyreállítási próbákat. A dokumentált terv és a végrehajtott képesség közötti különbség csak gyakorlati teszteléssel válik láthatóvá.

A reziliencia-orientált governance ezért a kontrollkatalógus helyett működési kimenetekre koncentrál. A kérdés nem pusztán az, hogy létezik-e redundancia, hanem hogy a tartalék rendszer valóban átveszi-e a kritikus funkciót; nem az, hogy van-e incidenskezelési terv, hanem hogy a döntési és kommunikációs lánc működik-e információhiány mellett; és nem az, hogy a beszállító szerződésben vállal-e rendelkezésre állást, hanem hogy a szervezet képes-e a szolgáltató kiesése esetén alternatív működést fenntartani.

2.5.3 NATO-reziliencia és nemzeti felelősség

A **NATO rezilienciafelfogása a nemzeti és kollektív védelem kapcsolatából indul ki**. A **2021-es Strengthened Resilience Commitment** a rezilienciát a hiteles elrettentés és védelem alapvető elemének tekinti, és hangsúlyozza a kritikus infrastruktúrák, az ellátási láncok és a kulcsfontosságú iparágak védelmét [36]. A reziliencia elsődlegesen nemzeti felelősség, ugyanakkor az egyik szövetséges sérülékenysége más tagállamok és a kollektív műveletek képességeire is hatással lehet.

A NATO-reziliencia különösen fontos technológiai szempontból, mert a katonai képességek jelentős része civil infrastruktúrákra támaszkodik. A katonai mobilitás közlekedési hálózatot, a vezetés kommunikációt és adatkapcsolatot, a logisztika energiát és kereskedelmi ellátási láncokat, a műveleti helyzetkép pedig űr- és digitális szolgáltatásokat igényel. A technológiai reziliencia ezért a civil és katonai képességek közötti interfészek rezilienciáját is jelenti.

A NATO és az Európai Unió 2023-ban a kritikus infrastruktúrák rezilienciáját energia, közlekedés, digitális infrastruktúra és űr területén közösen is vizsgálta [46]. Ez a négy terület jól mutatja, hogy a modern nemzeti reziliencia nem ágazati képességek egyszerű összege. A közös függőségek, szolgáltatói koncentrációk és határokon átnyúló hálózatok miatt a reziliencia több intézmény és több ország összehangolt működését igényli.

2.5.4 Adaptív governance és innovációs képesség

A technológiai innováció sebessége miatt a szabályozási rendszer adaptivitása önálló reziliencia képességgé válik. A túl lassú szabályozási reakció biztonsági rést és felelősségi bizonytalanságot teremthet; a túl korai, vagy túl merev szabályozás viszont megakadályozhatja a szükséges kísérletezést és innovációt. Az adaptív governance célja ezért stabil célokat és biztonsági korlátokat rögzíteni, miközben lehetővé teszi a követelmények és végrehajtási módszerek gyors módosítását a technológiai és fenyegetési környezet változásával.

A governance adaptivitásának egyik eszköze a szabályozási sandbox, a pilotprogram, a kísérleti beszerzés és a fokozatos megfelelési követelmény. Ezek lehetővé teszik, hogy az új technológiák valós környezetben tesztelhetők legyenek anélkül, hogy a teljes rendszer kockázatnak lenne kitéve. A technológiai reziliencia szempontjából a kísérletezés nem az ellenőrzés hiánya, hanem a kontrollált tanulás intézményesített formája.

Az adaptív governance szorosan kapcsolódik a szervezeti tanuláshoz. Ha a szabályozási rendszer nem képes a gyakorlatok, incidensek és technológiai tesztek

tapasztalatait visszacsatolni, a megfelelési rendszer idővel elszakad a valós kockázatoktól. A technológiai reziliencia ezért olyan irányítási ciklust igényel, amelyben a monitoring, az értékelés, a döntés, a módosítás és az újratesztelés folyamatosan ismétlődik.

2.3- ábra: A compliance-tól az adaptív reziliencia-governance-ig (saját szerkesztés)

2.5.5 Köz- és magánszféra együttműködése, gyakorlatok és stressztesztelés

A **kritikus technológiai infrastruktúrák jelentős része magántulajdonban vagy piaci szolgáltatói környezetben működik, miközben kiesésük következménye közérdekű és nemzetbiztonsági lehet**. Ez a tulajdonosi és felelősségi kettősség a reziliencia egyik legfontosabb governance-kihívása. Az állam szabályozhatja a minimumkövetelményeket, de a tényleges működési tudás, technológiai infrastruktúra és helyreállítási kapacitás sok esetben a szolgáltatóknál található. A reziliens rendszer ezért tartós köz- és magánszféra együttműködést igényel, nem csak incidens idején létrejövő ad hoc koordinációt.

A kölcsönös bizalom és információmegosztás kialakítása békeidős feladat. A vállalatok számára érzékeny lehet a sérülékenységi vagy incidensinformáció megosztása, az állami szereplők pedig nem minden fenyegetési adatot tehetnek nyilvánossá. A reziliencia-governance-nak ezért olyan információmegosztási mechanizmusokat kell kialakítania,

amelyek a szükséges technikai és stratégiai információt a megfelelő bizalmassági szinten eljuttatják a döntéshozókhoz és üzemeltetőkhöz. Enélkül a közös helyzetkép hiányos marad, és a koordináció csak a zavar bekövetkezése után kezdődik meg.

A gyakorlatok és stressztesztek az együttműködés valós képességének legfontosabb bizonyítékai. A **NIS2 és CER által megkövetelt kockázatkezelési és reziliencia-logika csak akkor válik működő képességgé**, ha a szervezetek rendszeresen tesztelik a kommunikációs, döntési és helyreállítási eljárásokat. A technikai teszt mellett érdemes több szervezetet és több ágazatot összekapcsoló forgatókönyveket alkalmazni, mert a kaszkádhatások és a felelősségi hézagok ilyen környezetben válnak láthatóvá. [25][26]

A **stresszteszt nem kizárólag a rendszer gyengeségeinek feltárását szolgálja**. Ugyanilyen fontos a sikeres adaptációk azonosítása: milyen informális kapcsolatok, alternatív eljárások vagy helyi döntések tették lehetővé a működés fenntartását. Ezek a tapasztalatok visszacsatolhatók a formális eljárásokba és szabályozásba. A reziliencia fejlesztés ezzel tanuló governance-ciklussá válik, amelyben a szabályozó, az üzemeltető, a védelmi és biztonsági szereplők közösen alakítják a következő felkészülési szintet.

2.6 Védelmi és nemzetbiztonsági következmények

2.6.1 Civil-katonai technológiai interdependencia

A **modern haderők működése egyre nagyobb mértékben támaszkodik civil és kereskedelmi technológiákra**. Felhőszolgáltatások, műholdas kommunikáció, logisztikai platformok, energiaellátás, közúti és vasúti infrastruktúra, félvezetők és kereskedelmi drónтechnológiák egyaránt beépülhetnek katonai képességekbe. Ez növeli az innováció sebességét és csökkentheti a költségeket, ugyanakkor a katonai működőképességet részben olyan civil szereplők döntéseitől és infrastruktúráitól teszi függővé, amelyek nem klasszikus katonai irányítás alatt állnak.

A **civil-katonai interdependencia reziliencia-követelménye** ezért nem az összes kritikus szolgáltatás katonai tulajdonba vétele. Sokkal inkább a függőségek előzetes azonosítására, a prioritások tisztázására, a szerződéses és jogi hozzáférés biztosítására, valamint a válsághelyzeti együttműködés rendszeres tesztelésére van szükség. A békeidőben hatékony piaci szolgáltatás csak akkor válik védelmi szempontból reziliens képességgé, ha válsághelyzetben is rendelkezésre áll és a katonai követelményekhez igazítható.

A dual-use innováció ezért technológiai reziliencia-eszköz is lehet. A civil piacon széles körben alkalmazott technológia nagyobb fejlesztői és beszállítói ökoszisztémára

támaszkodhat, gyorsabb innovációs ciklussal és több alternatív beszállítóval rendelkezhet. Ugyanakkor a katonai alkalmazás speciális biztonsági, megbízhatósági és ellátásbiztonsági követelményeit külön kell kezelni. A reziliens dual-use stratégia a civil innováció előnyeit a katonai működőképességhez szükséges kontrollokkal kapcsolja össze.

2.6.2 Többdoménes műveletek és döntési fölény

A **NATO Warfighting Capstone Concept a jövő műveleti környezetében a többdoménes integráció és a döntési előny jelentőségét hangsúlyozza** [38]. A döntési fölény azonban közvetlenül függ a technológiai infrastruktúra rezilienciájától. Ha a szenzorok, kommunikációs hálózatok, adatfeldolgozó platformok vagy C2-rendszerek kiesnek, a parancsnoki rendszer nem pusztán információt veszít, hanem időt és döntési szabadságot is. A technológiai reziliencia ezért műveleti tempót védő képesség.

A **hazai katonai műszaki és információbiztonsági kutatások** szintén fontos hátteret biztosítanak e kérdéshez. **Négyesi Imre munkássága** a katonai információs rendszerek, az információbiztonság és a katonai műszaki-technológiai fejlődés összefüggéseit kapcsolja össze; a katonai információbiztonság tudományos műhelyeiben betöltött szerepe a technikai rendszerek és a katonai alkalmazási környezet együttes vizsgálatát erősíti [54]. Ez a szemlélet a jelen kutatásban azért lényeges, mert a katonai technológiai reziliencia nem értelmezhető a híradó-informatikai infrastruktúra, az információbiztonság, a humán kezelői rendszer és a műveleti követelmények szétválasztásával.

A többdoménes környezetben a redundancia hagyományos értelmezése is változik. Nem feltétlenül azonos típusú tartalék rendszerre van szükség, hanem funkcionális alternatívára. A műholdas kommunikációt szükség esetén földi rádióhálózat, a GNSS-alapú navigációt inerciális vagy vizuális navigáció, a központi adatfeldolgozást edge-kapacitás, a digitális C2 egyes funkcióit pedig előre kialakított manuális eljárások helyettesíthetik. A heterogén redundancia csökkenti a közös hibamódok kockázatát.

A **döntési reziliencia szervezeti dimenziója ugyanolyan fontos, mint a technológiai**. A vezetési rendszernek információhiány, kommunikációs degradáció és gyorsan változó helyzet mellett is működőképesnek kell maradnia. Ez világos delegálási elveket, helyettesítési rendet, közös eljárásokat és gyakorolt decentralizált döntéshozatalt igényel. A technológiai reziliencia ebben a kontextusban a technikai és parancsnoki rendszer közös adaptív képessége.

2.6.3 Védelmi ipar, innováció és ellátásbiztonság

A **védelmi ipari reziliencia a technológiai képességek hosszú távú fenntarthatóságát jelenti.** Egy katonai rendszer beszerzése önmagában nem biztosít képességet, ha a karbantartás, a szoftverfrissítés, a lőszer-, alkatrész- vagy energiaellátás, illetve a szükséges szaktudás nem biztosítható tartósan. A reziliencia ezért a teljes életciklust vizsgálja: a fejlesztéstől és beszerzéstől az üzemeltetésen és javításon át a korszerűsítésig és kivonásig.

A geopolitikai versengésben a védelmi ipari ellátási láncok sérülékenysége stratégiai korláttá válhat. A kritikus nyersanyagok, félvezetők, energetikai komponensek és speciális gyártási kapacitások koncentrációja azt jelenti, hogy a termelési képesség válsághelyzetben nem pusztán pénzügyi kérdés. A technológiai reziliencia fejlesztésének ezért része a beszállítói térkép, a stratégiai készletezés, a javítási és gyártási kapacitás diverzifikációja, valamint az interoperábilis komponensek és nyílt interfészek alkalmazása.

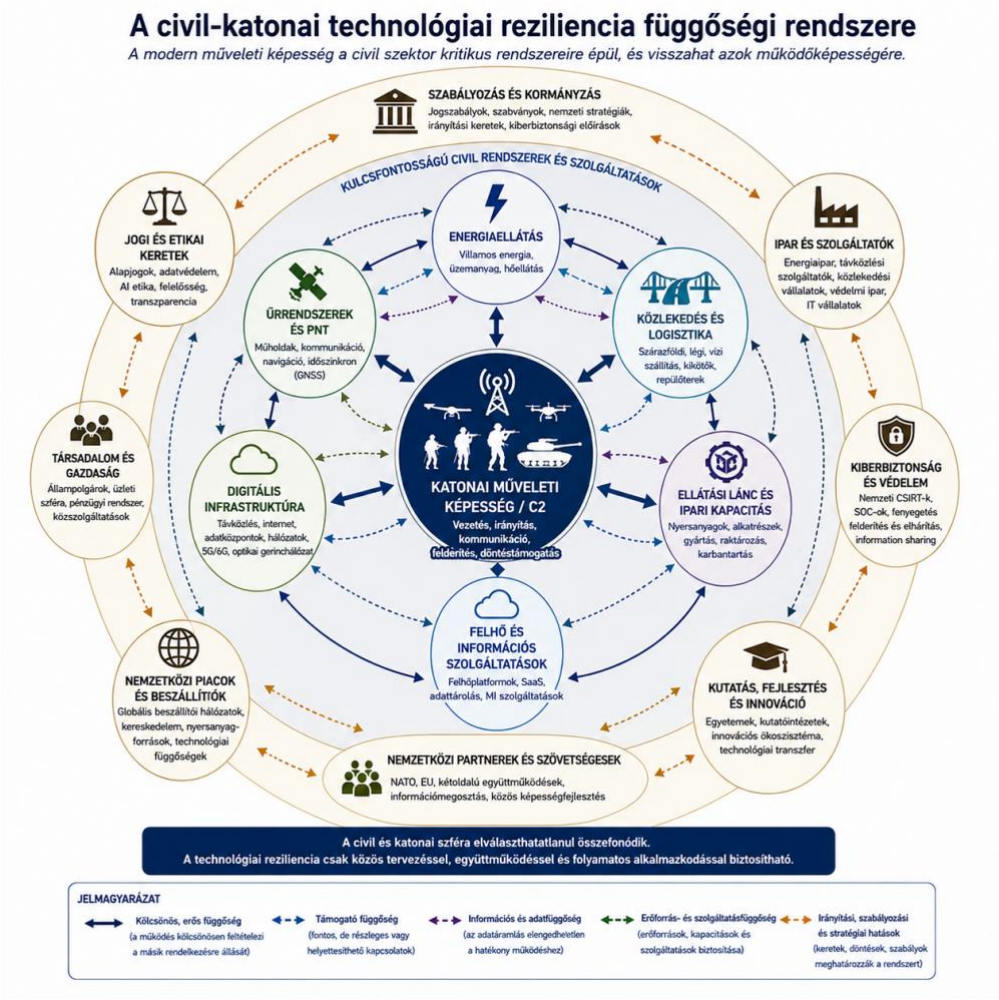
A gyors innováció és a hosszú katonai életciklus közötti feszültség különösen élesen jelenik meg a szoftverintenzív rendszereknél. A klasszikus többéves fejlesztési és beszerzési ciklus alatt a technológiai környezet jelentősen megváltozhat. A rezilienciát ezért támogatja a moduláris nyílt rendszerarchitektúra, a folyamatos szoftverfrissítés, a gyors prototipizálás és a kontrollált kísérletezés. A cél nem az, hogy minden rendszer folyamatosan a legújabb technológiát használja, hanem hogy a kritikus funkciók biztonságosan és fenntarthatóan korszerűsíthetők legyenek.

2.6.4 Nemzeti technológiai reziliencia és stratégiai autonómia

A technológiai reziliencia nemzeti szinten a működési szabadság fenntartásának képességeként értelmezhető. Az államnak nem kell minden technológiát saját maga előállítania, de ismernie kell azokat a kritikus technológiai rétegeket és függőségeket, amelyek kiesése aránytalanul nagy hatással lenne az alapvető állami, gazdasági vagy védelmi funkciókra. A stratégiai autonómia ilyen értelemben nem elszigetelődés, hanem döntési és cselekvési mozgástér.

A nemzeti technológiai reziliencia több szakpolitikai terület koordinációját igényli. A kiberbiztonság, az energia, a közlekedés, a távközlés, az iparpolitika, az oktatás, a kutatás-fejlesztés és a honvédelem külön-külön nem képes kezelni a rendszerszintű függőségeket. A stratégiai kihívás ezért governance-probléma: szükség van közös prioritásokra, információmegosztásra, interoperábilis kockázati nyelvre és olyan döntési fórumokra, amelyek válságon kívül is képesek a kritikus függőségek kezelésére.

A reziliencia nemzeti szintre emelése egyben mérési és prioritási kérdést is felvet. Nem minden technológiai függőség egyformán kritikus, és nem minden sérülékenység kezelhető azonos módon. A nemzeti reziliencia fejlesztésének ezért a kritikus funkciók azonosításából, a mögöttes technológiai és szervezeti függőségek feltérképezéséből, majd a legnagyobb rendszerszintű kockázatot jelentő interfészek kezeléséből kell kiindulnia. Ez a logika közvetlenül megalapozza a 3. fejezet dimenzió- és indikátoralapú modelljének szükségességét.



2.4- ábra: A civil-katonai technológiai reziliencia függőségi rendszere (saját szerkesztés)

2.6.5 Védelmi innováció, kísérletezés és gyors képességintegráció

A technológiai reziliencia és a védelmi innováció kapcsolata különösen a gyorsan változó technológiai környezetben válik fontossá. A hagyományos beszerzési és rendszeresítési ciklusok sok esetben lassabbak, mint a kereskedelmi technológia fejlődése vagy a műveleti fenyegetések adaptációja. A reziliens védelmi szervezetnek ezért képesnek

kell lennie kontrollált kísérletezésre, gyors prototípus-fejlesztésre és a felhasználói visszajelzések korai beépítésére. A kísérletezés célja nem a követelmények megkerülése, hanem a bizonytalanság csökkentése valós működési tapasztalatokon keresztül.

A gyors innováció ugyanakkor csak akkor erősíti a rezilienciát, ha a prototípusból fenntartható képesség válik. Sok innovációs program kockázata, hogy a demonstrátor sikeres, de nincs kialakított karbantartási, kiberbiztonsági, képzési, alkatrész- és szoftvertámogatási rendszer. A technológiai reziliencia ezért a kísérleti megoldások értékelésénél már korán vizsgálja a teljes életciklust, a beszállítói és licencfüggőségeket, az interoperabilitást és a skálázhatóságot. A „gyors" képesség nem azonos a „rövid életű" képességgel.

A dual-use technológiák védelmi integrációja előnyt jelenthet, mert a civil piac nagyobb felhasználói bázist, gyorsabb fejlesztési ciklust és szélesebb beszállítói ökoszisztémát biztosíthat. Ugyanakkor a kereskedelmi termékek biztonsági és rendelkezésre állási feltételei nem automatikusan felelnek meg katonai követelményeknek. A reziliens integráció ezért moduláris interfészekre, biztonsági hardeningra, független tesztelésre és alternatív beszállítói opciókra épül. A cél a civil innováció sebességének és a katonai működőképesség tartósságának összehangolása.

A **védelmi innovációs ökoszisztéma maga is reziliencia-képesség**. Egy ország vagy szövetség akkor képes gyorsan reagálni új technológiai fenyegetésre, ha rendelkezik kutatóhelyekkel, vállalkozásokkal, tesztközpontokkal, felhasználói szervezetekkel és finanszírozási mechanizmusokkal, amelyek között gyors információ- és tudásáramlás lehetséges. A technológiai reziliencia tehát nemcsak a meglévő rendszerek védelmét jelenti, hanem az új képességek gyors létrehozásának és integrációjának intézményi kapacitását is.

2.7 Stratégiai szintézis: a környezeti kihívásokból levezethető reziliencia-követelmények

A fejezet elemzése alapján a XXI. századi technológiai reziliencia legfontosabb sajátossága, hogy a kihívások és válaszképességek nem rendelhetők egyetlen szervezeti vagy technológiai szinthez. A hiperösszekapcsoltság technológiai architekturális kérdésnek tűnik, de egyben beszállítói, szabályozási és szervezeti koordinációs problémát is jelent. A mesterséges intelligencia technikai képesség, ugyanakkor adatminőségi, humán felügyeleti és jogi kockázatot teremt. A kritikus nyersanyagok gazdasági kérdésként jelennek meg, de közvetlenül befolyásolják a digitális és védelmi képességek fenntarthatóságát. A reziliencia ezért integrált válaszrendszert igényel.

A **környezeti kihívásokból három általános követelmény vezethető le**. **Elsőként** a technológiai rendszereknek funkcionális redundanciával, modularitással, monitorozhatósággal és kontrollált degradációs képességgel kell rendelkezniük. **Másodszor** a szervezeteknek gyors döntési, tanulási és újrakonfigurálási képességet kell kialakítaniuk, amely képes a technológiai erőforrásokat válsághelyzetben ténylegesen működésbe hozni. **Harmadszor** a szabályozási és stratégiai környezetnek olyan stabil, de adaptív keretet kell biztosítania, amely a kritikus függőségeket ágazati és nemzeti szinten is kezelhetővé teszi.

A három követelmény egymástól nem független. A technológiai redundancia szervezeti döntés nélkül nem aktiválódik; a gyors szervezeti reagálás megfelelő információs és technikai architektúra nélkül hatástalan; a szabályozási követelmény pedig csak akkor erősíti a rezilienciát, ha a gyakorlatban végrehajtható és a tapasztalatok alapján módosítható. Ez a kölcsönös függőség indokolja, hogy a technológiai rezilienciát a későbbi modell technológiai, szervezeti és szabályozási dimenziók együtteseként mérhetővé és értékelhetővé teszi.

A fejezet másik lényeges következtetése az idődimenzió jelentősége. A XXI. századi stratégiai környezetben a változás sebessége önálló kockázati tényező. A reziliens rendszernek ezért nemcsak erősnek kell lennie, hanem gyorsabban kell tanulnia és újrakonfigurálódnia, mint ahogyan a fenyegetési és függőségi környezet romlik. A technológiai reziliencia versenyképességi és biztonsági értéke ebből a dinamikából származik: az adaptáció sebessége közvetlenül növeli a szervezet vagy állam stratégiai mozgásterét.

Környezeti kihívás	Technológiai hatás	Szervezeti hatás	Governance-hatás	Kulcs reziliencia-válasz	Kapcsolat a 3. fejezettel
Hiperösszekapcsoltság	Kaszkád- és koncentrációs kockázat	Többszereplős koordináció	Interdependenciák kezelése	Modularitás, függőségtérkép, alternatív útvonal	Technológiai + szabályozási
AI és autonómia	Új hibamódok, modell- és adatfüggőség	Humán felügyelet és készségek	AI governance	Biztonságos degradáció, felügyelhetőség	Mindhárom dimenzió
Kiber/OT fenyegetés	Digitális-fizikai hatás	Incidens- és válságkezelés	NIS2/CER, felügyelet	Szegmentáció, monitoring, recovery	Technológiai + szervezeti
Ellátási lánc	Komponens- és szolgáltatáshiány	Beszerzési és kompetenciafüggés	Gazdaságbiztonság	Diverzifikáció, exit-képesség, készletezés	Technológiai + szabályozási
Információs műveletek	Bizalomvesztés, túlterhelés	Kommunikációs és döntési nyomás	Stratégiai kommunikáció	Hiteles helyzetkép, gyors kommunikáció	Szervezeti + szabályozási
Technológiai gyorsulás	Rövid életciklus, technikai adósság	Tanulási lemaradás	Szabályozási késés	Modularitás, gyors kísérletezés, adaptív governance	Mindhárom dimenzió

2.3. táblázat. A stratégiai környezet kihívásai és a levezethető technológiai reziliencia-követelmények (saját szerkesztés)

2.7.1 Átvezetés a technológiai reziliencia saját modelljéhez

A **2. fejezet feladata nem a technológiai reziliencia dimenzióinak** végleges definiálása vagy mérési indikátorainak meghatározása, hanem annak bizonyítása, hogy a stratégiai környezet önmagában kikényszeríti az integrált megközelítést. A technológiai, szervezeti és szabályozási tényezők szétválasztása elemzési szempontból hasznos, a valós működésben azonban folyamatos kölcsönhatásban vannak. A 3. fejezet ezért nem tetszőleges modellstruktúrát vezet be, hanem a jelen fejezetben azonosított környezeti kihívásokra építve mérhetővé és értékelhetővé teszi azt a hármas rendszert, amelyben a technológiai architektúra, a szervezeti adaptáció és a governance együttesen határozza meg a rezilienciát.

A 3**. fejezetben kidolgozandó modell** számára a jelen fejezet három konkrét követelményt fogalmaz meg. A modellnek képesnek kell lennie az egyes dimenziók önálló állapotának értékelésére; vizsgálnia kell a dimenziók közötti kapcsolatokat és interfészeket; valamint időbeli, adaptív folyamatként kell kezelnie a rezilienciát. E három követelmény nélkül a modell vagy statikus compliance-értékeléssé, vagy pusztán technikai megbízhatósági elemzéssé redukálódna.

A környezeti elemzés továbbá indokolja, hogy a későbbi validáció ne egyetlen ágazatra korlátozódjon. Az energia, közlekedés, elektronikus hírközlés és katonai C2 eltérő technológiai és szabályozási logikával működik, ugyanakkor közös függőségi és adaptációs problémákat mutat. Ha a modell ezekben az eltérő környezetekben is képes azonosítani a rezilienciát korlátozó tényezőket és interfészeket, az erősíti általánosíthatóságát. Ez teremti meg a közvetlen átmenetet a 4. fejezet összehasonlító ágazati validációjához.

2.8 Fejezetösszegzés

A 2. fejezet a technológiai rezilienciát a XXI. század stratégiai környezetében helyezte el. Az elemzés alapján a reziliencia jelentőségét nem egyetlen fenyegetés vagy technológiai trend növeli, hanem a tartós versengés, a technológiai gyorsulás, a hiperösszekapcsoltság, a digitalizáció és a társadalmi-institucionális változások együttes hatása. E tényezők olyan környezetet hoznak létre, amelyben a teljes hibamentesség és a kizárólag statikus kontrollokra épülő biztonság nem reális cél. A kritikus funkciók fenntartása adaptív, több rétegű és több szereplőt átfogó képességet követel.

A technológiai kihívások elemzése rámutatott, hogy a kiberfenyegetések, az IT/OT konvergencia, a mesterséges intelligencia, az autonóm rendszerek, a felhő- és platformfüggőség, az űr- és PNT-szolgáltatások, valamint az energia- és nyersanyagfüggőség egymással összekapcsolódó kockázati rendszert alkotnak. A technológiai reziliencia ezért a modularitás, redundancia, monitorozás és helyreállítás mellett függőségmenedzsmentet, alternatív működési módokat és életciklus-szemléletet is igényel.

A társadalmi és szervezeti vizsgálat azt mutatta, hogy a technológia tényleges rezilienciája a humán kompetenciától, a döntési sebességtől, a tanulási mechanizmusoktól és az intézményi bizalomtól is függ. A technológiai rendszer rendelkezésre állása önmagában nem elegendő, ha a felhasználók nem férnek hozzá, a szervezet nem tud reagálni, vagy a válságkommunikáció nem képes fenntartani a bizalmat. A reziliencia ezért társadalmi és szervezeti végrehajtási képesség is.

A szabályozási elemzés szerint a NIS2, a CER, a Cyber Resilience Act és az AI Act egyaránt a kockázatalapú, életciklus-szemléletű és vezetői felelősségre épülő governance irányába mozdítja a technológiai biztonságot. [25],[27] A megfelelőség azonban szükséges, de nem elégséges feltétel. A reziliencia a kontrollok tényleges működését, a stresszhelyzeti alkalmazhatóságot és a tapasztalatok alapján történő módosíthatóságot követeli meg.

Védelmi és nemzetbiztonsági szempontból a technológiai reziliencia a civil-katonai függőségek, a többdoménes műveletek, a védelmi ipari ellátás és a stratégiai autonómia közös alaprétegévé válik. A nemzeti működőképesség és a katonai képességek ugyanazon energia-, közlekedési, digitális és űralapú infrastruktúrákra támaszkodnak, ezért a reziliencia fejlesztése csak integrált megközelítésben értelmezhető.

A fejezet végső következtetése, hogy a XXI. századi környezet a technológiai rezilienciát három egymással kölcsönhatásban álló terület együttes képességeként teszi értelmezhetővé: a technológiai rendszer strukturális és működési alkalmazkodóképessége, a szervezet döntési és tanulási képessége, valamint a szabályozási-stratégiai környezet adaptív irányítási képessége. E három terület elméleti és módszertani mérhetővé és értékelhetővé tétele a 3. fejezet feladata.

3. fejezet: Az integrált technológiai reziliencia-modell kidolgozása és mérési keretrendszere

3.1 A fejezet célja és kutatási megközelítése

Az **első két fejezet szakirodalmi elemzése rámutatott arra**, hogy a reziliencia fogalma napjainkra számos tudományterületen meghatározó elemzési keretté vált. A különböző megközelítések ugyan jelentős tudományos eredményeket hoztak, azonban eltérő elemzési egységeik miatt jelenleg nem áll rendelkezésre olyan egységes elméleti modell, amely a technológiai rezilienciát komplex szocio-technikai rendszerként értelmezné.

A **szakirodalom kritikai elemzése alapján megállapítható, hogy a mérnöki, szervezeti és stratégiai rezilienciamodellek önállóan jól kidolgozottak, ugyanakkor csak részlegesen képesek magyarázni a modern technológiai rendszerek működését**. A három megközelítés integrációja jelenleg hiányzik, amely egyértelmű kutatási rést jelöl ki.

A **kutatás abból a felismerésből** indul ki, hogy a modern technológiai rendszerek ellenálló képessége **nem értelmezhető kizárólag technológiai szempontból**. A technológiai infrastruktúra, a működtető szervezet és a szabályozási környezet olyan kölcsönhatásban állnak egymással, amely indokolja egy új, integrált fogalmi modell kidolgozását**.**

Kutatásom alapfeltevése ezért az, hogy **a technológiai reziliencia nem önálló technológiai tulajdonság, hanem egy komplex szocio-technikai rendszer kialakuló jellemzője**, amely a technológiai, a szervezeti és a szabályozási dimenziók kölcsönhatásából alakul ki. A „kialakuló” jelző alkalmazása azért indokolt, mert a reziliencia nem vezethető vissza kizárólag az egyes komponensek tulajdonságaira. A kutatás alapfeltevése szerint a technológiai reziliencia nem önálló technológiai tulajdonság, hanem a technológiai, szervezeti és szabályozási dimenziók kölcsönhatásából kialakuló rendszerjellemző. Következésképpen a reziliencia nem vezethető vissza az egyes komponensek önálló fejlettségére, hanem kizárólag azok dinamikus együttműködésében értelmezhető.

A modell első változatát korábban önálló tanulmányban mutattam be, amely a *Hadtudományi Szemle* 2027. évi 1. számában jelenik meg **[**55]**[24]. A jelen értekezés ezt jelentősen továbbfejleszti azáltal, hogy részletesen elemzi a három dimenzió kölcsönhatásait, kidolgozza azok mérhetővé és értékelhetővé tételét, valamint javaslatot tesz a technológiai reziliencia mérésére szolgáló **Technological Resilience Index (TRI)** kialakítására.

A fejezet célja egy olyan integrált technológiai rezilienciamodell kidolgozása, amely egységes fogalmi keretben értelmezi a technológiai, szervezeti és szabályozási dimenziókat, valamint megalapozza azok empirikus vizsgálatát és mérhetőségét.

A fejezet eredményeként három, egymásra épülő tudományos hozzájárulást kívánok bemutatni. **(1) kidolgozom** az **integrált technológiai reziliencia háromdimenziós modelljét**, amely egységes rendszerben kapcsolja össze a technológiai, szervezeti és szabályozási dimenziókat. **(2) meghatározom** a **modell működési mechanizmusát** és bemutatom, hogy a három dimenzió kölcsönhatásai miként alakítják a rendszer alkalmazkodóképességét különböző zavarok és válsághelyzetek során. **(3) kidolgozom** a modell mérhetővé és értékelhetővé tételének alapelveit, és javaslatot teszek egy **Technological Resilience Index (TRI)** kialakítására, amely lehetőséget teremt a különböző technológiai rendszerek rezilienciájának objektív mérésére és összehasonlítására.

A modell tudományos újdonsága nem három reziliencia dimenzió azonosítása, hanem azok strukturális és dinamikus kapcsolatrendszerének mérhetővé és értékelhetővé tétele.

3.2 A technológiai reziliencia integrált fogalmi keretének kialakítása

3.2.1 A technológiai reziliencia integrált fogalmi keretének tudományos megalapozása

Véleményem szerint ez a fragmentált megközelítés egyre kevésbé alkalmas a XXI. századi digitális és kritikus infrastruktúrák működésének értelmezésére. Az ukrajnai háború, a globális ellátási láncok sérülékenysége, a kibertámadások növekvő komplexitása, valamint a mesterséges intelligencia gyors térnyerése egyértelműen azt mutatja, hogy a technológiai rendszerek működése már nem választható el a szervezeti döntéshozataltól, a stratégiai

[24] A kézirat lezárásakor (2026.08.17-én), a hivatkozott forrás még megjelenés előtt állt.

irányítástól és a szabályozási környezettől. Egy modern energetikai hálózat, egy intelligens közlekedési rendszer, egy felhőalapú kormányzati szolgáltatás vagy egy katonai vezetési és irányítási rendszer működőképességét nem kizárólag a technológiai architektúra minősége határozza meg, hanem legalább ilyen mértékben függ a szervezet felkészültségétől, a vezetési folyamatok rugalmasságától, valamint a szabályozási és stratégiai döntéshozatal minőségétől.

A technológiai reziliencia vizsgálata napjainkra a biztonságtudomány, a rendszerelmélet és a kritikus infrastruktúrák kutatásának egyik központi kérdésévé vált. A digitális transzformáció, a hálózatba kapcsolt rendszerek terjedése és a hibrid fenyegetések megjelenése következtében a technológiai rendszerek működése már nem értelmezhető kizárólag műszaki paraméterek alapján. A reziliens működés egyre inkább a technológiai infrastruktúra, a működtető szervezet és a szabályozási környezet összehangolt alkalmazkodóképességétől függ.

A reziliencia fogalma az elmúlt évtizedekben fokozatosan kilépett eredeti ökológiai értelmezési keretéből, és meghatározó elemévé vált a mérnöki rendszerek, a szervezeti működés, a kritikus infrastruktúrák, valamint a kibervédelem kutatásának. Bár az egyes megközelítések eltérő hangsúlyokat alkalmaznak, közös bennük annak felismerése, hogy a komplex rendszerek tartós működése nem kizárólag a meghibásodások elkerülésén, hanem az alkalmazkodóképességen alapul. [1],[12],[58],[4]

A modern technológiai rendszerek nyitott, adaptív és egymással szorosan összekapcsolt hálózatokat alkotnak. Egyetlen technológiai komponens működése gyakran több szervezet, digitális szolgáltatás és szabályozási mechanizmus együttes függvénye. Ez alapvetően megváltoztatja a reziliencia értelmezését is: a rendszer ellenálló képessége már nem vezethető vissza kizárólag az egyes technológiai elemek megbízhatóságára.

Ez a felismerés különösen jól szemléltethető a villamosenergia-ellátás, a közlekedési infrastruktúrák vagy a katonai vezetési rendszerek példáján. Egy korszerű villamosenergia-hálózat műszaki szempontból megfelelően redundáns lehet, rendelkezhet korszerű SCADA [25] -rendszerekkel, több kommunikációs útvonallal és fejlett hálózatfelügyeleti megoldásokkal. Mindez azonban önmagában nem garantálja a rendszer rezilienciáját. Ha az

[25] SCADA: Supervisory Control and Data Acquisition; felügyeleti irányító és adatgyűjtő rendszer.

üzemeltető szervezet nem rendelkezik megfelelő incidenskezelési eljárásokkal, ha a vezetői döntések lassúak, ha hiányzik a rendszeres gyakoroltatás vagy a szervezeti tanulás, akkor ugyanaz a technológia lényegesen sérülékenyebbé válik. Ugyanígy, ha a kritikus beszállítók nem tartoznak megfelelő kockázatkezelési követelmények alá, vagy hiányzik az állami koordináció és az ágazatok közötti együttműködés, akkor a rendszer stratégiai szinten válik sérülékennyé, függetlenül attól, hogy az egyes technológiai komponensek milyen fejlettséget képviselnek.

A fenti jelenség arra utal, hogy a technológiai reziliencia nem tekinthető egyetlen rendszerkomponens tulajdonságának. Sokkal inkább olyan kialakuló rendszerjellemzőként értelmezhető, amely a technológiai, szervezeti és szabályozási elemek kölcsönhatásából jön létre. A rendszer ellenálló képessége nem egyetlen komponens tulajdonsága, hanem a teljes rendszer működéséből kialakuló kialakuló tulajdonság. A komplex rendszerek elméletében a kialakuló tulajdonságok olyan jellemzők, amelyek nem vezethetők vissza az egyes elemek önálló vizsgálatára, hanem kizárólag azok kölcsönhatásaiból alakulnak ki [6]. Véleményem szerint a technológiai reziliencia is ilyen kialakuló rendszerjellemzőnek tekinthető.

A komplex adaptív rendszerek elmélete (Simon, Holland, Mitchell) közös alapfeltevése, hogy a rendszer egészének működése nem vezethető vissza az egyes elemek önálló viselkedésére. Az új tulajdonságok az elemek közötti kölcsönhatásokból, a visszacsatolásokból és az adaptív kapcsolatrendszerből alakulnak ki. [6],[76],[77],[7].

A jelen kutatás alapfeltevése szerint a technológiai reziliencia olyan kialakuló rendszerjellemző, amely a technológiai infrastruktúra, a szervezeti működés és a szabályozási környezet dinamikus kölcsönhatásából alakul ki. Ez az értelmezés összhangban áll Hollnagel reziliencia felfogásával, valamint Duchek adaptív szervezeti modelljével, ugyanakkor túl is mutat azokon, mivel a szervezeti dimenziót egy integrált technológiai rendszer részeként kezeli. [12],[4].

Az elmúlt évek európai szabályozási változásai – különösen a NIS2 irányelv, a CER irányelv és a Cyber Resilience Act – szintén arra utalnak, hogy a reziliencia fogalma fokozatosan kilépett a szűken értelmezett informatikai vagy mérnöki megközelítésből [25],[26],[27]. Ezek a szabályozások már nem kizárólag technikai védelmi intézkedéseket írnak elő, hanem a vezetői felelősséget, az ellátási láncok biztonságát, a kockázatirányítást, a folyamatos működés biztosítását és az intézményi koordinációt is a reziliencia részének

tekintik. Ez azt jelzi, hogy a gyakorlati szabályozás fejlődése megelőzte az egységes tudományos modell kialakulását.

A NATO rezilienciával kapcsolatos dokumentumai hasonló fejlődési irányt mutatnak. A szövetség rezilienciát már nem kizárólag katonai képességként értelmezi, hanem olyan nemzeti rendszerszintű tulajdonságként, amelyben a kritikus infrastruktúrák, a civil-katonai együttműködés, az ipari kapacitások, a digitális technológiák és a társadalmi alkalmazkodóképesség egyaránt meghatározó szerepet játszanak [23],[39]. Ez a szemlélet lényegében megerősíti azt a feltételezést, hogy a technológiai reziliencia csak integrált, többdimenziós megközelítésben értelmezhető.

A háromdimenziós modell kidolgozásának tudományos megalapozását a következő alfejezet részletes kritikai szakirodalmi elemzése támasztja alá, amely bemutatja a jelenlegi rezilienciaelméletek erősségeit, korlátait és az integrált megközelítés szükségességét.

3.2.2 A technológiai reziliencia jelenlegi tudományos modelljeinek kritikai elemzése

A technológiai rezilienciával foglalkozó szakirodalom napjainkra több, **egymástól eltérő elméleti irányzatot alakított ki.** Bár ezek a modellek saját elemzési szintjükön magas magyarázó erővel rendelkeznek, egyik sem képes önmagában a modern szocio-technikai rendszerek rezilienciájának teljes körű értelmezésére. A jelen alfejezet célja ezért nem a reziliencia elméletek ismertetése, hanem azok kritikai összehasonlítása és a kutatási rés pontos meghatározása.

A szakirodalom **három domináns megközelítés köré rendezhető**. **Az első a mérnöki reziliencia,** amely a technológiai rendszerek műszaki jellemzőire, a robusztusságra, a redundanciára és a helyreállítási képességre helyezi a hangsúlyt. A második **a szervezeti reziliencia**, amely az emberi tényezőket, a vezetési folyamatokat, a tanulási képességet és az adaptív működést tekinti a reziliencia alapjának.

A harmadik irányzat a kritikus infrastruktúrák és a nemzeti biztonság kutatásából fejlődött ki, amely a rezilienciát már **stratégiai, szabályozási és társadalmi** összefüggésben értelmezi [58],[4], [47], [87].

Megközelítés	Elemzési egység	Fő kérdés
Mérnöki	Technológia	Hogyan marad működőképes?
Szervezeti	Szervezet	Hogyan alkalmazkodik?
Szabályozási	Rendszer	Hogyan biztosítható a működés?

3.1. táblázat: a technológiai reziliencia összefüggései

E három megközelítés önállóan jelentős tudományos eredményeket hozott, ugyanakkor közös sajátosságuk, hogy eltérő elemzési szinteken vizsgálják ugyanazt a jelenséget. A mérnöki modellek elsősorban a technológiai architektúrát tekintik elemzési egységnek; a szervezeti modellek az intézményi működésre koncentrálnak; a stratégiai megközelítések pedig a nemzeti és nemzetközi szabályozási rendszerekből indulnak ki. A reziliencia tehát minden esetben ugyanazon rendszer eltérő metszeteként jelenik meg, nem pedig egységes rendszerjellemzőként.

Álláspontom szerint ez a fragmentált megközelítés jelenti a jelenlegi reziliencia kutatás egyik legfontosabb elméleti korlátját. A XXI. század technológiai rendszerei ugyanis nem különálló műszaki objektumokként működnek, hanem komplex szocio-technikai rendszerekként, amelyekben a technológiai infrastruktúra, a működtető szervezet, a szabályozási környezet és a külső partneri ökoszisztéma folyamatos kölcsönhatásban áll egymással. Egy kritikus infrastruktúra rezilienciája ezért nem vezethető le sem a műszaki architektúra megbízhatóságából, sem a szervezet adaptációs képességéből, sem a szabályozási megfelelőségből önmagában. A teljes rendszer ellenálló képessége e tényezők együttes működéséből alakul ki.

A modern digitális infrastruktúrák működése jól szemlélteti ezt a problémát. **Egy ország villamosenergia-ellátó rendszere műszaki szempontból magas fokú redundanciával rendelkezhet, korszerű vezérlőrendszereket alkalmazhat, valamint fejlett kibervédelmi megoldásokkal is felszerelhető**. Ennek ellenére egy súlyos kibertámadás vagy összetett hibrid művelet során a rendszer működése mégis összeomolhat, amennyiben a döntéshozatali folyamatok lassúak, a különböző szervezetek közötti koordináció nem megfelelő, vagy a szabályozási környezet nem biztosít elegendő rugalmasságot a gyors alkalmazkodáshoz. Ezzel szemben egy technológiailag kevésbé fejlett infrastruktúra is képes lehet magasabb rezilienciát mutatni, ha működtető szervezete gyorsan alkalmazkodik a változó környezethez, rendelkezik megfelelő vezetési kultúrával

és hatékony incidenskezelési eljárásokkal. A technológiai reziliencia tehát nem kizárólag technológiai tulajdonság, hanem a rendszer egészének működéséből fakadó képesség.

A **mérnöki reziliencia megközelítésének legnagyobb korlátja, hogy a rezilienciát alapvetően a technológiai architektúra tulajdonságaként kezeli**. A szervezeti döntések, a vezetési folyamatok és a szabályozási környezet többnyire háttérváltozóként jelennek meg, miközben a modern kritikus infrastruktúrák működésében ezek legalább akkora hatást gyakorolnak a rendszer alkalmazkodóképességére, mint maga a technológia.

A reziliencia modellek **kritikai elemzésének másik fontos tanulsága, hogy a legtöbb megközelítés implicit módon statikus rendszerképet feltételez**. A klasszikus rendszerbiztonsági modellek a rendszert meghatározott állapotban vizsgálják, és abból indulnak ki, hogy a környezet változásai korlátozott mértékűek vagy előre jelezhetők. A valóságban azonban a technológiai rendszerek folyamatos fejlődésen mennek keresztül. Új technológiák jelennek meg, a fenyegetések gyorsan változnak, az ellátási láncok átalakulnak, a mesterséges intelligencia új működési logikát vezet be, miközben a szabályozási környezet is folyamatosan módosul. Ebben a dinamikus környezetben a reziliencia nem tekinthető állandó tulajdonságnak; sokkal inkább olyan képességként értelmezhető, amelynek szintje időben változik, és amelyet a technológiai, szervezeti és szabályozási alkalmazkodás együttesen alakít.

Ez a felismerés **különösen hangsúlyossá vált az orosz–ukrán háború tapasztalatai alapján.** A konfliktus során világossá vált, hogy **a technológiai fölény önmagában nem garantálja a műveleti sikerességet.** A gyors innovációs ciklusok, a kereskedelmi technológiák katonai adaptációja, a szoftverek folyamatos módosítása, valamint a civil és katonai szereplők együttműködése sok esetben nagyobb jelentőséggel bírt, mint egy adott rendszer eredeti műszaki paraméterei. A reziliencia így már nem pusztán a túlélés vagy a helyreállítás képességét jelenti, hanem a folyamatos tanulás, az innováció és az adaptáció intézményesített képességét is. Ez a megközelítés ugyanakkor még csak részben jelenik meg a klasszikus reziliencia modellekben.

A szakirodalom további hiányossága, hogy a legtöbb modell nem vizsgálja megfelelő mélységben a különböző dimenziók közötti kölcsönhatásokat. A technológiai, szervezeti és szabályozási tényezők rendszerint egymástól elkülönítve jelennek meg, miközben a valós működés során ezek kölcsönösen erősítik vagy gyengítik egymást. Egy korszerű

technológiai megoldás csak akkor növeli a rezilienciát, ha a szervezet képes azt megfelelően alkalmazni, és a szabályozási környezet nem akadályozza annak adaptív használatát. Ugyanígy egy jól felépített szervezet sem képes magas rezilienciát elérni, ha az alkalmazott technológia elavult vagy a kritikus beszállítói láncok sérülékenyek. A reziliencia tehát nem az egyes dimenziók egyszerű összege, hanem azok kölcsönhatásából létrejövő kialakuló rendszerjellemző.

A reziliencia fogalmának fejlődése során külön figyelmet érdemel a szervezeti reziliencia kutatási irányzata, amely jelentősen kibővítette a korábban elsősorban műszaki szemléletű megközelítéseket. A szervezeti reziliencia képviselői abból indultak ki, hogy a komplex rendszerek működését nem kizárólag a technológiai infrastruktúra állapota határozza meg, hanem legalább ilyen jelentős szerepet játszanak a vezetési folyamatok, a döntéshozatal minősége, a szervezeti kultúra, a tudásmenedzsment, valamint a folyamatos tanulás képessége. A reziliencia ebben az értelmezésben már nem egy rendszer műszaki tulajdonsága, hanem olyan dinamikus szervezeti képesség, amely lehetővé teszi a bizonytalan környezethez való alkalmazkodást és a működőképesség fenntartását válsághelyzetekben is. [4],[59]

Ez a szemlélet jelentős előrelépést jelentett, mivel rámutatott arra, hogy az azonos technológiai háttérrel rendelkező szervezetek teljesítménye válsághelyzetben jelentősen eltérhet. A különbséget sok esetben nem a technológiai infrastruktúra minősége, hanem a vezetői döntéshozatal gyorsasága, a felelősségi körök egyértelműsége, a szervezeti kommunikáció, valamint a tanulási mechanizmusok hatékonysága magyarázza. Különösen igaz ez a kibervédelmi incidensek kezelésére, ahol a technikai védelem mellett meghatározó szerepet játszik az incidensreagáló csoportok felkészültsége, a döntési jogosultságok tisztázottsága és a szervezet adaptív működése.

Mindazonáltal a szervezeti rezilienciamodellek vizsgálata során hasonló korláttal találkozunk, mint a mérnöki megközelítések esetében, csak éppen ellenkező irányból. Míg a mérnöki modellek elsősorban a technológiára koncentrálnak és kevés figyelmet fordítanak a szervezeti tényezőkre, addig a szervezeti reziliencia kutatásai gyakran adottságként kezelik a technológiai infrastruktúrát. A technológia többnyire támogató háttérelemként jelenik meg, nem pedig olyan dinamikus komponensként, amely önmaga is folyamatosan fejlődik, sérülékenységeket hordoz és meghatározza a szervezeti alkalmazkodás lehetőségeit. Ez különösen problematikus a digitalizált működési környezetben, ahol a szervezet

alkalmazkodóképessége szorosan függ az alkalmazott technológiák rugalmasságától, interoperabilitásától és biztonsági architektúrájától.

A technológiai és szervezeti dimenziók mellett az elmúlt évtizedben önálló kutatási irányzattá fejlődött a cyber resilience, amely részben a klasszikus információbiztonsági modellek korlátaira adott válaszként jelent meg. Az információbiztonság hagyományosan a bizalmasság, sértetlenség és rendelkezésre állás (CIA-modell[26]) biztosítására koncentrált, abból a feltételezésből kiindulva, hogy megfelelő technikai és szervezeti kontrollok alkalmazásával a kockázatok elfogadható szintre csökkenthetők. A kibertér gyors változása azonban világossá tette, hogy a teljes védelem illúzió. A fejlett állami kiberműveletek, a zsarolóvírusok, az ellátási láncokat érintő támadások és a mesterséges intelligencia alkalmazása olyan fenyegetési környezetet hozott létre, amelyben a sikeres támadás lehetőségével minden szervezetnek számolnia kell.

A cyber resilience modellek elsősorban az információs rendszerek folytonos működésére és incidenskezelésére koncentrálnak. Ezért jól alkalmazhatók digitális infrastruktúrák vizsgálatára, ugyanakkor nem fedik le a fizikai infrastruktúrák, a szervezeti működés és a szabályozási környezet teljes kölcsönhatásrendszerét.

Jó példát szolgáltat erre a villamosenergia-ágazat számára kidolgozott hálózatbiztonsági monitorozási architektúra, amely Zeek, Suricata és SIEM [27] alapú eseményfeldolgozással képes az OT-protokollok folyamatos elemzésére. A technológiai eszközök önmagukban nem elegendők: a hatékony monitorozás előfeltétele a megfelelő architektúra kialakítása, a protokollspecifikus ismeretek, az incidenskezelési folyamatok és az üzemeltetési környezet sajátosságainak figyelembevétele. [78] Ez jól mutatja, hogy a cyber resilience gyakorlati megvalósítása is túlmutat a tisztán technológiai megközelítésen.

A NATO és az Európai Unió rezilienciával kapcsolatos dokumentumai egyaránt a teljes állami és társadalmi megközelítés (whole-of-government, whole-of-society) szükségességét hangsúlyozzák. E stratégiai szemlélet fontos előrelépést jelent, ugyanakkor

[26] CIA-modell – Confidentiality, Integrity, Availability, magyarul bizalmasság, sértetlenség és rendelkezésre állás. A „CIA” rövidítés tehát nem az amerikai hírszerző szervezetre utal, hanem az információbiztonság három klasszikus alapkövetelményének angol kezdőbetűiből képzett betűszó: az információhoz csak az arra jogosultak férjenek hozzá (bizalmasság), annak tartalma jogosulatlanul ne módosuljon (sértetlenség), valamint az információ és az azt kezelő rendszer szükség esetén hozzáférhető és működőképes legyen (rendelkezésre állás).

[27] SIEM: Security Information and Event management

elsősorban irányítási és szabályozási keretként jelenik meg, nem pedig mérhetővé és értékelhetővé tehető tudományos modellként. [23], [39].

E dokumentumok elemzése ugyanakkor arra is rámutat, hogy a gyakorlati szabályozás fejlődése gyorsabb volt, mint az azt alátámasztó tudományos modellek fejlődése. A szabályozások már rendszerszintű gondolkodást követelnek meg, azonban a szakirodalomban továbbra is kevés olyan modell található, amely egységes elméleti keretben képes lenne összekapcsolni a technológiai, a szervezeti és a szabályozási dimenziókat. A jelenlegi kutatások többsége továbbra is egy-egy részterületre fókuszál, így a dimenziók közötti kölcsönhatások vizsgálata háttérbe szorul.

Álláspontom szerint éppen ez jelenti a technológiai reziliencia kutatásának legfontosabb nyitott kérdését. A modern technológiai rendszerek ellenálló képessége nem érthető meg kizárólag műszaki paraméterek, szervezeti folyamatok vagy jogszabályi követelmények elemzésével. A reziliencia olyan komplex rendszerjellemző, amely a technológiai infrastruktúra, a működtető szervezet és a szabályozási környezet folyamatos kölcsönhatásából alakul ki. E három dimenzió egymástól nem választható el, mivel bármelyik gyengesége a teljes rendszer ellenálló képességét csökkenti, ugyanakkor bármelyik fejlesztése csak akkor eredményez tartós javulást, ha a másik két dimenzió is képes alkalmazkodni.

A kritikai elemzés alapján megállapítható, hogy a jelenlegi reziliencia elméletek három eltérő elemzési szintre koncentrálnak: a technológiai rendszerre, a szervezetre vagy a szabályozási környezetre. Jelenleg nem áll rendelkezésre olyan egységes fogalmi modell, amely e három dimenzió kölcsönhatását integrált szocio-technikai rendszerként írná le, valamint lehetővé tenné annak mérhetővé és értékelhetővé tételét és mérését. Ez képezi a jelen kutatás elsődleges kutatási résést.

A technológiai reziliencia értelmezésének további hiányossága, hogy a jelenlegi modellek többsége a rendszerek működését elsősorban reaktív szemléletben vizsgálja. A legtöbb definíció és módszertan abból indul ki, hogy valamilyen zavar, incidens vagy válság már bekövetkezett, és a reziliencia lényege ennek következményeinek kezelése, illetve a működés helyreállítása. Ez a megközelítés kétségtelenül fontos eleme a rezilienciának, azonban a XXI. század technológiai környezetében önmagában már nem elegendő.

A modern technológiai rendszerek működését ugyanis egyre inkább folyamatos változás jellemzi. A mesterséges intelligencia alkalmazása, a szoftverek napi szintű frissítése, a felhőszolgáltatások dinamikus konfigurációja, valamint az autonóm rendszerek adaptív működése következtében maga a rendszer is állandó fejlődésben van. Ehhez társul a fenyegetési környezet rendkívül gyors átalakulása: új kibertámadási módszerek, ellátási láncokat érintő sérülékenységek, hibrid műveletek, valamint a kereskedelmi technológiák katonai alkalmazása folyamatosan módosítják a működési feltételeket. Ebben a környezetben a reziliencia nem korlátozódhat kizárólag a helyreállítás képességére; legalább ilyen fontos az előrelátás, a folyamatos monitorozás, a korai alkalmazkodás és az innovációs képesség.

E szemléletváltás már megjelent a legújabb NATO- és európai uniós dokumentumokban, ahol a rezilienciát egyre inkább a stratégiai előrelátással, a képességfejlesztéssel és a folyamatos alkalmazkodással kapcsolják össze [23],[25],[26],[39]. Ugyanakkor a tudományos modellek jelentős része még mindig nem építi be ezt a dinamikus megközelítést. A reziliencia többnyire egy adott időpillanatban vizsgált rendszerjellemzőként jelenik meg, miközben kevés figyelmet kap az a kérdés, hogy maga a reziliencia hogyan fejlődik, hogyan romlik vagy miként alakítható tudatosan a rendszer teljes életciklusa során.

Álláspontom szerint a technológiai rezilienciát ezért nem állapotként, hanem képességként célszerű értelmezni. A képességalapú megközelítés lehetővé teszi annak vizsgálatát, hogy egy rendszer milyen mértékben képes érzékelni a környezet változásait, előre jelezni a potenciális fenyegetéseket, alkalmazkodni az új működési feltételekhez, valamint a megszerzett tapasztalatokat beépíteni későbbi működésébe. Ez a szemlélet közelebb áll a komplex adaptív rendszerek elméletéhez, mint a hagyományos rendszerbiztonsági modellekhez.

A reziliencia dinamikus értelmezése különösen fontos a kritikus infrastruktúrák esetében. Az energiaellátás, a közlekedési hálózatok, a kommunikációs rendszerek vagy az egészségügyi infrastruktúrák működése ma már nagymértékben függ a digitális technológiáktól. Ezek a rendszerek egyszerre fizikai és virtuális komponensekből állnak, működésüket pedig különböző szervezetek, szolgáltatók és szabályozó intézmények közösen biztosítják. Ennek következtében egyetlen technológiai változás – például egy új szoftverplatform bevezetése vagy egy mesterséges intelligencián alapuló döntéstámogató

rendszer alkalmazása – nemcsak a technológiai dimenziót érinti, hanem módosítja a szervezeti folyamatokat, az emberi feladatmegosztást, valamint a szabályozási követelményeket is.

Ez a jelenség rámutat arra, hogy a technológiai reziliencia nem lineáris folyamat. A három dimenzió – technológiai, szervezeti és szabályozási – kölcsönösen alakítja egymást, és ezek között folyamatos visszacsatolások működnek. Egy technológiai innováció új szervezeti képességeket igényel; a szervezeti alkalmazkodás új szabályozási megoldásokat tesz szükségessé; a szabályozási környezet pedig visszahat a technológiai fejlesztések irányára. Ez a kölcsönös függőség azt eredményezi, hogy a reziliencia nem írható le egyszerű ok-okozati kapcsolatokkal, hanem összetett adaptív folyamatként értelmezhető.

A nemzetközi szakirodalomban e kölcsönhatások csak részlegesen jelennek meg. Linkov és munkatársai hangsúlyozzák a különböző rendszerszintek integrált vizsgálatának szükségességét, azonban modelljük elsősorban a döntéstámogatásra és a kockázatkezelésre koncentrál [47]. A Resilience Engineering irányzat az operatív alkalmazkodás jelentőségét emeli ki, de kevésbé foglalkozik a stratégiai irányítás kérdéseivel [12]. A szervezeti reziliencia modelljei részletesen elemzik a vezetési és tanulási folyamatokat, ugyanakkor nem tárgyalják kellő mélységben a technológiai architektúra fejlődésének hatását [4]. A kritikus infrastruktúrák kutatása pedig elsősorban az állami szabályozásra és a nemzeti biztonságra koncentrál, miközben a technológiai innovációk szervezeti következményei háttérbe szorulnak.

Mindezek alapján megállapítható, hogy a jelenlegi modellek vertikálisan jól kidolgozottak, azonban horizontálisan kevéssé integráltak. Mélyreható elemzést adnak saját szakterületükön, de ritkán vizsgálják a más tudományterületekkel fennálló kölcsönhatásokat. A technológiai reziliencia átfogó értelmezéséhez viszont éppen ezeknek a kapcsolatoknak a feltárása szükséges. A modern szocio-technikai rendszerek ellenálló képessége ugyanis nem az egyes dimenziók önálló fejlettségéből, hanem azok összehangolt működéséből származik.

E felismerés alapján jelen értekezés második tudományos állítása az, hogy a technológiai reziliencia nem redukálható egyetlen tudományterület elemzési keretére. A technológiai, szervezeti és szabályozási dimenziók egymástól elválaszthatatlanok, és csak együttes vizsgálatuk teszi lehetővé a komplex rendszerek valós ellenálló képességének értékelését. Ennek megfelelően a következő alfejezetben bemutatott háromdimenziós

technológiai reziliencia-modell nem a meglévő elméletek alternatívájaként jelenik meg, hanem azok integrációjára törekszik. A modell célja, hogy egységes fogalmi keretben kapcsolja össze a mérnöki reziliencia technológiai megközelítését, a szervezeti reziliencia adaptív szemléletét és a kritikus infrastruktúrák stratégiai irányításának követelményeit, ezáltal új elméleti alapot biztosítva a technológiai reziliencia értelmezéséhez és méréséhez.

Modell	Elemzési egység	Fő fókusz	Erősség	Hiányosság	Mi indokolja az új modellt?
Mérnöki reziliencia (Hollnagel et al., 2006; Madni & Jackson, 2009) **[12],[14]**	Technológiai rendszer	Robusztusság, redundancia, helyreállítás	Erős műszaki alapok, jól mérhető paraméterek	A szervezeti és szabályozási tényezőket háttérfeltételként kezeli	A technológiai architektúra önmagában nem magyarázza a rendszer teljes rezilienciáját.
Resilience Engineering (Hollnagel et al., 2006)	Működési folyamatok	Adaptáció, monitorozás, tanulás	Dinamikus szemlélet, ember–technológia kapcsolat	Kevés hangsúlyt fektet a stratégiai irányításra és szabályozásra	Az operatív adaptáció mellett szükséges a szervezeti és szabályozási dimenzió integrálása.
Szervezeti reziliencia (Lengnick-Hall & Beck, 2005; Duchek, 2020) **[4],[59]**	Szervezet	Vezetés, tanulás, adaptív képesség	Jól magyarázza a szervezeti alkalmazkodást	A technológiai infrastruktúrát többnyire adottságként kezeli	A technológiai architektúra aktív szereplő, nem csupán háttérelem.
Cyber resilience (NIST, 2024; ENISA, 2024) **[40],[41]**	Digitális infrastruktúra	Incidenskezelés, üzletmenet-folytonosság	Korszerű kibervédelmi megközelítés	Elsősorban informatikai rendszerekre koncentrál	A technológiai reziliencia a fizikai, digitális és szervezeti rendszereket egyaránt magában foglalja.
Linkov-féle rezilienciakeret (Linkov et al., 2013; Linkov & Trump, 2019) **[58],[47]**	Komplex rendszerek	Kockázatkezelés, döntéstámogatás	Integrált szemlélet, mérhetőség	Kevésbé tárgyalja a szervezeti működés és szabályozás kölcsönhatásait	A dimenziók dinamikus kapcsolatrendszerének explicit modellezése szükséges.
Kritikus infrastruktúra/NATO–EU megközelítés (NATO, 2022; NATO STO, 2023; NIS2; CER) **[25],[26],[23],[39]**	Nemzeti rendszerek	Stratégiai irányítás, kritikus infrastruktúrák	Rendszerszintű gondolkodás, szabályozási keret	Inkább normatív követelményrendszer, mint tudományos modell	Szükség van egy általános, tudományosan megalapozott fogalmi modellre.
Jelen kutatás háromdimenziós technológiai rezilienciamodellje	Integrált szocio-technikai rendszer	Technológiai–szervezeti–szabályozási dimenziók kölcsönhatása	Egységes fogalmi keret, dinamikus kölcsönhatások, mérési lehetőség (TRI)	Empirikus validációt igényel	A kutatási résre adott válasz; a korábbi modellek integrációjára épülő új elméleti keret.

3.2. táblázat: A technológiai reziliencia meghatározó tudományos modelljeinek összehasonlítása (a jelzett források alapján, saját szerkesztés)

Az összehasonlító elemzés alapján megállapítható, hogy valamennyi modell fontos részeredményt nyújt a reziliencia értelmezéséhez, ugyanakkor egyik sem kezeli egységes rendszerben a technológiai, szervezeti és szabályozási dimenziók dinamikus kölcsönhatását. A jelen kutatás erre a hiányra válaszol a következő alfejezetben bemutatott háromdimenziós technológiai rezilienciamodell kidolgozásával.

A szakirodalom kritikai elemzése alapján ezért jelen kutatás **kutatási rését (research gap)** a következőképpen fogalmazom meg:

Az általam áttekintett hazai és nemzetközi szakirodalomban nem azonosítottam olyan integrált elméleti modellt, amely a technológiai rezilienciát a technológiai, a szervezeti és a szabályozási dimenziók dinamikus kölcsönhatásából létrejövő kialakuló rendszerjellemzőként értelmezné, és egyúttal alkalmas lenne e dimenziók kapcsolatának elemzésére és értékelésére.

Az elemzett megközelítések összevetése alapján a kutatási rés tehát nem az egyes technológiai, szervezeti vagy szabályozási–irányítási tényezők hiányában azonosítható, mivel ezek különböző formában már jelen vannak a szakirodalomban. A hiány abban ragadható meg, hogy e tényezők integrált kapcsolatrendszere, a dimenziók közötti korlátozó interfészek, a reziliencia időbeli adaptációja, valamint mindezek egységes mérhetővé és értékelhetővé tétele nem jelenik meg egyetlen koherens elemzési keretben. **E kutatási rés képezi a következő alfejezetben bemutatott háromdimenziós technológiai rezilienciamodell kidolgozásának közvetlen elméleti kiindulópontját.**

A következőkben bemutatott T–O–R modell tehát nem a hivatkozott rezilienciamodellek reprodukciója, hanem azok kritikai összevetéséből azonosított hiányosságokra adott saját integrációs és mérési és értékelési válasz.

3.2.3 A háromdimenziós technológiai reziliencia-modell koncepcionális alapjai

A 3.1.2 alfejezetben azonosított kutatási rés alapján jelen értekezés a technológiai rezilienciát olyan integrált szocio-technikai rendszerképességként értelmezi, amely a technológiai, a szervezeti és a szabályozási dimenziók dinamikus kölcsönhatásából alakul ki. A jelen alfejezet célja e háromdimenziós modell koncepcionális alapjainak meghatározása, valamint azon alapelvek rögzítése, amelyekre a modell későbbi szerkezeti felépítése, dinamikus működési logikája és mérhetővé és értékelhetővé tétele épül.

A modell kialakításának kiindulópontját a 3.1.2 alfejezetben elvégzett kritikai szintézis adja. Ennek alapján a mérnöki reziliencia, a Resilience Engineering, a szervezeti reziliencia, a cyber resilience, valamint a kritikus infrastruktúrák stratégiai és szabályozási megközelítései ugyanazon komplex rendszer eltérő aspektusait írják le. Jelen kutatás ezért nem újabb részmodellt kíván létrehozni, hanem e megközelítések releváns elemeit integrálja egy közös szocio-technikai keretbe**.**

A modell rendszerelméleti alapját a komplex adaptív rendszerek megközelítése biztosítja. Simon szerint a komplex rendszerek működése nem érthető meg kizárólag komponenseik izolált vizsgálatával, mivel viselkedésüket az elemek közötti kapcsolatok is meghatározzák. Holland ezt az adaptáció és a kialakuló tulajdonságok megjelenésével egészíti ki, míg Mitchell arra mutat rá, hogy a rendszer egészének viselkedése az elemek közötti kölcsönhatásokból alakul ki. [76], [77], [7] Ebből következően a technológiai reziliencia sem az egyes rendszerkomponensek egyszerű összegeként, hanem azok kölcsönhatásából kialakuló rendszerképességként értelmezhető.

E rendszerelméleti alapot egészíti ki a szocio-technikai rendszerek megközelítése, amely szerint a technológiai és az emberi-szervezeti alrendszerek egymástól nem választhatók el. [10],[11] A digitalizáció ezt a kölcsönös függőséget tovább erősítette: a technológiai változások módosítják a szervezeti működést és új szabályozási igényeket teremtenek, miközben a szervezeti és szabályozási környezet visszahat a technológiák fejlesztésére, alkalmazására és adaptációjára.

A jelen kutatás ebből kiindulva három, analitikusan elkülöníthető, ugyanakkor funkcionálisan egymástól elválaszthatatlan dimenziót azonosít: a technológiai, a szervezeti és a szabályozási dimenziót. A háromdimenziós felosztás nem önkényes kategorizálás, hanem a korábban bemutatott rezilienciamodellek kritikai szintéziséből levezetett elméleti konstrukció. A modell újdonsága ezért nem önmagában e tényezők azonosításában, hanem azok egyenrangú rendszerkomponensként történő integrálásában és kölcsönhatásaik explicit vizsgálatában rejlik. Különösen lényeges, hogy a szabályozási és irányítási dimenzió a modellben nem külső környezeti feltételként, hanem a technológiai reziliencia konstitutív elemeként jelenik meg. [55]

A modell kidolgozásának második alapfeltevése, hogy a technológiai rezilienciát **nem állapotként, hanem dinamikus képességként** célszerű értelmezni. Ez a megközelítés

összhangban áll Teece dinamikus képességek elméletével, amely szerint a hosszú távú versenyképességet nem az erőforrások megléte, hanem azok folyamatos újrakonfigurálásának képessége biztosítja.[33] Hasonló gondolat jelenik meg Duchek szervezeti reziliencia-modelljében is, ahol a reziliencia három egymást követő képesség – anticipáció, megküzdés és adaptáció – integrált működéseként jelenik meg. A jelen kutatás ezt a szemléletet kiterjeszti a technológiai rendszerek egészére, és azt feltételezi, hogy a reziliencia a technológiai infrastruktúra, a szervezeti működés és a szabályozási környezet együttes adaptációs képességében nyilvánul meg. [4], [55]

A modell kialakításakor meghatározó szempont volt, hogy alkalmas legyen mind a kritikus infrastruktúrák, mind a védelmi technológiák, mind pedig a polgári digitális rendszerek elemzésére. Ezért a modell nem egy adott ágazat sajátosságaira épül, hanem olyan általános rendszerelméleti alapelvekre, amelyek különböző technológiai környezetekben egyaránt alkalmazhatók. A háromdimenziós felépítés célja nem a rendszerek egyszerű kategorizálása, hanem annak bemutatása, hogy a reziliencia minden esetben e három dimenzió kölcsönhatásából jön létre.

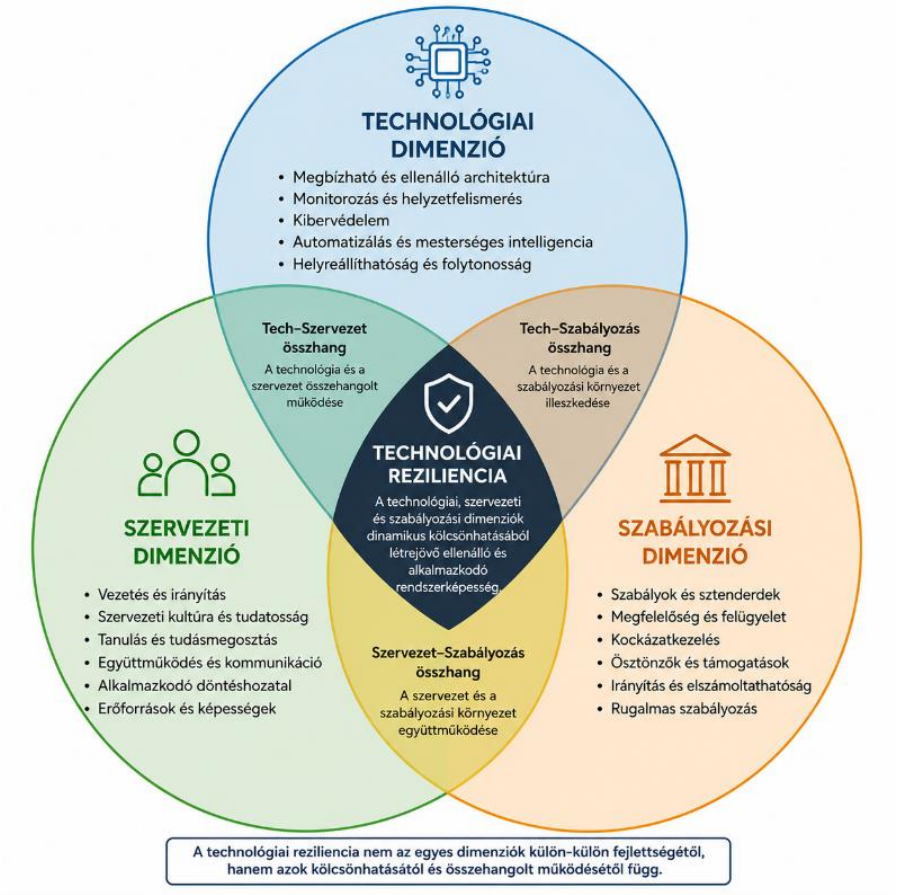
A **háromdimenziós modell kialakítása nem önkényes kategorizálás eredménye, hanem a rezilienciával foglalkozó nemzetközi szakirodalom kritikai szintéziséből levezetett elméleti következtetés**. A 3.1.2 alfejezet elemzése rámutatott arra, hogy a technológiai rezilienciát meghatározó tényezők három jól elkülöníthető, ugyanakkor egymástól elválaszthatatlan rendszerkomponens köré rendezhetők. Ezek a technológiai infrastruktúra, a működtető szervezet és az irányítási-szabályozási környezet. Bár a szakirodalomban ezek különböző hangsúllyal jelennek meg, egyik megközelítés sem képes önmagában a technológiai reziliencia teljes értelmezésére.

A mérnöki reziliencia elsősorban a technológiai rendszer belső tulajdonságait tekinti meghatározónak. A rendszer robusztussága, redundanciája, modularitása, hibatűrése, valamint helyreállítási képessége képezik a reziliens működés alapját. [12],[14],[57] Ez a megközelítés különösen jól alkalmazható zárt vagy jól definiálható műszaki rendszerek esetében, azonban a digitális transzformáció következtében kialakuló nyílt, hálózatos és folyamatosan változó rendszerek vizsgálatához már önmagában nem elegendő.

A szervezeti reziliencia kutatásai ezzel párhuzamosan arra mutattak rá, hogy ugyanazon technológiai infrastruktúra eltérő szervezeti környezetben jelentősen különböző

teljesítményt mutathat. A vezetési struktúra, a szervezeti kultúra, a tanulási folyamatok, a tudásmenedzsment és az adaptív döntéshozatal alapvetően befolyásolják a technológia tényleges alkalmazhatóságát. [4],[59],[32] Ez arra utal, hogy a technológiai képességek önmagukban nem hozzák létre a rezilienciát; azok eredményessége a szervezeti működés minőségétől is függ.

A harmadik meghatározó tényező a szabályozási és irányítási környezet. Az elmúlt években az Európai Unió, a NATO és számos nemzeti stratégia egyaránt felismerte, hogy a kritikus infrastruktúrák és a digitális rendszerek ellenálló képessége nem biztosítható kizárólag technológiai fejlesztésekkel. A reziliencia kialakításának nélkülözhetetlen feltétele a megfelelő irányítási rendszer, a kockázatalapú szabályozás, a megfelelőségi követelmények, a stratégiai koordináció és az intézményi együttműködés kialakítása. [23],[25],[26],[39] A szabályozási dimenzió tehát nem külső környezetként, hanem a technológiai rendszer működésének egyik meghatározó komponenseként jelenik meg.



3.1. ábra: A három dimenzió Venn-diagramja (saját szerkesztés)

Álláspontom szerint e három dimenzió együtt alkotja azt a minimális elméleti keretet, amely a technológiai reziliencia teljes körű értelmezéséhez szükséges. A három dimenzió kiválasztását nem gyakorlati megfontolások, hanem rendszerelméleti indokok támasztják alá.

Egyrészt **nem elegendő két dimenzió alkalmazása**. Amennyiben a modellt kizárólag technológiai és szervezeti komponensekre bontanánk, a szabályozási környezet csupán külső feltételként jelenne meg. Ez azonban ellentmond a jelenlegi európai és NATO-megközelítésnek, ahol a jogi, stratégiai és irányítási keretek közvetlenül meghatározzák a technológiai fejlesztések irányát, az innováció sebességét és a szervezeti működés lehetőségeit. **[**25],[23] A szabályozási dimenzió ezért nem tekinthető a rendszeren kívüli (exogén) tényezőnek, hanem annak szerves, működését közvetlenül alakító részét képezi.

Másrészt **nem indokolt a modell további dimenziókra bontása sem**. Felmerülhet például egy gazdasági, társadalmi vagy geopolitikai dimenzió önálló kezelése. A jelen

kutatás azonban abból indul ki, hogy ezek a tényezők közvetlenül valamelyik alapdimenzión keresztül fejtik ki hatásukat. A finanszírozási mechanizmusok például a szabályozási és irányítási rendszer részeként jelennek meg; a humán erőforrás kérdései a szervezeti dimenzióba illeszkednek; a technológiai innováció pedig értelemszerűen a technológiai dimenzió egyik meghatározó eleme. Ennek megfelelően a háromdimenziós modell egyszerre biztosít megfelelő részletezettséget és elméleti egyszerűséget, megfelelve Occam borotvája elvének, amely szerint az azonos magyarázó erejű modellek közül az egyszerűbb részesítendő előnyben. [79]

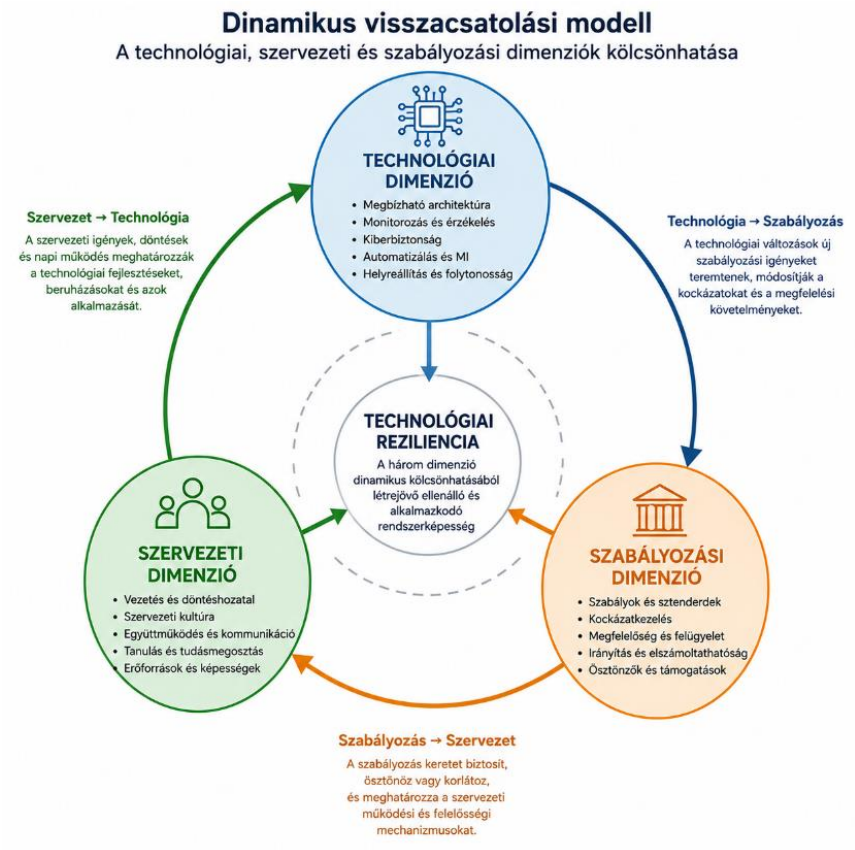
A modell kialakításakor meghatározó szempont volt továbbá, hogy alkalmas legyen különböző technológiai rendszerek összehasonlító elemzésére. Egy katonai vezetési rendszer, egy villamosenergia-hálózat, egy egészségügyi információs rendszer vagy egy autonóm járműrendszer technológiai sajátosságai jelentősen eltérnek egymástól. A háromdimenziós megközelítés ugyanakkor lehetővé teszi, hogy e rendszerek közös reziliencia jellemzőit egységes elemzési keretben vizsgáljuk. A modell így nem egyetlen technológiai terület sajátosságaira épül, hanem általános szocio-technikai rendszerként értelmezi a technológiai rezilienciát.

A modell nem hierarchikus, hanem hálózatos szemléletű. A technológiai, szervezeti és szabályozási dimenziók egyike sem tekinthető dominánsnak: kölcsönösen függnek egymástól, és bármely dimenzió tartós gyengesége korlátozhatja a teljes rendszer rezilienciáját. A modell ezért nem kizárólag az egyes dimenziók fejlettségét, hanem a közöttük fennálló kapcsolatok minőségét is vizsgálja.

A dimenziók kapcsolata dinamikus visszacsatolási rendszerként értelmezhető. A technológiai innováció módosítja a szervezeti működést; a szervezeti tanulás új technológiai igényeket generál; a szabályozás ösztönözheti vagy korlátozhatja az innovációt; a technológiai változás pedig új szabályozási igényeket hozhat létre. A reziliencia ebből következően nem lineáris ok-okozati kapcsolatok, hanem folyamatos adaptációs ciklusok eredménye. Ez a dinamikus szemlélet egyben megalapozza a következő fejezetben bemutatott működési modell és a Technological Resilience Index (TRI) kidolgozását is [55].

A háromdimenziós modell ugyanakkor nem statikus struktúraként értelmezendő. A technológiai, szervezeti és szabályozási dimenziók között folyamatos, kétirányú kölcsönhatások és visszacsatolások működnek. A technológiai változások módosítják a

szervezeti működés feltételeit és új szabályozási igényeket generálnak; a szervezeti tanulás és döntéshozatal új technológiai követelményeket hoz létre; a szabályozási és irányítási környezet pedig ösztönözheti vagy korlátozhatja mind a technológiai, mind a szervezeti adaptációt. A modell e dinamikus kapcsolatrendszerét a 3.2. ábra szemlélteti.



3.2. ábra: Dinamikus visszacsatolási modell (saját szerkesztés)

A visszacsatolási kapcsolatok azt fejezik ki, hogy a három dimenzió változásai kölcsönösen módosítják egymás állapotát és adaptációs képességét. A modellben ezért a technológiai reziliencia nem egyszeri egyensúlyi állapot, hanem folyamatos alkalmazkodási folyamat. Egy technológiai innováció szervezeti változást és új szabályozási igényt válthat ki, miközben a szabályozási környezet vagy a szervezeti működés változása új technológiai megoldások bevezetését teheti szükségessé.

Ebből következően a rendszer rezilienciáját nem kizárólag az egyes dimenziók aktuális fejlettsége, hanem azok alkalmazkodási sebessége, egymásra gyakorolt hatása és a visszacsatolási mechanizmusok működőképessége határozza meg. A reziliens rendszer tehát nem feltétlenül az, amelyben minden komponens optimális állapotban van, hanem az, amely

képes a zavarok hatására saját technológiai, szervezeti és szabályozási konfigurációját összehangoltan módosítani.

3.2.3.1 A háromdimenziós technológiai reziliencia-modell alapelvei

A modell koncepcionális felépítésének meghatározását követően szükséges azoknak az alapelveknek a rögzítése, amelyek meghatározzák a technológiai reziliencia értelmezésének logikai kereteit. Ezek az alapelvek nem egyszerű definíciók vagy módszertani ajánlások, hanem olyan elméleti tételek, amelyek meghatározzák a modell belső konzisztenciáját és egyben kijelölik annak alkalmazási tartományát. A jelen kutatásban kidolgozott háromdimenziós modell e négy alapelvre épül.

Az első alapelv: a technológiai reziliencia kialakuló rendszerképesség

A komplex rendszerek kutatásában széles körben elfogadott megközelítés, hogy a rendszer egészének viselkedése nem vezethető vissza az egyes komponensek tulajdonságaira. Simon már korán rámutatott arra, hogy a komplex rendszerek hierarchikus felépítése és a komponensek közötti kölcsönhatások olyan új tulajdonságokat eredményeznek, amelyek az alrendszerek önálló vizsgálatából nem vezethetők le. Holland ezt a jelenséget a komplex adaptív rendszerek emergenciájával magyarázza, míg Mitchell szerint a kialakuló tulajdonságok a rendszer elemei közötti nemlineáris kapcsolatokból származnak**.** [6], [7]

A reziliencia kutatásában hasonló szemlélet jelenik meg Hollnagel és munkatársainál, akik szerint a biztonság és a reziliencia nem egyetlen komponens jellemzője, hanem a rendszer egészének működéséből fakadó tulajdonság. Linkov és Trump ugyancsak hangsúlyozzák, hogy a rezilienciát nem célszerű kizárólag technológiai vagy szervezeti szinten értelmezni, hanem a különböző rendszerszintek integrált működésének eredményeként kell vizsgálni. [47]

A jelen kutatás ezt a gondolatmenetet továbbfejlesztve abból indul ki, hogy **a technológiai reziliencia nem vezethető vissza sem a technológiai infrastruktúra fejlettségére, sem a szervezet alkalmazkodóképességére, sem a szabályozási környezet minőségére önmagában. A technológiai reziliencia e három dimenzió dinamikus kölcsönhatásából létrejövő kialakuló rendszerképesség**. [55]

Ez azt jelenti, hogy két azonos technológiai rendszer eltérő szervezeti vagy szabályozási környezetben eltérő rezilienciával rendelkezhet, miközben két különböző technológiai architektúra hasonló rezilienciát mutathat megfelelő szervezeti adaptáció és irányítás mellett. A reziliencia tehát nem az egyes dimenziók abszolút fejlettségétől, hanem azok összehangolt működésétől függ.

A második alapelv: a technológiai reziliencia dinamikus képesség

A hagyományos biztonsági modellek a rendszereket általában statikus állapotként vizsgálják. A rendszer biztonsága vagy megbízhatósága egy adott időpontban mérhető tulajdonságként jelenik meg, amely megfelelő tervezéssel és karbantartással fenntartható [57]. A XXI. század technológiai környezetében azonban ez a megközelítés egyre kevésbé tartható.

A digitális rendszerek működése folyamatos változás alatt áll. A szoftverek rendszeres frissítése, a mesterséges intelligencia fejlődése, a felhőalapú infrastruktúrák dinamikus konfigurációja, valamint a kibertér fenyegetéseinek gyors változása következtében maga a rendszer is állandó adaptációs folyamatban van. [40], [41]

A reziliencia kutatásában ezt a szemléletet képviseli Duchek, aki a rezilienciát három egymást követő képesség – anticipáció, megküzdés és adaptáció – integrált működéseként értelmezi. Hasonló megközelítés jelenik meg Teece dinamikus képességek elméletében, amely szerint a szervezetek versenyelőnye nem az erőforrásaikból, hanem azok folyamatos újrakonfigurálásából származik. [4], [33]

A jelen kutatás e megközelítéseket integrálva abból indul ki, hogy **a technológiai reziliencia nem statikus rendszerállapot, hanem folyamatosan változó képesség**, amelyet a technológiai fejlődés, a szervezeti tanulás és a szabályozási alkalmazkodás együttesen alakít. [55]

Ennek megfelelően a technológiai rezilienciát nem elegendő egy adott időpillanatban mérni; annak vizsgálata során figyelembe kell venni a rendszer fejlődési pályáját, alkalmazkodási sebességét és innovációs képességét is.

A harmadik alapelv: a dimenziók kölcsönhatása fontosabb, mint azok önálló fejlettsége

A rezilienciamodellek jelentős része implicit módon abból indul ki, hogy a rendszer ellenálló képessége javítható az egyes komponensek fejlesztésével. A jelen kutatás ezzel szemben azt feltételezi, hogy a technológiai rezilienciát nem elsősorban az egyes dimenziók önálló fejlettsége, hanem azok együttműködésének minősége határozza meg.

Ez a megközelítés összhangban áll a komplex adaptív rendszerek elméletével, valamint a kritikus infrastruktúrák hálózatelméleti kutatásaival, amelyek szerint a rendszer teljesítményét gyakran a kapcsolatok minősége befolyásolja erősebben, mint az egyes elemek fejlettsége. [58], [77]

Ennek megfelelően egy korszerű mesterséges intelligenciával támogatott döntéstámogató rendszer sem növeli érdemben a rezilienciát, ha a szervezet nem képes annak alkalmazására vagy a szabályozási környezet nem teszi lehetővé annak gyors adaptációját. Ugyanakkor egy technológiailag szerényebb rendszer is magas rezilienciát érhet el, ha a szervezeti működés gyors, a döntéshozatal decentralizált, valamint a szabályozási környezet támogatja az innovációt.

A jelen modell ezért a dimenziók közötti kapcsolatok vizsgálatát tekinti elsődleges elemzési egységnek, nem pedig az egyes dimenziók önálló fejlettségét. [55]

A negyedik alapelv: a technológiai reziliencia fejleszthető rendszerképesség

A reziliencia nem veleszületett tulajdonság és nem kizárólag technológiai beruházások eredménye. A szakirodalom egyre szélesebb köre hangsúlyozza, hogy a reziliencia tudatos stratégiai irányítással, szervezeti tanulással, technológiai innovációval és megfelelő szabályozási környezet kialakításával fejleszthető**.** [47], [4]

A jelen kutatás ezt továbbfejlesztve azt állítja, hogy **a technológiai reziliencia olyan fejleszthető képesség, amelynek növelése kizárólag a technológiai, a szervezeti és a szabályozási dimenzió összehangolt fejlesztésével valósítható meg** [55]. Ebből következik, hogy a reziliencia fejlesztés nem tekinthető kizárólag informatikai vagy műszaki feladatnak, hanem stratégiai irányítási kérdés is.

E négy alapelv alkotja a háromdimenziós technológiai reziliencia-modell elméleti alapját. Ezek együttesen biztosítják a modell belső koherenciáját, kijelölik annak értelmezési

kereteit, valamint megalapozzák a következő alfejezetben bemutatott modell szerkezeti felépítését és későbbi mérhetővé és értékelhetővé tételét.

3.2.3.2. A három dimenzió rendszerkapcsolata

A korábbi fejezetekben bemutatott szakirodalmi elemzés, valamint a jelen kutatás során levont következtetések alapján megállapítható, hogy a technológiai reziliencia nem értelmezhető egyetlen szervezeti, technológiai vagy szabályozási tényező függvényében. A reziliens működés minden esetben több, egymással kölcsönhatásban álló rendszerkomponens együttes eredménye. Ennek megfelelően a jelen kutatás a technológiai rezilienciát három egymással szoros kapcsolatban álló dimenzió integrált működéseként értelmezi: **technológiai**, **szervezeti** és **szabályozási** dimenzióként.

A három dimenzió nem hierarchikus viszonyban áll egymással. Egyik sem tekinthető elsődlegesnek vagy alárendeltnek, mivel valamennyi önálló funkcióval rendelkezik, ugyanakkor működésük kölcsönösen feltételezi egymást. Ez a megközelítés összhangban áll a komplex adaptív rendszerek elméletével, amely szerint a rendszer stabilitása nem az egyes elemek fejlettségéből, hanem azok együttműködésének minőségéből fakad (Holland, 2006; Mitchell, 2009).

A háromdimenziós modell ezért nem három egymás mellé helyezett komponensből áll, hanem **egy integrált szocio-technikai rendszer** fogalmi leképezése. A technológiai infrastruktúra biztosítja a működés fizikai és digitális alapját, a szervezeti dimenzió teremti meg az alkalmazkodás és döntéshozatal képességét, míg a szabályozási dimenzió kijelöli azt a stratégiai és jogi keretet, amelyben a rendszer hosszú távon fenntarthatóan működhet. A három dimenzió közötti kölcsönhatások folyamatosak, kölcsönösek és nem lineárisak.

3.2.3.3 A technológiai dimenzió

A **modell első dimenzióját a technológiai infrastruktúra alkotja**. Ide tartoznak mindazon fizikai és digitális komponensek, amelyek közvetlenül biztosítják a rendszer működését. A technológiai dimenzió magában foglalja többek között a hardver- és szoftverarchitektúrát, a kommunikációs hálózatokat, az adatkezelési képességeket, a mesterséges intelligencia alkalmazásait, az automatizált vezérlőrendszereket, valamint a kritikus infrastruktúrák műszaki elemeit.

A **nemzetközi szakirodalom alapján e dimenzió rezilienciáját elsősorban** olyan tulajdonságok határozzák meg, mint a modularitás, a redundancia, a diverzitás, a hibatűrés, az önmonitorozás és a gyors helyreállítás képessége. [12], [14], [57],[103] Az elmúlt évek technológiai fejlődése azonban új elemeket is a reziliencia meghatározó komponenseivé tett. A mesterséges intelligencia támogatott döntéstámogatás, a prediktív karbantartás, a digitális ikermodellek (Digital Twin), valamint az autonóm működési képességek egyaránt növelhetik a rendszer alkalmazkodóképességét, ugyanakkor új sérülékenységeket is létrehozhatnak.

Ennek megfelelően a jelen kutatásban a technológiai dimenzió nem kizárólag a rendszer fizikai elemeinek összességét jelenti, hanem olyan dinamikus technológiai képességrendszert, amely folyamatosan képes érzékelni a működési környezet változásait, alkalmazkodni azokhoz, valamint biztosítani az alapvető funkciók fenntartását még részleges meghibásodás esetén is.

A technológia dimenzió javasolt, saját definíciója: A technológiai dimenzió a rendszer azon műszaki és digitális képességeinek összességét jelenti, amelyek lehetővé teszik a zavarok érzékelését, elviselését, a kritikus funkciók fenntartását, a helyreállítást és a technológiai adaptációt. Ide tartozik többek között a modularitás, a redundancia, a monitorozhatóság, az automatizáció és mesterséges intelligencia, a kiberbiztonsági ellenálló képesség, valamint a helyreállíthatóság.

3.2.3.4. A szervezeti dimenzió

A technológiai infrastruktúra önmagában nem képes reziliens működésre. A technológiai képességek tényleges kihasználása minden esetben emberi döntéshozatalon, szervezeti folyamatokon és vezetési mechanizmusokon keresztül valósul meg. **Ennek megfelelően a modell második dimenzióját a szervezeti működés alkotja.**

A szervezeti dimenzió magában foglalja a vezetési struktúrát, a döntéshozatali mechanizmusokat, a szervezeti kultúrát, a tudásmenedzsmentet, a képzési rendszereket, valamint az adaptív tanulási folyamatokat. **Weick és Sutcliffe szerint** a magas megbízhatóságú szervezetek egyik legfontosabb sajátossága, hogy képesek korán felismerni a működési rendellenességeket, valamint gyorsan reagálni azokra. **Duchek ezt a**

megközelítést továbbfejlesztve a rezilienciát a felkészülés, a megküzdés és a tanulás egymást követő ciklusaként írja le. [4]

A jelen modell értelmezésében a szervezeti dimenzió elsődleges feladata a technológiai lehetőségek működőképessé alakítása. Ugyanazon technológiai infrastruktúra jelentősen eltérő rezilienciát eredményezhet attól függően, hogy a szervezet mennyire képes decentralizált döntéshozatalra, tudásmegosztásra, gyors innovációra vagy akár a működési rutinok felülvizsgálatára. A szervezeti dimenzió tehát a technológiai képességek adaptív hasznosításának feltételrendszerét biztosítja.

A szervezeti dimenzió saját, javasolt definíciója: A szervezeti dimenzió azon vezetési, döntéshozatali, humán és tanulási képességeket foglalja magában, amelyek lehetővé teszik a technológiai változások és zavarok felismerését, értelmezését és a megfelelő szervezeti válasz kialakítását. Meghatározó elemei a vezetés, a szervezeti kultúra, a tanulás, a tudásmegosztás, az együttműködés és az adaptív döntéshozatal.

3.2.3.5. A szabályozási dimenzió

A **harmadik dimenzió a stratégiai irányítási és szabályozási környezetet foglalja magában.** A korábbi rezilienciamodellek ezt gyakran külső környezetként kezelték, azonban a jelen kutatás abból indul ki, hogy a XXI. század digitális rendszereiben a szabályozás közvetlenül alakítja a technológiai fejlődést és a szervezeti működést.

A szabályozási dimenzió részét képezik a nemzeti és nemzetközi jogszabályok, a szabványok, a kockázatkezelési keretrendszerek, a stratégiai dokumentumok, a felügyeleti mechanizmusok, valamint a kormányzási (governance) struktúrák. Az Európai Unió NIS2 irányelve, a CER irányelv, a Cyber Resilience Act, továbbá a NATO 2022-es Stratégiai Koncepciója egyaránt azt tükrözik, hogy a technológiai reziliencia ma már stratégiai irányítási kérdéssé vált. [23],[25],[26],[39]

A jelen modellben a szabályozási dimenzió nem csupán megfelelőségi követelményeket jelent, hanem olyan adaptív irányítási rendszert, amely képes egyensúlyt teremteni a biztonság, az innováció és a működési rugalmasság között. A szabályozás túlzott merevsége lassíthatja az alkalmazkodást, míg a túlzott rugalmasság növelheti a sérülékenységet. A reziliens rendszer ezért olyan szabályozási környezetet igényel, amely egyszerre biztosítja a kiszámíthatóságot és az adaptáció lehetőségét.

A szabályozási és irányítási dimenzió saját, javasolt definíciója: A szabályozási és irányítási dimenzió azon governance-, stratégiai és szabályozási mechanizmusok összessége, amelyek meghatározzák a technológiai rendszer működési kereteit, felelősségi viszonyait, kockázatkezelését, megfelelőségét és adaptációs lehetőségeit. E dimenzió rezilienciahatása abban áll, hogy a szabályozás nemcsak korlátozhatja, hanem megfelelő kialakítás esetén gyorsíthatja is a technológiai és szervezeti alkalmazkodást.

3.2.3.6. A dimenziók integrált működése

A **három dimenzió működése nem lineáris, hanem folyamatos visszacsatolási folyamatok révén valósul meg.** A technológiai innováció új szervezeti kompetenciákat követel meg; a szervezeti tanulás új technológiai fejlesztéseket indukál; a szabályozási környezet módosulása pedig egyszerre alakítja a technológiai beruházásokat és a szervezeti működést. Ezek a kölcsönhatások ciklikus jellegűek, és időben folyamatosan változnak.

Ennek következtében a technológiai reziliencia nem tekinthető egyetlen fejlesztési projekt eredményének, hanem olyan dinamikusan fejlődő rendszerképességnek, amely a három dimenzió egyensúlyán alapul. Bármelyik dimenzió tartós gyengülése a teljes rendszer alkalmazkodóképességének romlásához vezethet, még akkor is, ha a másik két dimenzió magas fejlettségi szintet ér el.

A jelen kutatás ezért a technológiai rezilienciát **integrált szocio-technikai rendszerképességként** definiálja, amely a technológiai, a szervezeti és a szabályozási dimenzió összehangolt működéséből jön létre, és amelynek célja a rendszer alapvető funkcióinak fenntartása, adaptív megújítása és hosszú távú fejlődőképességének biztosítása változó működési környezetben.

3.2.3.7. A modell tudományos újdonsága és kutatási hozzájárulása

A technológiai rezilienciával foglalkozó nemzetközi szakirodalom az elmúlt két évtizedben jelentős fejlődésen ment keresztül, ugyanakkor továbbra is megfigyelhető, hogy az egyes kutatási irányok jellemzően saját tudományterületük szempontrendszeréből közelítik meg a reziliencia fogalmát. A mérnöki megközelítések a technológiai rendszerek megbízhatóságára és robusztusságára koncentrálnak [14],[57],[103], a szervezeti kutatások a vezetésre, a tanulási folyamatokra és az alkalmazkodóképességre helyezik a hangsúlyt

(Duchek), míg a kritikus infrastruktúrák és a kiberreziliencia vizsgálatai elsősorban a kockázatkezelési és irányítási mechanizmusokat elemzik. [4], [47], [57]

E megközelítések közös jellemzője, hogy a rezilienciát egy domináns elemzési szinten értelmezik. A jelen kutatás ezzel szemben abból indul ki, hogy a XXI. század összetett digitális és fizikai rendszereiben a reziliencia kizárólag integrált szocio-technikai megközelítésben értelmezhető. A technológiai rendszerek működését ma már egyidejűleg alakítják a műszaki infrastruktúra sajátosságai, a szervezeti működés minősége, valamint a stratégiai és szabályozási környezet. E három tényező egyikének tartós gyengesége önmagában is képes a rendszer egészének rezilienciáját jelentősen csökkenteni, függetlenül a másik két dimenzió fejlettségétől.

A kutatás első tudományos hozzájárulása ezért annak elméleti igazolása, hogy a technológiai reziliencia **nem egyetlen rendszerkomponens tulajdonsága, hanem a technológiai, a szervezeti és a szabályozási dimenzió kölcsönhatásából kialakuló rendszerképesség**. Ez az értelmezés túlmutat a hagyományos mérnöki vagy szervezeti rezilienciamodelleken, mivel a rezilienciát nem statikus állapotként, hanem folyamatos alkalmazkodási folyamatként értelmezi.

A **kutatás második tudományos hozzájárulása a háromdimenziós modell kialakítása.** A modell olyan egységes fogalmi keretet biztosít, amelyben a technológiai infrastruktúra, a szervezeti működés és a szabályozási környezet egyaránt önálló elemzési dimenzióként jelenik meg, ugyanakkor ezek nem elkülönülten, hanem kölcsönösen egymást befolyásoló rendszerként értelmezhetők. A modell ily módon alkalmas arra, hogy különböző technológiai rendszerek – például kritikus infrastruktúrák, katonai vezetési rendszerek, ipari irányítórendszerek vagy mesterséges intelligencián alapuló platformok – rezilienciáját azonos elméleti keretben vizsgálja.

A kutatás harmadik tudományos eredménye annak felismerése, **hogy a reziliencia fejlesztésének elsődleges célterülete nem az egyes dimenziók önálló optimalizálása, hanem azok kapcsolatrendszerének fejlesztése.** A hagyományos fejlesztési modellek gyakran technológiai beruházásokkal vagy szervezeti reformokkal kívánják növelni a rezilienciát. A jelen kutatás ezzel szemben azt állítja, hogy a reziliencia növekedése elsősorban a dimenziók közötti koordináció, információáramlás, visszacsatolás és adaptív együttműködés javításából származik. Ez a megközelítés különösen fontos olyan

gyorsan változó technológiai környezetben, ahol a technológiai innováció, a szervezeti tanulás és a szabályozási alkalmazkodás egymástól elválaszthatatlan folyamatokat alkotnak.

A kutatás negyedik tudományos hozzájárulása a reziliencia dinamikus értelmezése. A jelen modell szerint a technológiai reziliencia nem tekinthető egyszeri állapotnak vagy kizárólag egy adott időpontban mérhető tulajdonságnak. A reziliencia folyamatosan változó rendszerképesség, amelyet a technológiai fejlődés, az új fenyegetések megjelenése, a szervezeti tanulás és a szabályozási környezet módosulása egyaránt alakít. Ez a szemlélet lehetővé teszi, hogy a rezilienciát ne csupán statikus mutatóként, hanem időben követhető fejlődési folyamatként vizsgáljuk.

A **kutatás ötödik tudományos eredménye a modell mérhetőségének és értékelhetőségének megalapozása.** A háromdimenziós koncepcionális modell nem pusztán elméleti konstrukcióként jelenik meg, hanem olyan elemzési keretet biztosít, amely alkalmas a későbbiekben kvantitatív indikátorok kialakítására és mérési módszerek kidolgozására. Ennek eredményeként a technológiai reziliencia nem kizárólag kvalitatív módon írható le, hanem lehetőség nyílik objektív értékelési rendszer kialakítására is. A dolgozat későbbi fejezeteiben ennek megfelelően kerül kidolgozásra a **Technological Resilience Index (TRI)** koncepciója, amely a három dimenzió fejlettségét és azok kölcsönhatását egyaránt figyelembe veszi.

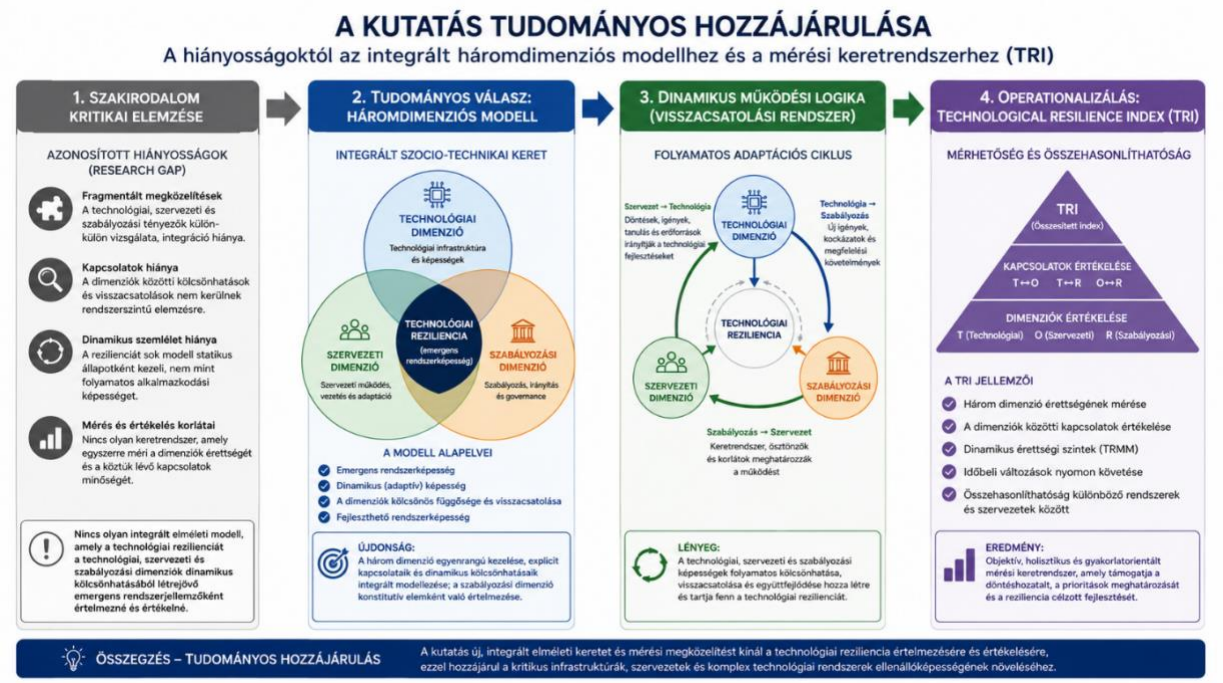
A modell gyakorlati jelentőségét tovább növeli, hogy nem kötődik egyetlen technológiai szektorhoz vagy iparághoz. Alkalmazható kritikus infrastruktúrák, honvédelmi rendszerek, kibervédelmi architektúrák, intelligens közlekedési rendszerek, energetikai hálózatok, egészségügyi digitális szolgáltatások vagy akár autonóm robotikai rendszerek vizsgálatára is. A háromdimenziós megközelítés ezáltal lehetőséget biztosít különböző technológiai környezetek összehasonlítható elemzésére, valamint a fejlesztési prioritások tudományosan megalapozott meghatározására.

A **kutatás eredményei különösen időszerűek a jelenlegi európai biztonsági és technológiai környezetben.** Az Európai Unió NIS2 irányelve, a CER irányelv, a Cyber Resilience Act, valamint a NATO stratégiai dokumentumai egyaránt hangsúlyozzák a kritikus rendszerek ellenálló képességének növelését. [26] Ugyanakkor ezek a dokumentumok elsősorban szabályozási és stratégiai célokat fogalmaznak meg, és nem nyújtanak egységes tudományos modellt a technológiai reziliencia értelmezésére. A jelen

kutatás által kidolgozott háromdimenziós modell ezt a hiányt kívánja pótolni egy olyan integrált elméleti keret kialakításával, amely egyszerre támaszkodik a rendszerelméletre, a reziliencia kutatásra, a szervezetelméletre és a technológiai innováció eredményeire.

A háromdimenziós technológiai rezilienciamodell tehát a rezilienciát integrált, dinamikus és fejleszthető szocio-technikai rendszerképességként értelmezi. Tudományos hozzáadott értéke nem pusztán három dimenzió együttes kezelésében, hanem azok egyenrangú rendszerkomponensként történő integrálásában, kölcsönhatásaik explicit vizsgálatában és a szabályozási dimenzió konstitutív szerepének beemelésében rejlik. A modell ezzel megteremti annak elméleti alapját, hogy a következő alfejezetekben meghatározhatók legyenek az egyes dimenziók komponensei, dinamikus kapcsolatai, majd ezek mérhetővé és értékelhetővé tételával a technológiai reziliencia mérési és érettségi keretrendszere.

A bemutatott koncepcionális alapok alapján a kutatás tudományos hozzájárulása egymásra épülő logikai lépésekben értelmezhető. A szakirodalom kritikai elemzése során azonosított fragmentáltságra, a dimenziók közötti kapcsolatok elégtelen vizsgálatára, a dinamikus szemlélet hiányára és a mérhetőség korlátaira a kutatás egy integrált háromdimenziós modellel válaszol. A modell a technológiai, szervezeti és szabályozási dimenziókat egyenrangú, kölcsönösen függő rendszerkomponensként kezeli, amelyek dinamikus visszacsatolási kapcsolatai hozzák létre a technológiai rezilienciát. E koncepcionális keret teremti meg a reziliencia későbbi mérhetővé és értékelhetővé tételének és mérésének elméleti alapját. A kutatás e logikai ívét a 3.3 ábra foglalja össze.



3.3. ábra: A kutatás tudományos hozzájárulása (saját szerkesztés)

Az ábra egyben kijelöli a kutatás további logikáját. A háromdimenziós modell koncepcionális keretet biztosít a technológiai reziliencia értelmezéséhez, a dinamikus visszacsatolási modell annak működési mechanizmusát írja le, míg az erre épülő mérési keretrendszer a koncepció gyakorlati mérhetővé és értékelhetővé tételét teszi lehetővé. A következő alfejezetek e három elem részletes kibontását és egymásra épülését mutatják be.

A modell célja tehát nem a szakirodalomban már azonosítható technológiai, szervezeti és szabályozási–irányítási tényezők egyszerű újracsoportosítása. A kutatás ezek kölcsönhatásait, a dimenziók közötti korlátozó kapcsolatokat, valamint a reziliencia időbeli adaptációját egységes rendszerben kívánja értelmezni és mérhetővé és értékelhetővé tenni. Ennek részletes modelljét és mérési logikáját a következő alfejezetek dolgozzák ki.

3.3 A háromdimenziós technológiai reziliencia-modell

3.3.1 A modell szerkezeti felépítése

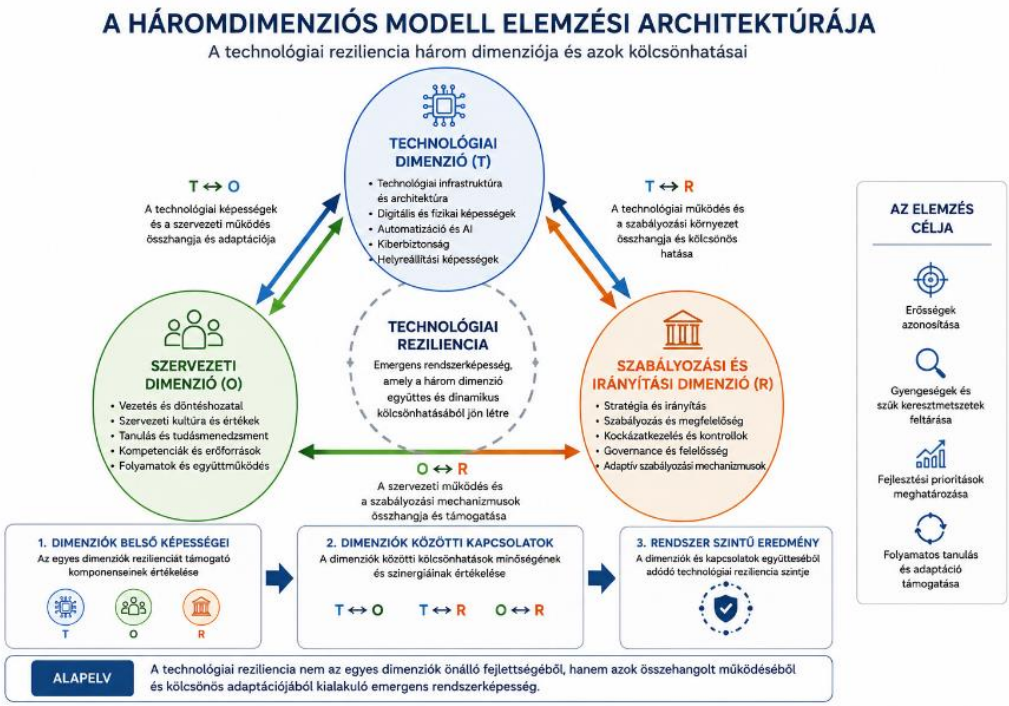
A 3.1 alfejezet meghatározta a háromdimenziós technológiai rezilienciamodell elméleti és koncepcionális alapjait. A jelen alfejezet célja ennek a koncepcionális keretnek a szerkezeti kibontása: annak meghatározása, hogy a technológiai, szervezeti és szabályozási dimenzió milyen belső komponensekből épül fel, ezek milyen reziliencia funkciókat töltenek

be, valamint milyen kapcsolatokon keresztül befolyásolják egymás működését. A hangsúly ezért a továbbiakban nem a modell szükségességének igazolásán, hanem annak elemzési architektúráján van.

A modell három elsődleges elemzési dimenziót különít el: **technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziót.** Ezek nem egymástól független alrendszerek, hanem ugyanazon komplex szocio-technikai rendszer analitikusan elkülöníthető, funkcionálisan azonban kölcsönösen függő rétegei.

A technológiai dimenzió a rendszer fizikai és digitális architektúrájának rezilienciát támogató képességeit foglalja magában. A szervezeti dimenzió azt fejezi ki, hogy a rendszert működtető szervezet milyen mértékben képes e technológiai képességek alkalmazására, fenntartására és adaptációjára. A szabályozási és irányítási dimenzió pedig azokat a governance-, stratégiai és normatív mechanizmusokat jeleníti meg, amelyek meghatározzák a technológiai és szervezeti alkalmazkodás kereteit és mozgásterét.

A modell elemzési architektúrája két egymásra épülő szintből áll. Az első szint az egyes dimenziók belső reziliencia képességeit vizsgálja. A második szint a dimenziók közötti kapcsolatok minőségét elemzi. A technológiai reziliencia értékelése ennek megfelelően nem korlátozható a T, O és R dimenziók önálló vizsgálatára, hanem ki kell terjednie a technológia–szervezet (T↔O), technológia–szabályozás (T↔R), valamint szervezet–szabályozás (O↔R) kapcsolatokra is. Ennek szemléltetésére a dolgozat 3.4. ábrája mutatja be a háromdimenziós technológiai rezilienciamodell szerkezeti felépítését.



3.4. ábra: A háromdimenziós technológiai rezilienciamodell elemzési architektúrája (saját szerkesztés)

Az ábra szemlélteti, hogy a modellben a technológiai reziliencia nem egyetlen dimenzió tulajdonságaként, hanem három belső képességterület és három interdimenzionális kapcsolat együttes eredményeként értelmezhető. Ez a szerkezeti logika teremti meg a modell későbbi mérhetővé és értékelhetővé tételének alapját.

3.3.2 A technológiai dimenzió részletes felépítése

A technológiai dimenzió azt fejezi ki, hogy a rendszer fizikai és digitális architektúrája milyen mértékben képes támogatni a zavarok érzékelését és elviselését, a kritikus funkciók fenntartását, a működés helyreállítását, valamint a megváltozott működési feltételekhez történő alkalmazkodást. A dimenzió értékelése ezért nem az alkalmazott technológia abszolút fejlettségi szintjére, hanem annak rezilienciát támogató funkcionális tulajdonságaira irányul. Egy technológiailag fejlettebb rendszer nem szükségszerűen reziliensebb, ha architektúrája merev, sérülékeny vagy nehezen helyreállítható**.**

A technológiai dimenzió hat fő komponensből épül fel:

- Modularitás
- Redundancia
- Monitorozhatóság

- Automatizáció és mesterséges intelligencia
- Kiberbiztonsági ellenálló képesség
- Helyreállítási képesség

Modularitás

A modularitás azt jelenti, hogy a rendszer funkcionális elemei elkülöníthetők, cserélhetők vagy újrakonfigurálhatók anélkül, hogy egyetlen komponens meghibásodása szükségszerűen a teljes rendszer működésképtelenségéhez vezetne. Reziliencia szempontjából a modularitás támogatja a hibák lokalizálását, az alternatív konfigurációk kialakítását és a technológiai adaptáció gyorsítását [80]. A modularitás ugyanakkor önmagában nem garantál magas rezilienciát: annak előnye csak akkor érvényesül, ha a szervezet rendelkezik az újrakonfiguráláshoz szükséges kompetenciákkal, eljárásokkal és döntési jogosultságokkal.

Redundancia

A redundancia a rezilienciakutatás egyik klasszikus eleme (Holling) [1]. A jelen kutatás azonban különbséget tesz:

- strukturális redundancia;
- funkcionális redundancia;
- digitális redundancia.

Ez különösen fontos mesterséges intelligenciával támogatott rendszerek esetében.

Monitorozhatóság

A kritikus infrastruktúrák gyakorlati működése jól szemlélteti az integrált technológiai reziliencia szükségességét. **Az energetikai alállomások hálózatbiztonsági monitorozására kidolgozott kutatások szerint** a korszerű NSM (Network Security Monitoring) architektúrák csak akkor képesek hatékony fenyegetésészlelésre, ha az OT-kommunikáció sajátosságaira optimalizált protokollelemzést, folyamatos monitorozást és incidenskezelési folyamatokat egyaránt alkalmaznak. A rendszer eredményességét nem kizárólag a technológiai eszközök, hanem azok szervezeti alkalmazása és integrációja

határozza meg [53]. Ez a megállapítás közvetlenül alátámasztja a jelen kutatás háromdimenziós technológiai rezilienciamodelljének létjogosultságát.

A reziliens rendszerek egyik legfontosabb jellemzője, hogy képesek saját állapotuk folyamatos megfigyelésére.

Ide tartozik

- szenzorhálózat,
- SIEM,
- SOC[28],
- OT monitoring,
- AI anomália detekció.

Ez biztosítja a korai beavatkozást.

Automatizáció és mesterséges intelligencia

A XXI. század technológiai rendszereiben az AI már nem külön képesség, hanem a reziliencia egyik alapvető komponense.

Az AI alkalmazható

- prediktív karbantartásra,
- támadásészlelésre,
- logisztikai optimalizálásra,
- döntéstámogatásra,
- autonóm működésre.

Ugyanakkor új sérülékenységeket is létrehoz.

Ezért a modellben az AI egyszerre rezilienciánövelő és rezilienciakockázati tényező.

Kiberbiztonsági ellenálló képesség

[28] SOC: Security Operation Center; biztonsági központ

A technológiai reziliencia nem választható el a cyber resilience fogalmától.

Ide tartozik

- Zero Trust,
- Identity Management,
- Secure by Design,
- Secure by Default,
- DevSecOps,
- Threat Intelligence.

Helyreállítási képesség

Nem elegendő egy támadást túlélni.

A rendszernek képesnek kell lennie

- gyors helyreállításra,
- működés újrakonfigurálására,
- tanulásra.

Ez kapcsolja össze a technológiai dimenziót a szervezeti dimenzióval.

A technológiai dimenzió összefoglalása

A **jelen kutatásban a technológiai dimenzió nem egyszerűen technikai infrastruktúrát jelent, hanem olyan adaptív technológiai képességrendszert, amely biztosítja a rendszer működésének folytonosságát, alkalmazkodóképességét és fejlődőképességét gyorsan változó környezetben.** A technológiai dimenzió fejlettsége azonban önmagában nem elegendő a reziliencia kialakulásához; annak tényleges érvényesülése a szervezeti és szabályozási dimenzióval való összehangolt működéstől függ.

3.5. ábra: A technológiai dimenzió reziliencia képességei (saját szerkesztés)

3.3.3 A szervezeti dimenzió

A **szervezeti dimenzió azt fejezi ki, hogy a technológiai rendszert működtető szervezet milyen mértékben képes a környezeti változások és zavarok felismerésére, értelmezésére, az ezekhez szükséges döntések meghozatalára, valamint működésének adaptív átalakítására**. A szervezeti dimenzió a jelen modellben nem önálló szervezeti rezilienciát jelent, hanem azt a képességrendszert, amely lehetővé teszi a technológiai potenciál tényleges rezilienciahatássá történő átalakítását.

Ez a megközelítés **összhangban áll Teece dinamikus képességek** elméletével, amely szerint a szervezetek hosszú távú sikerének alapja nem a rendelkezésre álló erőforrások mennyisége, hanem azok folyamatos újrakonfigurálásának képessége. Hasonló következtetésre jut Duchek, aki a szervezeti rezilienciát három egymást követő képesség – **anticipáció, megküzdés és adaptáció** – integrált működéseként írja le. [4]

A háromdimenziós technológiai rezilienciamodellben a szervezeti dimenzió feladata ezért nem a technológia működtetése, hanem annak **adaptív hasznosítása**.

3.3.3.1 A szervezeti dimenzió komponensei

A jelen kutatás alapján a szervezeti dimenzió hat, egymással kölcsönösen összefüggő komponensből épül fel.

Adaptív vezetés

A reziliens szervezet egyik legfontosabb jellemzője a változó környezethez igazodó vezetési képesség. A bizonytalanság növekedésével a centralizált döntéshozatali modellek egyre kevésbé hatékonyak. A magas megbízhatóságú szervezetek **(High Reliability Organizations – HRO[29]) kutatásai azt mutatják**, hogy a sikeres szervezetek képesek decentralizálni a döntéseket, miközben fenntartják a stratégiai kontrollt. [32],[108]

A technológiai reziliencia szempontjából az adaptív vezetés biztosítja, hogy a technológiai innováció ne pusztán technikai fejlesztésként jelenjen meg, hanem a szervezet működésének integrált részévé váljon.

Szervezeti tanulás

Argyris és Schön (1978) klasszikus munkája óta ismert, hogy a szervezetek fejlődésének egyik alapvető feltétele a folyamatos tanulás. [34] A jelen modellben a szervezeti tanulás nem kizárólag képzési tevékenységet jelent, hanem a tapasztalatok rendszerszintű feldolgozását, a hibákból való tanulást és az új működési rutinok kialakítását.

A technológiai rendszerek gyors fejlődése miatt a tanulási ciklusok lerövidültek. A reziliens szervezetek ezért képesek a működés során keletkező tapasztalatokat rövid idő alatt új technológiai vagy szervezeti megoldásokká alakítani.

Innovációs képesség

A technológiai reziliencia egyik meghatározó eleme az innovációs képesség. A jelen kutatásban az innováció nem kizárólag új technológiai termékek fejlesztését jelenti, hanem új működési folyamatok, szervezeti struktúrák és vezetési megoldások kialakítását is.

[29] HRO: High Reliability Organization: magas megbízhatóságú szervezet.

A különösen gyors innovációs ciklusokat alkalmazó ukrajnai tapasztalatok jól mutatják, hogy a reziliens szervezetek képesek a harctéri visszacsatolások alapján akár néhány hetes fejlesztési ciklusokban új technológiai megoldások bevezetésére. Ez a jelenség jelentősen eltér a hagyományos, több éves védelmi fejlesztési modellektől, és rámutat arra, hogy a szervezeti alkalmazkodóképesség a technológiai reziliencia egyik kulcstényezője.

Tudásmenedzsment

A technológiai rendszerek komplexitásának növekedésével a szervezeti tudás stratégiai erőforrássá vált. **Nonaka és Takeuchi tudásteremtési modellje** alapján a szervezetek versenyképessége nagymértékben függ attól, hogy képesek-e a hallgatólagos (tacit) és explicit tudás folyamatos átalakítására. [35]

A jelen modellben a tudásmenedzsment feladata, hogy biztosítsa a technológiai tapasztalatok szervezeti szintű megőrzését és továbbadását.

Együttműködési képesség

A modern technológiai rendszerek jellemzően több szervezet együttműködésében működnek. Kritikus infrastruktúrák, kibervédelmi rendszerek vagy védelmi innovációs ökoszisztémák esetében a reziliencia nem egyetlen szervezet tulajdonsága, hanem az együttműködő szereplők közötti koordináció eredménye.

Ezért a jelen kutatás önálló komponensként kezeli a hálózati együttműködési képességet, amely magában foglalja az információmegosztást, a közös döntéshozatalt és a partnerségi kapcsolatok működtetését.

Humán kompetenciák

A mesterséges intelligencia térnyerése ellenére az ember továbbra is a technológiai rendszerek egyik meghatározó eleme. A reziliens szervezet folyamatosan fejleszti munkatársainak digitális kompetenciáit, vezetői készségeit és problémamegoldó képességét.

A humán kompetenciák fejlesztése különösen fontos olyan rendszerek esetében, ahol az ember és a mesterséges intelligencia közös döntéshozatali környezetben működik.

A szervezeti dimenzió szerepe a technológiai rezilienciában

A szervezeti dimenzió ezért a technológiai képességek rezilienciahatását közvetítő és módosító rendszerkomponensként értelmezhető. A megfelelő szervezeti működés képes felerősíteni a technológiai képességek pozitív hatását, míg a vezetési, kompetencia- vagy tanulási hiányosságok jelentősen korlátozhatják azok tényleges hasznosulását. A kapcsolat ugyanakkor kétirányú: az új technológiák maguk is módosítják a szervezeti folyamatokat, kompetenciaigényeket és döntési struktúrákat.

3.3.4 A szabályozási és irányítási dimenzió

A szabályozási és irányítási dimenzió azokat a governance-, stratégiai, jogi és normatív mechanizmusokat foglalja magában, amelyek meghatározzák a technológiai rendszer működésének, fejlesztésének és adaptációjának kereteit. A háromdimenziós modell sajátossága, hogy ezt a dimenziót nem külső környezeti feltételként, hanem a technológiai reziliencia egyenrangú és aktív rendszerkomponenseként kezeli.

Reziliens szabályozási környezet alatt ezért nem pusztán magas megfelelőségi szintet értek. A szabályozási és irányítási rendszernek egyszerre kell biztosítania a működés biztonságát, a felelősségi viszonyok egyértelműségét és a stratégiai kontrollt, miközben megfelelő adaptációs mozgásteret kell biztosítania a technológiai és szervezeti változások számára.

A szabályozási és irányítási dimenzió fogalmi értelmezése

A jelen kutatásban a szabályozási és irányítási dimenzió nem kizárólag a jogi szabályozást jelenti. Ennél lényegesen szélesebb fogalomként értelmezhető, amely magában foglalja mindazon stratégiai, irányítási, intézményi és normatív mechanizmusokat, amelyek meghatározzák a technológiai rendszerek működésének feltételrendszerét.

A szabályozási dimenzió négy egymással összefüggő szinten jelenik meg.

- **Stratégiai szint**, amely meghatározza a hosszú távú célokat, prioritásokat és fejlesztési irányokat.
- **Kormányzási (governance) szint**, amely kijelöli a felelősségi viszonyokat, a koordinációs mechanizmusokat és a döntéshozatali struktúrát.

- **Normatív szint**, amely jogszabályok, szabványok és megfelelőségi követelmények formájában jelenik meg.
- **Operatív szabályozási szint**, amely az ellenőrzési, auditálási, incidenskezelési és folyamatos fejlesztési folyamatokat foglalja magában.

Ez a felosztás lehetővé teszi, hogy a szabályozási dimenzió ne pusztán jogi környezetként, hanem a technológiai rendszer működésének aktív irányító mechanizmusaként jelenjen meg.

3.3.5 A szabályozási és irányítási dimenzió fő komponensei

Stratégiai irányítás

A reziliens technológiai rendszerek kialakításának első feltétele az egyértelmű stratégiai irányítás. A stratégia meghatározza a fejlesztési prioritásokat, kijelöli a kockázatkezelési célokat, valamint biztosítja az erőforrások hosszú távú allokációját.

A NATO 2022-es Stratégiai Koncepciója és az Európai Unió digitális biztonsági stratégiái egyaránt hangsúlyozzák, hogy a reziliencia ma már nem kizárólag technológiai kérdés, hanem a nemzeti ellenálló képesség alapvető eleme. [23], [44]

A jelen modellben a stratégiai irányítás biztosítja a három dimenzió közös fejlődési irányát.

Governance

A governance a szabályozási dimenzió központi eleme. Míg a stratégia azt határozza meg, hogy **mit** kíván elérni egy szervezet vagy állam, addig a governance arra válaszol, hogy **ki**, **milyen felelősségi körben**, **milyen döntési mechanizmusok mentén** valósítja meg ezt.

A technológiai reziliencia szempontjából különösen fontos:

- egyértelmű felelősségi rendszer;
- koordináció az állami és piaci szereplők között;
- gyors döntéshozatal;
- horizontális információmegosztás;
- válsághelyzeti irányítás.

A jelen kutatás álláspontja szerint a nem megfelelő governance önmagában képes jelentősen csökkenteni a technológiai rezilienciát még akkor is, ha a technológiai infrastruktúra magas fejlettségi szintet ér el.

Ez különösen jól megfigyelhető olyan esetekben, amikor párhuzamos döntési fórumok, átfedő hatáskörök vagy koordinációs hiányosságok lassítják a technológiai innovációt vagy az incidensekre adott válaszokat.

Szabályozási megfelelőség

A digitális technológiák fejlődésével párhuzamosan jelentősen megnőtt a kötelező megfelelőségi követelmények szerepe.

A háromdimenziós modellben kiemelt jelentőségűek:

- NIS2;
- CER;
- Cyber Resilience Act;
- ISO/IEC30 27001.[84], [87], [112];
- IEC[31] 62443;
- NIST CSF 2.0;
- NATO Baseline Requirements.

A jelen kutatás azonban hangsúlyozza, hogy **a megfelelőség önmagában nem jelent rezilienciát**. Egy szervezet teljesítheti valamennyi auditkövetelményt, miközben valós alkalmazkodóképessége alacsony marad. A szabályozási megfelelőség ezért csak szükséges, de nem elégséges feltétele a reziliens működésnek.

Adaptív szabályozás

A jelen kutatás egyik legfontosabb új eleme az adaptív szabályozás szerepének hangsúlyozása. A hagyományos szabályozási rendszerek stabilitásra törekednek. A technológiai fejlődés azonban ennél lényegesen gyorsabb.

[31] IEC: International Electrotechnical Commission: Nemzetközi Elektrotechnikai Bizottság.

A mesterséges intelligencia, a kvantumtechnológia, az autonóm rendszerek vagy a digitális platformok fejlődése olyan sebességű, hogy a jogi környezet gyakran évekkel követi a technológiai innovációt.

Ezért a reziliens szabályozásnak képesnek kell lennie:

- gyors módosításra;
- kockázatalapú megközelítésre;
- kísérleti (sandbox) szabályozási megoldások alkalmazására;
- folyamatos visszacsatolásra.

Ez a szemlélet összhangban áll az OECD [81] és az Európai Bizottság új szabályozási megközelítéseivel, amelyek az **adaptive governance** és **agile regulation** elveit helyezik előtérbe.

A szabályozási és irányítási dimenzió integráló szerepe

A szabályozási dimenzió sajátos közvetítő szerepet tölt be a modellben, mivel a technológiai fejlesztés és a szervezeti alkalmazkodás mozgásterét egyaránt befolyásolja. Ez azonban nem jelent hierarchikus elsőbbséget a másik két dimenzióval szemben: a szabályozási környezet maga is folyamatosan alkalmazkodik a technológiai innováció és a szervezeti működés változásaihoz.

Ez az integráló szerep különösen jól megfigyelhető a kritikus infrastruktúrák, a védelmi innováció, valamint a kettős felhasználású (dual-use) technológiák esetében, ahol az innováció, a biztonság és a megfelelőség követelményei egyszerre jelennek meg. A megfelelően kialakított szabályozási környezet nem korlátozza, hanem irányítja és gyorsítja az adaptációs folyamatokat, ezáltal közvetlenül hozzájárul a technológiai reziliencia növeléséhez.

3.6. ábra: A reziliens governance kettős funkciója (saját szerkesztés)

3.3.6 A dimenziók közötti kapcsolat és a kapcsolati szűk keresztmetszetek

A háromdimenziós modell elemzési értéke nem kizárólag az egyes dimenziók elkülönített vizsgálatából, hanem a közöttük fennálló kapcsolatok értékeléséből származik. A technológiai reziliencia szempontjából három elsődleges interdimenzionális kapcsolat különíthető el: technológia–szervezet (T↔O), technológia–szabályozás (T↔R), valamint szervezet–szabályozás (O↔R). E kapcsolatok minősége határozza meg, hogy az egyes dimenziókban meglévő képességek milyen mértékben képesek rendszerszintű rezilienciahatássá összeállni.

A technológiai és a szervezeti dimenzió kölcsönhatása

A technológia–szervezet (T↔O) kapcsolat azt fejezi ki, hogy a rendelkezésre álló technológiai képességek milyen mértékben illeszkednek a szervezet kompetenciáihoz, folyamataihoz és döntési mechanizmusaihoz. Magas technológiai fejlettség alacsony szervezeti felkészültséggel nem eredményez szükségszerűen magas rezilienciát; ugyanakkor a szervezeti adaptáció új technológiai igényeket is generálhat.

A technológiai fejlesztések önmagukban nem eredményeznek magasabb rezilienciát. Egy új technológia – például mesterséges intelligencián alapuló döntéstámogatás, autonóm robotrendszer vagy digitális iker – csak akkor növeli a rendszer ellenálló képességét, ha a szervezet képes azt befogadni, alkalmazni és működtetni. Ennek hiányában a technológiai beruházások kihasználatlan kapacitásként jelennek meg, vagy akár új sérülékenységeket is létrehozhatnak.

A kapcsolat ugyanakkor fordított irányban is érvényesül. A szervezeti tanulás, az innovációs kultúra és a vezetői döntések új technológiai igényeket generálnak, amelyek további fejlesztéseket indukálnak. A két dimenzió között így **pozitív visszacsatolási hurok** alakul ki: a technológiai fejlődés elősegíti a szervezeti tanulást, a szervezeti tanulás pedig új technológiai innovációkat ösztönöz.

Ez a jelenség különösen jól megfigyelhető az ukrajnai háború tapasztalatai alapján, ahol a harctéri visszacsatolások néhány hetes innovációs ciklusokat eredményeztek. A gyors szervezeti tanulás lehetővé tette a technológiai megoldások folyamatos módosítását, míg az új technológiák új taktikai és szervezeti eljárások kialakulását ösztönözték. A reziliencia növekedése így nem kizárólag a fejlettebb technológiából, hanem a technológiai és szervezeti dimenzió közötti gyors visszacsatolásból származott.

A szervezeti és a szabályozási dimenzió kölcsönhatása

A szervezet–szabályozás (O↔R) kapcsolat azt fejezi ki, hogy a governance-, felelősségi és döntési struktúrák milyen mértékben támogatják a szervezet gyors reagálását, tanulását és adaptációját. A formálisan megfelelő szabályozási rendszer is csökkentheti a rezilienciát, ha válsághelyzetben indokolatlanul lassítja a döntéshozatalt vagy nem biztosít megfelelő cselekvési autonómiát.

A szervezeti működés nem független a szabályozási környezettől. A stratégiai irányítás, a jogszabályok, a szabványok és a megfelelőségi követelmények meghatározzák a szervezetek mozgásterét, ugyanakkor a szervezetek gyakorlati tapasztalatai visszahatnak a szabályozási rendszer fejlődésére is.

A reziliens szervezetek egyik sajátossága, hogy nem passzívan alkalmazkodnak a szabályozási változásokhoz, hanem képesek aktívan részt venni azok alakításában. Ez különösen igaz a gyorsan fejlődő technológiai területeken, ahol a szabályozási környezet

gyakran a gyakorlati tapasztalatok alapján módosul. Az Európai Unió digitális szabályozásának fejlődése – beleértve a NIS2 irányelvet vagy a Cyber Resilience Act-et – jól mutatja, hogy a szabályozási keretek folyamatos kölcsönhatásban állnak a technológiai és szervezeti fejlődéssel. [25], [27]

A technológiai és a szabályozási dimenzió kölcsönhatása

A technológia–szabályozás (T↔R) kapcsolat azt mutatja meg, hogy a szabályozási és irányítási környezet milyen mértékben támogatja a technológiai képességek biztonságos, ugyanakkor adaptív alkalmazását. A technológiai innováció új szabályozási követelményeket generálhat, míg a túlzottan merev szabályozás lassíthatja vagy korlátozhatja a szükséges technológiai alkalmazkodást.

A technológiai innováció és a szabályozási környezet kapcsolata kettős természetű. Egyrészt a szabályozás meghatározza a technológiai fejlesztések kereteit, biztonsági követelményeit és megfelelőségi elvárásait. Másrészt az új technológiák megjelenése új szabályozási kihívásokat teremt, amelyek a jogi és irányítási környezet folyamatos módosítását teszik szükségessé.

A mesterséges intelligencia, a kvantumtechnológia vagy az autonóm rendszerek fejlődése jól példázza ezt a folyamatot. A technológiai innováció gyorsabb ütemben halad, mint a szabályozás fejlődése, ezért a reziliens rendszerek kialakításához olyan adaptív szabályozási mechanizmusokra van szükség, amelyek képesek követni a technológiai változásokat anélkül, hogy indokolatlanul korlátoznák az innovációt.

A modellből következő további feltételezés, hogy a rendszer tényleges rezilienciáját jelentős mértékben korlátozhatja a dimenziók közötti leggyengébb kapcsolat. E jelenséget a jelen kutatás kapcsolati szűk keresztmetszetként (limiting interface)32 értelmezi. A fogalom arra utal, hogy egy magas érettségű technológiai, szervezeti vagy szabályozási dimenzió

[32] Limiting interface: a rendszer azon interdimenzionális kapcsolata, amelynek érettsége vagy működési teljesítménye a kapcsolódó dimenziók képességeinek tényleges kihasználását a legnagyobb mértékben korlátozza.

rezilienciahatása nem érvényesül teljes mértékben, ha a másik dimenzióhoz kapcsolódó interfész gyenge.

Egy fejlett, mesterséges intelligenciával támogatott kibervédelmi rendszer például magas technológiai képességet képviselhet, de tényleges rezilienciahatása alacsony maradhat, ha a szervezet nem rendelkezik megfelelő szakértelemmel és döntési eljárásokkal. Ebben az esetben nem maga a technológiai dimenzió, hanem a T↔O kapcsolat jelenti a rendszer rezilienciájának korlátozó tényezőjét.

3.7. ábra: A dimenziók közötti kapcsolatok és a kapcsolati szűk keresztmetszet (saját szerkesztés)

A három dimenzió integrált visszacsatolási rendszere

A jelen kutatás egyik központi megállapítása, hogy a technológiai reziliencia nem a három dimenzió egymástól elkülönülő működéséből, hanem azok **egymást erősítő vagy gyengítő visszacsatolási folyamataiból** alakul ki. A rendszer működésében pozitív és negatív visszacsatolások egyaránt megjelennek.

Pozitív visszacsatolás jön létre például akkor, amikor a technológiai innováció növeli a szervezeti tanulási képességet, amely újabb technológiai fejlesztéseket eredményez, miközben a szabályozási környezet támogatja ezek gyors bevezetését. Ebben az esetben a három dimenzió egymást erősítő módon járul hozzá a reziliencia növekedéséhez.

Negatív visszacsatolás figyelhető meg akkor, amikor valamelyik dimenzió fejlődése jelentősen elmarad a másik kettőtől. Például hiába rendelkezik egy szervezet korszerű technológiai infrastruktúrával és magas szintű szakmai kompetenciával, ha a szabályozási környezet nem teszi lehetővé az új megoldások gyors alkalmazását. Hasonlóképpen, a korszerű szabályozás sem képes növelni a rezilienciát, ha a technológiai infrastruktúra elavult vagy a szervezet nem rendelkezik megfelelő alkalmazkodóképességgel.

A kiegyensúlyozott fejlődés elve

A jelen kutatás alapján megfogalmazható egy új elméleti tétel:

A technológiai reziliencia növekedése nem az egyes dimenziók önálló fejlesztésének, hanem azok kiegyensúlyozott és összehangolt fejlődésének függvénye.

Ez a megállapítás lényeges eltérést jelent a hagyományos rezilienciamodellekhez képest, amelyek jellemzően egyetlen domináns tényezőre – technológiára, szervezetre vagy szabályozásra – helyezik a hangsúlyt. A háromdimenziós modell ezzel szemben azt állítja, hogy a reziliencia fejlődését a dimenziók közötti egyensúly határozza meg. A rendszer teljesítményét ezért mindig a leggyengébb kapcsolódási pontok korlátozzák, nem pedig a legerősebb komponensek fejlettsége.

Átvezetés a dinamikus modellhez

A három dimenzió közötti kölcsönhatások elemzése rámutat arra, hogy a technológiai reziliencia nem statikus állapot, hanem folyamatosan változó rendszerképesség. A technológiai fejlődés, a szervezeti tanulás és a szabályozási alkalmazkodás egymást követő ciklusokon keresztül alakítják a rendszer ellenálló képességét. Ennek megfelelően a következő alfejezet egy **dinamikus működési modellt** mutat be, amely szemlélteti a három dimenzió időbeli változását, valamint a reziliencia kialakulásának ciklikus folyamatát.

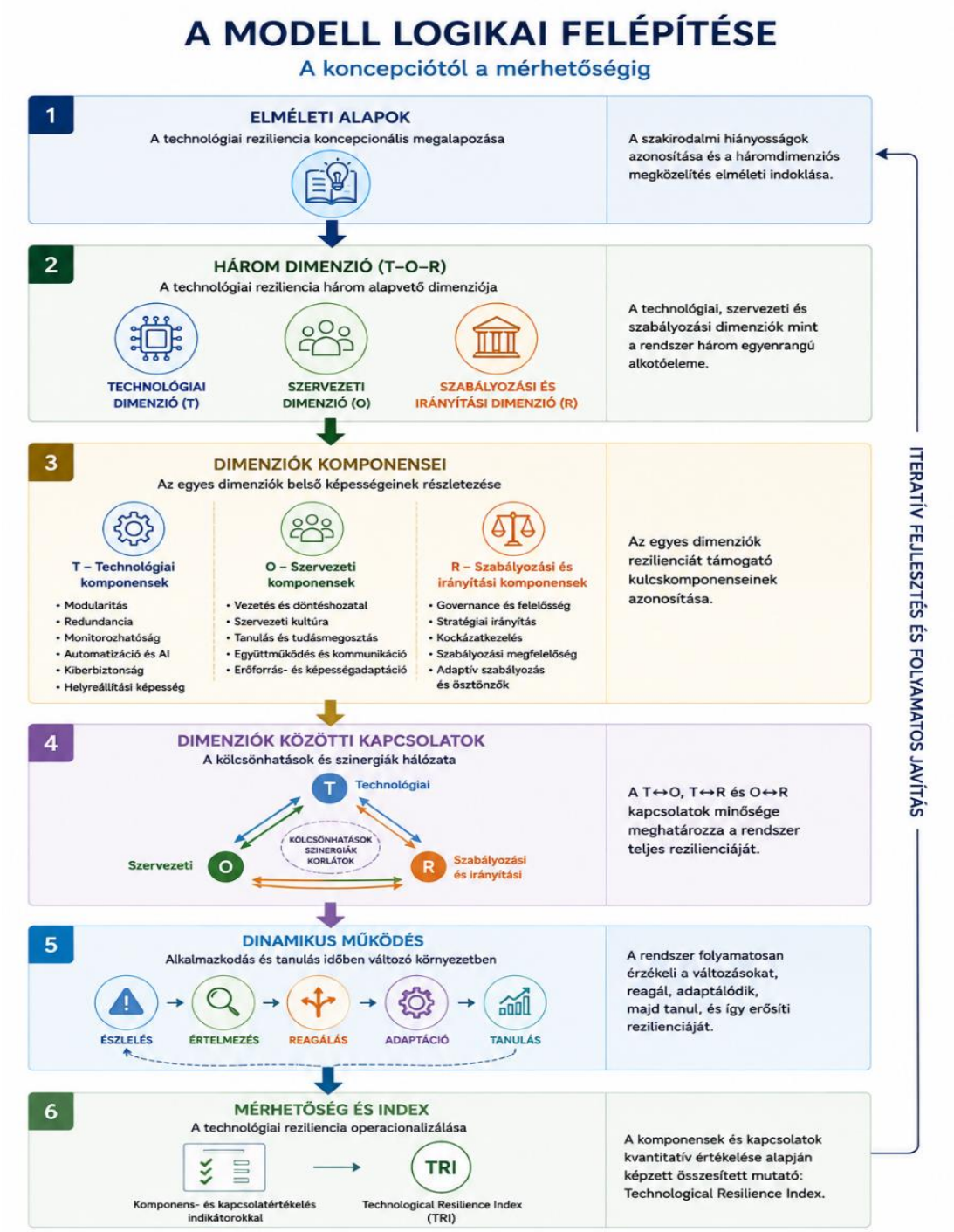
3.3.7 háromdimenziós modell szerkezeti összegzése

A háromdimenziós modell szerkezeti elemzése alapján a technológiai reziliencia nem vezethető le az egyes dimenziók önálló fejlettségéből. A rendszer rezilienciáját a technológiai, szervezeti és szabályozási képességek, valamint az azok között fennálló kapcsolatok együttes minősége határozza meg. A modell ennek megfelelően hat elsődleges

elemzési egységet különít el: három dimenziót – T, O és R –, valamint három interdimenzionális kapcsolatot – T↔O, T↔R és O↔R.

Ez a szerkezeti megközelítés egy adott időpontban lehetővé teszi a rendszer reziliencia architektúrájának feltárását, valamint az erős és gyenge képességterületek és kapcsolati szűk keresztmetszetek azonosítását. A technológiai reziliencia azonban nem statikus állapot. A dimenziók képességei és a közöttük fennálló kapcsolatok a környezeti változások, zavarok, technológiai innovációk, szervezeti tanulási folyamatok és szabályozási változások hatására időben módosulnak.

A modell teljes értelmezéséhez ezért a szerkezeti architektúra mellett annak időbeli működési mechanizmusát is meg kell határozni. A következő alfejezet ezt a dinamikus működést vizsgálja, és azt mutatja be, hogy a technológiai, szervezeti és szabályozási adaptáció miként kapcsolódik össze folyamatos visszacsatolási és tanulási folyamatokká.



3.8. ábra: A modell logikai felépítése (saját szerkesztés)

3.4 A technológiai reziliencia dinamikus működési modellje

3.4.1 A dinamikus működés értelmezési kerete

A 3.2 alfejezet a háromdimenziós technológiai rezilienciamodell szerkezeti architektúráját határozta meg: a technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziókat, valamint a közöttük fennálló T↔O, T↔R és O↔R kapcsolatokat. Ez a

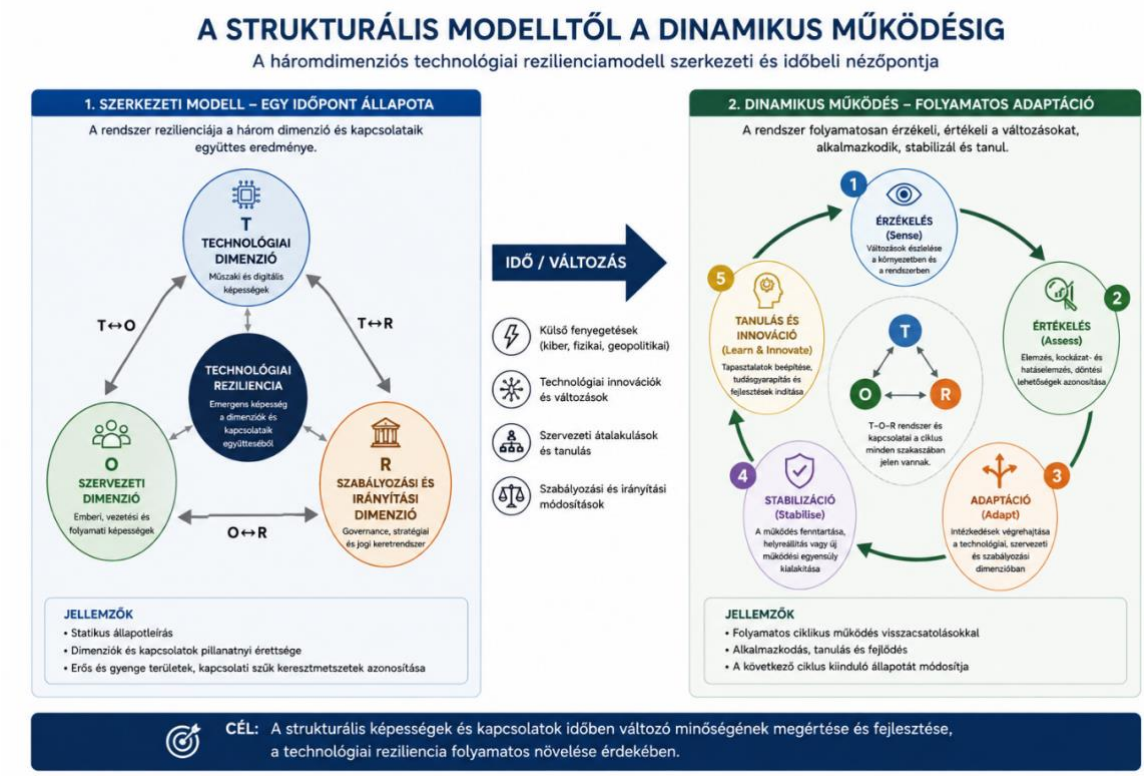
szerkezeti modell azonban egy adott időpontban fennálló rendszerállapotot ír le. A technológiai reziliencia teljes értelmezéséhez azt is vizsgálni szükséges, hogy e képességek és kapcsolatok miként változnak időben.

A **jelen kutatás dinamikus megközelítése abból indul ki, hogy a technológiai rendszer folyamatosan változó környezetben működik.** A fenyegetések, technológiai innovációk, szervezeti változások és szabályozási módosulások egyaránt megváltoztathatják a rendszer működési feltételeit. A reziliencia ezért nem pusztán a zavar előtti vagy utáni rendszerállapottal, hanem a változások felismerésének, értelmezésének és az azokhoz történő alkalmazkodásnak a folyamatával írható le.

A dinamikus modell célja ennek megfelelően annak leírása, hogy a háromdimenziós rendszer miként érzékeli a környezet változásait, hogyan értékeli azok jelentőségét, milyen adaptív választ alakít ki, miként stabilizálja működését, végül hogyan építi be a megszerzett tapasztalatokat a következő működési ciklusba.

A modell dinamikus szemlélete kapcsolódik **Holling reziliencia értelmezésének** rendszerelméleti logikájához [1], a **Gunderson és Holling által kidolgozott adaptív ciklushoz** [99], **Holland komplex adaptív rendszerekről** alkotott megközelítéséhez [6], valamint **Duchek anticipáció–megküzdés–adaptáció modelljéhez** [4]. A jelen kutatás azonban e megközelítéseket nem közvetlenül veszi át, hanem a háromdimenziós technológiai rezilienciamodell szerkezetére alkalmazza. A dinamikus működés elemzési egysége ezért nem önmagában a technológia vagy a szervezet, **hanem a T–O–R rendszer és annak interdimenzionális kapcsolatrendszere.**

A kutatás által javasolt új dinamikus modell tehát a technológiai, szervezeti és szabályozási dimenziók együttes fejlődését írja le.



3.9. ábra: A strukturális architektúrától a dinamikus működésig (saját szerkesztés)

3.4.2 A szerző által javasolt Adaptív Technológiai Reziliencia Ciklus (BATR-ciklus)

A dinamikus működés leírására jelen kutatás bevezeti a szerző által javasolt (Balogh-féle) **Adaptív Technológiai Reziliencia Ciklust (Balogh Adaptive Technological Resilience Cycle – BATR).** A BATR a háromdimenziós modell időbeli működési mechanizmusát írja le. Alapfeltevése szerint a reziliens rendszer működése nem egyszeri zavar–válasz folyamat, hanem egymást követő, visszacsatolásokkal összekapcsolt adaptációs ciklusok sorozata.

A BATR kialakítása során a reziliencia szakirodalmában megjelenő ciklikus és adaptív megközelítéseket elméleti előzményként vettem figyelembe, azonban a ciklus fázisstruktúrája, T–O–R integrációja és a kapcsolati szűk keresztmetszetekhez való kapcsolása a jelen kutatásban kialakított konstrukció.

A BATR-ciklus öt funkcionális szakaszt különít el: érzékelés **(Sense),** értékelés **(Assess)**, adaptáció **(Adapt)**, stabilizáció **(Stabilise)**, valamint tanulás és innováció **(Learn & Innovate)**. A szakaszok analitikai elkülönítése a működés értelmezését szolgálja; a

gyakorlatban közöttük átfedések, párhuzamos folyamatok és visszacsatolások is kialakulhatnak.

I. Érzékelés (Sense)

A **ciklus első funkciója** a rendszer belső állapotának és külső működési környezetének folyamatos megfigyelése. Az érzékelés magában foglalhatja a technológiai állapotmonitorozást, a fenyegetések és sérülékenységek felismerését, a technológiai trendfigyelést, a kiberfelderítést, a szenzoradatok feldolgozását és az AI alapú prediktív elemzést. Funkciója nem kizárólag a már bekövetkezett zavar felismerése, hanem a potenciális változások és gyenge jelek lehetőség szerinti korai azonosítása.

Az érzékelés mindhárom dimenzióban értelmezhető: technológiai szinten monitoring és diagnosztikai képességként, szervezeti szinten helyzetismeretként és információmegosztásként, szabályozási szinten pedig a környezeti, jogi és stratégiai változások követéseként.

A reziliens rendszer képes korán felismerni azokat a változásokat, amelyek később működési kockázatot jelenthetnek.

II. Értékelés (Assess)

Az **érzékelt információ önmagában nem eredményez reziliens működést**. A rendszernek képesnek kell lennie annak értelmezésére, hogy az azonosított változás milyen hatással lehet a kritikus funkciókra, a függőségekre és a rendszer egészének működésére. A második szakasz ezért a technológiai és környezeti információk szervezeti és stratégiai jelentésének meghatározását szolgálja.

Ebben a szakaszban különösen fontossá válik a T↔O, T↔R és O↔R kapcsolatok minősége, mivel a technológiai információt szervezeti döntéssé, majd szabályozási és irányítási szempontból végrehajtható cselekvéssé kell alakítani.

Ebben a szakaszban kapcsolódik össze először a három dimenzió. A technológia adatot szolgáltat. A szervezet értékeli azt. A szabályozás kijelöli az elfogadható kockázati szintet.

III. Adaptáció (Adapt)

A **harmadik szakasz a modell központi eleme**. Az értékelés eredménye alapján a rendszer módosítja működésének azon elemeit, amelyek a megváltozott környezethez történő alkalmazkodáshoz szükségesek. Az adaptáció technológiai szinten jelenthet újrakonfigurálást, alternatív működési mód alkalmazását, szoftver- vagy biztonsági módosítást; szervezeti szinten döntési, folyamat- vagy erőforrás-átrendezést; szabályozási szinten pedig eljárások, prioritások vagy irányítási mechanizmusok módosítását.

A háromdimenziós modell szempontjából az adaptáció akkor tekinthető hatékonynak, ha nem izoláltan egyetlen dimenzióban történik, hanem a változás által érintett T–O–R kapcsolatrendszer összehangolt újrakonfigurálását eredményezi.

Ez különbözteti meg a modellt a hagyományos incidenskezelési modellektől. Nem pusztán helyreállítás történik. Hanem maga a rendszer változik meg.

IV. Stabilizáció (Stabilize)

Az **adaptációt követően a rendszer célja nem feltétlenül a zavar előtti állapot teljes visszaállítása**, hanem egy elfogadható és fenntartható működési állapot kialakítása. A stabilizáció ezért magában foglalhatja az eredeti működés helyreállítását, degradált működési mód fenntartását vagy egy új, tartósan alkalmazható működési konfiguráció kialakítását.

V. Tanulás és innováció (Learn)

A **ciklus utolsó funkcionális szakasza a tapasztalatok rendszerszintű feldolgozása és beépítése.** A tanulás nem kizárólag az esemény utáni értékelést jelenti, hanem annak vizsgálatát is, hogy milyen technológiai, szervezeti vagy szabályozási változtatások szükségesek a későbbi alkalmazkodóképesség növeléséhez.

A BATR logikájában ezért a tanulás és innováció nem a folyamat lezárását jelenti. Az itt létrejövő új tudás, technológiai képesség és intézményi tapasztalat megváltoztatja a rendszer következő ciklusának kiinduló állapotát. Ez indítja el a következő ciklust. A reziliencia tehát **spirálisan fejlődik**, nem körkörösen ismétlődik.

3.10. ábra: Balogh-féle Adaptív Technológiai Reziliencia Ciklus (BATR-ciklus) (saját szerkesztés)

3.4.3 A három dimenzió szerepe a BATR-ciklusban

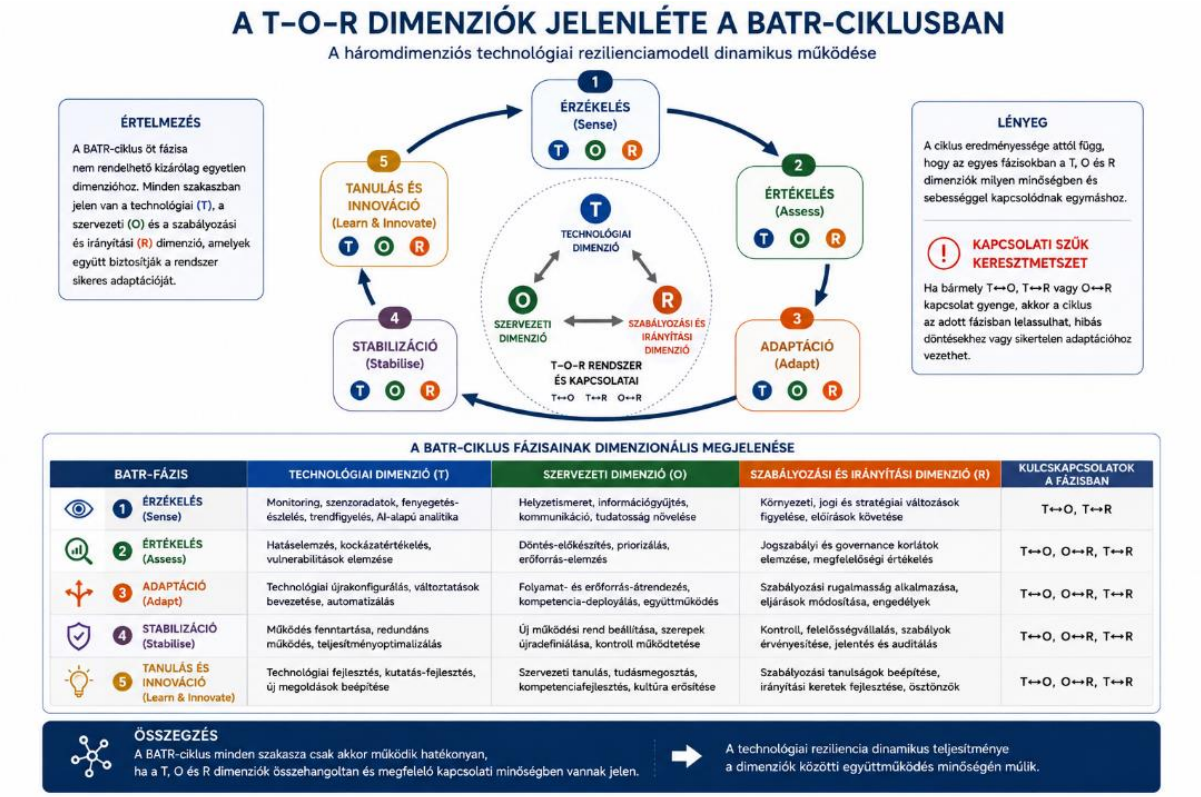
A BATR-ciklus nem a háromdimenziós modell mellett álló, attól független második modell, hanem annak dinamikus működési leképezése. Minden BATR-fázisban jelen van a technológiai, szervezeti és szabályozási dimenzió, azonban azok relatív szerepe és kölcsönhatása fázisonként eltérhet.

BATR-fázis	Technológiai (T)	Szervezeti (O)	Szabályozási (R)
Érzékelés	monitoring, szenzorok, AI	helyzetismeret, információmegosztás	stratégiai/jogi környezet figyelése
Értékelés	technikai hatáselemzés	döntés-előkészítés	jogi/governance korlátok
Adaptáció	újrakonfigurálás	folyamat- és erőforrás-adaptáció	szabályozási rugalmasság
Stabilizáció	működés fenntartása	új működési rend	kontroll és legitimáció
Tanulás	technológiai fejlesztés	szervezeti tanulás	szabályozási korrekció

3.3. táblázat: A három dimenzió szerepe a BATR-ciklusban (saját szerkesztés)

A táblázat azt mutatja, hogy a BATR egyes szakaszai nem rendelhetők kizárólag egyetlen dimenzióhoz. A ciklus eredményessége éppen attól függ, hogy a T, O és R képességek az adott fázisban megfelelően kapcsolódnak-e egymáshoz. A 3.2-ben meghatározott kapcsolati szűk keresztmetszet ezért dinamikus értelemben is megjelenhet:

egy gyenge T↔O, T↔R vagy O↔R kapcsolat a BATR-ciklus valamely szakaszának késését, hibáját vagy blokkolását eredményezheti.



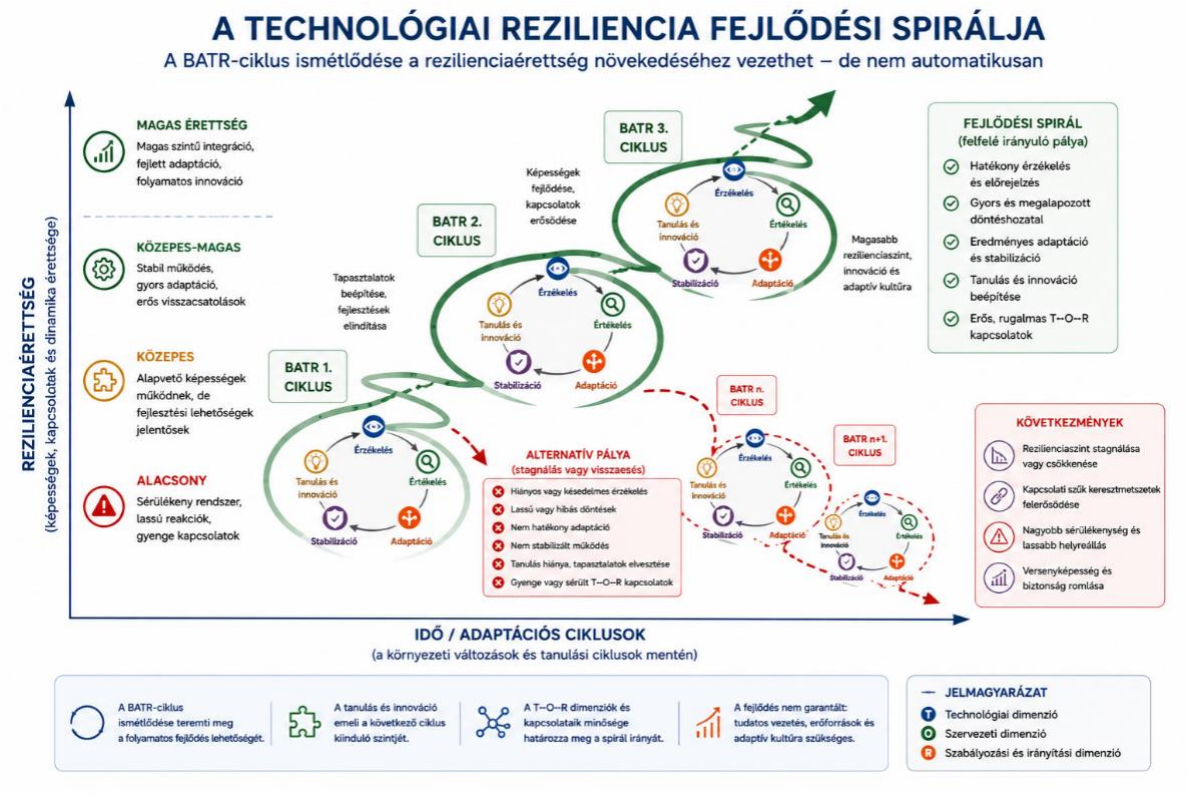
3.11. ábra: A T–O–R dimenziók jelenléte a BATR ciklusban (saját szerkesztés)

3.4.4 Visszacsatolás, tanulás és fejlődési spirál

A BATR-ciklus nem merev lineáris folyamat. Az egyes funkcionális szakaszok között előre- és visszacsatolások működhetnek, és a rendszer szükség esetén korábbi szakaszhoz is visszatérhet. Az értékelés például új érzékelési igényt tárhat fel, az adaptáció során pedig kiderülhet, hogy a választott megoldás szabályozási vagy szervezeti korlát miatt nem végrehajtható, ami ismételt értékelést tesz szükségessé. **A BATR a T–O–R strukturális modell dinamikus folyamatmodellje, amely a reziliencia időbeli működését írja le tehát.**

Egy új mesterségesintelligencia-alapú technológia bevezetése például új technológiai képességet hozhat létre, amely módosíthatja a szervezeti munkafolyamatokat és kompetenciaigényeket. Ez új governance- és szabályozási követelményeket generálhat, amelyek visszahatnak a technológia további fejlesztésére és alkalmazási feltételeire. A visszacsatolás tehát nem kizárólag egy BATR-fázison belül, hanem a T–O–R dimenziók között is végbemegy.

A **BATR-ciklus ismétlődése fejlődési spirálként értelmezhető, amennyiben a rendszer képes a megszerzett tapasztalatok tényleges beépítésére.** A tanulási folyamat eredményeként növekedhet a tudásszint, fejlődhet a technológiai architektúra, érettebbé válhat a szervezeti működés és adaptívabbá válhat a szabályozási környezet. Ez azonban nem automatikus folyamat. Hiányos tanulás, erőforráshiány, szervezeti ellenállás vagy szabályozási merevség esetén a következő ciklus kiinduló rezilienciaszintje változatlan maradhat, vagy akár romolhat is. A fejlődési spirál ezért nem szükségszerűen felfelé irányuló pályát, hanem a rendszer tanulási és adaptációs képességétől függő dinamikus fejlődési lehetőséget jelent.



3.12. ábra: A technológiai reziliencia fejlődési spirálja (saját szerkesztés)

3.4.5 Dinamikus mérhetővé és értékelhetővé tétel és TRI

A **BATR-ciklus jelentősége nem kizárólag** a technológiai reziliencia dinamikus működésének koncepcionális leírásában áll. **Az öt funkcionális szakasz lehetőséget teremt a dinamikus alkalmazkodóképesség későbbi mérhetővé és értékelhetővé tételére is**. A rendszer rezilienciája ugyanis nemcsak az alapján értékelhető, hogy milyen képességekkel rendelkezik, hanem az alapján is, hogy ezeket milyen gyorsan és eredményesen képes működésbe hozni.

A dinamikus működés értékelése során ezért többek között vizsgálható az érzékelési idő, a döntési sebesség, az adaptáció végrehajtási ideje, a stabilizációhoz szükséges idő, a tanulási mechanizmusok működése, valamint az innovációs visszacsatolás eredményessége. Ezek a jellemzők a későbbiekben a technológiai reziliencia dinamikus érettségének indikátoraivá alakíthatók.

BATR-fázis	Lehetséges dinamikus indikátor
Sense	észlelési idő, lefedettség
Assess	értékelési/döntési idő
Adapt	adaptációs idő, sikerarány
Stabilise	helyreállási/stabilizációs idő
Learn & Innovate	tanulságok beépítési aránya, innovációs ciklus

3.4. táblázat: A BATR-fázisok és a dinamikus indikátorok kapcsolata (saját szerkesztés)

A BATR-modell tudományos hozzáadott értéke abban áll, hogy a háromdimenziós technológiai rezilienciamodell szerkezeti elemeit időbeli működési mechanizmussal kapcsolja össze. A rezilienciát nem kizárólag zavarokra adott reakcióként, hanem folyamatos érzékelési, értékelési, adaptációs, stabilizációs és tanulási folyamatként értelmezi. A modell ezen túlmenően lehetővé teszi a dinamikus működés mérhetővé és értékelhetővé tételét, ezáltal közvetlen elméleti kapcsolatot teremt a háromdimenziós modell és a Technological Resilience Index között.

3.5 A Technological Resilience Index (TRI) koncepcionális értékelési keretrendszere

3.5.1 A technológiai reziliencia mérhetővé és értékelhetővé tételének szükségessége

A **rezilienciával foglalkozó szakirodalom egyik meghatározó módszertani problémája,** hogy miközben a reziliencia fogalma elméleti szempontból széles körben megalapozott, annak gyakorlati értékelése továbbra is jelentős kihívást jelent. **A rezilienciavizsgálatok jelentős része kvalitatív szakértői értékelésre, egy-egy részterülethez kapcsolódó indikátorokra vagy specifikus teljesítménymutatókra épül.** Ezek fontos információkat biztosíthatnak a rendszer egyes tulajdonságairól, ugyanakkor önmagukban nem feltétlenül alkalmasak a komplex technológiai reziliencia átfogó értékelésére**. A jelenlegi változat ugyanezt a mérési problémát azonosítja a TRI kialakításának kiindulópontjaként.** [47],[58], [94], [102], [105].

A jelen kutatásban kidolgozott háromdimenziós modell alapján a technológiai reziliencia értékelése különösen összetett feladat. A rendszer rezilienciája nem vezethető le kizárólag a technológiai infrastruktúra fejlettségéből, mivel annak tényleges működőképességét a szervezeti képességek, a szabályozási és irányítási környezet, valamint az e dimenziók között fennálló kapcsolatok egyaránt befolyásolják. A 3.3 alfejezetben bemutatott dinamikus modell ezen túlmenően azt is megmutatta, hogy a reziliencia időben változó rendszerképesség, amelynek meghatározó eleme a változások érzékelése, értékelése, az adaptáció, a stabilizáció, valamint a tanulás és innováció.

A **technológiai reziliencia mérhetővé és értékelhetővé tételének ezért egyszerre kell figyelembe vennie három elemzési réteget: az egyes dimenziók belső képességeit, a dimenziók közötti kapcsolatok minőségét, valamint a rendszer dinamikus adaptációs képességét. [**90], [91], [94] [95], [113]

E követelmény teljesítésére vezetem be a **Technological Resilience Indexet (TRI)**. A TRI a jelen kutatásban nem kizárólag aggregált numerikus indexként, hanem **strukturált, többdimenziós rezilienciaértékelési és diagnosztikai keretrendszerként** értelmezendő. Elsődleges funkciója annak meghatározása, hogy a vizsgált rendszer mely területeken rendelkezik megfelelő rezilienciaképességgel, hol találhatók fejlesztendő területek, milyen kapcsolati szűk keresztmetszetek korlátozzák a rendszerszintű működést, valamint hogyan változik a rendszer adaptációs képessége az időben.

A kutatás jelen szakaszában ezért nem célom az értékelési területek matematikai súlyozása vagy egyetlen aggregált pontszámmá történő összevonása. Az ilyen típusú kvantitatív aggregáció megalapozása az indikátorok empirikus validációját, megfelelő elemszámú alkalmazási mintát és az egyes értékelési tényezők közötti kapcsolatok további vizsgálatát igényelné. A TRI elsődleges eredménye ennek megfelelően egy **többdimenziós technológiai rezilienciaprofil**.

3.5.2 A TRI értékelési alapelvei

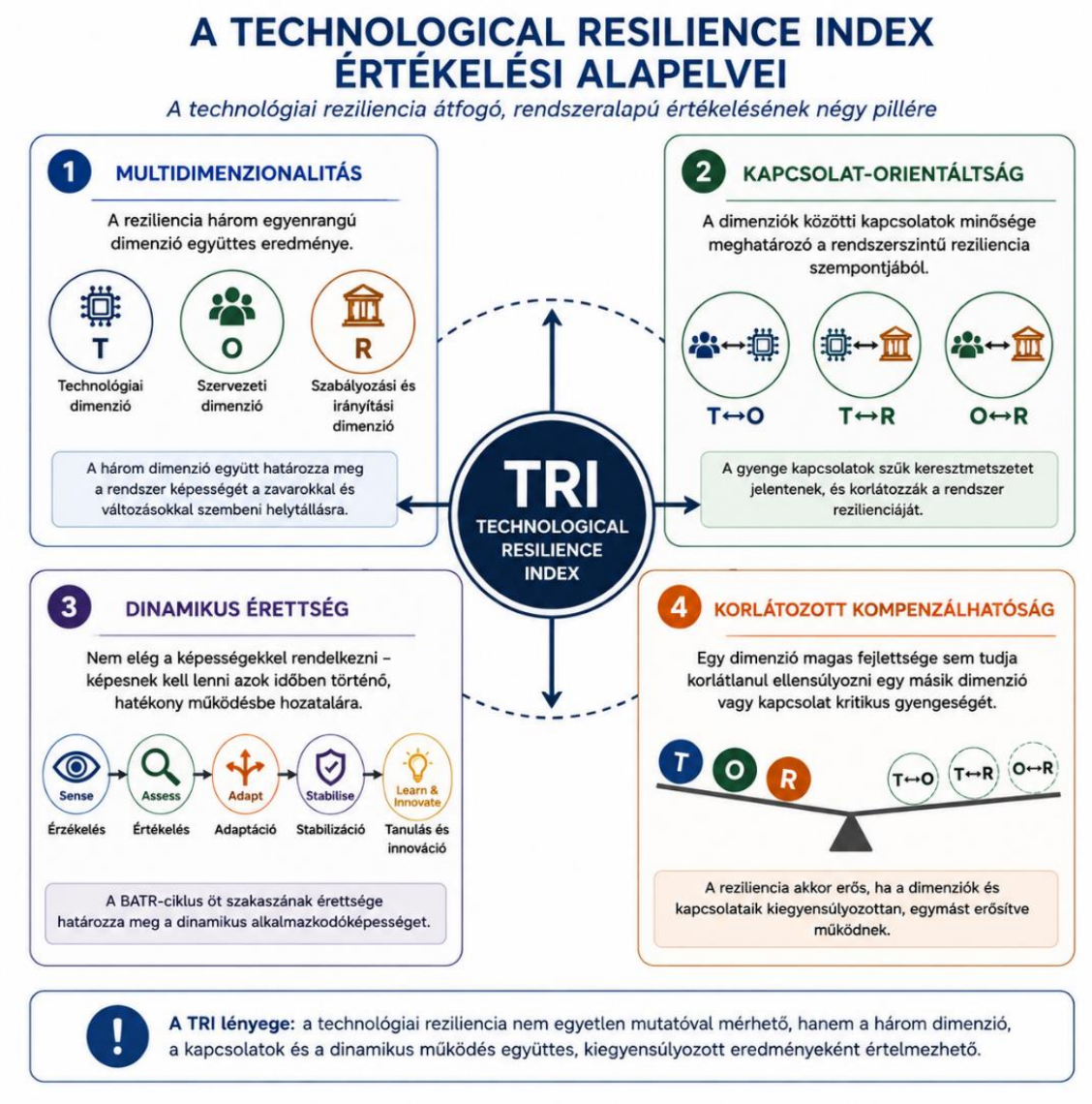
A TRI felépítése négy, egymással összefüggő értékelési alapelvre épül. Az első három már megjelenik a jelenlegi változatban – multidimenzionalitás, kapcsolat-orientált értékelés és dinamikus érettség –, ezeket azonban a 3.2-ben bevezetett kapcsolati szűk keresztmetszet miatt egy negyedik alapelvvel egészítem ki.

Az első alapelv a multidimenzionalitás. A technológiai reziliencia nem írható le egyetlen technikai, szervezeti vagy szabályozási mutatóval. A TRI ezért önállóan vizsgálja a technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziót. Az elkülönített értékelés lehetővé teszi annak meghatározását, hogy az adott rendszer mely dimenziókban rendelkezik fejlett képességekkel, illetve hol mutatkoznak strukturális hiányosságok. [92]

A második alapelv a kapcsolat-orientált értékelés. A háromdimenziós modellből következően a magas dimenzióérettség önmagában nem garantál maga rendszerszintű rezilienciát. A TRI ezért külön értékeli a technológia és szervezet (T↔O), a technológia és szabályozás (T↔R), valamint a szervezet és szabályozás (O↔R) közötti kapcsolatok minőségét. Ezzel lehetővé válik a 3.2 alfejezetben meghatározott kapcsolati szűk keresztmetszetek – limiting interfaces – gyakorlati azonosítása.

A harmadik alapelv a dinamikus érettség. A TRI nem kizárólag azt vizsgálja, hogy a rendszer milyen képességekkel rendelkezik egy adott időpontban, hanem azt is, hogy e képességeket milyen következetesen és eredményesen képes működésbe hozni változó körülmények között. A dinamikus érettség értékelési alapját a 3.3 alfejezetben kidolgozott BATR-ciklus öt funkcionális szakasza – Sense, Assess, Adapt, Stabilise, Learn & Innovate – biztosítja.

A negyedik alapelv a korlátozott kompenzálhatóság. A háromdimenziós modell alapján valamely dimenzió kiemelkedően magas fejlettsége nem képes automatikusan ellensúlyozni egy másik dimenzió vagy interdimenzionális kapcsolat kritikus gyengeségét. Egy technológiailag fejlett rendszer például nem tekinthető magas rezilienciájúnak, ha a szervezet nem képes annak hatékony alkalmazására, vagy a szabályozási környezet akadályozza az adaptív működést. A TRI ezért nem az egyes értékelési területek egyszerű átlagolására, hanem azok profilalapú, összefüggéseket is feltáró értelmezésére épül.



3.13. ábra: A Technological Resilience Index négy értékelési alapelve (saját szerkesztés)

3.5.3 A TRI hierarchikus értékelési architektúrája

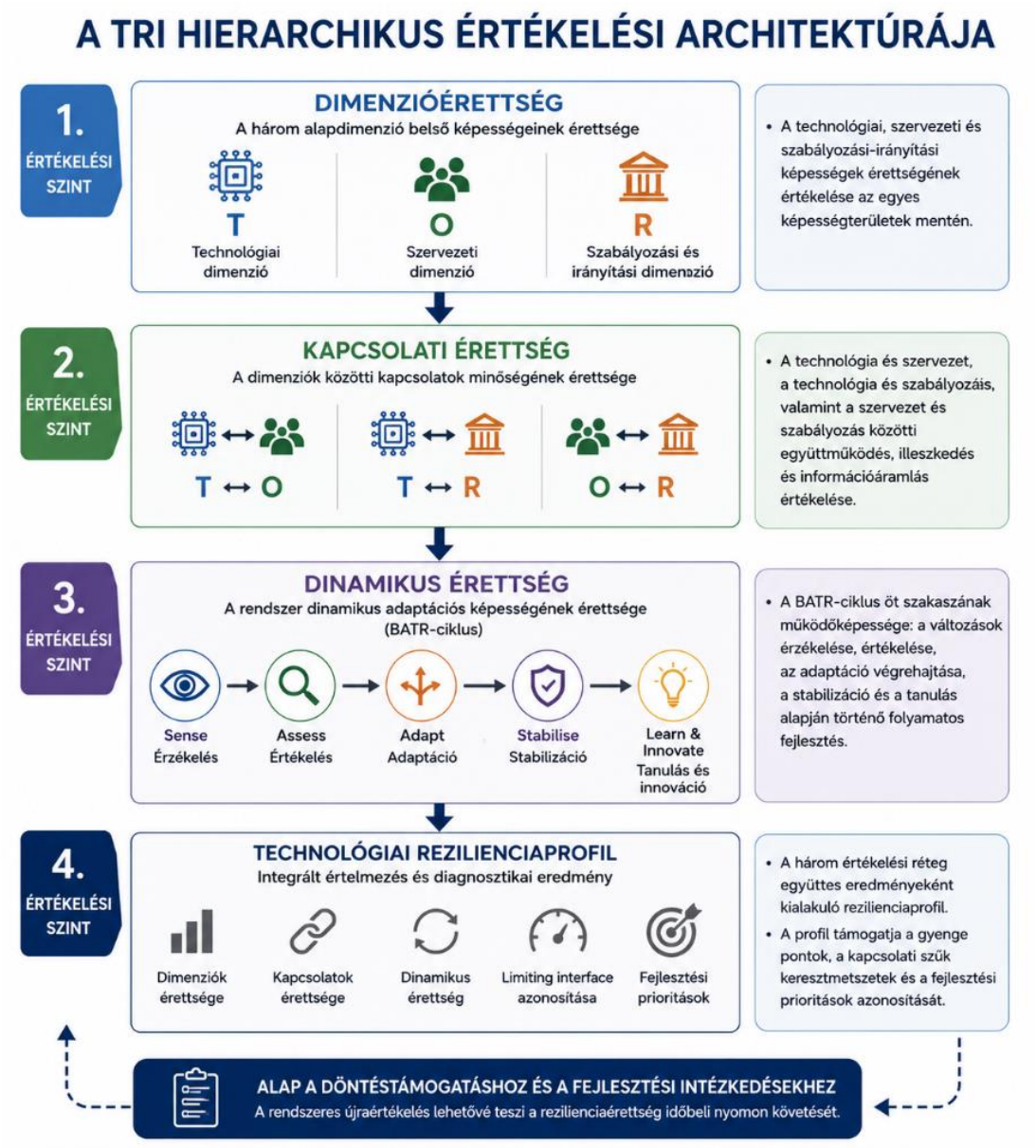
A TRI hierarchikus értékelési keretrendszerként épül fel. A hierarchikus struktúra célja, hogy az egyes képességterületekből kiindulva fokozatosan tegye lehetővé a dimenziószintű, kapcsolati, dinamikus és végül rendszerszintű reziliencia értelmezését. A jelenlegi változatban szereplő négyszintű struktúrát ezért megtartanám, de a matematikai aggregáció helyett diagnosztikai logikában alkalmaznám.

Az **első értékelési szint a dimenzióérettség**, amely a technológiai, szervezeti és szabályozási–irányítási dimenziók belső képességeit vizsgálja.

A **második értékelési szint a kapcsolati érettség**, amely a T↔O, T↔R és O↔R interfészek működőképességét és összehangoltságát értékeli.

A **harmadik értékelési szint a dinamikus érettség**, amely a BATR-ciklus öt funkcionális szakaszának működését vizsgálja.

A **negyedik szint a rendszerszintű rezilienciaprofil**, amely nem egyetlen aggregált értékben, hanem az előző három értékelési réteg együttes megjelenítésében és értelmezésében fejezi ki a rendszer technológiai rezilienciáját.



3.14. ábra: A TRI hierarchikus értékelési architektúrája (saját szerkesztés)

3.5.4 A dimenzióérettség értékelése

A dimenzióérettség értékelése annak meghatározására irányul, hogy a 3.2 alfejezetben azonosított technológiai, szervezeti és szabályozási–irányítási képességek

milyen fejlettségi szinten működnek. Az értékelés célja nem az egyes dimenziók közötti rangsor felállítása, hanem az erős és fejlesztendő képességterületek strukturált feltárása.

A **technológiai dimenzió (T)** értékelési területei:

- modularitás és újrakonfigurálhatóság;
- redundancia és alternatív működési lehetőségek;
- monitorozási és érzékelési képesség;
- kiberbiztonsági ellenálló képesség;
- automatizációs és intelligens adaptációs képesség;
- helyreállíthatóság.

A **szervezeti dimenzió (O)** értékelési területei:

- vezetés és döntéshozatal;
- szervezeti kultúra;
- tanulás és tudásmegosztás;
- együttműködés és kommunikáció;
- humán kompetenciák;
- erőforrás- és képességadaptáció.

A **szabályozási és irányítási dimenzió (R)** értékelési területei:

- governance és felelősségi rendszer;
- stratégiai irányítás;
- kockázatkezelés;
- szabályozási megfelelőség;
- adaptív szabályozás;
- ellenőrzés és visszacsatolás.

Az egyes képességterületek értékelése egységes, ötfokozatú érettségi logika szerint történhet. Ennek részletes módszertani kidolgozását a Technological Resilience Maturity Model (TRMM) biztosítja. A TRI ebben az értelemben meghatározza az értékelés **tárgyát és szerkezetét**, míg a TRMM az egyes értékelési elemek **érettségi szintjének meghatározását** támogatja.

3.5.5 A kapcsolati érettség értékelése

A háromdimenziós modell egyik központi állítása, hogy a technológiai reziliencia nem kizárólag az egyes dimenziók belső fejlettségéből, hanem azok együttműködésének minőségéből is származik. A TRI ezért a dimenziók értékelését három interdimenzionális kapcsolat vizsgálatával egészíti ki.

A **technológia–szervezet (T↔O) kapcsolat** azt fejezi ki, hogy a technológiai képességek milyen mértékben illeszkednek a szervezeti folyamatokhoz, kompetenciákhoz és döntési mechanizmusokhoz. Az értékelés vizsgálhatja többek között a technológia és a működési folyamatok illeszkedését, a szükséges kompetenciák rendelkezésre állását, a technológiai információk döntéshozatalba történő beépülését, valamint az új technológiák szervezeti befogadásának képességét.

A **technológia–szabályozás (T↔R) kapcsolat** azt mutatja meg, hogy a governance- és szabályozási környezet milyen mértékben támogatja a technológiai képességek biztonságos és adaptív alkalmazását. Vizsgálható a technológiai változások szabályozási lekövetése, az innováció számára rendelkezésre álló mozgástér, a technológiai kockázatok governance-rendszerbe történő integrációja, valamint a szabályozási reakcióképesség.

A **szervezet–szabályozás (O↔R) kapcsolat** azt fejezi ki, hogy a szervezeti működés és az irányítási-szabályozási struktúra milyen mértékben támogatja egymást. Az értékelés kiterjedhet a döntési és felelősségi jogosultságok egyértelműségére, az információáramlásra, a döntési autonómiára, valamint arra, hogy a governance-rendszer mennyiben támogatja vagy korlátozza a szervezeti adaptációt.

A kapcsolati érettség vizsgálata teszi lehetővé a 3.2-ben meghatározott **kapcsolati szűk keresztmetszet mérhetővé és értékelhetővé tételét**. A limiting interface így nem kizárólag elméleti fogalom, hanem az értékelési folyamatban azonosítható diagnosztikai jelenség.

Egy rendszer például magas technológiai és szervezeti érettséggel rendelkezhet, miközben a T↔O kapcsolat alacsony érettségű. Ebben az esetben a technológiai képességek szervezeti hasznosulása jelenti a rendszer fő reziliencia korlátját. A TRI feladata ezért nem csupán annak kimutatása, hogy „melyik dimenzió gyenge”, hanem annak feltárása is, hogy **hol nem működik megfelelően a dimenziók közötti kapcsolat**.

3.5.6 A dinamikus érettség értékelése

A TRI harmadik értékelési rétege a rendszer dinamikus adaptációs képességét vizsgálja. Ennek alapját a 3.3 alfejezetben bemutatott BATR-ciklus biztosítja.

A dinamikus érettség abban különbözik a dimenzióérettségtől, hogy nem elsősorban azt vizsgálja, **milyen képességekkel rendelkezik a rendszer**, hanem azt, hogy **ezeket a képességeket mennyire eredményesen képes működésbe hozni változó körülmények között**. [106]

Az értékelés ennek megfelelően a BATR öt funkcionális szakaszára épül:

Érzékelés (Sense): mennyire képes a rendszer a releváns belső és külső változások, fenyegetések, sérülékenységek és gyenge jelek időbeni felismerésére.

Értékelés (Assess): mennyire képes az érzékelt információk értelmezésére, a lehetséges következmények meghatározására, a prioritások kialakítására és a döntések előkészítésére.

Adaptáció (Adapt): mennyire képes technológiai, szervezeti és szabályozási működésének összehangolt módosítására.

Stabilizáció (Stabilise): mennyire képes az adaptációt követően fenntartható működési állapot kialakítására és a kritikus funkciók megfelelő szintű fenntartására.

Tanulás és innováció (Learn & Innovate): mennyire képes a tapasztalatokat feldolgozni, intézményesíteni és technológiai, szervezeti vagy szabályozási fejlesztésekbe visszaforgatni.

A BATR-alapú értékelésben különösen fontos, hogy az öt szakaszt ne kizárólag egymástól elkülönült képességekként vizsgáljuk. A dinamikus reziliencia érettségét az is meghatározza, hogy a rendszer képes-e az egyes fázisok között megfelelő információáramlást és visszacsatolást biztosítani.

BATR-fázis	Elsődleges értékelési kérdés
Sense	Felismeri-e időben a változást?
Assess	Képes-e annak jelentőségét megfelelően értékelni?
Adapt	Képes-e összehangolt választ kialakítani és végrehajtani?
Stabilise	Képes-e fenntartható működési állapotot létrehozni?
Learn & Innovate	Képes-e a tapasztalatot tartós képességfejlődéssé alakítani?

3.5 táblázat: a BATR fázis és az elsődleges értékelés (saját szerkesztés)

3.5.7 A TRI-profil és a kapcsolati szűk keresztmetszetek azonosítása

A TRI értékelési folyamatának eredménye elsődlegesen nem egyetlen összesített számérték, hanem a vizsgált rendszer **technológiai rezilienciaprofilja**. A profil egyidejűleg jeleníti meg a három dimenzió, a három interdimenzionális kapcsolat és a dinamikus adaptáció érettségét.

A profilalapú megközelítés egyik előnye, hogy megőrzi azokat az információkat, amelyek egyetlen aggregált mutató alkalmazása esetén elvesznének. Két rendszer rendelkezhetne azonos átlagos értékkel, miközben reziliencia szerkezetük alapvetően eltérő. Az egyik rendszer kiegyensúlyozott közepes képességekkel rendelkezhet, míg a másik magas technológiai fejlettség mellett kritikus szervezeti vagy kapcsolati hiányosságokat mutathat.

A TRI ezért az értékelés eredményét többdimenziós profilként jeleníti meg. Ennek egyik lehetséges szemléltetése:

Értékelési terület	Példa érettségi szint
Technológiai dimenzió – T	4
Szervezeti dimenzió – O	3
Szabályozási dimenzió – R	4
Technológia ↔ szervezet	**2**
Technológia ↔ szabályozás	3
Szervezet ↔ szabályozás	3
BATR dinamikus érettség	3

3.6. táblázat: TRI többdimenziós profilként – példa (saját szerkesztés)

A példában a rendszer technológiai fejlettsége magas, miközben a technológiai és szervezeti dimenzió közötti kapcsolat lényegesen alacsonyabb érettségű. A **T↔O kapcsolat**

ezért kapcsolati szűk keresztmetszetként azonosítható, amely korlátozhatja a rendszer egészének technológiai rezilienciáját.

A TRI-profil ilyen módon nemcsak értékelő, hanem **diagnosztikai és döntéstámogató funkcióval** is rendelkezik. Segítségével azonosíthatók azok a területek, ahol a további technológiai beruházás önmagában már nem feltétlenül növeli érdemben a rezilienciát, és a fejlesztési erőforrásokat inkább szervezeti, szabályozási vagy kapcsolati képességek javítására célszerű fordítani.

3.5.8 A TRI és a TRMM kapcsolata

A TRI mérhetővé és értékelhetővé tétele szükségessé teszi annak meghatározását is, hogy az egyes értékelési területek milyen fejlettségi szinten állnak. Ezt a funkciót tölti be a **Technological Resilience Maturity Model (TRMM)**.

A TRI és a TRMM nem két egymással versengő mérési megközelítés, hanem ugyanazon értékelési rendszer két, egymást kiegészítő eleme. **A két elem funkcionális különbsége röviden úgy foglalható össze, hogy a TRMM az érettségi szintek meghatározásának strukturált modellje, míg a TRI az értékelés eredményeinek integrált, többdimenziós technológiai reziliencia profilba rendezését szolgáló keret.**

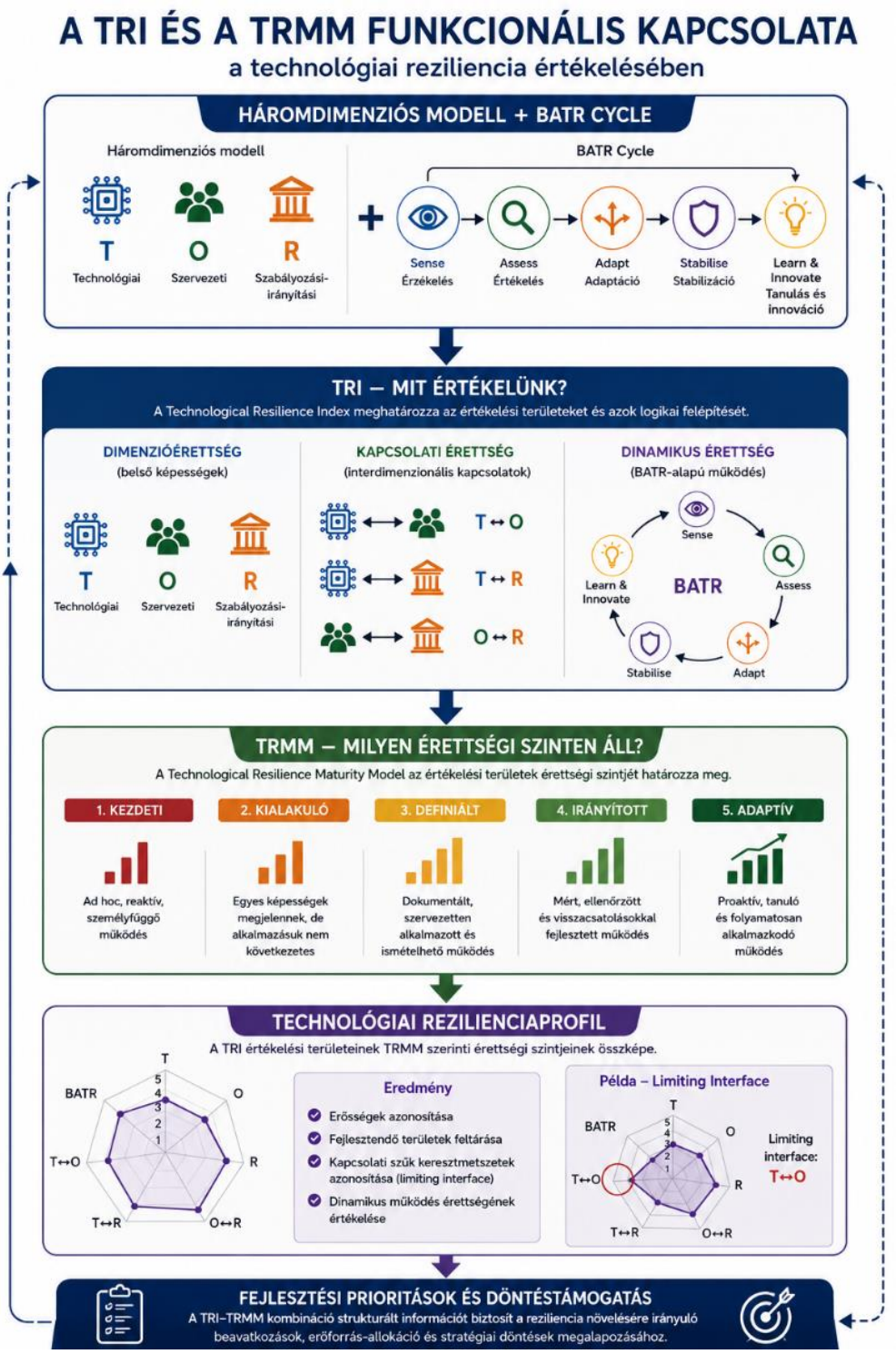
A **TRI azt határozza meg, hogy mit kell értékelni**: a technológiai, szervezeti és szabályozási dimenziókat, a közöttük fennálló kapcsolatokat, valamint a BATR alapján értelmezett dinamikus működést.A **TRMM azt határozza meg, hogy az adott értékelési elem milyen érettségi szinten áll**. Az érettségi modell egységes ötfokozatú skálát alkalmazhat:

Szint	Megnevezés	Általános jellemző
1.	Kezdeti	Ad hoc, reaktív, személyfüggő működés
2.	Kialakuló (emergens)	Egyes képességek megjelennek, de alkalmazásuk nem következetes
3.	Definiált	Dokumentált, szervezetten alkalmazott és ismételhető működés
4.	Irányított	Mért, ellenőrzött és visszacsatolásokkal fejlesztett működés
5.	Adaptív	Proaktív, tanuló és a változó környezethez folyamatosan alkalmazkodó működés

3.7. táblázat: Ötfokozatú érettségi modell (saját szerkesztés)

Az egyes szintekhez a későbbi módszertani kidolgozás során dimenzió- és indikátorspecifikus szintjellemzők (értékelési szintleírások) rendelhetők. Így például az 5.

szintű technológiai monitoring, az 5. szintű szervezeti tanulás és az 5. szintű T↔O kapcsolat eltérő konkrét követelményeket jelenthet, miközben ugyanazt az általános érettségi logikát követi.



3.15. ábra: A TRI és a TRMM funkcionális kapcsolata (saját szerkesztés)

A TRI–TRMM keretrendszer alkalmazásakor az értékelés bemeneti információi részben már meglévő ellenőrzési, audit- és kockázatértékelési eredményekből is származhatnak. Ilyen bemeneti forrást jelenthetnek például a NIS2 követelményeihez kapcsolódó hazai kiberbiztonsági auditok eredményei. A TRMM ezek megállapításait nem

helyettesítené vagy ismételné meg, hanem a technológiai dimenzió értékelésének egyik bizonyítékalapú inputjaként használná fel, majd azokat a szervezeti és szabályozási–irányítási dimenziók, illetve a dimenziók közötti kapcsolatok értékelésével egészítené ki. A TRI ennek eredményeként a megfelelőségi megállapításokat egy szélesebb, integrált technológiai reziliencia profil részeként jeleníthetné meg

3.5.9 Részösszegzés

A Technological Resilience Index a jelen kutatásban kidolgozott háromdimenziós technológiai reziliencia modell és a BATR dinamikus működési modell mérhetővé és értékelhetővé tételét szolgáló értékelési keretrendszer. **A TRI alapvető sajátossága, hogy a technológiai rezilienciát nem egyetlen homogén tulajdonságként kezeli, hanem három egymással összefüggő elemzési rétegben vizsgálja: a dimenziók belső érettségében, a dimenziók közötti kapcsolatok minőségében, valamint a rendszer dinamikus adaptációs képességében.**

A keretrendszer egyik meghatározó sajátossága a kapcsolat-orientált értékelés. A T↔O, T↔R és O↔R kapcsolatok önálló vizsgálata lehetővé teszi annak meghatározását, hogy a rendszer rezilienciáját nem valamely önálló képességterület, hanem a dimenziók közötti elégtelen együttműködés korlátozza-e. Ezzel a 3.2 alfejezetben meghatározott kapcsolati szűk keresztmetszet fogalma mérhetővé és értékelhetővé tehető elemzési kategóriává válik.

A TRI további sajátossága, hogy a BATR-ciklus integrálásával a strukturális képességek mellett a rendszer dinamikus működését is értékeli. Ez lehetővé teszi annak vizsgálatát, hogy a rendszer mennyire képes a változásokat érzékelni és értékelni, működését adaptálni és stabilizálni, valamint a tapasztalatokat tanulási és innovációs folyamatokon keresztül tartós képességfejlődéssé alakítani.

A TRI eredménye elsődlegesen **technológiai reziliencia profil**, nem pedig egyetlen aggregált numerikus érték. Ez a megközelítés megőrzi az egyes dimenziók és kapcsolatok közötti különbségeket, láthatóvá teszi a rendszer belső egyensúlytalanságait, és lehetővé teszi a fejlesztési prioritások célzott meghatározását. Az érettségi szintek egységes értelmezését a TRMM biztosítja, amely a TRI értékelési architektúráját ötfokozatú érettségi logikával egészíti ki.

A jelen kutatásban a TRI és a TRMM **koncepcionális és módszertani keretrendszerként** kerül meghatározásra. A cél nem egy matematikailag súlyozott, univerzális reziliencia érték létrehozása, hanem egy olyan strukturált értékelési módszer megalapozása, amely alkalmas lehet különböző technológiai rendszerek diagnosztikai vizsgálatára, összehasonlítására, fejlesztési prioritásaik azonosítására és reziliencia érettségük időbeli követésére.

Az indikátorok részletes értékelési szintleírásainak, az értékelési módszer reprodukálhatóságának és a keretrendszer különböző alkalmazási területeken történő empirikus vizsgálatának kidolgozása a modell további validációjának feladata. Ez összhangban van a jelenlegi kézirat azon megállapításával, hogy a TRI empirikus validálása és az indikátorok további módszertani fejlesztése későbbi kutatási feladat.

3.6 A háromdimenziós technológiai reziliencia modell koncepcionális validálása

A háromdimenziós technológiai reziliencia modell kidolgozását követően szükséges annak vizsgálata, hogy a létrehozott konstrukció megfelel-e azoknak az alapvető követelményeknek, amelyek lehetővé teszik tudományos elemzési keretként és későbbi empirikus vizsgálatok alapjaként történő alkalmazását. A jelen alfejezet ezért a modell **koncepcionális validálását** végzi el. Ennek célja nem a modell teljes körű empirikus igazolása, hanem annak vizsgálata, hogy elméletileg megalapozott, belső szerkezetében konzisztens, mérhetővé és értékelhetővé tehető és gyakorlati alkalmazásra alkalmas konstrukciót alkot-e.

A koncepcionális és az empirikus validálás megkülönböztetése a kutatás logikája szempontjából lényeges. A 3. fejezet az elméleti modellalkotásra, annak működési mechanizmusára és értékelési keretrendszerére koncentrál. A következő, 4. fejezet feladata ezzel szemben annak vizsgálata, hogy a kialakított megközelítés konkrét technológiai és kritikusinfrastruktúra-környezetekben mennyiben alkalmazható. A jelen alfejezet így **módszertani hidat képez az elméleti modellalkotás és a gyakorlati alkalmazás között**.

3.6.1 Elméleti megalapozottság és belső konzisztencia

A modell koncepcionális validitásának első feltétele, hogy annak dimenziói és kapcsolatai ne önkényesen kijelölt kategóriák legyenek, hanem a szakirodalmi elemzésből és az azonosított kutatási résből logikusan következzenek. A 3.1 alfejezet kritikai elemzése alapján a technológiai reziliencia kutatásában három meghatározó nézőpont azonosítható: a technológiai-mérnöki, a szervezeti, valamint a stratégiai-szabályozási megközelítés. Ezek jelentős magyarázó erővel rendelkeznek saját elemzési területükön, azonban csak részlegesen képesek értelmezni a modern komplex szocio-technikai rendszerek rezilienciáját.

A háromdimenziós modell erre a kutatási résre ad integratív választ. A technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziókat ugyanazon rendszer egymást kiegészítő összetevőiként értelmezi. A technológiai dimenzió a rendszer fizikai és digitális képességeit, a szervezeti dimenzió azok alkalmazásának vezetési, humán és adaptációs feltételeit, míg a szabályozási-irányítási dimenzió a működés governance-, stratégiai és normatív kereteit jeleníti meg.

A modell belső logikájának meghatározó eleme, hogy a technológiai rezilienciát nem e három dimenzió egyszerű összegeként, hanem kölcsönhatásukból **kialakuló rendszerképességként** értelmezi. Ebből közvetlenül következik a T↔O, T↔R és O↔R kapcsolatok önálló elemzési jelentősége. A rendszer rezilienciáját ezért nem kizárólag valamely dimenzió hiányossága, hanem a dimenziók közötti kapcsolat elégtelen működése is korlátozhatja. Ezt fejezi ki a 3.2 alfejezetben bevezetett **kapcsolati szűk keresztmetszet (limiting interface)** koncepció.

A modell időbeli működését a 3.3 alfejezetben meghatározott BATR-ciklus egészíti ki. A Sense–Assess–Adapt–Stabilise–Learn & Innovate folyamat nem a háromdimenziós modelltől független konstrukció, hanem annak dinamikus leképezése: azt írja le, hogy a technológiai, szervezeti és szabályozási képességek miként aktiválódnak és kapcsolódnak össze változó körülmények között.

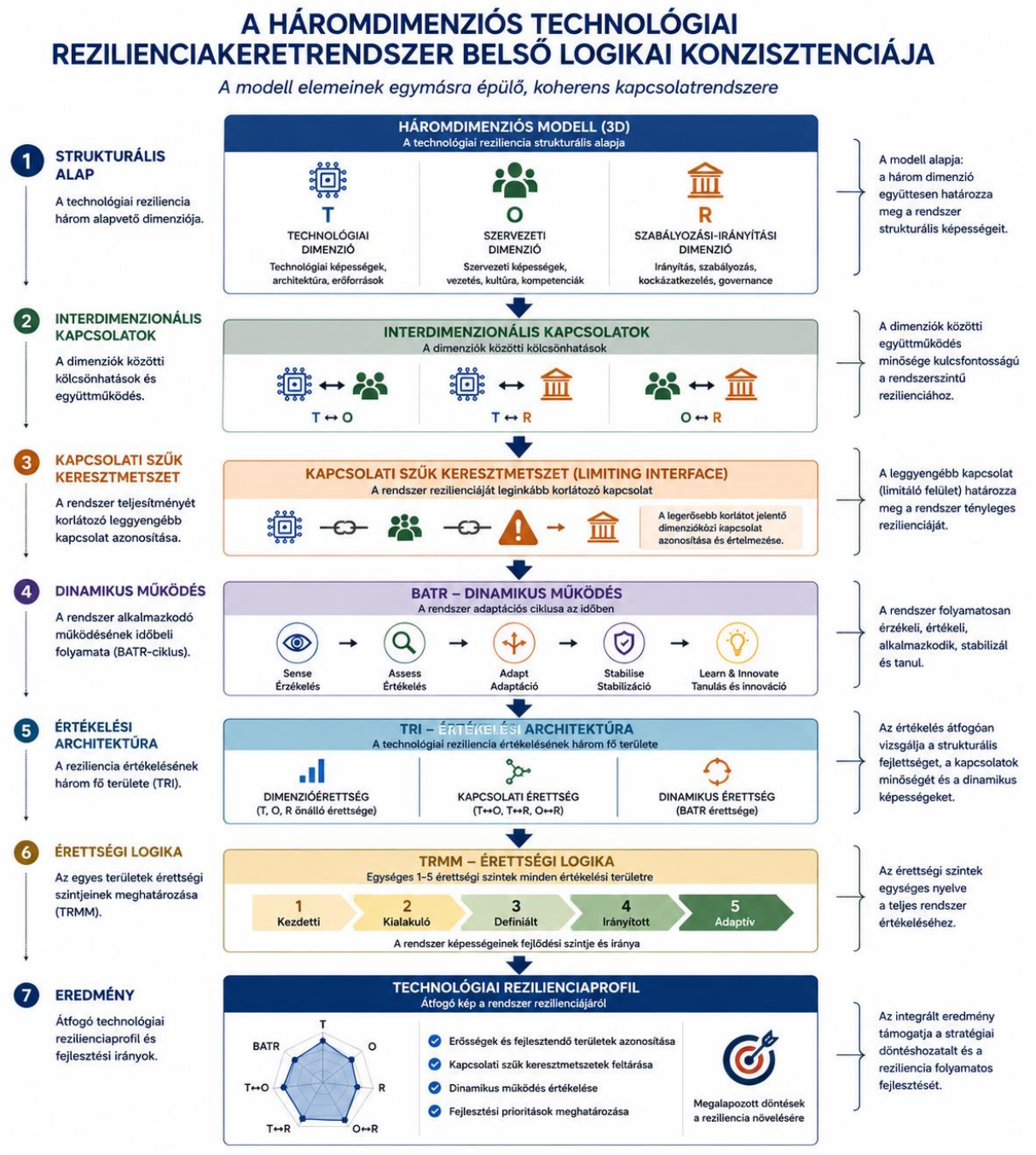
A 3.4 alfejezetben kialakított TRI és TRMM e strukturális és dinamikus rendszer mérhetővé és értékelhetővé tételét támogatja. A TRI meghatározza az értékelés fő területeit

– a dimenzióérettséget, a kapcsolati érettséget és a dinamikus érettséget –, míg a TRMM egységes érettségi logikát biztosít azok értelmezéséhez.

A modellkomponensek között ennek megfelelően következetes logikai kapcsolat áll fenn:

háromdimenziós modell → interdimenzionális kapcsolatok → limiting interface → BATR → TRI → TRMM → technológiai rezilienciaprofil.

Ez arra utal, hogy a 3. fejezetben kidolgozott elemek nem egymás mellé helyezett részmodellek, hanem ugyanazon technológiai reziliencia keretrendszer strukturális, dinamikus és értékelési nézőpontjai.



3.16. ábra: A háromdimenziós technológiai reziliencia keretrendszer belső logikai konzisztenciája (saját szerkesztés)

3.6.2 mérhetőség és értékelhetőség és alkalmazhatóság

A koncepcionális validálás második szempontja annak vizsgálata, hogy a modell elméleti konstrukciói átalakíthatók-e olyan értékelési kategóriákká, amelyek valós rendszerek vizsgálata során is alkalmazhatók. E szempont különösen fontos, mivel a modell tudományos értéke nem kizárólag fogalmi integrációjából, hanem abból is származik, hogy struktúrája alkalmas lehet a technológiai reziliencia gyakorlati elemzésére.

A technológiai, szervezeti és szabályozási–irányítási dimenziók a 3.2 és 3.4 alfejezetben meghatározott képességterületekre bonthatók. Ennek megfelelően értékelhető többek között a technológiai modularitás, redundancia és helyreállíthatóság; a szervezeti vezetés, tanulás és kompetencia; valamint a governance, a kockázatkezelés és az adaptív szabályozás.

A modell sajátossága, hogy az mérhetővé és értékelhetővé tétel nem korlátozódik az egyes dimenziókra. A T↔O, T↔R és O↔R kapcsolatok szintén vizsgálható értékelési kategóriákká alakíthatók. Így például elemezhető, hogy a technológiai információ megfelelően beépül-e a szervezeti döntéshozatalba, a szabályozási környezet képes-e követni a technológiai változásokat, vagy az irányítási struktúra biztosítja-e a szervezet számára az adaptációhoz szükséges mozgásteret.

Ezáltal a limiting interface is **diagnosztikai kategóriává** válik: segítségével meghatározható, hogy egy rendszer rezilienciájának fő korlátja nem valamely önálló képességben, hanem két dimenzió elégtelen együttműködésében található-e.

A BATR-ciklus ehhez a rendszer dinamikus működésének értékelését kapcsolja. A modell vizsgálhatóvá teszi, hogy a rendszer milyen képességgel rendelkezik a változások érzékelésére és értékelésére, az adaptáció végrehajtására, az új működési állapot stabilizálására, valamint a tapasztalatok tanulási és innovációs folyamatokba történő visszacsatolására.

A TRI–TRMM megközelítés mindezeket egységes értékelési architektúrába rendezi. Ennek eredménye nem szükségszerűen egyetlen összesített mutató, hanem olyan **többdimenziós technológiai reziliencia profil**, amely megőrzi a dimenziók, kapcsolatok és dinamikus képességek közötti különbségeket. Ez lehetővé teszi az erősségek, a fejlesztendő területek és a kapcsolati szűk keresztmetszetek azonosítását.

A modell absztrakciós szintje egyben azt is lehetővé teszi, hogy eltérő technológiai rendszerek vizsgálatára alkalmazható legyen. Egy energetikai infrastruktúra, közlekedési rendszer, digitális platform vagy katonai technológiai rendszer konkrét indikátorai eltérhetnek, de valamennyi esetében vizsgálható a technológiai, szervezeti és szabályozási dimenzió, azok kapcsolatrendszere és dinamikus adaptációja. A modell transzferálhatósága tehát nem az indikátorok azonosságára, hanem **a közös elemzési logikára** épül. [93].

3.6.3 Korlátok és átvezetés a gyakorlati alkalmazáshoz

A jelen alfejezetben elvégzett vizsgálat koncepcionális validálásnak tekinthető, ezért nem helyettesíti a modell empirikus vizsgálatát. Az elméleti megalapozottság, a belső konzisztencia és az mérhetőség és értékelhetőség alátámasztja a keretrendszer további alkalmazását, ugyanakkor önmagában nem igazolja, hogy a modell valamennyi technológiai vagy ágazati környezetben azonos diagnosztikai értékkel rendelkezik.

A következő validációs szint ezért a modell konkrét alkalmazási környezetekben történő vizsgálata. Ennek során elsősorban azt kell értékelni, hogy az elméletileg meghatározott dimenziók és kapcsolatok a gyakorlatban is azonosíthatók-e; a limiting interface képes-e tényleges rendszerkorlátok feltárására; a BATR alkalmas-e az adaptációs folyamatok strukturált értelmezésére; valamint a TRI–TRMM értékelés eredményei használható diagnosztikai és fejlesztési információt biztosítanak-e.

További módszertani követelmény az értékelés reprodukálhatóságának vizsgálata. A TRMM érettségi szintjeihez rendelt későbbi részletes értékelési szintleírásoknak lehetővé kell tenniük, hogy azonos információk alapján különböző értékelők lehetőség szerint hasonló következtetésekre jussanak. Ennek vizsgálata az empirikus validáció fontos része.

A 3. fejezet eredményeként kialakított keretrendszer tehát **koncepcionálisan megalapozott és empirikusan vizsgálható konstrukcióként** értelmezhető. A következő lépés annak meghatározása, hogy a modell miként működik konkrét alkalmazási környezetekben.

A 4. fejezet ennek megfelelően az elméleti modellalkotásról a gyakorlati alkalmazás irányába lép tovább. A vizsgálat középpontjába konkrét technológiai és kritikusinfrastruktúra-rendszerek kerülnek, amelyek lehetőséget teremtenek a háromdimenziós modell strukturális összefüggéseinek, a kapcsolati szűk keresztmetszeteknek, a BATR dinamikus működésének, valamint a TRI–TRMM értékelési logika gyakorlati alkalmazhatóságának vizsgálatára. A hangsúly így a továbbiakban már nem az elméleti konstrukció bővítésén, hanem annak diagnosztikai értékén és empirikus alkalmazhatóságán van.

3.7 A háromdimenziós technológiai reziliencia modell tudományos hozzájárulása, alkalmazhatósága és korlátai

A 3. fejezetben bemutatott kutatás célja olyan integrált elméleti és értékelési keretrendszer kialakítása volt, amely a technológiai rezilienciát nem kizárólag technológiai vagy mérnöki tulajdonságként, hanem komplex szocio-technikai rendszerképességként értelmezi. A szakirodalmi elemzés alapján azonosított kutatási rés arra mutatott rá, hogy a mérnöki-technológiai, szervezeti, illetve szabályozási és irányítási reziliencia megközelítések jelentős magyarázó erővel rendelkeznek saját elemzési területükön, azonban csak korlátozottan képesek e tényezők rendszerszintű kölcsönhatásainak egységes értelmezésére.

A kutatás erre a hiányra egy háromdimenziós, dinamikus és mérhetővé és értékelhetővé tehető technológiai reziliencia keretrendszer kialakításával válaszol. A tudományos hozzájárulás ennek megfelelően nem egyetlen új fogalom vagy mutató bevezetésében, hanem három egymásra épülő eredményben ragadható meg: a technológiai reziliencia strukturális újraértelmezésében; a kapcsolati és dinamikus működés modellezésében; valamint az elméleti konstrukció diagnosztikai és érettségi értékelési keretrendszerré történő mérhetővé és értékelhetővé tételában.

3.7.1 A modell tudományos hozzájárulása

A kutatás eredményeként **három, egymásra épülő tudományos hozzájárulás** azonosítható. Ezek együtt alkotják a háromdimenziós technológiai reziliencia keretrendszer elméleti és módszertani magját.

Első tudományos hozzájárulás: a technológiai reziliencia háromdimenziós, integrált szocio-technikai modelljének kidolgozása.

A kutatás első tudományos hozzájárulása a technológiai reziliencia olyan háromdimenziós modelljének kialakítása, amely a **technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziókat egyenrangú, kölcsönösen függő rendszerkomponensként** kezeli. A modell újdonsága nem önmagában e tényezők azonosításában rejlik, hanem abban, hogy azokat egységes szocio-technikai és rendszerelméleti keretben integrálja.

A technológiai dimenzió a rendszer fizikai és digitális architektúrájához, modularitásához, redundanciájához, monitorozhatóságához, kiberbiztonsági ellenálló képességéhez és helyreállíthatóságához kapcsolódó képességeket foglalja magában. A szervezeti dimenzió azokat a vezetési, döntéshozatali, tanulási, együttműködési és humán képességeket jeleníti meg, amelyek lehetővé teszik a technológiai erőforrások tényleges és adaptív alkalmazását. A szabályozási–irányítási dimenzió pedig a governance, a felelősségi rendszer, a stratégiai irányítás, a kockázatkezelés és a szabályozási alkalmazkodás feltételeit integrálja.

A modell központi állítása, hogy a technológiai reziliencia nem e három dimenzió egyszerű összege, hanem azok kölcsönhatásából k**ialakuló rendszerképesség**. Egy technológiailag fejlett rendszer ezért nem szükségszerűen reziliens, ha a szervezet nem képes annak megfelelő alkalmazására, vagy ha a szabályozási–irányítási környezet korlátozza az adaptív működést. Hasonlóképpen, fejlett szervezeti képességek sem képesek teljes mértékben kompenzálni egy merev vagy sérülékeny technológiai architektúrát.

A modell egyik meghatározó sajátossága, hogy a szabályozási és irányítási dimenziót nem a technológiai rendszer külső környezeti feltételeként, hanem a reziliencia **konstitutív elemeként** kezeli. Ezzel a technológiai reziliencia értelmezése túlmutat azokon a megközelítéseken, amelyek a szabályozást elsősorban megfelelőségi, jogi vagy külső intézményi tényezőként értelmezik.

Az első tudományos hozzájárulás ezért a technológiai reziliencia strukturális újraértelmezéseként foglalható össze:

A technológiai reziliencia a technológiai, szervezeti és szabályozási–irányítási dimenziók integrált, kölcsönösen függő működéséből kialakuló rendszerképesség.

Második tudományos hozzájárulás: az interdimenzionális kapcsolatok és a kapcsolati szűk keresztmetszet koncepciójának bevezetése, valamint a technológiai reziliencia dinamikus működési modelljének kidolgozása.

A kutatás második tudományos hozzájárulása annak modellezése, hogy a rendszerszintű technológiai rezilienciát nem elegendő az egyes dimenziók önálló fejlettsége alapján értékelni. A rendszer működőképességét meghatározza a **technológia–szervezet**

(T↔O), technológia–szabályozás (T↔R), valamint szervezet–szabályozás (O↔R) kapcsolatok minősége is.

A kapcsolatok önálló elemzési szintként történő kezelése a vizsgálat fókuszát a komponensek tulajdonságairól részben a komponensek közötti illeszkedésre, információáramlásra, döntési kapcsolatokra és adaptív együttműködésre helyezi át. Ez különösen fontos komplex technológiai rendszerekben, ahol valamely fejlett technológiai képesség tényleges értéke jelentősen csökkenhet, ha annak szervezeti vagy szabályozási integrációja elégtelen.

Ebből vezettem le a **kapcsolati szűk keresztmetszet – limiting interface –** fogalmát. A koncepció szerint a rendszer rezilienciájának meghatározó korlátja nem szükségszerűen valamely önálló dimenzió alacsony érettségében található. Kritikus gyengeség alakulhat ki két egyébként megfelelően fejlett dimenzió között is. Egy technológiailag magas színvonalú rendszer például alacsony rendszerszintű rezilienciahatást eredményezhet, ha a szervezet nem képes a technológiai információkat döntéssé és cselekvéssé alakítani. Ebben az esetben a T↔O kapcsolat jelenti a tényleges reziliencia korlátot.

A limiting interface koncepció tudományos jelentősége ezért abban áll, hogy a reziliencia vizsgálatban megjeleníti a **kapcsolatok minőségét, mint önálló rendszerjellemzőt**, és ezzel diagnosztikai szempontból is értelmezhetővé teszi a rendszerszintű teljesítmény korlátozó tényezőit.

A **második tudományos hozzájárulás másik eleme** a strukturális modell időbeli kiterjesztése a Balogh-féle Adaptív Technológiai Reziliencia Ciklus – BATR-ciklus – kialakításával. A BATR a technológiai rezilienciát nem statikus állapotként, hanem folyamatos alkalmazkodási folyamatként értelmezi. A Sense–Assess–Adapt–Stabilise–Learn & Innovate ciklus azt írja le, hogyan érzékeli a rendszer a változásokat, miként értékeli azok jelentőségét, hogyan alakítja át működését, miként stabilizálja az új állapotot, majd hogyan építi vissza a megszerzett tapasztalatokat a következő működési ciklusba.

A BATR sajátossága nem önmagában az adaptációs ciklus alkalmazása, hanem annak **a háromdimenziós T–O–R rendszerre történő integrálása**. A ciklus valamennyi

szakaszában jelen vannak a technológiai, szervezeti és szabályozási képességek, és a folyamat eredményessége az interdimenzionális kapcsolatok minőségétől is függ.

A második tudományos hozzájárulás ezért a technológiai reziliencia kapcsolati és dinamikus újraértelmezéseként foglalható össze:

A technológiai reziliencia rendszerszintű teljesítményét nemcsak a dimenziók képességei, hanem azok kapcsolati minősége és időbeli, ciklikus adaptációja is meghatározza.

Harmadik tudományos hozzájárulás: a technológiai reziliencia mérhetővé és értékelhetővé tehető diagnosztikai és érettségi értékelési keretrendszerének kialakítása.

A **kutatás harmadik tudományos hozzájárulása a háromdimenziós modell** és a BATR értékelhetőségének megteremtése a **Technological Resilience Index (TRI)** és a **Technological Resilience Maturity Model (TRMM)** funkcionális összekapcsolásával.

A TRI a jelen kutatásban nem matematikailag aggregált mutatóként, hanem **többszintű diagnosztikai értékelési architektúraként** értelmezendő. Három értékelési réteget különít el: a dimenzióérettséget, a kapcsolati érettséget és a dinamikus érettséget. Ezáltal az értékelés egyaránt kiterjed a T, O és R képességekre, a T↔O, T↔R és O↔R kapcsolatokra, valamint a BATR-ciklus működésére.

A TRMM ehhez egységes érettségi logikát biztosít. Funkcionális kapcsolatuk világosan elkülöníthető: **a TRI azt határozza meg, hogy mit értékelünk, míg a TRMM azt, hogy az adott értékelési terület milyen érettségi szinten áll**.

Az értékelés eredménye ennek megfelelően nem egyetlen összesített számérték, hanem **technológiai reziliencia profil**. A profil megőrzi az egyes dimenziók, kapcsolatok és dinamikus képességek közötti különbségeket, így alkalmas az erősségek, fejlesztendő területek és kapcsolati szűk keresztmetszetek azonosítására. Ez egyben csökkenti annak kockázatát is, hogy valamely magas dimenzióérték elfedjen egy kritikus kapcsolati gyengeséget.

A harmadik tudományos hozzájárulás ezért a technológiai reziliencia mérhetővé és értékelhetővé tételeként foglalható össze:

A strukturális és dinamikus elméleti modell olyan diagnosztikai és érettségi keretrendszerré alakítható, amely a technológiai rezilienciát többdimenziós profilként értékeli, és támogatja a fejlesztési prioritások meghatározását.

A három tudományos hozzájárulás egymásra épül. Az első meghatározza, **miből áll** a technológiai reziliencia; a második azt mutatja meg, **hogyan kapcsolódnak egymáshoz és hogyan alkalmazkodnak időben** a rendszer komponensei; a harmadik pedig lehetővé teszi annak strukturált vizsgálatát, hogy **milyen érettségi szinten működnek ezek a képességek és kapcsolatok**.

A modell tudományos újdonsága nem önmagában a technológiai, szervezeti és szabályozási–irányítási tényezők azonosításában áll, mivel ezek egyes elemei a reziliencia különböző szakirodalmi megközelítéseiben korábban is megjelentek. A kutatás hozzáadott értékét e tényezők egységes, dinamikus és mérhetővé és értékelhetővé tehető rendszerbe szervezése adja. A T–O–R modell a három dimenziót nem egymástól elkülönült értékelési területként, hanem kölcsönösen függő alrendszerekként kezeli, amelyek kapcsolataiban olyan szűk keresztmetszetek – limiting interface-ek – alakulhatnak ki, amelyek a teljes rendszer rezilienciáját korlátozzák. A statikus szerkezeti modellt a BATR időbeli és adaptív működési logikája egészíti ki, míg a TRI és a TRMM a modell mérhetővé és értékelhetővé tételét és értékelhetőségét teremti meg. Az így kialakított keret ágazati rendszerekre történő alkalmazása lehetővé teszi a modell összehasonlító vizsgálatát, az eredmények NTRGF[33]-be történő integrálása pedig szervezeti és ágazati szintről a stratégiai irányítás szintjére terjeszti ki a megközelítést. A tudományos újdonság ezért nem három korábban is ismert tényező újracsoportosításában, hanem a **T–O–R → interdimenzionális kapcsolatok → limiting interface → BATR → TRI/TRMM → ágazati alkalmazás → NTRGF** egymásra épülő, egységes elemzési és irányítási architektúrájának kialakításában ragadható meg.

[33] NTRGF: National Technological Resilience Governance Framework: Nemzeti Technológiai Reziliencia Irányítási Keretrendszer.

A modell hadtudományi hozzáadott értéke abban áll, hogy a katonai képességek technológiai megbízhatóságán túl azok működési fenntarthatóságát is vizsgálhatóvá teszi. A technológiai, szervezeti és szabályozási–irányítási dimenzió együttes értékelése lehetőséget teremt annak feltárására, hogy egy katonai képesség technikai rendelkezésre állása mögött milyen szervezeti, civil infrastrukturális, beszállítói vagy szabályozási függőségek találhatók, és ezek miként befolyásolhatják a műveleti feladat végrehajthatóságát. A modell így a technológiai rezilienciát a képességtervezés, a műveleti kockázatértékelés és a katonai döntéstámogatás szempontjából is értelmezhetővé teszi.

3.7.2 A modell alkalmazhatósága

A háromdimenziós technológiai reziliencia keretrendszer potenciális gyakorlati értéke abból következik, hogy a rezilienciát nem kizárólag elméleti konstrukcióként, hanem értékelhető és fejleszthető rendszerképességként kezeli. Alkalmazhatósága három egymással összefüggő funkcióban ragadható meg: **elemzési, diagnosztikai és döntéstámogató funkcióban**.

Elemzési keretként a modell lehetővé teszi komplex technológiai rendszerek reziliencia jellemzőinek strukturált feltárását. A T–O–R megközelítés segítségével elkülöníthetők a technológiai, szervezeti és szabályozási feltételek, miközben az interdimenzionális kapcsolatok vizsgálata biztosítja, hogy ezek ne egymástól elszigetelten jelenjenek meg. A BATR ehhez időbeli perspektívát kapcsol, így a rendszer egy adott állapot mellett annak adaptációs folyamatában is vizsgálható.

Diagnosztikai keretként a TRI–TRMM lehetőséget teremthet az erős és fejlesztendő képességterületek, valamint a limiting interface-ek azonosítására. Ennek gyakorlati jelentősége, hogy a reziliencia fejlesztése nem automatikusan további technológiai beruházást jelent. Ha például a technológiai dimenzió magas érettségű, miközben a T↔O kapcsolat gyenge, a fejlesztési prioritás inkább a kompetenciák, a szervezeti integráció, a döntési folyamatok vagy az információáramlás javítása lehet.

Döntéstámogató keretként a modell hozzájárulhat a fejlesztési prioritások meghatározásához, az erőforrások célzottabb allokációjához és a reziliencia időbeli változásának nyomon követéséhez. Ismételt értékelések segítségével vizsgálhatóvá válhat,

hogy egy technológiai, szervezeti vagy governance-beavatkozás miként változtatja meg a rendszer reziliencia profilját.

A modell alkalmazása különösen releváns lehet **honvédelmi és védelmi innovációs környezetben**. A korszerű katonai képességek egyre összetettebb technológiai ökoszisztémákra épülnek, amelyek digitális infrastruktúráktól, adatkapcsolatoktól, autonóm vagy részben autonóm rendszerektől, mesterségesintelligencia-alapú technológiáktól, logisztikai rendszerektől és összetett szervezeti struktúráktól függenek. Ilyen rendszerek esetében a műszaki teljesítmény önmagában nem írja le a tényleges alkalmazhatóságot. A szervezeti integráció, a humán kompetencia, a döntéshozatal, a fenntartási képesség, a biztonsági követelmények és a szabályozási környezet egyaránt meghatározó.

A modell **kritikus infrastruktúrák** vizsgálatában is alkalmazható lehet. Az energia-, közlekedési, elektronikus hírközlési és digitális infrastruktúrák fizikai és digitális komponensei erős kölcsönös függőségben működnek. A technikai redundancia vagy kiberbiztonsági kontrollok ezért csak akkor biztosítanak tényleges rezilienciahatást, ha megfelelő szervezeti reagálási, helyreállítási és governance-képességek kapcsolódnak hozzájuk.

A **kiberbiztonsági alkalmazás** különösen jól szemlélteti a háromdimenziós megközelítés jelentőségét. Egy szervezet kiberrezilienciája nem vezethető le kizárólag a technikai védelmi eszközök meglétéből. Meghatározó a szervezeti tudatosság, az incidenskezelés, az üzletmenet-folytonosság, a vezetői döntéshozatal, a felelősségi struktúra, valamint a szabályozási és kockázatkezelési környezet. A TRI–TRMM ezért egy hagyományos kiberbiztonsági vagy megfelelőségi audit kiegészítő reziliencia értékelési rétegeként is értelmezhető lehet.

A modell további alkalmazási területét jelenthetik a **technológiai innovációs és képességfejlesztési programok**. Egy új technológia bevezetésekor a műszaki érettség önmagában nem biztosítja a sikeres alkalmazást. A háromdimenziós modell lehetővé teszi annak vizsgálatát, hogy a technológiai fejlesztéssel párhuzamosan rendelkezésre állnak-e a szükséges szervezeti kompetenciák, megfelelő-e az irányítási struktúra, illetve a szabályozási környezet képes-e támogatni az innováció bevezetését.

A modell absztrakciós szintje lehetővé teszi eltérő ágazati környezetekben történő alkalmazásának vizsgálatát, ugyanakkor ez nem jelent automatikus általánosíthatóságot. A konkrét indikátorokat és érettségi értékelési szintleírásokat a vizsgált rendszer sajátosságaihoz kell igazítani. A közös elemzési architektúrát a T–O–R dimenziók, az interdimenzionális kapcsolatok, a BATR dinamikus logikája és a TRI–TRMM értékelési struktúrája biztosítja.

A modell tényleges alkalmazhatóságának vizsgálatában ezért nem az a döntő kérdés, hogy különböző rendszerekre formálisan ráilleszthető-e, hanem az, hogy **képes-e azok működése szempontjából releváns eltéréseket, gyengeségeket, kapcsolati problémákat és fejlesztési prioritásokat feltárni**.

3.7.3 A modell korlátai és további kutatási irányai

A háromdimenziós technológiai reziliencia modell alkalmazása során szükséges egyértelműen meghatározni annak jelenlegi korlátait. Ezek egyben kijelölik a modell további empirikus és módszertani fejlesztésének irányait.

Az első korlát a modell **koncepcionális és módszertani érettségéhez** kapcsolódik. A 3.5 alfejezetben elvégzett koncepcionális validálás alátámasztja a modell elméleti megalapozottságát, belső konzisztenciáját és mérhetőség és értékelhetőségát, azonban nem helyettesíti a különböző alkalmazási környezetekben történő empirikus vizsgálatot. További kutatás szükséges annak meghatározására, hogy a T–O–R dimenziók, az interdimenzionális kapcsolatok és a BATR-funkciók a gyakorlatban mennyiben azonosíthatók következetesen.

A második korlát az **indikátorok és érettségi értékelési szintleírások kontextusfüggősége**. A TRI általános értékelési architektúrát, a TRMM közös érettségi logikát biztosít, de a konkrét értékelési kritériumok ágazatonként eltérhetnek. Egy katonai vezetési rendszer, energetikai infrastruktúra vagy digitális szolgáltatási platform technológiai és szervezeti jellemzői szükségszerűen különböznek. A módszertani kihívás ezért olyan ágazatspecifikus értékelési szintleírások kialakítása, amelyek alkalmazkodnak az adott környezethez, ugyanakkor megőrzik a közös elemzési struktúrát.

A harmadik korlát a **szakértői értékelésből fakadó szubjektivitás**. Különösen a szervezeti adaptáció, az adaptív governance vagy az interdimenzionális kapcsolatok minőségének értékelése tartalmazhat értelmezési elemeket. A szubjektivitás csökkentéséhez

pontos indikátordefiníciókra, részletes érettségi értékelési szintleírásokra és egységes értékelési útmutatóra van szükség. A későbbi empirikus vizsgálatok egyik fontos feladata ezért annak meghatározása, hogy azonos információk alapján különböző értékelők mennyiben jutnak azonos vagy hasonló következtetésekre.

A negyedik korlát a modell **kontextusérzékenysége**. Az egyes dimenziók és kapcsolatok jelentősége a rendszer funkciójától, működési környezetétől, kritikus feladataitól és fenyegetettségétől függhet. A modell ezért nem alkalmazható mechanikus, univerzális checklistként. A vizsgálat során figyelembe kell venni a rendszer kritikus funkcióit, függőségeit és elfogadható kockázati szintjét.

Az ötödik korlát a **technológiai és szabályozási környezet folyamatos változása**. A mesterséges intelligencia, autonóm rendszerek, IoT, edge és cloud technológiák, illetve más új megoldások folyamatosan változtatják a technológiai reziliencia feltételeit. Ezzel párhuzamosan a szabályozási környezet is fejlődik. Emiatt a TRI-indikátorok és TRMM-értékelési szintleírások rendszeres felülvizsgálata szükséges.

E korlátokból három kiemelt további kutatási irány vezethető le.

Elsőként szükséges a TRI–TRMM keretrendszer különböző alkalmazási környezetekben történő empirikus vizsgálata. Ennek célja annak meghatározása, hogy az értékelési architektúra képes-e a valós rendszerek közötti releváns reziliencia különbségek feltárására és reprodukálható diagnosztikai eredmények biztosítására.

Másodikként indokolt a limiting interface koncepció empirikus tesztelése. Vizsgálni kell, hogy a modell által azonosított kapcsolati szűk keresztmetszetek megfelelnek-e a gyakorlatban tapasztalt rendszerkorlátoknak, illetve kimutatható-e kapcsolat az interdimenzionális gyengeségek és a rendszer tényleges adaptációs teljesítménye között.

Harmadikként szükséges a TRMM értékelési megbízhatóságának és időbeli alkalmazhatóságának vizsgálata. A részletes értékelési szintleírások kidolgozását követően értékelhetővé válik, hogy különböző szakértők mennyiben jutnak azonos eredményre, továbbá, hogy az ismételt értékelések képesek-e megbízhatóan jelezni a rendszer rezilienciájának fejlődését vagy romlását.

Hosszabb távon a keretrendszer **longitudinális alkalmazása** lehetővé teheti annak vizsgálatát is, hogy egy adott fejlesztési beavatkozás miként módosítja a reziliencia profilt, megszünteti-e a korábban azonosított kapcsolati szűk keresztmetszetet, illetve javítja-e a BATR által leírt adaptációs folyamatokat. Ez a keretrendszer alkalmazását az egyszeri diagnosztikai értékeléstől a folyamatos reziliencia menedzsment irányába terjesztheti ki.

A további kutatás célja ezért nem feltétlenül egyetlen univerzális vagy matematikailag aggregált reziliencia érték létrehozása, hanem annak empirikus meghatározása, hogy a kialakított keretrendszer milyen feltételek között képes **megbízható, reprodukálható és döntési szempontból releváns információt biztosítani** komplex technológiai rendszerek rezilienciájáról.

3-8 Összegzés

A 3. fejezetben végzett kutatás eredménye három egymásra épülő tudományos hozzájárulásban foglalható össze. **Elsőként** létrejött a technológiai reziliencia háromdimenziós T–O–R modellje, amely a rezilienciát technológiai, szervezeti és szabályozási–irányítási dimenziók kölcsönhatásából kialakuló rendszerképességként értelmezi. **Másodikként** az interdimenzionális kapcsolatok, a limiting interface koncepció és a BATR-ciklus bevezetésével a modell kiegészült a kapcsolati és dinamikus működés értelmezésével. **Harmadikként** a TRI–TRMM keretrendszer kialakításával a modell olyan diagnosztikai és érettségi értékelési struktúrává vált, amely technológiai reziliencia profil formájában teszi vizsgálhatóvá a rendszer strukturális, kapcsolati és dinamikus sajátosságait.

A kutatás következő lépése ezért már nem a modell további koncepcionális bővítése, hanem annak gyakorlati alkalmazása és empirikus vizsgálata. A modell tudományos értéke csak részben ítélhető meg belső logikai konzisztenciája alapján; legalább ilyen fontos annak vizsgálata, hogy konkrét rendszerek esetében képes-e releváns gyengeségeket, összefüggéseket és fejlesztési prioritásokat azonosítani.

A 4. fejezet ennek megfelelően az elméleti modellalkotásról a gyakorlati alkalmazás irányába lép tovább. Központi kérdése az lesz, hogy a T–O–R modell, az interdimenzionális kapcsolatok és a limiting interface koncepció, a BATR dinamikus működési logikája, valamint a TRI–TRMM értékelési keretrendszer konkrét

technológiai és kritikusinfrastruktúra-környezetekben milyen elemzési, diagnosztikai és fejlesztéstámogató értékkel rendelkezik.

4. fejezet: A háromdimenziós technológiai rezilienciamodell szakági alkalmazhatósági vizsgálata és validációja

4.1 A fejezet célja

A 3. fejezetben kidolgozott háromdimenziós technológiai rezilienciamodell meghatározta a technológiai reziliencia strukturális, kapcsolati és dinamikus értelmezési keretét. A kutatás eredményeként létrejött a **technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziókat integráló modell**, amelyet a **Balogh-féle Adaptív Technológiai Reziliencia Ciklus (BATR)**, valamint a **Technological Resilience Index (TRI)** és a **Technological Resilience Maturity Model (TRMM)** egészít ki.

A modellalkotás önmagában azonban nem elegendő annak igazolására, hogy a kialakított keretrendszer tudományos és gyakorlati szempontból egyaránt alkalmazható. A doktori kutatás következő lépése ezért a modell gyakorlati alkalmazhatóságának strukturált vizsgálata, különböző technológiai rendszerekre történő alkalmazása, valamint annak értékelése, hogy a kialakított keretrendszer képes-e következetesen feltárni a rezilienciát meghatározó tényezőket, az interdimenzionális összefüggéseket, a kapcsolati szűk keresztmetszeteket és a fejlesztési prioritásokat. A vizsgálat többes esettanulmány-logikát követ, amely eltérő működési és szabályozási környezetű kritikus infrastruktúrák összehasonlító elemzésén keresztül értékeli a modell analitikai alkalmazhatóságát. [68], [69].

A **jelen fejezet elsődleges célja ezért a háromdimenziós technológiai reziliencia modell strukturált, többes esettanulmány-alapú kvalitatív validálása** különböző kritikus infrastruktúrák és komplex technológiai rendszerek elemzésén keresztül. [70] A validálás ebben a kutatásban nem statisztikai vagy kvantitatív modellhitelesítést jelent, hanem annak vizsgálatát, hogy a 3. fejezetben meghatározott elméleti konstrukciók – a T–O–R dimenziók, az interdimenzionális kapcsolatok, a limiting interface koncepció és a BATR adaptációs logikája – eltérő technológiai környezetekben következetesen alkalmazhatók-e, és releváns elemzési eredményeket szolgáltatnak-e.[34]

[34] A modell összehasonlító validációja négy eltérő karakterű elemzési egységen történt: (1) villamosenergia-rendszer, (2) vasúti közlekedési rendszer, (3) magyar elektronikus hírközlési rendszer, valamint (4) NATO szárazföldi C2 funkcionális rendszer. A validáció strukturált dokumentumelemzésre épült.

A jelen kutatásban alkalmazott szakági validáció nem statisztikai vagy kísérleti validációt jelent, hanem strukturált dokumentumelemzésen alapuló analitikai alkalmazhatósági vizsgálatot.

A fejezet ugyanakkor **nem egyetlen esettanulmány vizsgálatára** korlátozódik. Az eltérő működési logikájú kritikus infrastruktúrák összehasonlító elemzése lehetőséget biztosít annak vizsgálatára, hogy a modell által azonosított strukturális és kapcsolati összefüggések ágazatspecifikus jelenségek-e, vagy több technológiai környezetben is következetesen megjelennek.35

E felismerés jelentős tudományos következményekkel jár. **Ha a technológiai reziliencia különböző kritikus infrastruktúrák esetében azonos rendszerszintű törvényszerűségeket mutat, akkor a reziliencia nem kezelhető kizárólag ágazati kérdésként.** Az energetika, a közlekedés, az elektronikus hírközlés, az egészségügy, a védelmi ipar vagy a katonai vezetési rendszerek rezilienciája nem egymástól független képességek összessége, hanem egy közös nemzeti technológiai ökoszisztéma eltérő megjelenési formái. Az egyes rendszerek közötti függőségek miatt az egyik ágazat sérülékenysége közvetlen hatással lehet más infrastruktúrák működőképességére is. [30], [31]

A kutatás ebből kiindulva arra a kérdésre keresi a választ, hogy a technológiai reziliencia értelmezhető-e nemzeti stratégiai képességként, és amennyiben igen, milyen irányítási mechanizmusok szükségesek annak összehangolt fejlesztéséhez. A fejezet második részének központi célja ezért egy olyan integrált stratégiai irányítási keretrendszer

A felhasznált ágazati, szabályozási és doktrinális dokumentumok nem pusztán szakirodalmi háttérként, hanem a kvalitatív elemzés adatforrásaiként szolgáltak. Tartalmuk előzetesen meghatározott T–O–R kategóriák szerint került feldolgozásra, majd az azonosított interdimenzionális kapcsolatok kritikalitása, függőségi erőssége és adaptációs jelentősége alapján került meghatározásra az egyes rendszerek elsődleges limiting interface-e. A BATR alkalmazhatóságát annak vizsgálata jelentette, hogy az elemzett dokumentumokban leírt működési és reagálási folyamatok megfeleltethetők-e a Sense–Assess–Adapt–Stabilise–Learn & Innovate funkcionális ciklusnak.

[35] Az ágazatok explicit kiválasztási logikája: eltérő technológiai karakter + magas interdependencia + civil–katonai relevancia + szabályozási heterogenitás + megfelelő dokumentáltság.

kidolgozása, amely képes összekapcsolni a különböző ágazatok technológiai rezilienciáját, valamint támogatni azok összehangolt fejlesztését.

Ennek eredményeként dolgozom ki a **Nemzeti Technológiai Reziliencia Irányítási Keretrendszert (National Technological Resilience Governance Framework – NTRGF)**.

Az NTRGF nem újabb technológiai rezilienciamodell, hanem a jelen kutatás során kidolgozott tudományos eredmények stratégiai alkalmazási kerete. Míg a háromdimenziós T–O–R modell meghatározza a technológiai reziliencia szerkezetét, a BATR leírja annak adaptív működését, a TRI és a TRMM pedig biztosítják a diagnosztikai és érettségi értékelés módszertanát, addig az NTRGF ezen eredményeket egységes államirányítási és stratégiai döntéstámogatási rendszerbe integrálja.

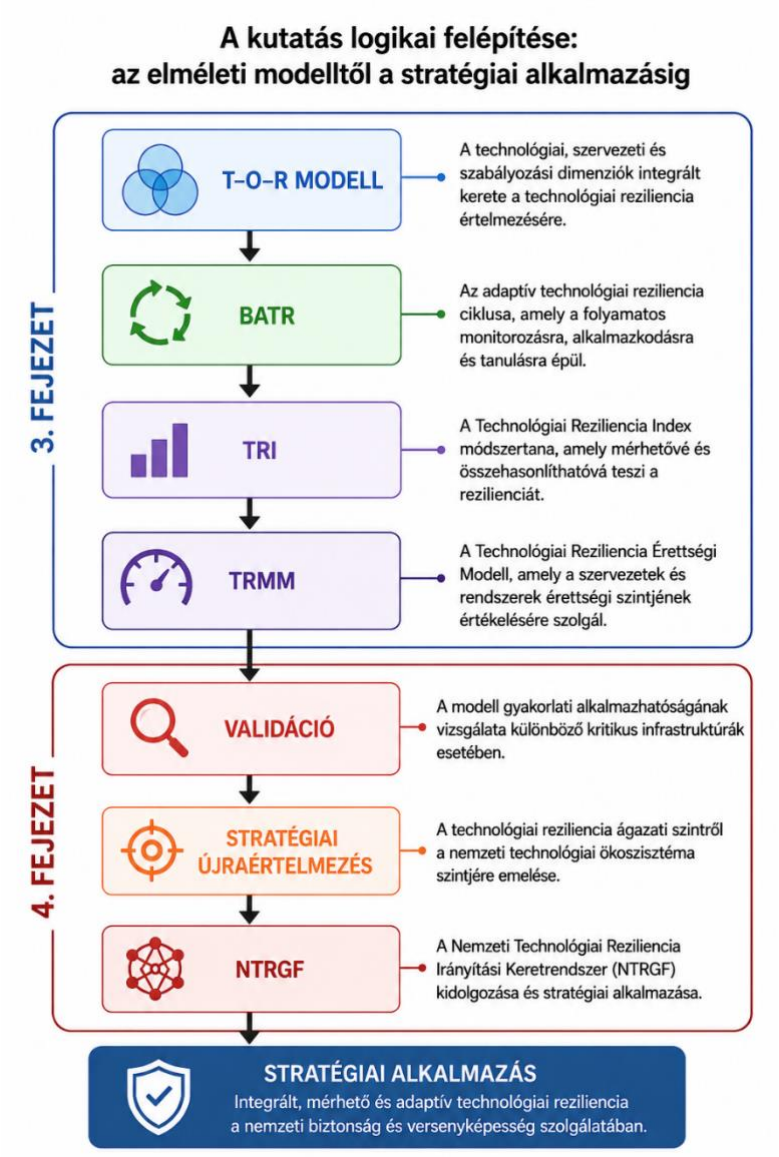
Az NTRGF alapfeltevése, hogy a technológiai reziliencia fejlesztése nem valósítható meg egymástól elkülönülő szakpolitikák, önálló ágazati programok vagy izolált technológiai beruházások eredményeként. A digitális transzformáció, a kiberbiztonság, a kritikus infrastruktúrák fejlesztése, a technológiai innováció és a nemzeti reziliencia stratégia olyan kölcsönösen függő rendszert alkotnak, amelynek irányítása integrált governance-megközelítést igényel.

Ennek megfelelően a fejezet négy egymásra épülő kutatási célt valósít meg.

- Elsőként bemutatja a háromdimenziós technológiai rezilienciamodell alkalmazását különböző kritikus infrastruktúrák elemzésében.
- Másodikként a TRI és a TRMM értékelési logikájára támaszkodva vizsgálja, hogy a különböző infrastruktúrák rezilienciája egységes dimenzionális, kapcsolati és érettségi szempontrendszerben összehasonlítható-e, valamint, hogy az értékelési keret alkalmas-e közös reziliencia mintázatok és fejlesztési prioritások azonosítására.
- Harmadikként a különböző ágazatok elemzési eredményeinek szintézisével feltárja a technológiai reziliencia nemzeti szintű összefüggéseit és a jelenlegi irányítási megközelítések korlátait.
- Negyedikként pedig kidolgozza a **Nemzeti Technológiai Reziliencia Irányítási Keretrendszert (NTRGF)**, amely a kutatás során létrejött háromdimenziós modell, a BATR, a TRI és a TRMM eredményeire építve egységes stratégiai keretet biztosít

a technológiai reziliencia nemzeti szintű tervezéséhez, koordinációjához, értékeléséhez és folyamatos fejlesztéséhez.

A fejezet tudományos célja tehát kettős. Egyrészt strukturált összehasonlító elemzés keretében vizsgálja és kvalitatív módon alátámasztja a háromdimenziós technológiai rezilienciamodell alkalmazhatóságát különböző kritikus infrastruktúrák esetében; másrészt megteremti azt az elméleti és módszertani alapot, amelyre építve a technológiai reziliencia a nemzeti stratégiai irányítás önálló, integrált képességterületeként értelmezhető.



4.1. ábra: A kutatás logikai felépítése: az elméleti modelltől a stratégiai alkalmazásig (saját szerkesztés)

4.2 A háromdimenziós technológiai reziliencia modell összehasonlító alkalmazása és kvalitatív validálása kritikus infrastruktúrákon

4.2.1 A szakági vizsgálat módszertana és a vizsgált területek kiválasztása

A szakági validáció strukturált dokumentumelemzésen alapuló, kvalitatív alkalmazhatósági vizsgálat. A kiválasztott kritikus infrastruktúra-területek eltérő technológiai és intézményi környezetet képviselnek; összehasonlító elemzésük célja annak vizsgálata, hogy a T–O–R modell dimenziói, interdimenzionális kapcsolatai, valamint a TRI–TRMM értékelési logika azonos szempontrendszer szerint alkalmazhatók-e, és mely elemek igényelnek ágazatspecifikus adaptációt.

4.2.2 Az energetikai infrastruktúra rezilienciájának elemzése

Az energetikai infrastruktúra a modern társadalmak egyik legalapvetőbb kritikus infrastruktúrája. Az elektromosenergia-termelés, az átviteli hálózatok, a földgázellátás, a megújuló energiaforrások és az ezekhez kapcsolódó digitális irányítási rendszerek együttesen olyan komplex szocio-technikai rendszert alkotnak, amelynek működése közvetlen hatással van valamennyi további kritikus infrastruktúrára. **Az energiaellátás zavara nem kizárólag gazdasági veszteségeket okoz, hanem közvetlenül befolyásolja a közlekedési rendszerek, az elektronikus hírközlés, az egészségügy, a honvédelem és az államigazgatás működőképességét is**. [26]

A technológiai reziliencia szempontjából ezért az energetikai infrastruktúra különösen alkalmas a háromdimenziós modell validálására, mivel egyszerre jelennek meg benne a fejlett technológiai rendszerek, az összetett szervezeti együttműködések és a szigorúan szabályozott működési környezet. [85]

A technológiai dimenzió értékelése

A technológiai dimenzió vizsgálata során megállapítható, hogy az **energetikai infrastruktúrák rezilienciáját elsősorban a hálózati redundancia, a modularitás, a digitális felügyeleti rendszerek (SCADA, EMS, DMS), az automatizált hibadetektálás, valamint a fizikai és kiberbiztonsági védelmi képességek határozzák meg.** [62]

Az elmúlt években végrehajtott digitalizáció következtében az energiatermelő és -elosztó rendszerek egyre inkább cyber-physical rendszerekké váltak. Ez jelentősen javította az üzemeltetés hatékonyságát, ugyanakkor új sérülékenységeket is létrehozott. A hagyományos műszaki meghibásodások mellett ma már az informatikai incidensek, a kommunikációs hálózatok kiesése, a beszállítói láncok sérülése vagy akár mesterséges

intelligenciával támogatott kibertámadások is közvetlenül veszélyeztethetik az energiaellátást.

A háromdimenziós modell technológiai dimenziója ezért nem csupán a fizikai infrastruktúra robusztusságát értékeli, hanem annak digitális függőségeit és adaptív képességeit is.

A szervezeti dimenzió értékelése

Az energetikai infrastruktúra működése jelentős mértékben függ az üzemeltető szervezetek felkészültségétől. A technológia önmagában nem képes biztosítani a rezilienciát, amennyiben a szervezet nem rendelkezik megfelelő incidenskezelési eljárásokkal, döntéstámogatási mechanizmusokkal, képzett személyzettel és adaptív vezetési kultúrával.

Az elemzés rámutat arra, hogy az **energiarendszerekben a technológiai fejlesztések sok esetben gyorsabban valósulnak meg, mint a szervezeti alkalmazkodás**. Az új digitális technológiák bevezetése nem minden esetben jár együtt a működési folyamatok, a kompetenciák vagy a vezetési mechanizmusok átalakulásával. Ennek következtében a technológiai fejlettség és a szervezeti adaptáció között jelentős eltérések alakulhatnak ki.

Ez a jelenség jól illusztrálja a háromdimenziós modell egyik alapfeltevését, amely szerint a rezilienciát nem az egyes dimenziók önálló fejlettsége, hanem azok összehangolt működése határozza meg.

A szabályozási–irányítási dimenzió értékelése

Az energetikai ágazat a legszigorúbban szabályozott kritikus infrastruktúrák közé tartozik. Az európai uniós szabályozás, a nemzeti energia- és klímastratégiák, a kritikus infrastruktúra-védelmi előírások, a NIS2 irányelv, valamint az ágazati biztonsági követelmények együttesen határozzák meg a működés kereteit. [26],[25]

A szabályozási dimenzió ugyanakkor nem kizárólag megfelelőségi kérdésként jelenik meg. A **kutatás során kidolgozott modell alapján a governance feladata a technológiai fejlesztések, a szervezeti működés és a stratégiai célkitűzések összehangolása**. Ez különösen fontossá válik olyan időszakokban, amikor egyszerre zajlik az energiaátmenet, a digitalizáció és a kibervédelmi követelmények szigorodása.

Az interdimenzionális kapcsolatok elemzése

A háromdimenziós modell egyik legfontosabb újítása az interdimenzionális kapcsolatok önálló elemzése. Az energetikai infrastruktúrában a legerősebb kapcsolat a technológiai és szervezeti dimenzió között figyelhető meg. A fejlett digitális irányítási

rendszerek csak akkor képesek tényleges reziliencia növekedést eredményezni, ha az üzemeltető szervezet megfelelő döntési és reagálási képességekkel rendelkezik.

Hasonló jelentőségű a technológia és a szabályozási környezet kapcsolata is. Az új technológiák – például intelligens hálózatok, decentralizált energiatermelés vagy mesterséges intelligenciával támogatott hálózatirányítás – csak akkor alkalmazhatók biztonságosan, ha a szabályozási környezet képes azok integrálására.

Limiting interface az energetikai infrastruktúrában

Az elemzés alapján a **legjelentősebb kapcsolati szűk keresztmetszet a technológiai és szervezeti dimenzió között** jelenik meg. Számos esetben nem maga a technológia jelenti a reziliencia korlátját, hanem annak szervezeti alkalmazása. A korszerű monitoring- és döntéstámogató rendszerek által biztosított információk csak akkor növelik a rendszer alkalmazkodóképességét, ha azokat a szervezet képes megfelelő sebességgel értelmezni és döntéssé alakítani.

Ez az eredmény megerősíti a limiting interface koncepció gyakorlati relevanciáját. A rezilienciát nem feltétlenül a leggyengébb technológiai komponens korlátozza, hanem az a kapcsolat, amelyen keresztül a technológiai képességek szervezeti működéssé alakulnak.

A BATR-ciklus értékelése

Az energetikai infrastruktúrák működése jól illeszthető a BATR adaptációs ciklus logikájához.

Az elemzett energetikai dokumentumok T–O–R és BATR-alapú értelmezése során a monitoringfunkciók a **Sense**, a hálózatirányítási és döntéstámogatási folyamatok az **Assess**, míg az automatikus átterhelések, tartalékaktiválás és incidenskezelési folyamatok az Adapt szakaszhoz rendelhetők. A **Stabilise** szakaszhoz a szolgáltatás helyreállítását és a degradált működés fenntartását, a **Learn** szakaszhoz pedig az incidensek tapasztalatainak feldolgozását és a szabályozási, szervezeti, illetve technológiai korrekciókat rendeltem.

A tapasztalatok elemzése, a hálózat fejlesztése és a szabályozás módosítása alkotja a Learn & Innovate ciklust. A BATR alkalmazása alátámasztja, hogy az energetikai reziliencia nem egyszeri esemény, hanem folyamatos tanulási és alkalmazkodási folyamat.

Részkövetkeztetés

Az **energetikai infrastruktúra elemzése megerősíti, hogy a háromdimenziós technológiai rezilienciamodell alkalmas a komplex kritikus infrastruktúrák egységes értelmezésére.** Az elemzés megerősíti, hogy a technológiai, szervezeti és szabályozási

dimenziók egymástól nem választhatók el, és a rendszerszintű reziliencia döntően azok kölcsönhatásából alakul ki A vizsgálat továbbá alátámasztja a limiting interface koncepció analitikai alkalmazhatóságát, valamint azt, hogy a BATR adaptációs ciklus alkalmas az energetikai infrastruktúra dinamikus reziliencia működésének strukturált értelmezésére.[36]

4.2.3 A közlekedési infrastruktúra technológiai rezilienciájának elemzése

A közlekedési infrastruktúrák a modern társadalmak egyik legösszetettebb kritikus rendszerei. **A vasúti, közúti, légi és vízi közlekedés, valamint az ezeket kiszolgáló digitális irányítási és logisztikai rendszerek együttesen biztosítják a személy- és áruszállítás folyamatosságát, valamint közvetlenül támogatják az energiaellátás, az egészségügy, a gazdaság és a honvédelem működését.** A közlekedési infrastruktúrák rezilienciája ezért nem kizárólag az adott ágazat működőképességét befolyásolja, hanem meghatározó szerepet játszik a teljes nemzeti kritikus infrastruktúra-rendszer stabilitásában.

A digitalizáció következtében a közlekedési rendszerek működése egyre inkább adatvezérelt, hálózatba kapcsolt környezetben valósul meg. A forgalomirányítás, a navigáció, a járműkommunikáció, az intelligens közlekedési rendszerek (ITS), valamint az

[36] A modell energetikai infrastruktúrán történő validációjának alapját a villamosenergia-rendszer képezte. A vizsgálat strukturált dokumentumelemzésre épült, amelynek adatforrásait az Európai Parlament és a Tanács kritikus szervezetek rezilienciájáról szóló (EU) 2022/2557 irányelve (CER), a hálózati és információs rendszerek biztonságáról szóló (EU) 2022/2555 irányelve (NIS2), valamint az Európai Bizottság (EU) 2024/1366 felhatalmazáson alapuló rendelete képezte. [26],[25],[67] Utóbbi kifejezetten a határokon átnyúló villamosenergia-áramlások kiberbiztonsági követelményeit, kockázatértékelését, monitoringját, incidenskezelését, üzletmenet-folytonosságát és gyakorlatrendszerét szabályozza, ezért különösen alkalmas volt a T–O–R dimenziók közötti kapcsolatok vizsgálatára. A dokumentumokat előzetesen meghatározott elemzési kategóriák szerint dolgoztam fel: a technológiai dimenzióban a hálózati redundancia, a digitális irányítási és monitoringrendszerek, az automatizált hibadetektálás és a kiberfizikai védelem; a szervezeti dimenzióban a rendszerirányítás, incidenskezelés, döntéshozatal, üzletmenet-folytonosság és válságkezelés; a szabályozási–irányítási dimenzióban pedig a kockázatkezelési, biztonsági, jelentési és együttműködési követelmények kerültek azonosításra. Az elemzés eredményeként valamennyi T–O–R dimenzió kimutatható volt, ugyanakkor a rendszer adaptív működése szempontjából meghatározó függőség a technológiai érzékelési és irányítási képességek, valamint az ezekből származó információ szervezeti értékelése és a szükséges beavatkozás között jelentkezett. Ennek alapján a T↔O kapcsolat került elsődleges limiting interface-ként azonosításra. A kockázatok érzékelése, értékelése, a válaszintézkedések végrehajtása, a működés stabilizálása, valamint a gyakorlatokból és incidensekből származó tapasztalatok visszacsatolása egyúttal megfeleltethető volt a BATR Sense–Assess–Adapt–Stabilise–Learn & Innovate ciklusának.

autonóm és részben autonóm közlekedési megoldások jelentősen növelik a működés hatékonyságát, ugyanakkor új típusú technológiai és kiberbiztonsági függőségeket is létrehoznak. [63] Ennek következtében a közlekedési reziliencia vizsgálata kiváló lehetőséget biztosít a háromdimenziós technológiai rezilienciamodell alkalmazhatóságának értékelésére.

A technológiai dimenzió értékelése

A technológiai dimenzióban a közlekedési rendszerek rezilienciáját elsősorban az infrastruktúra fizikai robusztussága, a digitális irányítási rendszerek rendelkezésre állása, a kommunikációs hálózatok megbízhatósága, a navigációs rendszerek redundanciája, valamint a kibervédelmi képességek határozzák meg.

Az intelligens közlekedési rendszerek elterjedésével a hagyományos fizikai sérülékenységek mellett egyre nagyobb jelentőséget kapnak a szoftverhibák, az adatmanipuláció, a GNSS-alapú szolgáltatások sérülékenysége, valamint a kommunikációs hálózatok kiesése. A technológiai reziliencia ezért már nem kizárólag a fizikai infrastruktúra ellenálló képességét jelenti, hanem annak digitális működési környezetét is magában foglalja.

A szervezeti dimenzió értékelése

A közlekedési rendszerek működését számos, egymással együttműködő szervezet biztosítja. Az infrastruktúra-üzemeltetők, közlekedési szolgáltatók, forgalomirányító központok, rendvédelmi szervek, katasztrófavédelmi szervezetek és szabályozó hatóságok közötti koordináció alapvetően meghatározza a rendszer alkalmazkodóképességét.

Az elemzés rámutat arra, hogy a technológiai fejlesztések csak akkor eredményeznek valódi reziliencia növekedést, ha azokhoz megfelelő szervezeti kompetenciák, közös döntési mechanizmusok, rendszeres gyakorlatok és egységes incidenskezelési eljárások kapcsolódnak. A szervezeti dimenzió ezért nem pusztán támogató szerepet tölt be, hanem a technológiai képességek gyakorlati hasznosításának alapfeltétele.

A szabályozási–irányítási dimenzió értékelése

A közlekedési infrastruktúrák működését összetett nemzetközi és nemzeti szabályozási rendszer határozza meg. Az európai uniós közlekedéspolitika, a kritikus infrastruktúra-védelmi követelmények, a NIS2 irányelv, valamint az egyes közlekedési alágazatok speciális biztonsági szabályai együttesen biztosítják a működés kereteit. [25][63][71][72]

A **szabályozási dimenzió szerepe azonban túlmutat** a megfelelőségi követelményeken. Feladata **annak biztosítása, hogy a gyors technológiai fejlődéshez alkalmazkodni képes irányítási és koordinációs mechanizmusok jöjjenek létre**, amelyek támogatják az innovációt, ugyanakkor fenntartják a rendszer biztonságát és üzembiztonságát.

Az interdimenzionális kapcsolatok értékelése

A közlekedési infrastruktúra elemzése alapján azonosítható, hogy a három dimenzió nem önállóan fejti ki hatását.

A technológiai fejlesztések eredményessége jelentős mértékben függ a szervezeti alkalmazkodóképességtől. Hasonlóképpen a szabályozási környezet rugalmassága meghatározza, hogy az új technológiák milyen sebességgel és milyen biztonsági feltételek mellett vezethetők be.

A vizsgálat során különösen erős kapcsolat figyelhető meg a szervezeti és szabályozási dimenzió között. A közlekedési rendszerekben működő számos szereplő együttműködését csak egységes governance-mechanizmus képes biztosítani.

Limiting interface

A közlekedési infrastruktúrában az elsődleges limiting interface a szervezeti és szabályozási dimenzió között jelenik meg.

A technológiai fejlesztések sok esetben gyorsabban valósulnak meg, mint a szabályozási környezet módosítása vagy a szervezeti működés átalakítása. Ennek következtében átmeneti időszakokban a rendszer alkalmazkodóképességét nem a technológia korlátozza, hanem az irányítási és koordinációs mechanizmusok fejletlensége.

Ez az eredmény ismét megerősíti a háromdimenziós modell alapfeltevését, miszerint a reziliencia meghatározó korlátja gyakran nem valamely önálló dimenzióban, hanem azok kapcsolatában jelenik meg.

A BATR-ciklus értékelése

A közlekedési rendszerek működése jól illeszkedik a BATR adaptációs ciklus logikájához.

- **Sense:** forgalomfigyelés, szenzorhálózatok, járműkommunikáció.
- **Assess:** forgalomirányítási és döntéstámogató központok.
- **Adapt:** útvonal-átterhelések, forgalomszabályozás, alternatív szállítási útvonalak.
- **Stabilise:** szolgáltatások helyreállítása és normál üzem visszaállítása.

- **Learn & Innovate:** eseményelemzés, szabályozási korrekciók és technológiai fejlesztések.

A ciklus jól mutatja, hogy a közlekedési reziliencia nem statikus állapot, hanem folyamatos adaptációs folyamat.

Részkövetkeztetés

A közlekedési infrastruktúra vizsgálata megerősíti az energetikai rendszereknél levont következtetéseket. A reziliencia nem vezethető le kizárólag a technológiai fejlettségből, hanem a technológiai, szervezeti és szabályozási dimenziók összehangolt működésének eredménye. **A limiting interface és a BATR gyakorlati alkalmazhatósága ebben az ágazatban is megerősíti a koncepcionális alkalmazhatóságot**.[37]

[37] A közlekedési infrastruktúra esetében a modell validációjának elsődleges elemzési egységét a vasúti közlekedési rendszer képezte. A választást az indokolta, hogy a vasút olyan komplex szocio-technikai rendszer, amelyben a fizikai infrastruktúra, a járművek, a digitális forgalomirányítás és kommunikáció, az infrastruktúra-üzemeltetők és vasúti társaságok szervezeti együttműködése, valamint a részletes biztonsági és interoperabilitási szabályozás szorosan összekapcsolódik. A strukturált dokumentumelemzés adatforrásait a CER és NIS2 irányelvek mellett az ENISA *Railway Cybersecurity – Good Practices in Cyber Risk Management* című 2021-es jelentése [71], az ENISA *Transport Threat Landscape* című 2023-as jelentése, valamint az Európai Unió Vasúti Ügynökségének *Report on Railway Safety and Interoperability in the EU* jelentése képezte. [72] Az ENISA vasúti kiberbiztonsági jelentése kifejezetten a vasúttársaságok és infrastruktúra-működtetők kiberkockázat-kezelési folyamatait vizsgálja, míg a Transport Threat Landscape a vasúti, közúti, légi és tengeri alágazat tényleges incidenseiből és fenyegetési mintázataiból indul ki. Az elemzés során a technológiai dimenzióban a fizikai és digitális infrastruktúra, a forgalomirányítás, kommunikáció, interoperabilitás és redundancia; a szervezeti dimenzióban az üzemeltetés, kockázatkezelés, válságkezelés és szervezetközi koordináció; a szabályozási–irányítási dimenzióban pedig a biztonsági, interoperabilitási és kiberbiztonsági követelmények kerültek kódolásra. Az elemzés eredménye azt mutatta, hogy valamennyi T–O–R dimenzió azonosítható, ugyanakkor a rendszer alkalmazkodóképességét jelentős mértékben a szervezeti reagálóképesség és az azt meghatározó szabályozási, felelősségi és eljárási keretek kapcsolata befolyásolja. Ez alapján az O↔R kapcsolat került elsődleges limiting interface-ként azonosításra. A zavar észlelésétől a helyzetértékelésen és az alternatív működési rend kialakításán keresztül a stabilizációig, majd a tapasztalatok visszacsatolásáig a BATR valamennyi funkcionális szakasza értelmezhető volt.

Az ERA 2026-os jelentése különösen jó kiegészítő forrás, mert az Ügynökség a vasúti rendszer biztonsági és interoperabilitási teljesítményét gyűjtött adatok alapján monitorozza és elemzi. [72]

4.2.4 Az elektronikus hírközlési és digitális infrastruktúrák technológiai rezilienciájának elemzése

Az elektronikus hírközlési és digitális infrastruktúrák napjainkra valamennyi kritikus infrastruktúra közös működési alapjává váltak. **A vezetékes és vezeték nélküli kommunikációs hálózatok, az internetes gerinchálózatok, az adatközpontok, a felhőalapú szolgáltatások, az 5G/6G[38] rendszerek, valamint a műholdas kommunikáció együttesen biztosítják azt a digitális környezetet, amelyre a gazdaság, a közigazgatás, a honvédelem és a társadalom működése egyaránt épül.**

A digitális infrastruktúrák sajátossága, hogy más kritikus infrastruktúrákkal szemben nem csupán önálló szolgáltatási rendszert alkotnak, hanem valamennyi más infrastruktúra működésének alapfeltételét is jelentik. Ennek következtében **sérülésük vagy kiesésük láncreakciószerű hatásokat válthat ki** az energiaellátásban, a közlekedésben, a pénzügyi szolgáltatásokban, az egészségügyben vagy akár a katonai vezetési rendszerekben.

A hazai kiberbiztonsági auditok eredményei ebben az összefüggésben a technológiai reziliencia értékelés fontos, bizonyítékalapú bemeneti információforrását jelenthetik. A háromdimenziós modell alkalmazásának hozzáadott értéke azonban éppen abban áll, hogy az audit során feltárt technológiai és kiberbiztonsági állapotot nem önmagában, hanem a szervezeti és szabályozási–irányítási képességekkel, valamint az ezek között fennálló függőségekkel együtt értékeli. A TRI–TRMM ilyen irányú alkalmazhatóságát részletesebben a 4.4.5 alfejezet tárgyalja

A technológiai dimenzió

A technológiai dimenzióban a rezilienciát elsősorban a hálózati redundancia, a földrajzi diverzitás, az adatközpontok rendelkezésre állása, a hálózati szegmentáció, a titkosítási megoldások, a kiberbiztonsági architektúrák, valamint az automatizált monitorozó és incidensészlelő rendszerek határozzák meg.

A digitalizáció gyors fejlődése következtében ugyanakkor folyamatosan növekszik a rendszer komplexitása. Az egyre több felhőszolgáltatás, API-kapcsolat, IoT-eszköz, mesterséges intelligenciát alkalmazó szolgáltatás és külső szolgáltató megjelenése új függőségeket hoz létre. [64] Ez a technológiai rezilienciát egyre inkább ökoszisztéma-szintű kérdéssé teszi.

[38] 6G: Sixth Generation Mobile Network: hatodik generációs mobilhálózat.

A szervezeti dimenzió

Az elektronikus hírközlési infrastruktúrák működésében **kiemelt jelentősége van a biztonsági műveleti központoknak** (SOC), a CERT/CSIRT [39] szervezeteknek, az incidenskezelési folyamatoknak, valamint a szolgáltatók és állami szervezetek közötti információmegosztásnak.

A vizsgálat rámutat arra, hogy a technológiai fejlettség önmagában nem garantálja a magas rezilienciát. A gyors incidensészlelés, a döntéshozatal, a szervezeti tanulás és az együttműködés minősége alapvetően meghatározza a rendszer alkalmazkodóképességét.

A szabályozási–irányítási dimenzió

A digitális infrastruktúrák működését egyre nagyobb mértékben határozzák meg az európai uniós szabályozások, különösen a NIS2 irányelv, a Cyber Resilience Act, a DORA[40], valamint a kritikus infrastruktúrákra vonatkozó reziliencia-követelmények. [26],[25],[27],[66]

A háromdimenziós modell alkalmazása során ugyanakkor megállapítható, hogy a **governance szerepe nem merül ki a megfelelőség biztosításában**. Az irányítás feladata az is, hogy koordinálja a technológiai innováció, a biztonsági követelmények és a működési folyamatok összehangolását.

Interdimenzionális kapcsolatok és limiting interface

Az elemzés alapján a **legkritikusabb kapcsolat a technológiai és szabályozási dimenzió között jelenik** meg. A technológiai fejlődés sebessége gyakran meghaladja a szabályozási környezet alkalmazkodóképességét, ami átmeneti biztonsági és irányítási hiányosságokat eredményezhet.

Emellett jelentős szerepet játszik a technológiai és szervezeti dimenzió közötti kapcsolat is, különösen az **incidenskezelés, a threat hunting, a digitális forenzika** és a helyreállítási folyamatok során.

[39] CSIRT: Computer Security Incident Response Team: számítógép-biztonsági incidenskezelő csoport.

[40] DORA: Digital Operational Resilience Act: digitális működési rezilienciáról szóló uniós rendelet.

Részkövetkeztetés

Az elektronikus hírközlési infrastruktúrák elemzése megerősíti, hogy **a háromdimenziós technológiai rezilienciamodell nem csupán fizikai infrastruktúrákra, hanem nagymértékben virtualizált, adatvezérelt rendszerekre is alkalmazható**. A limiting interface koncepció ebben a környezetben különösen hangsúlyosan jelenik meg, mivel a technológiai innováció sebessége és a szervezeti, illetve szabályozási alkalmazkodás között gyakran jelentős eltérés figyelhető meg.[41]

4.2.5 A katonai vezetési és irányítási rendszerek technológiai rezilienciájának elemzése

A katonai vezetési és irányítási rendszerek (Command and Control – C2) a honvédelem egyik legkritikusabb technológiai képességterületét jelentik. Sajátosságuk, hogy működésük során egyszerre támaszkodnak informatikai rendszerekre, kommunikációs infrastruktúrákra, hírszerzési és felderítési képességekre, valamint a döntéshozatali lánc valamennyi szervezeti elemére. Ennek következtében a technológiai reziliencia vizsgálata ebben a környezetben különösen összetett feladat.

[41] Az elektronikus hírközlési infrastruktúra validációjának elemzési egységét a magyar elektronikus hírközlési rendszer szolgáltatási, technológiai és szabályozási környezete képezte. A strukturált dokumentumelemzés elsődleges forrásai a NIS2 és CER irányelvek, az ENISA NIS2-ágazatok kiberbiztonsági érettségét vizsgáló NIS360 jelentése [65], valamint magyar ágazati forrásként a Nemzeti Média- és Hírközlési Hatóság *Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2025 – üzleti felmérés* című kutatása voltak. [73] Az NMHH-vizsgálat nem kizárólag összefoglaló jelentést, hanem a 2025-ös kutatás eredménytábláit, kérdőívét és SPSS-formátumú adatbázisát is hozzáférhetővé teszi, ezért a magyar elektronikus hírközlési környezet vizsgálatához empirikus adatforrásként is felhasználható. [73] A dokumentumok elemzése során a technológiai dimenzióban a hálózati infrastruktúra, redundancia, digitális szolgáltatások, monitoring és incidensészlelés; a szervezeti dimenzióban a szolgáltatói működés, incidenskezelés, üzletmenet-folytonosság és információmegosztás; a szabályozási–irányítási dimenzióban pedig a kiberbiztonsági, szolgáltatásfolytonossági és incidensjelentési követelmények kerültek vizsgálatra. Az elemzés valamennyi T–O–R dimenzió jelenlétét kimutatta, ugyanakkor különösen erős kölcsönhatás volt azonosítható a technológiai és szabályozási dimenzió között: a szabályozási követelmények közvetlenül alakítják a technológiai biztonsági architektúrát, miközben a technológiai fejlődés és az új digitális függőségek új szabályozási és governance-igényeket hoznak létre. Ennek alapján a T↔R kapcsolat került elsődleges limiting interface-ként azonosításra. Az incidensészlelés, értékelés, alkalmazkodás, szolgáltatás-stabilizáció és a tapasztalatok visszacsatolása egyúttal megfeleltethető volt a BATR ciklus funkcionális szakaszainak.

Az NMHH-felmérés piaci/felhasználói adatokat tartalmaz, ezért önmagában nem bizonyítja a T↔R limiting interface-t. Ehhez a NIS2 és az ENISA szabályozási/kiberbiztonsági dokumentumokkal együtt kell használni. Az NMHH-forrás a magyar kontextust és az empirikus hátteret erősíti.

A technológiai dimenzió

A katonai C2 rendszerek technológiai rezilienciáját meghatározza a kommunikációs hálózatok rendelkezésre állása, a többcsatornás adatkapcsolatok, a műholdas és rádiókommunikáció redundanciája, az elektronikai hadviseléssel szembeni ellenálló képesség, a kiberbiztonsági architektúrák, valamint a döntéstámogató rendszerek működése.

A modern hadviselésben a technológiai reziliencia már nem kizárólag a rendszer túlélőképességét jelenti, hanem azt is, hogy a vezetési rendszer képes-e folyamatosan fenntartani a döntési fölényt a gyorsan változó műveleti környezetben. [38]

A szervezeti dimenzió

A katonai rendszerek esetében a **szervezeti dimenzió különösen hangsúlyos szerepet** kap. A **döntéshozatal sebessége, a parancsnoki lánc rugalmassága, a személyi állomány felkészültsége, a kiképzés, valamint az interoperabilitás egyaránt meghatározza** a technológiai képességek tényleges alkalmazhatóságát.

A vizsgálat arra mutat rá, hogy a fejlett vezetési rendszerek önmagukban nem biztosítanak rezilienciát, amennyiben a szervezet nem képes az információ gyors értelmezésére és adaptív döntések meghozatalára.

A szabályozási–irányítási dimenzió

A katonai környezetben a **szabályozási dimenzió elsősorban a NATO-doktrínák, a nemzeti katonai szabályozás, a műveleti eljárások, az interoperabilitási követelmények** és a stratégiai irányítás összhangját foglalja magában. [74][75]

A governance ebben az esetben nem csupán adminisztratív funkció, hanem közvetlenül meghatározza a vezetési rendszer működési rugalmasságát és alkalmazkodóképességét.

Interdimenzionális kapcsolatok és limiting interface

A katonai vezetési rendszerek elemzése során **a legerősebb kapcsolat a technológiai és a szervezeti dimenzió között** figyelhető meg. A technológiai fölény csak akkor eredményez műveleti előnyt, ha azt megfelelő szervezeti döntéshozatal és adaptív vezetési kultúra támogatja.

A limiting interface ebben a környezetben elsősorban az információból döntéssé történő átalakulás folyamatában jelenik meg. **A technológiai képességek és a vezetési folyamatok közötti kapcsolat határozza meg a rendszer tényleges rezilienciáját.**

Részkövetkeztetés

A **katonai vezetési rendszerek vizsgálata megerősíti a háromdimenziós technológiai rezilienciamodell általános alkalmazhatóságát**. A technológiai, szervezeti és szabályozási dimenziók szoros kölcsönhatása, valamint a kapcsolati szűk keresztmetszetek meghatározó szerepe ebben a környezetben is egyértelműen kimutatható. A vizsgálat ugyanakkor **rámutat arra is**, hogy a technológiai reziliencia közvetlen kapcsolatban áll **a műveleti döntési képesség fenntartásával**, amely stratégiai jelentőséget ad a modell alkalmazásának.[42]

4.2.6 A háromdimenziós technológiai rezilienciamodell összehasonlító validálása

A különböző kritikus infrastruktúrák elemzése lehetővé tette annak vizsgálatát, hogy a háromdimenziós technológiai rezilienciamodell mennyiben tekinthető általánosan alkalmazható elemzési keretnek. Az energetikai, közlekedési, elektronikus hírközlési és katonai vezetési rendszerek eltérő technológiai környezetet, szervezeti felépítést és szabályozási struktúrát képviselnek, ugyanakkor az elemzések eredményei figyelemre méltó hasonlóságokat mutattak.

A vizsgálatok első fontos eredménye, hogy valamennyi elemzett infrastruktúra esetében azonosítható volt a technológiai (T), szervezeti (O) és szabályozási–irányítási

[42] A katonai vezetési és irányítási képesség validációja – tekintettel a konkrét nemzeti C2-rendszerek részben minősített jellegére – funkcionális és doktrinális szinten történt. Az elemzési egységet a NATO szárazföldi műveleteinek vezetési és irányítási rendszere képezte. A dokumentumelemzés elsődleges forrása az *AJP-3.2 Allied Joint Doctrine for Land Operations* [74], valamint az abban meghatározott doktrinális rendszer részeként az *ATP-3.2.2 Command and Control of Allied Land Forces* volt. [75] Az AJP-3.2 az ATP-3.2.2-t kifejezetten a szárazföldi erők vezetésére és irányítására vonatkozó alapdokumentumként határozza meg, amely a döntéshozatal és tervezés eljárásait tartalmazza. [74],[75] Az elemzés során a technológiai dimenzióban a kommunikációs és információs rendszerek rendelkezésre állása, redundanciája, interoperabilitása és a szenzor–C2 kapcsolatok; a szervezeti dimenzióban a parancsnoki struktúra, döntéshozatal, törzsmunka, decentralizált végrehajtás és személyi felkészültség; a szabályozási–irányítási dimenzióban pedig a doktrinális, interoperabilitási és biztonsági követelmények kerültek értékelésre. A három dimenzió valamennyi vizsgált eleme azonosítható volt, ugyanakkor kritikus függőség az információ technológiai előállítása és továbbítása, valamint annak parancsnoki értelmezése és döntéssé alakítása között jelentkezett. Ennek alapján a T↔O kapcsolat – ezen belül az információból döntéssé történő átmenet – került elsődleges limiting interface-ként azonosításra. A helyzetérzékelés, helyzetértékelés, döntés és adaptáció, a működés stabilizálása, majd a műveleti tapasztalatok doktrinális és kiképzési visszacsatolása egyúttal megfeleltethető volt a BATR ciklus funkcionális logikájának.

(R) dimenzió egyidejű jelenléte. Egyetlen vizsgált rendszer sem volt értelmezhető kizárólag technológiai vagy kizárólag szervezeti megközelítés alapján. A rezilienciát minden esetben a három dimenzió együttes működése határozta meg.

A **második közös megállapítás** az interdimenzionális kapcsolatok meghatározó szerepe volt. Bár az egyes ágazatokban eltérő kapcsolatok bizonyultak elsődlegesnek, valamennyi infrastruktúrában kimutatható volt, hogy a rendszerszintű rezilienciát nem önmagában valamely dimenzió fejlettsége, hanem a dimenziók közötti együttműködés minősége határozza meg.

Harmadik fontos eredményként valamennyi vizsgált infrastruktúrában azonosítható volt legalább egy olyan **kapcsolati szűk keresztmetszet (limiting interface)**, amely jelentősebb hatást gyakorolt a rendszer alkalmazkodóképességére, mint az egyes technológiai komponensek fejlettsége. Ez alátámasztja a 3. fejezetben bevezetett limiting interface koncepció gyakorlati relevanciáját.

A **negyedik közös tapasztalat a BATR adaptációs ciklus alkalmazhatóságának** igazolása volt. Az eltérő működési logikájú infrastruktúrák ellenére valamennyi rendszerben azonosíthatók voltak az érzékelés, értékelés, alkalmazkodás, stabilizáció és szervezeti tanulás egymást követő folyamatai. A BATR ezért nem egy adott ágazatra kidolgozott modellként, hanem a technológiai reziliencia általános működési mechanizmusaként értelmezhető. A vizsgálatok eredményeit a 4.1. táblázat foglalja össze.

Vizsgált infrastruktúra	Domináns technológiai tényezők	Meghatározó szervezeti tényezők	Meghatározó governance tényezők	Elsődleges limiting interface
Energetika	SCADA, intelligens hálózatok, redundancia	incidenskezelés, üzemeltetés	energiairányítás, NIS2	T ↔ O
Közlekedés	ITS, digitális irányítás, GNSS	koordináció, üzemeltetés	közlekedési governance	O ↔ R
Elektronikus hírközlés	adatközpontok, felhő, hálózatok	SOC, CERT[43], threat hunting	NIS2, CRA[44]	T ↔ R
Katonai C2	C4ISR[45], kommunikáció, EW	vezetés, kiképzés	NATO doktrínák	T ↔ O

4.1. táblázat A háromdimenziós technológiai reziliencia modell kvalitatív összehasonlító értékelése (saját szerkesztés)

[43] CERT: Computer Emergency Response Team: számítógép-biztonsági incidenskezelő csoport.

[44] CRA: Cyber Resilience Act: kiberrezilienciáról szóló uniós rendelet.

[45] C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance: vezetés, irányítás, kommunikáció, számítástechnika, hírszerzés, megfigyelés és felderítés.

A táblázat alapján megállapítható, hogy bár az egyes infrastruktúrák technológiai sajátosságai jelentősen eltérnek, a reziliencia szerkezete minden esetben azonos logikát követ. Ez arra utal, hogy a háromdimenziós modell nem ágazatspecifikus megoldás, hanem olyan általános elemzési keret, amely különböző kritikus infrastruktúrák esetében is alkalmazható.

A háromdimenziós modell validálásának eredményei

A háromdimenziós modell összehasonlító alkalmazásának eredményei:

A vizsgált kritikus infrastruktúrák összehasonlító elemzése alapján a háromdimenziós technológiai reziliencia modell alkalmazhatósága négy egymással összefüggő szempont mentén nyert alátámasztást.

Elsőként a modell strukturális konzisztenciája jelent meg valamennyi vizsgált infrastruktúrában. Az energetikai, közlekedési, elektronikus hírközlési és katonai vezetési rendszerek esetében egyaránt azonosítható volt a technológiai, szervezeti és szabályozási–irányítási dimenzió egyidejű jelenléte. Ez arra utal, hogy a T–O–R struktúra eltérő technológiai környezetek elemzésében is következetesen alkalmazható.

Másodikként valamennyi vizsgált rendszerben meghatározó szerepet játszottak az interdimenzionális kapcsolatok. Az elemzések azt mutatták, hogy a reziliencia nem vezethető vissza kizárólag az egyes dimenziók önálló fejlettségére, hanem jelentős mértékben azok összehangolt működésétől függ.

Harmadikként valamennyi vizsgált infrastruktúra esetében azonosítható volt legalább egy olyan kapcsolati szűk keresztmetszet, amely megfelelt a 3. fejezetben meghatározott limiting interface koncepciónak. A szűk keresztmetszetek helye és jellege ágazatonként eltért, ugyanakkor minden esetben a dimenziók közötti kapcsolat működésében jelent meg.

Negyedikként a BATR adaptációs ciklus egyes funkcionális szakaszai – Sense, Assess, Adapt, Stabilise, valamint Learn & Innovate – valamennyi vizsgált infrastruktúrában értelmezhetők voltak. Ez alátámasztja a BATR alkalmazhatóságát a technológiai reziliencia dinamikus, időbeli működésének elemzésére.

Az összehasonlító vizsgálat eredményei összességében azt támasztják alá, hogy a háromdimenziós technológiai rezilienciamodell egységes kvalitatív elemzési keretként

alkalmazható eltérő kritikus infrastruktúrák esetében, miközben lehetőséget biztosít azok ágazatspecifikus sajátosságainak megjelenítésére is.

A validáció stratégiai következményei

A komparatív elemzés ugyanakkor egy további, a kutatás szempontjából kiemelt jelentőségű összefüggésre is rámutatott. **A vizsgált infrastruktúrák nem önálló rendszerekként működnek, hanem egymással szoros kölcsönhatásban álló nemzeti technológiai ökoszisztéma részei.** Az elektronikus hírközlés biztosítja az energiaellátás digitális működését, az energiaellátás alapfeltétele a közlekedési és kommunikációs rendszerek működésének, míg a katonai vezetési rendszerek valamennyi infrastruktúrától függenek.

Ennek következtében egyetlen infrastruktúra rezilienciája sem fejleszthető tartósan a többi infrastruktúrától függetlenül. A technológiai reziliencia valójában **rendszerek rendszere (system of systems)** jellegű képesség, amelynek meghatározó elemei különböző szervezetek, ágazatok és szabályozási környezetek között oszlanak meg.

A négy vizsgált rendszer összehasonlítása hadtudományi szempontból arra is rámutat, hogy a katonai műveleti képesség rezilienciája nem határolható le a fegyveres erők saját technológiai rendszereire. Az energiaellátás, a közlekedés, az elektronikus hírközlés és a digitális szolgáltatások olyan külső képességfüggőségeket alkotnak, amelyek kiesése közvetlenül korlátozhatja a vezetést és irányítást, az erők mozgatását, az utánpótlást, a helyzetismeretet és a műveleti tempót. **Ebből következően a kritikus infrastruktúrák technológiai rezilienciája a katonai műveleti képesség külső feltételrendszerének részeként értelmezhető.**

A kutatás ezen felismerése túlmutat a háromdimenziós modell validálásán. **Ha a reziliencia meghatározó tényezői különböző kritikus infrastruktúrákban azonos logika szerint működnek, akkor indokolttá válik egy olyan integrált irányítási megközelítés kialakítása,** amely nem egyes infrastruktúrákat, hanem a teljes nemzeti technológiai ökoszisztémát kezeli elemzési és fejlesztési egységként.

Ez a felismerés képezi a következő alfejezet alapját, amelyben a technológiai reziliencia stratégiai újraértelmezése történik meg. Az összehasonlító elemzések eredményeire építve bemutatásra kerül, hogy a technológiai reziliencia nem csupán infrastruktúra- vagy szervezetspecifikus jellemző, hanem **önálló nemzeti stratégiai képesség**, amely integrált irányítási megközelítést igényel. Ebből a tudományos következtetésből vezethető le a **Nemzeti Technológiai Reziliencia Irányítási**

Keretrendszer (National Technological Resilience Governance Framework – NTRGF) kialakításának szükségessége.

4.3 A technológiai reziliencia stratégiai újraértelmezése

4.3.1 A technológiai reziliencia mint nemzeti stratégiai képesség

A kritikus infrastruktúrák összehasonlító elemzése alapján megállapítható, hogy a technológiai reziliencia nem értelmezhető kizárólag egy-egy infrastruktúra vagy szervezet tulajdonságaként. Bár az energetikai, közlekedési, elektronikus hírközlési és katonai vezetési rendszerek eltérő funkciókat látnak el, működésük során azonos strukturális törvényszerűségek figyelhetők meg. A rezilienciát valamennyi esetben a technológiai, szervezeti és szabályozási–irányítási dimenziók együttes működése, valamint az azok közötti kapcsolatok minősége határozza meg.

A kutatás egyik legfontosabb megállapítása, hogy a kritikus infrastruktúrák rezilienciája nem független egymástól. **Az egyes infrastruktúrák működését egyre inkább kölcsönös technológiai függőségek jellemzik.** Az energetikai infrastruktúrák működése digitális kommunikációs rendszerektől függ, a kommunikációs infrastruktúrák energiaellátás nélkül működésképtelenné válnak, míg a közlekedési rendszerek mindkét infrastruktúra folyamatos rendelkezésre állását igénylik. Hasonló kölcsönös függőség figyelhető meg az egészségügyi ellátórendszerek, a pénzügyi szolgáltatások, az államigazgatás és a honvédelmi rendszerek esetében is. [30], [31], [61]

Ez a jelenség alapvetően megváltoztatja a technológiai reziliencia értelmezését. **Míg korábban a reziliencia elsősorban egy-egy szervezet vagy infrastruktúra belső képességeként jelent meg, napjainkban egyre inkább egy összetett technológiai ökoszisztéma tulajdonságává válik.** A rendszerek közötti kapcsolatok számának növekedésével párhuzamosan a rezilienciát meghatározó tényezők is egyre inkább a rendszerek közötti együttműködésben, adatcserében és közös döntési mechanizmusokban jelennek meg.

Ennek következtében a technológiai reziliencia többé nem tekinthető kizárólag műszaki vagy ágazati kérdésnek. A reziliens működés kialakítása és fenntartása olyan stratégiai koordinációt igényel, amely egyszerre képes figyelembe venni a technológiai innovációt, a szervezeti alkalmazkodást, a szabályozási környezetet és a kritikus infrastruktúrák közötti kölcsönös függőségeket.

A kutatás eredményei alapján ezért megállapítható, hogy a technológiai reziliencia **önálló nemzeti stratégiai képességként** értelmezhető. E stratégiai képesség nem egyetlen szervezethez vagy ágazathoz kapcsolódik, hanem a teljes állami, gazdasági és társadalmi technológiai ökoszisztéma működéséből alakul ki. A reziliencia fejlesztése ezért nem valósítható meg kizárólag ágazati fejlesztési programok vagy önálló technológiai beruházások útján, hanem integrált, kormányzati szintű irányítási megközelítést igényel.

Ez az **értelmezés összhangban áll a NATO által megfogalmazott nemzeti reziliencia követelményekkel,** amelyek szerint a tagállamok ellenálló képessége a kritikus nemzeti funkciók folyamatos biztosítására épül, valamint az Európai Unió kritikus infrastruktúrákra és kiberbiztonságra vonatkozó szabályozási törekvéseivel, amelyek egyre inkább a rendszerszintű rezilienciát helyezik előtérbe. [26],[25],[23],[36],[60] Ugyanakkor a jelen kutatás túlmutat ezen megközelítéseken, mivel a technológiai rezilienciát nem csupán szakpolitikai célkitűzésként, hanem önálló tudományos elemzési és irányítási kategóriaként értelmezi.

A technológiai reziliencia nemzeti stratégiai képességként történő újraértelmezése egyben új irányítási szemléletet is szükségessé tesz. A következő alfejezet ezért azt vizsgálja, hogy a hagyományos, ágazati irányítási modellek milyen korlátokkal rendelkeznek, és miért indokolt egy integrált, rendszerszintű technológiai reziliencia-governance kialakítása.

4.3.2 Az ágazati reziliencia governance korlátai és az integrált irányítás szükségessége

A kritikus infrastruktúrák elemzésének egyik legfontosabb tanulsága, hogy a technológiai rezilienciát meghatározó tényezők nem illeszthetők egyetlen szervezeti vagy ágazati felelősségi körbe. A technológiai rendszerek fejlődése, a digitalizáció felgyorsulása, a hálózatos működés és a kibertér jelentőségének növekedése következtében a kritikus infrastruktúrák közötti kölcsönös függőségek jelentősen erősödtek. Ennek eredményeként a reziliencia egyre kevésbé értelmezhető önálló ágazati képességként, sokkal inkább egy összetett, több szereplő által létrehozott rendszerszintű tulajdonságként jelenik meg.

A hagyományos államigazgatási struktúrák ugyanakkor továbbra is döntően ágazati logika szerint működnek. Az energiaügy, a közlekedés, a digitális infrastruktúrák, az egészségügy, a honvédelem vagy a belbiztonság fejlesztési és szabályozási rendszerei külön intézményi keretek között működnek, eltérő stratégiai dokumentumok, finanszírozási mechanizmusok és irányítási struktúrák alapján. Bár az egyes ágazatok között számos

koordinációs mechanizmus létezik, ezek elsődlegesen együttműködési fórumokat jelentenek, és nem biztosítanak egységes reziliencia irányítást.

A kutatás során elvégzett összehasonlító elemzés rámutatott arra, hogy a rezilienciát meghatározó kritikus sérülékenységek jelentős része éppen ezeknél az ágazatok közötti kapcsolódási pontoknál jelenik meg. A technológiai függőségek, az adatmegosztás, a közös kommunikációs infrastruktúrák, a beszállítói láncok vagy a közös digitális platformok olyan kapcsolati elemeket alkotnak, amelyekért egyetlen ágazati szereplő sem visel teljes körű felelősséget. Ennek következtében a rezilienciát korlátozó tényezők gyakran kívül esnek az egyes szervezetek közvetlen beavatkozási lehetőségein.

Ez a jelenség összhangban áll a 3. fejezetben bevezetett **limiting interface** fogalmával. Az összehasonlító elemzés eredményei arra mutattak rá, hogy a vizsgált infrastruktúrákban a rezilienciát korlátozó tényezők több esetben nem valamely technológiai komponens önálló hiányosságaként, hanem a technológiai, szervezeti és szabályozási–irányítási dimenziók kapcsolódási pontjain jelentek meg. Másként fogalmazva: **a reziliencia kritikus szűk keresztmetszete nem feltétlenül egy rendszeren belül, hanem a rendszerek és dimenziók közötti interfészeken alakul ki.**

Ez a felismerés alapvető következményekkel jár a stratégiai irányítás számára. Amennyiben a reziliencia meghatározó tényezői ágazatokon átívelő kapcsolatokban jelennek meg, akkor azok fejlesztése sem valósítható meg kizárólag ágazati szemléletben. A jelenlegi irányítási modellek ugyanis jellemzően saját szakterületük optimalizálására törekednek, miközben kevés figyelmet fordítanak a rendszerek közötti kölcsönhatásokra. Ez a megközelítés rövid távon növelheti egy-egy infrastruktúra teljesítményét, ugyanakkor nem feltétlenül javítja a teljes nemzeti technológiai ökoszisztéma ellenálló képességét.

A kutatás eredményei alapján ezért megállapítható, hogy a technológiai reziliencia **fejlesztése új irányítási logikát** igényel. Ennek középpontjában nem az egyes infrastruktúrák elkülönített fejlesztése, hanem azok kölcsönös függőségeinek kezelése áll. A stratégiai irányítás feladata ebben az értelmezésben nem pusztán a szabályozási megfelelőség biztosítása, hanem a technológiai, szervezeti és szabályozási dimenziók összehangolt fejlesztése, valamint a közöttük kialakuló kapcsolatok folyamatos monitorozása és fejlesztése.

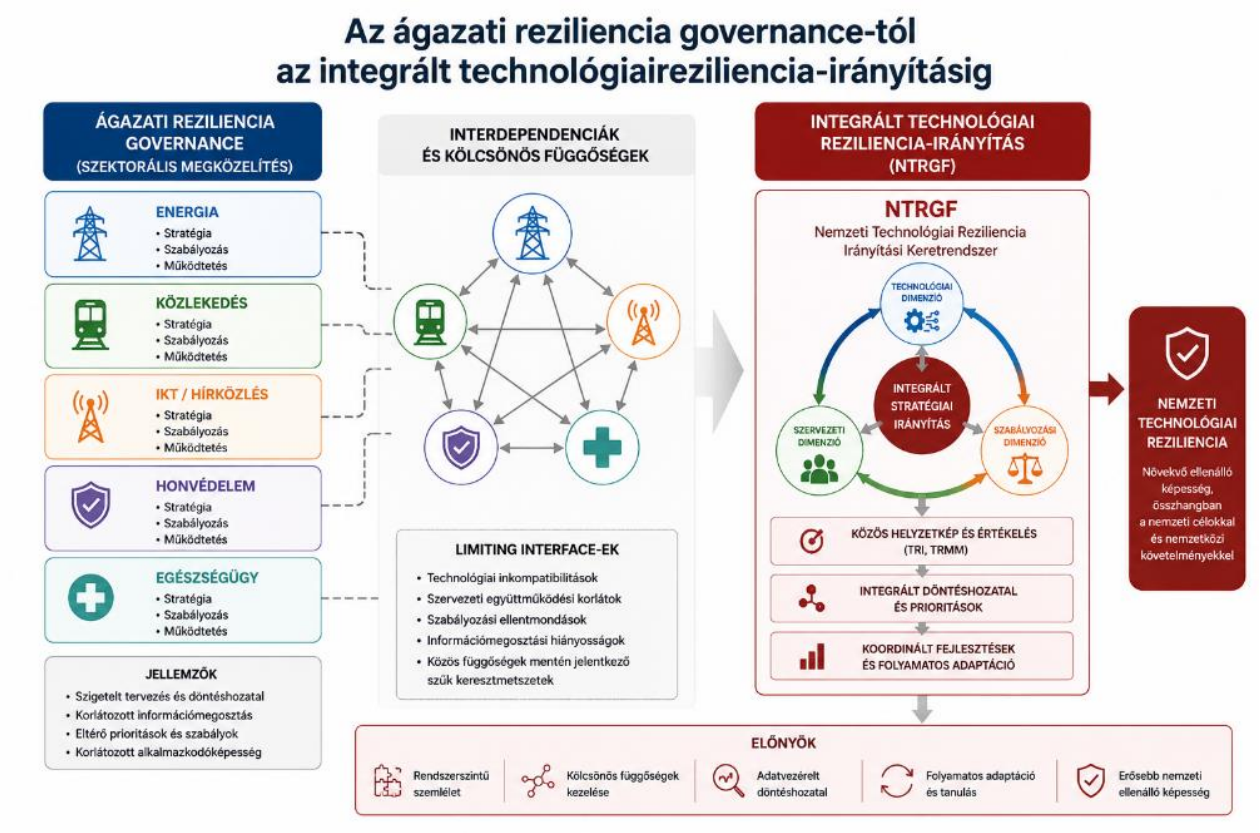
Ez a megközelítés egyben új szerepet is kijelöl a governance számára. A governance nem egyszerűen koordinációs vagy adminisztratív funkcióként jelenik meg, hanem a technológiai reziliencia önálló képességterületeként. Feladata a különböző ágazatok stratégiai céljainak összehangolása, a közös kockázatok értékelése, a fejlesztési prioritások

meghatározása, valamint a reziliencia folyamatos mérésének és visszacsatolásának biztosítása.

A nemzetközi környezetben egyre több kezdeményezés jelenik meg ebbe az irányba. A **NATO Baseline Requirements for National Resilience** rendszere, az **Európai Unió CER irányelve**, a **NIS2 irányelv**, a **Critical Infrastructure Protection** megközelítések vagy a stratégiai autonómiával kapcsolatos uniós törekvések egyaránt azt jelzik, hogy a reziliencia fokozatosan kilép az egyes ágazatok keretei közül. [26][25][36][60] Ezek a kezdeményezések azonban elsősorban szabályozási vagy szakpolitikai koordinációt biztosítanak, és nem kínálnak egységes, tudományosan megalapozott technológiai reziliencia-irányítási modellt.

A jelen kutatás ebből a szempontból új megközelítést képvisel. A háromdimenziós technológiai rezilienciamodell, a BATR adaptációs ciklus, a TRI és a TRMM együttes alkalmazása lehetővé teszi, hogy a technológiai reziliencia ne csupán mérhető legyen, hanem stratégiai szinten is irányíthatóvá váljon. Ez teremti meg annak lehetőségét, hogy a technológiai reziliencia önálló államirányítási képességként jelenjen meg.

A vizsgált ágazati irányítási logikák összehasonlítása alapján megállapítható, hogy az önálló ágazati governance-mechanizmusok nem kezelik teljeskörűen a technológiai rezilienciát meghatározó ágazatközi függőségeket és kapcsolati szűk keresztmetszeteket. Ez indokolja olyan integrált irányítási keret kialakítását, amely közös elemzési és döntéstámogatási logikába rendezi az ágazati reziliencia feladatokat anélkül, hogy átvenné az egyes szereplők meglévő szakpolitikai vagy intézményi felelősségét.



4.2. ábra: Az ágazati reziliencia governance-tól az integrált technológiai reziliencia-irányításig (saját szerkesztés)

A kutatás eredményei alapján ennek megvalósítására dolgoztam ki a Nemzeti Technológiai Reziliencia Irányítási Keretrendszert (National Technological Resilience Governance Framework – NTRGF), amely a következő alfejezetben kerül részletes bemutatásra.

4.4 Nemzeti Technológiai Reziliencia Irányítási Keretrendszer (National Technological Resilience Governance Framework – NTRGF)

4.4.1 Az NTRGF fogalma és célja

A 3. fejezetben kidolgozott háromdimenziós technológiai rezilienciamodell, valamint a jelen fejezetben elvégzett összehasonlító elemzés eredményei arra mutatnak, hogy a technológiai reziliencia nem kizárólag az egyes kritikus infrastruktúrák vagy szervezetek belső tulajdonságaként értelmezhető. A vizsgált rendszerek közötti kölcsönös függőségek, valamint a technológiai, szervezeti és szabályozási–irányítási kapcsolatok alapján indokolt a technológiai reziliencia magasabb absztrakciós szinten, nemzeti stratégiai képességként történő értelmezése.

A kutatás során végzett elemzések ugyanakkor arra is rámutattak, **hogy a jelenlegi ágazati irányítási modellek elsősorban saját szakterületük optimalizálására törekednek.** Az energetikai, közlekedési, elektronikus hírközlési, egészségügyi vagy honvédelmi fejlesztések önálló szakpolitikai logika szerint valósulnak meg, miközben a technológiai rezilienciát meghatározó kapcsolatok jelentős része ezek között az ágazatok között jön létre.

Ennek következtében a technológiai reziliencia fejlesztése nem valósítható meg kizárólag ágazati programok összehangolásával. **Olyan integrált irányítási megközelítésre van szükség, amely képes egységes rendszerben kezelni a technológiai, szervezeti és szabályozási dimenziók kölcsönhatásait**, biztosítani azok folyamatos értékelését, valamint támogatni a stratégiai döntéshozatalt.

A kutatás eredményeként ennek megvalósítására került kidolgozásra a **Nemzeti Technológiai Reziliencia Irányítási Keretrendszer (National Technological Resilience Governance Framework – NTRGF).**

Az **NTRGF** olyan integrált, többszintű stratégiai irányítási keretrendszer, amely a háromdimenziós technológiai rezilienciamodellre, a Balogh-féle Adaptív Technológiai Reziliencia Ciklusra (BATR), a Technological Resilience Indexre (TRI) és a Technological Resilience Maturity Modelre (TRMM) építve biztosítja a technológiai reziliencia nemzeti szintű tervezését, koordinációját, mérését, fejlesztését és folyamatos visszacsatolását.

Az **NTRGF alapvető célja nem új intézményrendszer létrehozása**. A keretrendszer nem kívánja kiváltani a jelenlegi nemzeti vagy európai szabályozási rendszereket, illetve nem helyettesíti az ágazati felelősségi struktúrákat sem. Feladata ezzel szemben egy olyan közös stratégiai irányítási logika biztosítása, amely lehetővé teszi a különböző ágazatok technológiai rezilienciájának összehangolt fejlesztését.

Ennek megfelelően az NTRGF három alapelvre épül.

Az első alapelv a rendszerszemlélet.

A technológiai rezilienciát nem önálló infrastruktúrák összességeként, hanem egymással kölcsönösen összekapcsolt technológiai ökoszisztémaként értelmezi. A fejlesztési döntések során ezért nem kizárólag az egyes rendszerek saját teljesítménye, hanem azok más infrastruktúrákra gyakorolt hatása is értékelésre kerül.

A második alapelv az adaptív irányítás.

A technológiai környezet folyamatos változása miatt a **reziliencia nem tekinthető statikus állapotnak.** Az NTRGF a BATR-ciklus logikájára építve biztosítja a folyamatos monitorozást, az értékelést, a beavatkozást, a stabilizációt és a szervezeti tanulást.

A harmadik alapelv az evidenciaalapú döntéshozatal.

Az irányítási döntések alapját **nem kizárólag szakpolitikai megfontolások vagy szakértői becslések jelentik**, hanem a TRI és a TRMM segítségével előállított strukturált és összehasonlítható reziliencia értékelések. Ez lehetővé teszi a fejlesztési prioritások összehasonlítható, átlátható és visszamérhető meghatározását.

A keretrendszer alkalmazásával a technológiai reziliencia fejlesztése folyamatos stratégiai ciklussá válik, amelyben az értékelés, a fejlesztés és az újraértékelés egymást követő, ismétlődő folyamatot alkot. Ennek eredményeként a reziliencia nem egyszeri projektként, hanem hosszú távú nemzeti képességként jelenik meg.

Az **NTRGF működési logikája jelentősen eltér a hagyományos reziliencia programoktól**. Míg azok jellemzően egy-egy ágazat vagy szervezet fejlesztésére koncentrálnak, az NTRGF elsődleges elemzési egysége a **kapcsolatrendszer**. A keretrendszer abból indul ki, hogy a technológiai rezilienciát legnagyobb mértékben nem az egyes rendszerek önálló fejlettsége, hanem a közöttük kialakuló technológiai, szervezeti és szabályozási kapcsolatok minősége határozza meg.

Ez a szemlélet közvetlenül kapcsolódik a kutatás során kidolgozott **limiting interface** koncepcióhoz. Az NTRGF egyik legfontosabb feladata e kapcsolati szűk keresztmetszetek azonosítása, folyamatos monitorozása és célzott fejlesztése. Ennek eredményeként a stratégiai fejlesztések nem kizárólag technológiai beruházásokra irányulnak, hanem azokra a kapcsolati pontokra koncentrálnak, amelyek a teljes nemzeti technológiai ökoszisztéma alkalmazkodóképességét meghatározzák.

A kutatás álláspontja szerint ez jelenti a technológiai reziliencia stratégiai irányításának alapvető szemléletváltását. A hangsúly a rendszerek fejlesztéséről a **rendszerek közötti kapcsolatok fejlesztésére** helyeződik át. Ez biztosítja, hogy a technológiai reziliencia ne csupán egyes szervezetek vagy infrastruktúrák saját képességeként, hanem integrált nemzeti stratégiai képességként jelenjen meg.

4.4.2 Az NTRGF logikai felépítése

A Nemzeti Technológiai Reziliencia Irányítási Keretrendszer kialakításának alapja az a felismerés, hogy a technológiai reziliencia fejlesztése nem egyetlen szervezet, ágazat

vagy szabályozási terület feladata. A reziliens működés olyan összetett rendszerszintű tulajdonság, amely kizárólag a technológiai, szervezeti és szabályozási dimenziók összehangolt fejlesztésével biztosítható. Az NTRGF ennek megfelelően nem új intézményi struktúrát hoz létre, hanem olyan irányítási architektúrát definiál, amely összekapcsolja a stratégiai célkitűzéseket, az elemzési módszereket, a döntéstámogatási folyamatokat és a fejlesztési beavatkozásokat.

Az NTRGF négy egymásra épülő funkcionális rétegből áll.

1. Stratégiai irányítási réteg

A felső szintet a nemzeti stratégiai célok alkotják. Ide tartoznak a nemzetbiztonsági, honvédelmi, gazdasági, digitális, energia- és innovációs stratégiák, valamint a kritikus infrastruktúrák rezilienciáját meghatározó nemzeti és európai uniós követelmények. E réteg feladata nem az operatív irányítás, hanem a közös stratégiai prioritások meghatározása és a fejlesztési irányok kijelölése.

Az **NTRGF ebben a szakaszban biztosítja, hogy a különböző szakpolitikák ne egymástól elkülönülten**, hanem egységes reziliencia szemlélet alapján kerüljenek összehangolásra.

2. Integrált governance-réteg

A második réteg alkotja az NTRGF központi elemét. **Ebben történik a technológiai, szervezeti és szabályozási dimenziók összehangolt elemzése**, a fejlesztési prioritások kijelölése, valamint a különböző ágazatok közötti koordináció.

Az integrált governance-réteg elsődleges feladatai:

- a technológiai kockázatok és függőségek rendszerszintű értékelése;
- az interdependenciák és limiting interface-ek azonosítása;
- a fejlesztési prioritások meghatározása;
- az ágazatok közötti koordináció biztosítása;
- a stratégiai döntések előkészítése.

E réteg sajátossága, hogy nem helyettesíti az ágazati irányítást, hanem annak felette elhelyezkedő koordinációs és döntéstámogató funkciót lát el.

3. Elemzési és értékelési réteg

A harmadik réteg biztosítja a döntések szakmai megalapozását. A kutatás során kidolgozott TRI és TRMM ebben a szakaszban válik a stratégiai irányítás eszközévé.

A **TRI egységes indikátorrendszert biztosít** az egyes rendszerek technológiai rezilienciájának strukturált értékeléséhez, míg a TRMM az értékelt képességek érettségi szintjeinek meghatározását és összehasonlítását támogatja. Az így kialakított reziliencia profilok országos szinten is felhasználhatók a fejlesztési prioritások összehasonlítható és transzparens meghatározásához.

A döntések ezáltal mérhető mutatókra, összehasonlítható indikátorokra és rendszeres értékelési ciklusokra épülnek.

4. Fejlesztési és adaptációs réteg

A negyedik réteg a stratégiai döntések végrehajtását támogatja. Ide tartoznak a technológiai beruházások, a szervezeti fejlesztések, a szabályozási módosítások, a képzési programok, valamint a kutatás-fejlesztési és innovációs kezdeményezések.

A **fejlesztések eredményeit az NTRGF nem tekinti lezárt folyamatna**k. A megvalósított intézkedések ismételt TRI- és TRMM-értékelésen mennek keresztül, amelynek eredményei visszacsatolódnak a stratégiai irányításba. Ez biztosítja a folyamatos adaptációt és a reziliencia hosszú távú fejlesztését.

A rétegek közötti kapcsolat

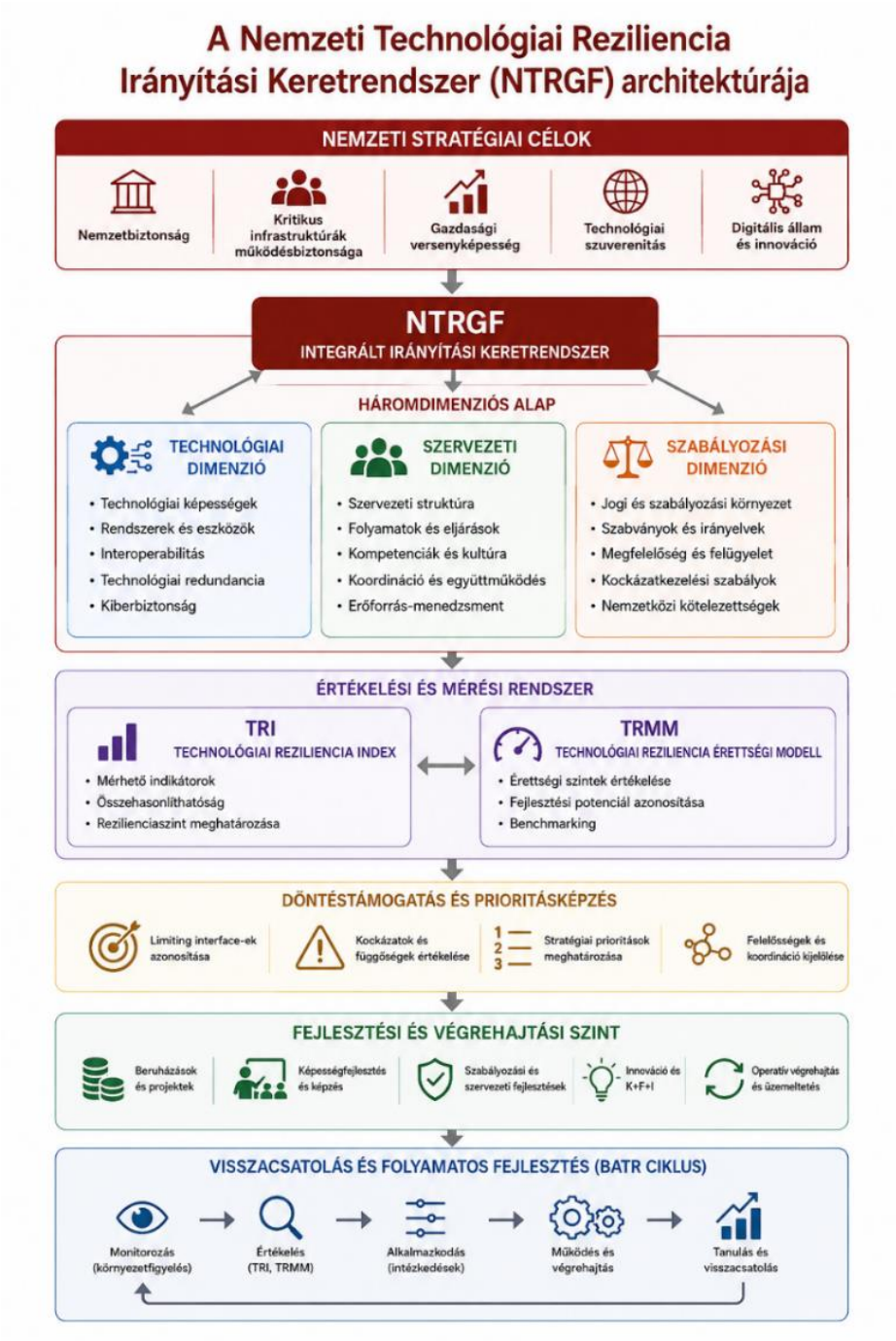
Az NTRGF működése ciklikus. A stratégiai célkitűzések meghatározzák az elemzési prioritásokat. Az elemzési eredmények megalapozzák a fejlesztési döntéseket. A fejlesztések végrehajtását követően újabb értékelés történik, amely visszahat a stratégiai célokra.

Ez a működési logika közvetlenül kapcsolódik a 3. fejezetben bemutatott **Balogh-féle Adaptív Technológiai Reziliencia Ciklushoz (BATR)**. Míg a BATR egy szervezet vagy infrastruktúra adaptációs folyamatát írja le, addig az NTRGF ugyanezt a logikát alkalmazza nemzeti stratégiai szinten. A két modell tehát nem egymás alternatívája, hanem eltérő absztrakciós szinten ugyanazt az adaptív működési elvet valósítja meg.

Tudományos újdonság

Az NTRGF tudományos újdonsága nem egy újabb reziliencia fogalom bevezetésében rejlik, hanem abban, hogy **integrálja a dolgozat valamennyi korábbi eredményét egy egységes stratégiai irányítási architektúrába**. A háromdimenziós T–O–R modell adja a szerkezeti alapot, a BATR biztosítja az adaptív működési logikát, a TRI és a TRMM szolgáltatják a mérési és értékelési módszertant, míg az NTRGF ezekre építve teremti meg a technológiai reziliencia stratégiai irányításának keretét.

Ezért az NTRGF nem egyszerű szakpolitikai ajánlás, hanem a kutatás során kidolgozott modellek szintézise és a technológiai reziliencia nemzeti szintű mérhetővé és értékelhetővé tételára tett javaslat.



4.3. ábra: A Nemzeti Technológiai Reziliencia Irányítási Keretrendszer (NTRGF) architektúrája (saját szerkesztés)

4.4.3 Az NTRGF működési mechanizmusa

A Nemzeti Technológiai Reziliencia Irányítási Keretrendszer működésének alapja, hogy a technológiai rezilienciát nem statikus állapotként, hanem folyamatosan változó

stratégiai képességként értelmezi. A technológiai fejlődés gyors üteme, az új fenyegetések megjelenése, a geopolitikai környezet változásai, valamint a kritikus infrastruktúrák közötti egyre szorosabb kölcsönös függőségek következtében a reziliencia fejlesztése nem egyszeri projektként, hanem folyamatos irányítási és döntéstámogatási folyamatként jelenik meg.

Ennek megfelelően az NTRGF működése zárt visszacsatolási ciklusra épül, amely biztosítja, hogy a stratégiai célkitűzések, az operatív fejlesztések és az értékelési eredmények egymást folyamatosan befolyásolják. A keretrendszer működése öt egymásra épülő funkcionális lépésből áll.

1. A stratégiai környezet folyamatos monitorozása

Az **első lépés a technológiai rezilienciát befolyásoló külső és belső környezet folyamatos figyelemmel kísérése**. Ide tartozik a technológiai trendek elemzése, a kiberfenyegetések változásának nyomon követése, a kritikus infrastruktúrák állapotának monitorozása, a beszállítói láncok sérülékenységének vizsgálata, valamint a szabályozási környezet változásainak értékelése.

Az NTRGF ebben a szakaszban nem csupán adatgyűjtést végez, hanem a különböző ágazatokból származó információkat közös elemzési keretbe rendezi. Ez biztosítja, hogy a stratégiai döntések ne izolált információkra, hanem rendszerszintű helyzetképre épüljenek.

2. Integrált rezilienciaértékelés

A **második lépésben történik a technológiai reziliencia tényleges értékelése**. A vizsgálat alapját a TRI és a TRMM képezik.

A TRI strukturálja és profilként megjeleníti a vizsgált rendszer rezilienciájának értékelési eredményeit, míg a TRMM az egyes értékelési területek érettségi szintjének meghatározását biztosítja. a technológiai, szervezeti és szabályozási dimenziókban.

Az értékelés nem kizárólag az egyes infrastruktúrák állapotát vizsgálja, hanem kiemelt figyelmet fordít a közöttük fennálló kapcsolatokra is. Ennek eredményeként azonosíthatók azok a kapcsolati szűk keresztmetszetek (limiting interface-ek), amelyek a teljes nemzeti technológiai ökoszisztéma működésére kihatnak.

3. Stratégiai prioritások meghatározása

Az integrált értékelés eredményeire építve meghatározhatók azok a fejlesztési területek, amelyek a legnagyobb hatást gyakorolják a technológiai rezilienciára.

Az **NTRGF egyik alapvető sajátossága, hogy a fejlesztési prioritások kijelölése nem kizárólag az egyes infrastruktúrák sérülékenysége alapján** történik. Az irányítás figyelembe veszi az adott rendszer más infrastruktúrákra gyakorolt hatását, a kölcsönös függőségeket, valamint a várható kaszkádhatásokat is.

Ennek következtében a fejlesztési döntések nem az egyes ágazatok optimalizálását, hanem a teljes nemzeti technológiai ökoszisztéma rezilienciájának növelését szolgálják.

4. Fejlesztések végrehajtása

A negyedik lépésben történik a **kijelölt fejlesztési intézkedések végrehajtása**. Ezek magukban foglalhatják:

- technológiai beruházások megvalósítását;
- szervezeti fejlesztéseket;
- képzési programok indítását;
- szabályozási módosításokat;
- kutatás-fejlesztési és innovációs programokat;
- új interoperabilitási megoldások kialakítását.

Az NTRGF ebben a szakaszban nem maga hajtja végre a fejlesztéseket, hanem biztosítja azok stratégiai koordinációját.

5. Visszacsatolás és szervezeti tanulás

A fejlesztések végrehajtását követően ismételt rezilienciaértékelés történik. **A TRI és a TRMM újbóli alkalmazása lehetővé teszi annak strukturált és összehasonlítható értékelését, hogy az egyes intézkedések milyen mértékben járultak hozzá a technológiai reziliencia változásához.** Az így keletkező tapasztalatok visszacsatolódnak a stratégiai irányításba, amely ennek megfelelően módosítja a fejlesztési prioritásokat.

Ez a működési logika biztosítja, hogy az NTRGF adaptív rendszerként működjön, amely folyamatosan tanul a saját működéséből.

Az NTRGF működésének sajátosságai

A kutatás során kidolgozott keretrendszer három olyan jellemzővel rendelkezik, amely megkülönbözteti a jelenlegi reziliencia irányítási megközelítésektől.

Integrált szemlélet

Az NTRGF nem különálló infrastruktúrákat vizsgál, hanem azok kölcsönös függőségeit és kapcsolati rendszerét elemzi. Ez lehetővé teszi a rendszerszintű sérülékenységek azonosítását.

Adatvezérelt döntéstámogatás

A stratégiai döntések nem kizárólag szakértői becslésekre vagy ágazati tapasztalatokra épülnek, hanem a TRI és a TRMM által biztosított összehasonlítható indikátorokra. Ez biztosítja a fejlesztési döntések objektivitását és visszamérhetőségét.

Adaptív irányítás

Az NTRGF nem lineáris fejlesztési modellt követ, hanem folyamatos tanulási ciklusként működik. Ez közvetlenül kapcsolódik a Balogh-féle Adaptív Technológiai Reziliencia Ciklushoz (BATR), amely az NTRGF működésének dinamikus alapját biztosítja.

4.4. ábra: Az NTRGF működési ciklusa (saját szerkesztés)

4.4.4 Az NTRGF alkalmazása a magyar technológiai reziliencia-politikában

Az NTRGF nem új intézményi struktúra létrehozását feltételezi, hanem a meglévő nemzeti és nemzetközi reziliencia-, kiberbiztonsági és kritikusinfrastruktúra-védelmi

keretek közötti integrált irányítási kapcsolat kialakítását. Ennek megfelelően alkalmazási logikája összekapcsolható a NATO nemzeti reziliencia követelményeivel [60], a CER és NIS2 végrehajtásával [25], [26], a hazai kritikusinfrastruktúra-védelemmel, a digitális állam fejlesztésével, a védelmi innovációval és a technológiai szuverenitás erősítésével.

- a NATO Baseline Requirements for National Resilience rendszeréhez [60];
- a CER és a NIS2 végrehajtásához [25] [26];
- a magyar kritikus infrastruktúra-védelemhez;
- a digitális államhoz;
- a védelmi innovációhoz;
- és a technológiai szuverenitás erősítéséhez.

4.4.5 Az NTRGF alkalmazása a nemzeti technológiai reziliencia irányításában

A **Nemzeti Technológiai Reziliencia Irányítási Keretrendszer alkalmazásának célja nem egy új közigazgatási struktúra kialakítása, hanem olyan egységes stratégiai irányítási logika biztosítása, amely képes összehangolni a technológiai rezilienciát meghatározó különböző szakpolitikai, szervezeti és technológiai folyamatokat**.

A kutatás során kidolgozott háromdimenziós modell, a BATR adaptációs ciklus, a TRI és a TRMM együttes alkalmazása lehetővé teszi, hogy a technológiai reziliencia fejlesztése a hagyományos megfelelőségközpontú megközelítés helyett folyamatos, adatvezérelt és adaptív stratégiai irányítási folyamattá váljon.

Az NTRGF alkalmazása során az irányítás három egymást kiegészítő döntési szinten valósul meg:

- **stratégiai szint**, ahol a nemzeti célkitűzések, prioritások és fejlesztési irányok kerülnek meghatározásra;
- **programszint**, ahol a különböző ágazati fejlesztések összehangolása történik;
- **operatív szint**, ahol az infrastruktúra-üzemeltetők és szervezetek végrehajtják a fejlesztéseket és biztosítják a folyamatos működést.

Az NTRGF újdonsága, hogy e három szintet nem különálló irányítási egységként kezeli, hanem egyetlen visszacsatolt döntési rendszer részeként.

Stratégiai szint

A stratégiai szint feladata annak meghatározása, hogy a technológiai reziliencia fejlesztése milyen nemzeti célokat szolgál.

Ide tartozik különösen

- a nemzetbiztonság;
- a honvédelmi képességfejlesztés;
- a gazdasági versenyképesség;
- a kritikus infrastruktúrák működésbiztonsága;
- a technológiai szuverenitás;
- a digitális állam fejlesztése;
- az innovációs ökoszisztéma fejlesztése.

Az NTRGF ebben a szakaszban nem konkrét projekteket választ ki, hanem meghatározza azokat a stratégiai prioritásokat, amelyek alapján a fejlesztések történnek.

Programszint

A második szinten jelennek meg azok a fejlesztési programok, amelyek több ágazatot is érintenek.

Ilyenek például

- kritikus infrastruktúra-fejlesztések;
- kiberbiztonsági programok;
- digitális transzformáció;
- mesterséges intelligencia alkalmazása;
- autonóm rendszerek;
- intelligens energiahálózatok;
- védelmi innováció.

Az NTRGF sajátossága, hogy ezen programokat nem külön-külön értékeli, hanem azok technológiai rezilienciára gyakorolt együttes hatását vizsgálja.

Operatív szint

Az operatív szinten történik a fejlesztések végrehajtása.

Ez foglalja magában

- az infrastruktúrák üzemeltetését;
- az incidenskezelést;
- a szervezeti felkészítést;

- a technológiai beruházásokat;
- a szabályozási módosítások végrehajtását.

A végrehajtás során keletkező adatok ismét visszakerülnek a TRI és a TRMM értékelési rendszerébe, amely strukturált, indikátoralapú visszajelzést biztosít a fejlesztések eredményességéről.

Az NTRGF kapcsolata a nemzetközi reziliencia keretekkel

A kutatás során kialakított NTRGF nem helyettesíti a meglévő nemzetközi szabályozási és stratégiai keretrendszereket. Ellenkezőleg, azok integrált alkalmazását támogatja.

- A **NATO Baseline Requirements for National Resilience** [60] a nemzeti ellenálló képesség alapvető funkcionális területeit határozza meg.
- A **CER** [26] a kritikus szervezetek működőképességének fenntartását széles, többféle zavarforrást figyelembe vevő reziliencia-megközelítésben kezeli.
- A **NIS2** a kiberbiztonsági irányítás és a digitális infrastruktúrák védelmének követelményeit rögzíti.
- A **DORA** a pénzügyi szektor digitális működési rezilienciáját szabályozza.
- A **Cyber Resilience Act** [27] a digitális elemeket tartalmazó termékek biztonságát életciklus-szemléletű fejlesztői és gyártói felelősségekhez kapcsolja.

E keretrendszerek közös jellemzője, hogy egy-egy szakterület vagy szabályozási cél mentén határozzák meg a rezilienciával kapcsolatos követelményeket.

Az **NTRGF** ezzel szemben nem újabb szabályozási keretet jelent, hanem olyan **integráló irányítási modellt, amely képes összekapcsolni ezen követelményeket** egy közös technológiai reziliencia-szemléletben.

Ennek következtében az NTRGF alkalmazható olyan stratégiai koordinációs eszközként, amely támogatja a különböző nemzetközi követelmények összehangolt végrehajtását, miközben figyelembe veszi a nemzeti sajátosságokat és fejlesztési prioritásokat.

Az NTRGF stratégiai előnyei

A kutatás alapján az NTRGF alkalmazása öt stratégiai előnyt biztosít.

Elsőként lehetővé teszi a technológiai reziliencia egységes értelmezését a különböző ágazatok között.

Másodikként biztosítja, hogy a fejlesztési döntések összehasonlítható reziliencia indikátorokra épüljenek.

Harmadikként támogatja az ágazatok közötti kölcsönös függőségek kezelését és a kaszkádhatások megelőzését.

Negyedikként összekapcsolja a stratégiai tervezést a folyamatos mérési és visszacsatolási mechanizmusokkal.

Ötödikként lehetővé teszi a technológiai reziliencia folyamatos fejlesztését anélkül, hogy új intézményrendszer létrehozását tenné szükségessé.

A kutatás álláspontja szerint e tulajdonságok teszik az NTRGF-et alkalmassá arra, hogy a technológiai reziliencia stratégiai irányításának egységes kereteként szolgáljon.

4.4.6 A kutatás gyakorlati alkalmazhatósága

A kutatás eredményei alapján kidolgozott háromdimenziós technológiai rezilienciamodell, a BATR adaptációs ciklus, a TRI, a TRMM és az NTRGF nem kizárólag elméleti konstrukciók, hanem közvetlenül alkalmazhatók a technológiai reziliencia tervezése, értékelése és fejlesztése során. **Az integrált technológiai reziliencia értékelés gyakorlati alkalmazhatóságát jól szemlélteti a kiberbiztonsági megfelelőség és a szervezeti reziliencia értékelés összekapcsolásának lehetősége., alkalmazkodni, helyreállítani kritikus képességeit és tanulni az eseményből**.

A keretrendszer alkalmazási lehetőségei különösen az alábbi területeken jelentősek:

- kritikus infrastruktúrák reziliencia értékelése;
- nemzeti reziliencia stratégiák kidolgozása;
- technológiai és digitális transzformációs programok támogatása;
- kiberbiztonsági auditok és képességértékelések;
- honvédelmi és nemzetbiztonsági képességfejlesztés;
- védelmi innovációs és kutatás-fejlesztési programok priorizálása;
- állami beruházások stratégiai döntéstámogatása.

Egy valóságos és a szerző által javasolt alkalmazási lehetőség: A kutatásban kidolgozott modellrendszer gyakorlati és tudományos alkalmazhatóságának egyik konkrét hazai területét a **NIS2 irányelv magyarországi adaptációjához kapcsolódó kiberbiztonsági követelmények** jelenthetik. A hazai kiberbiztonsági szabályozás hatálya alá tartozó szervezetek meghatározott körében kiberbiztonsági auditot kell végrehajtani,

amely a szervezet elektronikus információs rendszereinek biztonsági állapotáról, a követelmények teljesüléséről és a feltárt hiányosságokról ad strukturált képet.

Az általam kidolgozott **TRMM azonban nem az audit helyettesítésére szolgálna**, hanem annak eredményeit – más szervezeti, működési és szabályozási információkkal együtt – bemeneti adatként felhasználva magasabb szintű reziliencia értékelést tenne lehetővé. A háromdimenziós technológiai rezilienciamodell alapján az audit technológiai és kiberbiztonsági megállapításai összekapcsolhatók a **technológiai, szervezeti és szabályozási–irányítási dimenziók**, valamint az azok közötti függőségek és kapcsolati szűk keresztmetszetek értékelésével. A **TRMM** az érettségi szintek meghatározását, míg a **TRI** az eredmények integrált reziliencia profilként történő strukturálását támogathatja. A megközelítés így a megfelelőség vizsgálatán túl a felső vezetés számára is közvetlenül hasznosítható döntéstámogató információt adhat arról, hogy **mely technológiai, szervezeti vagy irányítási hiányosság, illetve mely dimenziók közötti kapcsolat korlátozza leginkább a szervezet működési rezilienciáját, és mely fejlesztési beavatkozások élvezzenek prioritást**. Ez megfelel a kidolgozott módszertan azon logikájának, amely szerint a TRMM nem különálló cyber-, OT- vagy fizikai biztonsági pontszámokat állít elő, hanem a három dimenziót és azok kölcsönhatásait egységes értékelési rendszerben kezeli. A megközelítés végső célja tehát nem pusztán annak megállapítása, hogy a szervezet megfelel-e az előírt követelményeknek, hanem annak értékelése, hogy súlyos, összetett zavar esetén **képes-e fenntartani alapvető működését**

A keretrendszer egyik legfontosabb előnye, hogy valamennyi alkalmazási területen azonos elemzési logikát biztosít, ezáltal lehetővé teszi a különböző szervezetek és ágazatok összehasonlítható reziliencia értékelését, valamint a fejlesztési prioritások módszertanilag egységes és visszamérhető meghatározását. Az ilyen szervezeti szintű rezilienciaprofilok aggregált eredményei egyúttal az NTRGF ágazati és nemzeti szintű döntéstámogatásának bemeneti információiként is felhasználhatók, ezáltal kapcsolatot teremtve a szervezeti megfelelőségértékelés, a működési reziliencia és a nemzeti szintű technológiai rezilienciairányítás között.

4.5 A fejezet összegzése és tudományos következtetései

A jelen fejezet célja a 3. fejezetben kidolgozott háromdimenziós technológiai rezilienciamodell gyakorlati alkalmazhatóságának vizsgálata, kvalitatív összehasonlító validálása, valamint stratégiai kiterjesztése volt. A többes esettanulmány-logikára épülő

elemzés azt vizsgálta, hogy a modell strukturális, kapcsolati és dinamikus elemei eltérő működési környezetű kritikus infrastruktúrák esetében következetesen alkalmazhatók-e.

Az energetikai, közlekedési, elektronikus hírközlési és katonai vezetési rendszerek elemzése valamennyi vizsgált esetben lehetővé tette a technológiai, szervezeti és szabályozási–irányítási dimenziók azonosítását. Az eredmények arra mutatnak, hogy a technológiai reziliencia nem vezethető vissza kizárólag a technológiai fejlettség szintjére; a reziliens működés szempontjából meghatározó jelentőségű a három dimenzió összehangolt működése és kölcsönhatása. Ez kvalitatív módon alátámasztja a háromdimenziós technológiai rezilienciamodell strukturális alkalmazhatóságát eltérő kritikus infrastruktúrák elemzésében.

Az összehasonlító elemzés **további eredménye az interdimenzionális kapcsolatok meghatározó szerepének azonosítása**. A vizsgált infrastruktúrákban több esetben a rezilienciát korlátozó tényezők nem az egyes dimenziókon belül, hanem azok kapcsolódási pontjain jelentek meg. A limiting interface koncepció ezáltal a vizsgált esetekben olyan analitikai kategóriának bizonyult, amely alkalmas a dimenziók közötti kritikus kapcsolatok és fejlesztési szűk keresztmetszetek feltárására.

A **vizsgálatok a BATR adaptációs ciklus alkalmazhatóságát is alátámasztották**. Az eltérő technológiai környezetekben egyaránt azonosíthatók voltak az érzékelés, értékelés, alkalmazkodás, stabilizáció és tanulás funkcionális elemei. Ez arra utal, hogy a BATR alkalmas a technológiai reziliencia dinamikus működésének egységes értelmezésére különböző rendszerekben.

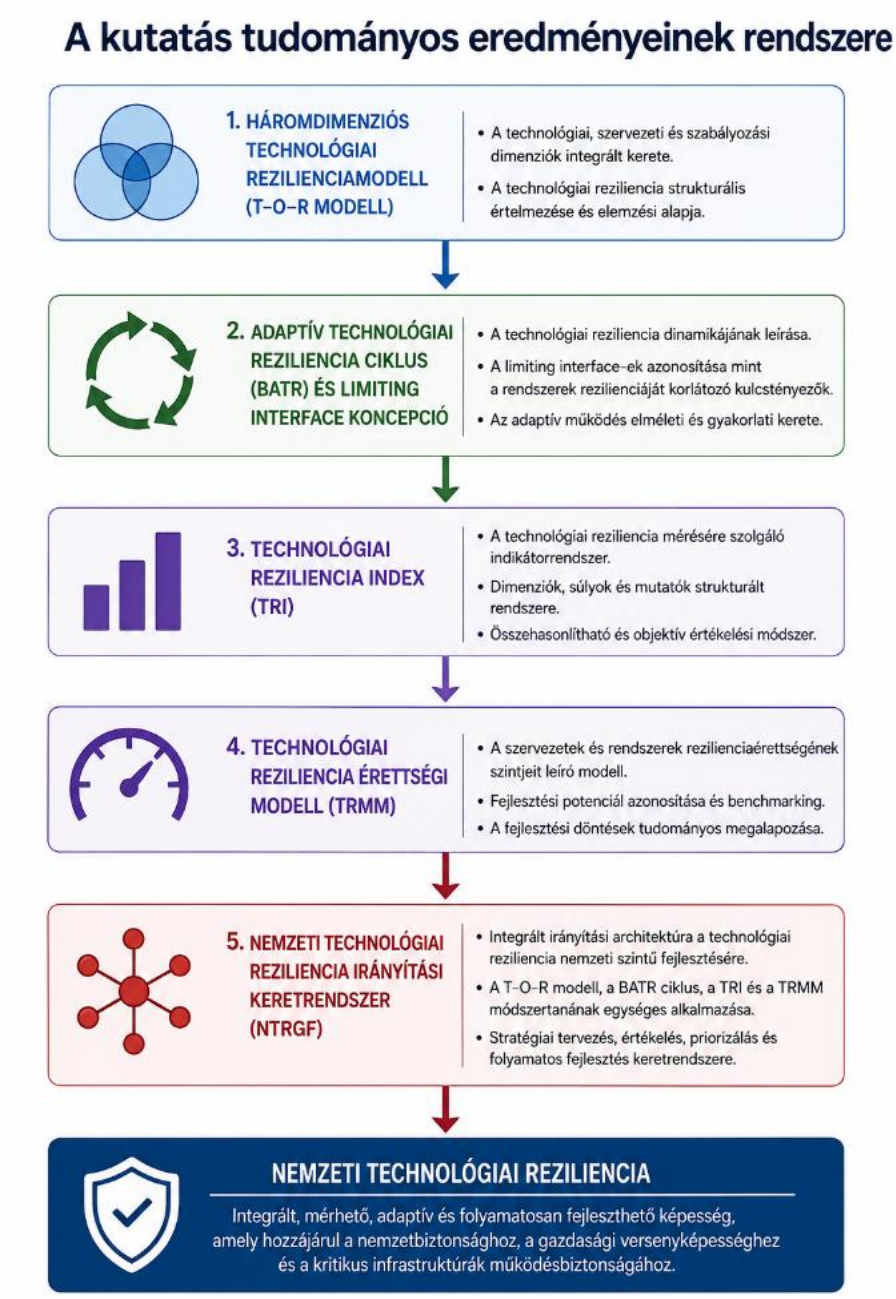
A TRI és a TRMM tekintetében a fejezet nem teljes körű kvantitatív vagy statisztikai validációt végzett, hanem azok értékelési logikájának gyakorlati alkalmazhatóságát vizsgálta. Az elemzés alapján a TRI–TRMM keretrendszer alkalmas lehet arra, hogy egységes struktúrában jelenítse meg a dimenzionális, kapcsolati és dinamikus reziliencia tulajdonságokat, valamint érettségi szintekhez kapcsolja azokat. A keretrendszer további empirikus és kvantitatív validálása ugyanakkor a kutatás későbbi fejlesztési irányát képezi.

A **fejezet összehasonlító elemzéséből levezethető stratégiai következtetés túlmutat** az egyes infrastruktúrák szintjén. Az összehasonlító elemzés alapján megállapítható, hogy a technológiai reziliencia nem kizárólag egyes szervezetek vagy kritikus infrastruktúrák sajátossága, hanem a nemzeti technológiai ökoszisztéma egészének működéséből kialakuló képességként is értelmezhető. A rendszerek közötti kölcsönös függőségek következtében az egyes infrastruktúrák rezilienciája csak integrált megközelítésben értelmezhető és fejleszthető.

E felismerés alapján a kutatás kidolgozta a **Nemzeti Technológiai Reziliencia Irányítási Keretrendszert (National Technological Resilience Governance Framework – NTRGF)**. Az NTRGF nem új szabályozási rendszerként, hanem integrált stratégiai irányítási architektúraként értelmezhető, amely egységes keretbe foglalja a háromdimenziós technológiai rezilienciamodellt, a BATR adaptációs ciklust, valamint a TRI és a TRMM értékelési módszertanát. Ezáltal biztosítja a technológiai reziliencia nemzeti szintű tervezését, mérését, koordinációját és folyamatos fejlesztését.

A kutatás eredményei alapján megállapítható, hogy a technológiai reziliencia fejlesztése nem érhető el kizárólag technológiai beruházásokkal vagy ágazati fejlesztési programokkal. **A reziliens működés megteremtéséhez olyan integrált irányítási megközelítés szükséges, amely egyidejűleg kezeli a technológiai, szervezeti és szabályozási dimenziókat, figyelembe veszi azok kölcsönhatásait, és támogatja a folyamatos alkalmazkodást.**

A jelen fejezetben bemutatott eredmények egyben megalapozzák a dolgozat végső tudományos következtetéseit is. A kutatás során kidolgozott háromdimenziós technológiai rezilienciamodell, a BATR adaptációs ciklus, a TRI–TRMM értékelési keretrendszer és az NTRGF egymásra épülő, koherens rendszert alkotnak. A kutatás során kidolgozott háromdimenziós technológiai rezilienciamodell, a BATR adaptációs ciklus, a TRI–TRMM értékelési keretrendszer és az NTRGF egymásra épülő, koherens rendszert alkotnak. Együttesen olyan elméleti, módszertani és stratégiai megközelítést kínálnak, amely közös fogalmi és elemzési keretet biztosít a technológiai reziliencia értelmezéséhez, strukturált értékeléséhez és stratégiai fejlesztéséhez különböző kritikus infrastruktúrák, valamint nemzeti szintű technológiai ökoszisztémák esetében.



4.5. ábra: A kutatás tudományos eredményeinek rendszere (saját szerkesztés)

5. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

5.1. A kutatás összegzése

A disszertáció kiindulópontját az a felismerés jelentette, hogy a 21. század magas fokú digitalizációval, technológiai összekapcsoltsággal és kölcsönös függőségekkel jellemezhető rendszereinek működőképessége nem értelmezhető kizárólag műszaki megbízhatósági vagy kiberbiztonsági kérdésként. Az energiaellátás, a közlekedés, az elektronikus hírközlés, a digitális szolgáltatások, a felhő- és adatközponti infrastruktúrák, a műholdas kommunikáció és PNT-szolgáltatások, valamint a katonai vezetési és irányítási rendszerek olyan egymásba kapcsolódó technológiai ökoszisztémát alkotnak, amelyben egy lokális zavar más rendszerek működésére is tovagyűrűző hatást gyakorolhat.

A kutatás **központi problémája** ezért annak meghatározása volt, hogy a **technológiai reziliencia milyen elméleti keretben értelmezhető**, milyen tényezők alakítják, miként tehető strukturáltan értékelhetővé, és hogyan emelhető a szervezeti vagy ágazati szintről nemzeti stratégiai képességgé. A **vizsgálat logikai íve ennek megfelelően az elméleti megalapozástól** a környezeti kihívások elemzésén és a saját modellalkotáson keresztül az ágazati validációig, majd a stratégiai irányítási következtetésekig vezetett.

Az **1. fejezet** a **reziliencia fogalmának tudományos evolúcióját** vizsgálta. Az ökológiai, mérnöki, szervezeti, kiberbiztonsági és kritikusinfrastruktúra-megközelítések összehasonlítása azt mutatta, hogy **a reziliencia nem azonosítható egyszerűen a robusztussággal vagy a meghibásodások elkerülésével**. A **fogalom lényegi** elemei az **ellenállás** mellett a **kritikus funkciók fenntartása**, a **helyreállítás**, az **alkalmazkodás,** a **tanulás** és a **megváltozott környezethez történő újbóli igazodás**. Ebből következett a technológiai reziliencia szocio-technikai értelmezésének szükségessége.

A **2. fejezet** a **fogalmi keretet a 21. század stratégiai és technológiai környezetében** helyezte el. Az elemzés alapján a **reziliencia jelentőségét nem egyetlen fenyegetés vagy technológiai trend növeli, hanem a technológiai gyorsulás, a hiperösszekapcsoltság, a kiber- és hibrid fenyegetések, az IT/OT-konvergencia, a mesterséges intelligencia és autonóm rendszerek, a felhő- és platformfüggőség, az űr- és PNT-szolgáltatások, az energia- és nyersanyagfüggőség, valamint a beszállítói és geopolitikai kitettségek együttes hatása.** A fejezet következtetése szerint a **teljes hibamentesség és a kizárólag statikus kontrollokra épülő biztonság nem reális cél**; a kritikus funkciók fenntartása adaptív, többrétegű és több szereplőt összekapcsoló képességet igényel.

A 2. fejezet **három követelményt vezetett le a későbbi modell számára**: legyen képes az **egyes dimenziók önálló állapotának értékelésére**; **tegye láthatóvá a dimenziók közötti kapcsolatokat és interfészeket**; valamint a **rezilienciát időbeli, adaptív folyamatként** kezelje. Ezzel a környezeti elemzés közvetlenül megalapozta a 3. fejezet modellalkotását, és egyben indokolta, hogy a validáció több, eltérő működési és szabályozási logikájú kritikus infrastruktúra-rendszerre terjedjen ki.

A **3. fejezetben kidolgozott háromdimenziós technológiai rezilienciamodell** a technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziót **integrált rendszerként** kezeli. A **modell lényegi állítása, hogy a reziliencia nem az egyes dimenziók egyszerű összege, hanem azok kölcsönhatásából létrejövő rendszerszintű tulajdonság.** A technológiai architektúra, a redundancia, modularitás, monitorozás és kiberbiztonsági képességek **csak akkor eredményeznek tartós működőképességet**, ha megfelelő szervezeti döntéshozatal, tanulási és adaptációs képesség, valamint támogató governance- és szabályozási környezet kapcsolódik hozzájuk.

A modell statikus szerkezetét a **Balogh-féle Adaptív Technológiai Reziliencia Ciklus (BATR-ciklus)** egészíti ki. A BATR öt funkcionális szakaszban – érzékelés, értékelés, adaptáció, stabilizáció, valamint tanulás és innováció – írja le a reziliens rendszer időbeli működését. A ciklus nem a háromdimenziós modelltől független konstrukció, hanem annak dinamikus leképezése**. Különösen fontos következtetés, hogy a tanulás és innováció nem a folyamat lezárása: az új tudás, technológiai képesség és intézményi tapasztalat megváltoztatja a következő ciklus kiinduló állapotát, ezért a reziliencia fejlődése spirális folyamatként értelmezhető.**

A strukturális és dinamikus modell mérhetővé és értékelhetővé tételára a 3. fejezet a **Technological Resilience Index (TRI)** értékelési logikáját és a **Technological Resilience Maturity Model (TRMM)** ötfokozatú érettségi rendszerét alkalmazza. **A TRI elsődleges eredménye nem egyetlen aggregált számérték, hanem technológiai rezilienciaprofil, amely láthatóvá teszi a dimenziók közötti egyensúlytalanságokat és a fejlesztési prioritásokat. A TRMM ehhez egységes érettségi értelmezést biztosít.** A kutatás tudatosan nem univerzális, matematikailag súlyozott rezilienciaindexet kíván létrehozni, hanem strukturált diagnosztikai és összehasonlító értékelési keretet.

A **4. fejezet** a modell **koncepcionális és szakági alkalmazhatóságát** eltérő kritikus infrastruktúra-környezetekben **vizsgálta.** Az összehasonlító elemzés egyik **legfontosabb eredménye, hogy az energia, a közlekedés, az elektronikus hírközlés/digitális infrastruktúra és a katonai C2 eltérő technológiai és szabályozási logikája ellenére a**

rezilienciát meghatározó technológiai, szervezeti és szabályozási kölcsönhatások hasonló szerkezeti mintázatot mutatnak. A validáció ezért **alátámasztja a háromdimenziós modell ágazatokon átívelő elemzési alkalmazhatóságát**, ugyanakkor nem teszi szükségtelenné az ágazatspecifikus indikátorok és értékelési szintleírások további fejlesztését.

A komparatív elemzés egy további **stratégiai következtetéshez** vezetett: a **vizsgált infrastruktúrák** nem önálló rendszerekként, **hanem egymással kölcsönösen függő nemzeti technológiai ökoszisztéma részeiként** működnek. Az elektronikus hírközlés az energiaellátás digitális működését támogatja, az energiaellátás a kommunikációs és közlekedési rendszerek alapfeltétele, a katonai vezetési rendszerek pedig több civil infrastruktúrától is függnek. **Ebből következik, hogy egyetlen ágazat rezilienciája sem fejleszthető tartósan a kapcsolódó infrastruktúráktól függetlenül**.

E felismerésből vezethető le a **Nemzeti Technológiai Reziliencia Irányítási Keretrendszer (National Technological Resilience Governance Framework – NTRGF)** koncepciója. Az NTRGF nem újabb technológiai rezilienciamodell, hanem a kutatás eredményeinek stratégiai alkalmazási kerete. Feladata a kritikus infrastruktúrák, a digitális transzformáció, a kiberbiztonság, a védelmi követelmények, az ipar, az innováció és a nemzeti ellenálló képesség közötti koordináció támogatása.

A disszertáció teljes logikai íve így az elméleti fogalomalkotástól az adaptív működés és mérhetőség kérdésén át a szakági alkalmazhatóságig és a nemzeti szintű governance-ig vezet. A kutatás eredményei alapján a technológiai reziliencia nem egy újabb elkülönült biztonsági részterület, hanem olyan integráló szemlélet, amely a technológiai rendszerek működőképességét a technológia, a szervezet és az irányítás egymásra hatásában értelmezi.

Az **5. fejezet összegzi a kutatás eredményeit**, megválaszolja a kutatási kérdéseket, értékeli a hipotéziseket, tételesen megfogalmazza az új tudományos eredményeket, valamint meghatározza a gyakorlati alkalmazás és a további kutatás irányait.

5.2. A kutatási kérdések megválaszolása

5.2.1. K1 – A technológiai reziliencia integrált értelmezése

A kutatási kérdés arra irányult, hogyan értelmezhető a technológiai reziliencia olyan integrált szocio-technikai rendszertulajdonságként, amely egyidejűleg képes megragadni a technológiai, szervezeti és szabályozási–irányítási tényezők hatását.

A kutatás eredménye alapján a technológiai reziliencia olyan dinamikus, adaptív rendszerszintű képességként értelmezhető, amely lehetővé teszi a kritikus funkciók fenntartását, a zavarok hatásának elnyelését, a működés stabilizálását és helyreállítását, valamint a tapasztalatok szervezeti és technológiai tanulássá alakítását. A reziliencia hordozója nem kizárólag a technológiai infrastruktúra, hanem a technológia, az azt működtető szervezet és a működés feltételeit meghatározó szabályozási–irányítási környezet együttese.

A **háromdimenziós T–O–R modell ezért nem három párhuzamos ellenőrzési listát** jelent. Tudományos jelentősége abban áll, hogy az interdimenzionális kapcsolatok vizsgálatát a rezilienciaelemzés részévé teszi. Egy technikailag redundáns rendszer például szervezetileg sérülékeny maradhat, ha nincs megfelelő döntési jogosultság vagy felkészült személyi állomány; egy jól felkészült szervezet pedig nem képes megfelelően adaptálódni, ha a szabályozási környezet nem biztosítja a szükséges mozgásteret. A technológiai reziliencia ezért relációs és rendszerszintű tulajdonság.

5.2.2. K2 – A rezilienciát alakító környezeti tényezők és függőségek

A második kutatási kérdés a technológiai, szervezeti, kiberbiztonsági, ellátásilánc- és governance-tényezők, valamint azok kölcsönös függőségeinek azonosítására irányult.

A 2. fejezet elemzése alapján a technológiai rezilienciát nem egyetlen domináns kockázat alakítja. A kiberfenyegetések, az IT/OT-konvergencia, a mesterséges intelligencia és autonóm rendszerek, a felhő- és platformfüggőség, a PNT- és űrszolgáltatások, az energiaellátás, a félvezetők és kritikus nyersanyagok, valamint a beszállítói láncok egymásra épülő függőségi rétegeket alkotnak. Ezekhez társul a humán kompetencia, a vezetés, a szervezeti kultúra, a tudásmegosztás, a szabályozási alkalmazkodás és a köz- és magánszféra koordinációja.

A **kutatás egyik lényeges következtetése**, hogy a függőség önmagában nem azonos a sérülékenységgel. A függőség akkor válik reziliencia kockázattá, ha koncentrált, nem átlátható, nehezen helyettesíthető, tartalék nélküli vagy válsághelyzetben nem kezelhető. A technológiai szuverenitás ezért nem teljes technológiai önellátást jelent, hanem olyan stratégiai mozgásteret, amely a kritikus funkciók fenntartását külső zavar esetén is lehetővé teszi.

5.2.3. K3 – A technológiai reziliencia mérhetősége

A harmadik kutatási kérdés arra kereste a választ, milyen dimenziók, indikátorok és érettségi szintek segítségével tehető a technológiai reziliencia összehasonlíthatóan értékelhetővé anélkül, hogy komplexitása egyetlen technikai mutatóra redukálódna.

A **kutatás válasza a háromdimenziós értékelési architektúra**, a TRI-profil és az ötfokozatú TRMM együttes alkalmazása. A technológiai, szervezeti és szabályozási–irányítási dimenzió külön-külön értékelhető, ugyanakkor az interfészek és függőségek is az elemzés tárgyát képezik. A BATR-ciklus ehhez időbeli indikátorokat is kapcsolhat, például az észlelési, értékelési, adaptációs és stabilizációs időt, illetve a tanulságok beépítésének eredményességét.

A kutatás alapján a technológiai reziliencia mérésének célszerű eredménye nem feltétlenül egyetlen összesített pontszám. A rezilienciaprofil több információt őriz meg, mert megmutatja, mely dimenziók fejlettek, hol vannak kritikus hiányosságok, és milyen kapcsolati gyengeségek korlátozzák a teljes rendszer alkalmazkodóképességét. A TRMM így elsősorban diagnosztikai és fejlesztésorientált keret.

5.2.4. K4 – A modell ágazati alkalmazhatósága

A negyedik kutatási kérdés azt vizsgálta, hogy a háromdimenziós modell és az érettségi megközelítés mennyiben alkalmazható eltérő kritikus infrastruktúra-ágazatokban, és milyen közös, illetve ágazatspecifikus reziliencia-követelmények azonosíthatók.

A 4. fejezet **összehasonlító szakági validációja alapján** a T–O–R szerkezet eltérő technológiai környezetekben is értelmezhető. Az energia, a közlekedés, az elektronikus hírközlés/digitális infrastruktúra és a katonai C2 esetében eltérnek a konkrét technológiák, szabályozási követelmények, üzemeltetési modellek és fenyegetési prioritások, de mindegyikben azonosítható a technológiai ellenálló és helyreállítási képesség, a szervezeti adaptáció, valamint a szabályozási–irányítási koordináció szükségessége.

A **modell tehát közös metakeretet biztosít, de nem helyettesíti** az ágazatspecifikus szakmai követelményeket. A validáció eredménye éppen azt támasztja alá, hogy az általános modell és az ágazati értékelési szintleírások kettős szintje szükséges: az előbbi összehasonlíthatóságot, az utóbbi szakmai pontosságot biztosít.

5.2.5. K5 – A nemzeti szintű stratégiai irányítás szükségessége

Az ötödik kutatási kérdés arra irányult, milyen stratégiai és intézményi irányítási keret szükséges ahhoz, hogy az ágazati, civil–katonai és technológiai függőségek nemzeti szinten összehangolt reziliencia fejlesztéssé alakíthatók legyenek.

A **komparatív validáció alapján a technológiai reziliencia rendszerek rendszere jellegű képesség.** Az egyes ágazatok működőképessége más infrastruktúrák szolgáltatásaitól függ, ezért az ágazati optimalizálás önmagában nem garantálja a nemzeti technológiai ökoszisztéma rezilienciáját. Ebből következik az NTRGF szükségessége, mint olyan stratégiai governance-keret, amely a különböző ágazati szereplők, állami intézmények, védelmi szervezetek, szolgáltatók, ipari és kutatás-fejlesztési szereplők közötti koordinációt támogatja.

Az NTRGF értelmezésében a governance nem kizárólag szabályozási megfelelést jelent. A keretrendszer logikája adaptív: monitorozásra, gyakorlatokra és incidensekre, értékelésre, módosításra, újratesztelésre és visszacsatolásra épül. Ezzel a kutatás a compliance-orientált megközelítést a folyamatos technológiai reziliencia fejlesztés irányába terjeszti ki.

5.3. A hipotézisek értékelése

A hipotézisek értékelése során fontos módszertani korlát, hogy a disszertáció elsősorban kvalitatív, konceptuális és dokumentumalapú összehasonlító vizsgálatra épül. Ezért az „igazolt” megjelölés a dolgozatban alkalmazott módszerek által alátámasztott elméleti és szakági érvényességet jelenti, és nem nagymintás statisztikai bizonyítást.

5.3.1. H1 – A reziliencia háromdimenziós meghatározottsága

H1 – igazolt. A kutatás eredményei igazolják, hogy a technológiai rendszerek rezilienciája nem írható le kielégítően kizárólag technikai vagy kiberbiztonsági mutatókkal; a reziliencia szintjét a technológiai, szervezeti és szabályozási–irányítási dimenziók együttes állapota és kölcsönhatása határozza meg.

Az 1. fejezet elméleti szintézise, a 2. fejezet környezeti elemzése, a 3. fejezet modellalkotása és a 4. fejezet szakági összehasonlítása egyaránt azt támasztja alá, hogy a technikai képességek önmagukban nem elegendők. A reziliencia gyengesége sok esetben az interfészeken jelenik meg: például technológiai esemény és szervezeti döntéshozatal, szervezeti adaptáció és szabályozási felhatalmazás vagy technológiai fejlesztés és

kompetenciafejlesztés között. A hipotézis ezért a kutatás módszertani keretei között igazoltnak tekinthető.

5.3.2. H2 – A technológiai reziliencia strukturált értékelhetősége

H2 – koncepcionálisan alátámasztott, empirikus továbbvalidálást igényel. A technológiai reziliencia összehasonlíthatóan értékelhető, ha a három dimenzióhoz egységes értelmezési logika szerint kialakított indikátorok és egymásra épülő érettségi szintek kapcsolódnak.

A TRI és a TRMM kialakítása megteremti az összehasonlítható értékelés módszertani alapját, és a szakági validáció azt mutatja, hogy a háromdimenziós struktúra eltérő környezetekben is alkalmazható. Ugyanakkor a 3. fejezet maga is rögzíti, hogy az indikátorok részletes értékelési szintleírásainak, a reprodukálhatóságnak és a különböző alkalmazási területeken történő empirikus vizsgálatnak a továbbfejlesztése későbbi kutatási feladat. Emiatt a hipotézis teljes körű empirikus igazolása további vizsgálatot igényel.

5.3.3. H3 – Közös rezilienciamintázat eltérő ágazatokban

H3 – alátámasztott. Az eltérő kritikus infrastruktúra-ágazatokban a konkrét technológiai kitettségek különböznek, ugyanakkor a reziliencia alapvető szerkezete közös technológiai, szervezeti és szabályozási–irányítási mintázatot mutat.

A 4. fejezet összehasonlító elemzése alapján a vizsgált rendszerek eltérő technológiai és szabályozási logikája ellenére mindhárom dimenzió következetesen megjelenik. A hipotézis igazolása ugyanakkor nem jelenti azt, hogy azonos indikátorkészlet változtatás nélkül minden ágazatra alkalmazható. Az általános szerkezet közös, a konkrét mérési értékelési szintleírások ágazati adaptációt igényelnek.

5.3.4. H4 – Az interdependenciák meghatározó szerepe

H4 – alátámasztott. A magas fokú technológiai interdependencia miatt egy ágazat rezilienciája nem értékelhető kizárólag saját belső képességei alapján; a kapcsolódó energia-, kommunikációs, digitális, közlekedési, PNT-, felhő- és ellátásilánc-függőségek érdemben befolyásolják a működőképességet és a kaszkádhatások kockázatát.

A 2. fejezet függőségi elemzése és a 4. fejezet ágazati összehasonlítása egyaránt azt mutatja, hogy a technológiai reziliencia system of systems jellegű. A külső függőségek figyelmen kívül hagyása hamis biztonságérzethez vezethet: egy belsőleg magas érettségű rendszer is sérülékeny lehet, ha kritikus külső szolgáltatásai nem helyettesíthetők vagy nem rendelkeznek megfelelő rezilienciával.

5.3.5. H5 – Az adaptív governance szükségessége

H5 – alátámasztott. A statikus megfelelőségorientált irányítás önmagában nem biztosít megfelelő technológiai rezilienciát; magasabb rezilienciaszint ott érhető el, ahol a governance folyamatos monitorozásra, gyakorlatokra és incidensekre, értékelésre, szervezeti tanulásra, módosításra és újratesztelésre épül.

A BATR-ciklus és a 2. fejezet compliance–adaptív governance megkülönböztetése ugyanarra az elvre vezet: a reziliencia időbeli képesség, ezért nem állapítható meg egyszeri megfelelőségi állapotként. A követelmények teljesítése szükséges alap, de a környezet, a fenyegetések és a technológia változása miatt a rendszernek folyamatosan újra kell értékelnie saját működését.

5.3.6. H6 – Integrált nemzeti irányítás

H6 – koncepcionálisan és a szakági összehasonlítás alapján alátámasztott. Az ágazati reziliencia fejlesztések nemzeti szintű hatékonysága növelhető olyan integrált technológiai reziliencia-irányítási kerettel, amely összekapcsolja a kritikus infrastruktúrák, a védelmi szféra, a szabályozás, az ipar, a kutatás-fejlesztés és a nemzetközi együttműködés szereplőit.

A 4. fejezet validációja megalapozza az integrált governance szükségességét, és ebből vezethető le az NTRGF koncepciója. A hipotézis teljes szervezeti és szakpolitikai hatásvizsgálata azonban csak az NTRGF gyakorlati implementációját követően lenne elvégezhető. A jelen disszertáció ezért a szükségességet és a koncepcionális működési logikát támasztja alá, nem pedig egy már bevezetett nemzeti rendszer eredményességét méri.

6. Új TUDOMÁNYOS EREDMÉNYEK, AZOK GYAKORLATI ALKALMAZHATÓSÁGA

6.1. Új tudományos eredmények

A kutatás elméleti, módszertani és összehasonlító eredményeinek szintézise alapján az alábbi, egymásra épülő új tudományos eredményeket fogalmazom meg:

1. Kidolgoztam a technológiai reziliencia integrált szocio-technikai modelljét, amely a technológiai (T), szervezeti (O) és szabályozási–irányítási (R) dimenziókat nem elkülönült tényezőkként, hanem egymással kölcsönhatásban álló rendszerként értelmezi.

Kimutattam, hogy a technológiai reziliencia rendszerszintű minőségét nem önmagában az egyes dimenziók fejlettsége, hanem a közöttük fennálló kapcsolatok, interfészek és visszacsatolások is meghatározzák.

A modell hozzáadott értéke, hogy egységes elemzési térbe helyezi a műszaki architektúra, a szervezeti adaptáció és a governance kérdését. Ez lehetővé teszi olyan reziliencia gyengeségek azonosítását is, amelyek hagyományos technikai vagy compliance-értékelésben rejtve maradnának.

A modell tudományos újdonsága nem önmagában a technológiai, szervezeti és szabályozási–irányítási dimenziók elkülönítésében áll, hanem azok kölcsönhatásainak és interdimenzionális szűk keresztmetszeteinek egységes rendszerben történő értelmezésében. A modell ezáltal a technológiai rezilienciát nem elkülönült tényezők összességeként, hanem a három dimenzió kölcsönhatásából kialakuló rendszerképességként értelmezi.

2. Kidolgoztam az Adaptív Technológiai Reziliencia Ciklust (B-ATR-ciklus), amely a háromdimenziós modell időbeli működését az érzékelés, értékelés, adaptáció, stabilizáció, valamint tanulás és innováció egymásba kapcsolódó szakaszaival írja le.

A ciklus révén a reziliencia nem statikus állapotként, hanem ismétlődő, visszacsatolásokon alapuló fejlődési folyamatként értelmezhető.

Ehhez kapcsolódóan kialakítottam a TRI technológiai rezilienciaprofil és az ötfokozatú TRMM érettségi modell koncepcionális értékelési architektúráját. A megközelítés a rezilienciát nem egyetlen aggregált számmá redukálja, hanem a dimenziók,

kapcsolatok és dinamikus képességek állapotát együttesen teszi értékelhetővé. A keret ezáltal diagnosztikai, összehasonlító és fejlesztéstervezési célokra használható.

3. Bebizonyítottam, hogy a konkrét technológiai megoldások és szabályozási környezetek különbözősége ellenére a technológiai reziliencia alapvető szerkezete azonos T–O–R logika szerint írható le.

Egyúttal kimutattam, hogy a reziliencia értékelésének elemzési egysége nem korlátozható az egyes szervezetre vagy infrastruktúrára, mert a külső technológiai és szolgáltatási interdependenciák érdemben meghatározzák annak működőképességét.

Eredményként a technológiai rezilienciát system of systems jellegű képességként értelmeztem, amelyben a kaszkádhatások, a civil–katonai függőségek és az ágazatközi szolgáltatási kapcsolatok az értékelés szerves részét képezik. Ez teremti meg az átmenetet az ágazati rezilienciától a nemzeti technológiai reziliencia fogalmához.

4. Kidolgoztam a Nemzeti Technológiai Reziliencia Irányítási Keretrendszer (NTRGF) koncepcióját, amely a technológiai rezilienciát nemzeti stratégiai képességként kezeli.

A keretrendszer összekapcsolja a kritikus infrastruktúrák, a digitális transzformáció, a kiberbiztonság, a védelmi követelmények, az ipar, az innováció és a nemzeti ellenálló képesség szempontjait, és ezek összehangolását adaptív governance-folyamatként értelmezi.

Az NTRGF tudományos jelentősége abban áll, hogy az ágazati rezilienciafejlesztést egy magasabb, rendszerszintű koordinációs logikába helyezi. A keretrendszer nem centralizált operatív irányítást feltételez, hanem közös értékelési szemléletet, függőségfeltárást, prioritásképzést, információmegosztást, gyakorlatokat, visszacsatolást és folyamatos fejlesztést.

A kutatás hadtudományi következtetése, hogy a technológiai reziliencia nem kizárólag kritikusinfrastruktúra-védelmi vagy kiberbiztonsági kategória, hanem a katonai képesség fenntartásának és alkalmazhatóságának egyik rendszerszintű meghatározója. A modern fegyveres erők civil technológiai infrastruktúráktól és szolgáltatásoktól való függősége miatt a nemzeti technológiai reziliencia egyben a katonai műveleti szabadság, a szövetségi feladatok teljesíthetősége és a kollektív védelem technológiai előfeltétele is.

6.2. Az eredmények gyakorlati alkalmazhatósága

A kutatás eredményeinek gyakorlati jelentősége abból adódik, hogy a modell nem kizárólag elméleti tipológiaként, hanem szervezeti és stratégiai döntéstámogató keretként is értelmezhető. A T–O–R struktúra segítségével egy technológiai rendszer vizsgálata túlterjeszthető a hagyományos műszaki állapotfelmérésen, és azonosíthatók azok a szervezeti vagy governance-hiányosságok is, amelyek technológiai zavar esetén a működőképességet korlátozhatják.

A TRMM alkalmazható kritikus infrastruktúra-üzemeltetők, állami és védelmi szervezetek, valamint komplex digitális rendszerek reziliencia érettségének strukturált felmérésére. Az értékelés alapján meghatározhatók a fejlesztési prioritások, összevethetők különböző szervezeti egységek vagy időszakok, és nyomon követhető, hogy egy fejlesztési program ténylegesen javítja-e a rezilienciát.

A BATR-ciklus gyakorlati felhasználási területe a gyakorlatok, stressztesztek és incidens utáni értékelések tervezése. A rendszer működése nemcsak abból a szempontból vizsgálható, hogy fennmaradt-e egy szolgáltatás, hanem abból is, milyen gyorsan érzékelte a zavart, milyen minőségben értékelte annak hatását, mennyi idő alatt hajtotta végre az adaptációt, hogyan stabilizálta a működést, és milyen változtatásokat vezetett be a tapasztalatok alapján.

A modell a digitális transzformáció és technológiai innováció értékelésében is használható. Egy új mesterségesintelligencia-alapú, autonóm vagy felhőalapú megoldás bevezetése nem kizárólag technikai teljesítménykérdés. Megváltoztatja a munkafolyamatokat, kompetenciaigényeket, adatkezelést, felelősségi viszonyokat és szabályozási követelményeket. A T–O–R elemzés ezért már a fejlesztési és beszerzési döntések során segíthet azonosítani a későbbi reziliencia kockázatokat.

A védelmi alkalmazásban különösen jelentős a civil–katonai függőségek vizsgálata. A katonai C2, logisztika, energiaellátás, kommunikáció, PNT és adatfeldolgozás számos civil vagy kettős felhasználású szolgáltatásra épül. A modell segítségével a katonai képességfejlesztés során nemcsak a saját rendszerek technikai rendelkezésre állása, hanem a kritikus külső függőségek helyettesíthetősége, redundanciája és governance-háttere is értékelhető.

Az NTRGF gyakorlati alkalmazása a nemzeti szintű koordinációt támogathatja. A keretrendszer közös értékelési nyelvet teremthet az ágazatok között, segítheti a keresztfüggőségek feltárását, a nemzeti szintű kritikus technológiai csomópontok azonosítását, valamint a fejlesztési és beruházási prioritások összehangolását. E

megközelítésben a technológiai reziliencia nem kizárólag biztonsági kiadás, hanem a működőképesség, a technológiai szuverenitás és az innováció fenntarthatóságának feltétele.

A kutatás egyik gyakorlati üzenete, hogy a TRMM nem compliance-eszköz. A jogszabályi és szabványkövetelmények teljesítése fontos bemeneti feltétel, de a reziliencia értékelése azt vizsgálja, hogy a rendszer ténylegesen képes-e érzékelni, reagálni, alkalmazkodni, stabilizálódni és tanulni. A megfelelőség ezért a reziliencia szükséges, de nem elégséges feltétele.

A kutatás gyakorlati alkalmazhatóságának egyik lehetséges területe a kötelező kiberbiztonsági auditok és a szélesebb szervezeti reziliencia értékelés összekapcsolása. A TRMM az audit eredményeit bizonyítékalapú bemeneti információként felhasználva kiterjesztheti az értékelést a technológiai megfelelőségről a szervezeti és szabályozási–irányítási képességekre, valamint azok kölcsönhatásaira. A TRI ezek eredményeit integrált rezilienciaprofilként teheti értelmezhetővé a vezetés számára. A megközelítés ezáltal a megfelelőségértékelés eredményeit stratégiai és fejlesztési döntések támogatására is felhasználhatóvá teheti.

6.3. A kutatás korlátai

A kutatás eredményeinek értelmezése során szükséges egyértelműen meghatározni azok érvényességi határait. A disszertáció elsődlegesen elméleti, konceptuális és összehasonlító dokumentumelemzésre épül. A kidolgozott modell tudományos értéke a fogalmi integrációban, az mérhetővé és értékelhetővé tételi logikában és az eltérő szakági környezetekben végrehajtott koncepcionális validációban áll; **a kutatás nem állítja, hogy a TRMM valamennyi indikátora nagymintás empirikus mérésben már statisztikailag validált**.

A második korlát az ágazati lefedettség. A vizsgált kritikus infrastruktúra-rendszerek tudatosan eltérő működési logikájú területeket képviselnek, ami alkalmas a modell transzferálhatóságának vizsgálatára, de nem jelenti valamennyi kritikus ágazat teljes körű elemzését. További ágazatok bevonása pontosíthatja az általános és ágazatspecifikus indikátorok közötti határvonalat.

A harmadik korlát a mérési rendszer részletezettsége. A TRI és TRMM jelen formájában koncepcionális és módszertani keret. Az indikátorok súlyozása, a küszöbértékek meghatározása, az értékelők közötti megbízhatóság és az időbeli összehasonlíthatóság

további empirikus vizsgálatot igényel. Különösen fontos annak elkerülése, hogy a későbbi számszerűsítés elfedje a dimenziók közötti kritikus gyengeségeket.

A negyedik korlát az NTRGF intézményi státusza. A keretrendszer a disszertációban tudományosan levezetett koncepcionális governance-javaslatként jelenik meg. Nem egy már bevezetett és hatásvizsgálattal értékelt államigazgatási rendszer. Gyakorlati implementációjához további jogi, szervezeti, felelősségi, adatmegosztási és erőforrás-elemzés szükséges.

Végül a technológiai környezet gyors változása önmagában is korlátot jelent. A mesterséges intelligencia, autonóm rendszerek, kvantumtechnológiák, űrszolgáltatások, felhőarchitektúrák és kiberfenyegetések fejlődése miatt az indikátorkészlet nem tekinthető véglegesnek. A modell tartósságát ezért nem az egyes technológiák felsorolása, hanem a T–O–R szerkezet és az adaptív értékelési logika biztosíthatja.

6.4. További kutatási irányok

A disszertáció eredményei több közvetlen további kutatási és gyakorlati alkalmazási irányt jelölnek ki. Elsőként indokolt a TRMM empirikus tesztelése konkrét szervezetekben és infrastruktúra-rendszerekben. Magyarországon elsődleges alkalmazási területként a honvédelmi és a katonai működést közvetlenül támogató rendszereket javaslom. **A Magyar Honvédség esetében a modell alkalmazható lenne a vezetési és irányítási (C2), kommunikációs és információs, logisztikai, műveleti energiaellátási, valamint felderítést és helyzetismeretet támogató technológiai rendszerek rezilienciájának értékelésére.** Különösen indokoltnak tartom olyan **képességek vizsgálatát, amelyek működése jelentős mértékben függ civil infrastruktúráktól, kereskedelmi szolgáltatóktól vagy több technológiai rendszer egyidejű rendelkezésre állásától.** A TRMM gyakorlati tesztelése ebben a környezetben lehetőséget teremtene annak vizsgálatára, hogy az indikátorok és az érettségi szintek mennyiben **képesek feltárni a katonai működőképességet és a műveleti folytonosságot veszélyeztető technológiai, szervezeti és irányítási hiányosságokat.**

A katonai alkalmazás mellett indokolt a modell tesztelése **a honvédelmi feladatok szempontjából kritikus civil infrastruktúrákban** is. Ilyen alkalmazási környezetet jelenthetnek a villamosenergia-rendszer kijelölt elemei, az elektronikus hírközlési infrastruktúrák, az országos és regionális adatközponti és felhőszolgáltatások, valamint a katonai mobilitás szempontjából meghatározó közúti és vasúti infrastruktúrák. Ezek vizsgálata lehetővé tenné annak értékelését is, hogy a civil infrastruktúrák technológiai

rezilienciájának szintje milyen mértékben befolyásolja a katonai képességek rendelkezésre állását, a befogadó nemzeti támogatást és a szövetségi feladatok végrehajthatóságát.

Második kutatási irány az ágazatspecifikus TRMM-értékelési jellemzők kidolgozása. A közös T–O–R struktúra megtartása mellett külön értékelési profil kialakítását javaslom az energetikai, közlekedési, elektronikus hírközlési, egészségügyi, védelmi ipari és katonai C2-rendszerek számára. Katonai alkalmazás esetén az értékelési jellemzők között hangsúlyosan meg kell jeleníteni a műveleti rendelkezésre állást, a redundanciát, a degradált működési képességet, az interoperabilitást, a vezetés folytonosságát, a civil infrastruktúráktól való függőséget, valamint az ellenséges behatásokkal szembeni alkalmazkodóképességet. Ez egyszerre biztosíthatná az ágazati szakmai pontosságot és a különböző rendszerek nemzeti szintű összehasonlíthatóságát.

Harmadik irány a BATR dinamikus indikátorainak empirikus vizsgálata. Ennek elsődleges környezetét olyan nemzeti és NATO-gyakorlatok jelenthetik, amelyekben technológiai zavarok, kibertámadások, kommunikációs kiesések, GNSS/PNT-zavarás, energiaellátási problémák vagy több rendszer egyidejű degradációja jelenik meg. A gyakorlatok során mérhetővé válhat az észlelési idő, a döntési sebesség, az adaptáció végrehajtási ideje, a kritikus funkciók fenntartásának képessége, a stabilizációhoz és helyreállításhoz szükséges idő, valamint a tanulságok szervezeti és technológiai beépítésének eredményessége. A BATR ilyen alkalmazása a hagyományos gyakorlatértékelést kiegészíthetné a technológiai reziliencia dinamikus teljesítményének mérésével.

Negyedik kutatási irány az interdependenciák hálózati modellezése. Ennek gyakorlati alkalmazását elsőként a honvédelmi feladatok szempontjából kritikus civil–katonai függőségek feltérképezésében javaslom. A katonai C2, az energiaellátás, az elektronikus hírközlés, az adat- és felhőszolgáltatások, a PNT-szolgáltatások, a közlekedési infrastruktúra és a logisztikai ellátási láncok közötti kapcsolatok gráfalapú vagy digitális ikerrel támogatott modellezése lehetővé teheti azon kritikus csomópontok, egyedi hibapontok és kaszkádhatási útvonalak azonosítását, amelyek kiesése aránytalanul nagy hatást gyakorolhat a katonai működőképességre. E módszer különösen hasznos lehet a befogadó nemzeti támogatás, a katonai mobilitás és a többdoménes műveletek technológiai feltételrendszerének vizsgálatában.

Ötödik irány a mesterséges intelligencia alkalmazása a reziliencia értékelésében. Az MI támogathatja az anomáliák felismerését, a technológiai és szervezeti függőségi mintázatok azonosítását, a lehetséges kaszkádhatások előrejelzését, a

forgatókönyv-elemzést és a dinamikus rezilienciaprofil frissítését. Katonai környezetben külön kutatási területet jelenthet annak vizsgálata, hogy az MI-alapú döntéstámogatás miként alkalmazható a technológiai degradáció műveleti következményeinek előrejelzésére. Ezzel párhuzamosan azonban magának az MI-nek a rezilienciája, adatfüggősége, modellkockázata és irányítása is a T–O–R értékelés tárgyává válik.

Hatodik irány az NTRGF intézményi és jogi alkalmazhatóságának vizsgálata. Magyarország esetében ennek első lépéseként a honvédelmi, katasztrófavédelmi, kiberbiztonsági, kritikusinfrastruktúra-védelmi, közlekedési, energetikai és hírközlési szereplők közötti felelősségi, döntési és információáramlási kapcsolatok feltérképezését javaslom. Ennek alapján vizsgálható, hogy a jelenlegi intézményrendszerben hol találhatók koordinációs hiányok, párhuzamosságok vagy tisztázatlan felelősségi határok. Kiemelt kutatási kérdésként indokolt vizsgálni a Honvédelmi Minisztérium és a Magyar Honvédség, valamint a katonai működést támogató civil infrastruktúrák és szolgáltatók közötti reziliencia-koordináció intézményi lehetőségeit. Az NTRGF alkalmazásának célja ebben az esetben nem újabb párhuzamos intézmény létrehozása, hanem a meglévő szereplők közötti stratégiai koordináció és közös helyzetértékelés erősítése.

Végül indokolt a modell nemzetközi összehasonlító alkalmazhatóságának vizsgálata. Első lépésként a NATO keleti szárnyának olyan tagállamaiban lenne célszerű összehasonlító vizsgálatot végezni, amelyek hasonló biztonsági kihívásokkal, ugyanakkor eltérő kritikusinfrastruktúra-, haderő- és intézményi struktúrával rendelkeznek. Azonos T–O–R és TRMM értékelési logika alkalmazása lehetővé tenné annak vizsgálatát, hogy mely reziliencia mintázatok tekinthetők nemzeti sajátosságnak, és melyek mutatnak általánosabb, szövetségi szinten is értelmezhető összefüggéseket. Az eredmények hosszabb távon hozzájárulhatnak a NATO- és EU-szintű technológiai reziliencia értékelési megközelítések továbbfejlesztéséhez.

A felsorolt további kutatási irányok közül elsődleges gyakorlati prioritásnak a katonai C2-rendszerek és az azok működését támogató civil technológiai infrastruktúrák együttes, TRMM-alapú empirikus értékelését tekintem. Ez közvetlen folytatását jelentené a disszertációban elvégzett analitikai validációnak, és egyidejűleg teremtene lehetőséget a modell gyakorlati alkalmazhatóságának, a civil–katonai technológiai függőségeknek, valamint a technológiai reziliencia katonai műveleti képességre gyakorolt hatásának vizsgálatára. Második lépésként a módszert valós vagy gyakorlati környezetben végrehajtott, BATR-alapú dinamikus reziliencia értékeléssel, harmadik lépésként pedig az NTRGF nemzeti szintű alkalmazhatóságának vizsgálatával

javaslom továbbfejleszteni. E három egymásra épülő kutatási lépés az elméleti modellalkotástól a szervezeti és műveleti szintű empirikus vizsgálaton keresztül a nemzeti szintű alkalmazhatóságig terjesztené ki a jelen értekezés eredményeit.

6.5. Záró következtetések

A disszertáció alapvető következtetése, hogy a technológiai reziliencia nem tekinthető kizárólag technológiai vagy kiberbiztonsági képességnek. A modern társadalmak, kritikus infrastruktúrák és védelmi rendszerek működőképessége olyan szocio-technikai környezetben jön létre, amelyben a technológiai architektúra, a szervezeti működés és a szabályozási–irányítási rendszer egymást kölcsönösen feltételezi. A reziliencia ezért e három dimenzió együttes tulajdonsága.

A kutatás azt is megmutatta, hogy a reziliencia nem statikus állapot. Egy rendszer nem azért reziliens, mert egy adott időpontban megfelel bizonyos követelményeknek, hanem azért, mert képes a környezet változásait érzékelni, azok jelentőségét értékelni, működését adaptálni, a kritikus funkciókat stabilizálni, majd a tapasztalatokat tartós fejlődéssé alakítani. A BATR-ciklus ezt az időbeli működést teszi explicitté, a TRI és TRMM pedig annak strukturált értékeléséhez biztosít keretet.

Az ágazati összehasonlítás eredménye alapján a technológiai reziliencia nem zárható az egyes infrastruktúrák szervezeti vagy szabályozási határai közé. A rendszerek közötti kölcsönös függőségek miatt a reziliencia egyre inkább nemzeti technológiai ökoszisztéma-szintű kérdés. A civil energia-, közlekedési, kommunikációs, digitális és űralapú szolgáltatások, valamint a katonai képességek közötti kapcsolatok azt jelentik, hogy egy ágazat sérülékenysége más ágazatok működőképességét is korlátozhatja.

Ebből következik, hogy a technológiai reziliencia fejlesztése sem valósítható meg kizárólag elkülönült ágazati programokkal. Szükség van közös értékelési szemléletre, a kritikus interdependenciák láthatóvá tételére, a fejlesztési prioritások összehangolására és olyan adaptív governance-ra, amely a tapasztalatokat folyamatosan visszavezeti a technológiai, szervezeti és szabályozási fejlesztésekbe. Az NTRGF ennek a stratégiai következtetésnek a szervező kerete.

A technológiai fejlődés önmagában tehát nem teszi rezilienssé sem a társadalmat, sem az államot, sem a fegyveres erőt. Valódi technológiai reziliencia akkor jön létre, ha a korszerű technológiai képességekhez alkalmazkodó szervezetek, felkészült emberek, adaptív irányítás, tanulási képesség és a kölcsönös függőségeket

felismerő stratégiai szemlélet társul. A technológiai reziliencia ebben az értelemben nem végállapot, hanem folyamatosan fejlesztendő nemzeti képesség.

FELHASZNÁLT IRODALOM JEGYZÉKE

Az online elérhetőségek ellenőrzésének dátuma: 2026. augusztus 17.

[1] HOLLING, Crawford S.: Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics, 4. (1973), 1–23. DOI: 10.1146/annurev.es.04.110173.000245. Elérhető: https://doi.org/10.1146/annurev.es.04.110173.000245

[2] MASTEN, Ann S.: Ordinary Magic: Resilience Processes in Development. American Psychologist, 56. évf. 3. sz. (2001), 227–238. DOI: 10.1037/0003-066X.56.3.227. Elérhető: https://doi.org/10.1037/0003-066X.56.3.227

[3] LENGNICK-HALL, Cynthia A. – BECK, Tammy E. – LENGNICK-HALL, Mark L.: Developing a Capacity for Organizational Resilience through Strategic Human Resource Management. Human Resource Management Review, 21. évf. 3. sz. (2011), 243–255. DOI: 10.1016/j.hrmr.2010.07.001. Elérhető: https://doi.org/10.1016/j.hrmr.2010.07.001

[4] DUCHEK, Stephanie: Organizational Resilience: A Capability-Based Conceptualization. Business Research, 13. (2020), 215–246. DOI: 10.1007/s40685-019-0085-7. Elérhető: https://doi.org/10.1007/s40685-019-0085-7

[5] BOIN, Arjen – VAN EETEN, Michel J. G.: The Resilient Organization. Public Management Review, 15. évf. 3. sz. (2013), 429–445. DOI: 10.1080/14719037.2013.769856. Elérhető: https://doi.org/10.1080/14719037.2013.769856

[6] HOLLAND, John H.: Complex Adaptive Systems. Daedalus, 121. évf. 1. sz. (1992), 17–30.

[7] MITCHELL, Melanie: Complexity: A Guided Tour. New York: Oxford University Press, 2009.

[8] PERROW, Charles: Normal Accidents: Living with High-Risk Technologies. Princeton: Princeton University Press, 1984.

[9] KRUCHTEN, Philippe – NORD, Robert L. – OZKAYA, Ipek: Technical Debt: From Metaphor to Theory and Practice. IEEE Software, 29. évf. 6. sz. (2012), 18–21. DOI: 10.1109/MS.2012.167. Elérhető: https://doi.org/10.1109/MS.2012.167

[10] TRIST, Eric L. – BAMFORTH, Ken W.: Some Social and Psychological Consequences of the Longwall Method of Coal-Getting. Human Relations, 4. évf. 1. sz. (1951), 3–38. DOI: 10.1177/001872675100400101. Elérhető: https://doi.org/10.1177/001872675100400101

[11] BAXTER, Gordon – SOMMERVILLE, Ian: Socio-technical Systems: From Design Methods to Systems Engineering. Interacting with Computers, 23. évf. 1. sz. (2011), 4–17. DOI: 10.1016/j.intcom.2010.07.003. Elérhető: https://doi.org/10.1016/j.intcom.2010.07.003

[12] HOLLNAGEL, Erik – WOODS, David D. – LEVESON, Nancy (eds.): Resilience Engineering: Concepts and Precepts. Aldershot: Ashgate, 2006.

[13] WOODS, David D.: Four Concepts for Resilience and the Implications for the Future of Resilience Engineering. Reliability Engineering & System Safety, 141. (2015), 5–9. DOI: 10.1016/j.ress.2015.03.018. Elérhető: https://doi.org/10.1016/j.ress.2015.03.018

[14] MADNI, Azad M. – JACKSON, Scott: Towards a Conceptual Framework for Resilience Engineering. IEEE Systems Journal, 3. évf. 2. sz. (2009), 181–191. DOI: 10.1109/JSYST.2009.2017397. Elérhető: https://doi.org/10.1109/JSYST.2009.2017397

[15] LINKOV, Igor – KOTT, Alexander: Fundamental Concepts of Cyber Resilience: Introduction and Overview. IEEE Systems Journal, 13. évf. 1. sz. (2019), 1–3. DOI: 10.1109/JSYST.2018.2880647. Elérhető: https://doi.org/10.1109/JSYST.2018.2880647

[16] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST, 2018. DOI: 10.6028/NIST.CSWP.04162018. Elérhető: https://doi.org/10.6028/NIST.CSWP.04162018

[17] VUGRIN, Eric D. – WARREN, Drake E. – EHLEN, Mark A.: A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane. Process Safety Progress, 30. évf. 3. sz. (2011), 280–290. DOI: 10.1002/prs.10437. Elérhető: https://doi.org/10.1002/prs.10437

[18] BARABÁSI, Albert-László: Network Science and Resilience. Nature Physics, 12. (2016), 901–902. DOI: 10.1038/nphys3928. Elérhető: https://doi.org/10.1038/nphys3928

[19] SHEFFI, Yossi – RICE, James B.: A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Review, 47. évf. 1. sz. (2005), 41–48.

[20] KOVÁCS László: Kiberbiztonság és stratégia. Budapest: Dialóg Campus Kiadó, 2018.

[21] HAIG Zsolt – KOVÁCS László: Kritikus információs infrastruktúrák elleni fenyegetések és védelmük. In: Az informatikai biztonság kézikönyve. Budapest: Dashöfer, 2008.

[22] KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010/1., 44–56.

[23] NATO: NATO 2022 Strategic Concept. Brussels: North Atlantic Treaty Organization, 2022. Elérhető: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

[24] OECD: Building Resilience: New Strategies for Strengthening Infrastructure Resilience and Maintenance. OECD Public Governance Policy Papers, No. 5. Paris: OECD Publishing, 2021. DOI: 10.1787/354aa2aa-en. Elérhető: https://doi.org/10.1787/354aa2aa-en

[25] EUROPEAN PARLIAMENT AND COUNCIL: Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 27 December 2022, 80–152. Elérhető: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[26] EUROPEAN PARLIAMENT AND COUNCIL: Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive). Official Journal of the European Union, L 333, 27 December 2022, 164–198. Elérhető: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[27] EUROPEAN PARLIAMENT AND COUNCIL: Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union, 2024/2847. Elérhető: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[28] KOVÁCS László: National Cybersecurity Strategy Framework. AARMS – Academic and Applied Research in Military and Public Management Science, 18. évf. 2. sz. (2019), 65–76. DOI: 10.32565/aarms.2019.2.6. Elérhető: https://doi.org/10.32565/aarms.2019.2.6

[29] KRASZNAY Csaba: Kiberbiztonság a negyedik ipari forradalom korában. Híradástechnika, 74. évf. 1. sz. (2019), 25–29.

[30] RINALDI, Steven M. – PEERENBOOM, James P. – KELLY, Terrence K.: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 21. évf. 6. sz. (2001), 11–25. DOI: 10.1109/37.969131. Elérhető: https://doi.org/10.1109/37.969131

[31] OUYANG, Min: Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. Reliability Engineering & System Safety, 121. (2014), 43–60. DOI: 10.1016/j.ress.2013.06.040. Elérhető: https://doi.org/10.1016/j.ress.2013.06.040

[32] WEICK, Karl E. – SUTCLIFFE, Kathleen M.: Managing the Unexpected: Sustained Performance in a Complex World. 3rd ed. San Francisco: Jossey-Bass, 2015.

[33] TEECE, David J.: Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance. Strategic Management Journal, 28. évf. 13. sz. (2007), 1319–1350. DOI: 10.1002/smj.640. Elérhető: https://doi.org/10.1002/smj.640

[34] ARGYRIS, Chris – SCHÖN, Donald A.: Organizational Learning: A Theory of Action Perspective. Reading, MA: Addison-Wesley, 1978.

[35] NONAKA, Ikujiro – TAKEUCHI, Hirotaka: The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press, 1995.

[36] NATO: Strengthened Resilience Commitment. Brussels, 14 June 2021. Elérhető: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/strengthened-resilience-commitment

[37] NATO ALLIED COMMAND TRANSFORMATION: Strategic Foresight Analysis 2023. Norfolk: Allied Command Transformation, 2023. Elérhető: https://www.act.nato.int/activities/allied-command-transformation-strategic-foresight-work/

[38] NATO ALLIED COMMAND TRANSFORMATION: NATO Warfighting Capstone Concept. Norfolk: Allied Command Transformation, 2021. Elérhető: https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/

[39] NATO SCIENCE AND TECHNOLOGY ORGANIZATION: Science & Technology Trends 2023–2043: Exploring the S&T Edge. Brussels: NATO STO, 2023.

[40] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: NIST, 2024. DOI: 10.6028/NIST.CSWP.29. Elérhető: https://doi.org/10.6028/NIST.CSWP.29

[41] EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA: ENISA Threat Landscape 2024. Athens–Heraklion: ENISA, 2024. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[42] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Artificial Intelligence Risk Management Framework (AI RMF [46] 1.0). NIST AI 100-1. Gaithersburg, MD: NIST, 2023. DOI: 10.6028/NIST.AI.100-1. Elérhető: https://doi.org/10.6028/NIST.AI.100-1

[43] EUROPEAN PARLIAMENT AND COUNCIL: Regulation (EU) 2024/1252 of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials. Official Journal of the European Union, 2024/1252, 3 May 2024. Elérhető: https://eur-lex.europa.eu/eli/reg/2024/1252/oj

[44] EUROPEAN COMMISSION – HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY: Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy". JOIN(2023) 20 final. Brussels, 20 June 2023. Elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0020

[45] EUROPEAN PARLIAMENT AND COUNCIL: Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024/1689. Elérhető: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[46] AI RMF: Artificial Intelligence Risk Management Framework; magyarul: mesterségesintelligencia-kockázatkezelési keretrendszer.

[46] NATO – EUROPEAN UNION: Final Assessment Report of the NATO-EU Task Force on the Resilience of Critical Infrastructure. 2023. Elérhető: https://www.nato.int/en/news-and-events/articles/news/2023/06/29/nato-and-european-union-release-final-assessment-report-on-resilience-of-critical-infrastructure

[47] LINKOV, Igor – TRUMP, Benjamin D. (eds.): The Science and Practice of Resilience. Cham: Springer, 2019. DOI: 10.1007/978-3-030-04565-4. Elérhető: https://doi.org/10.1007/978-3-030-04565-4

[48] KOVÁCS László: Offenzív kiberműveletek II.: Kibererők és képességeik. Hadmérnök, 16. évf. 3. sz. (2021), 119–137. DOI: 10.32567/hm.2021.3.7. Elérhető: https://doi.org/10.32567/hm.2021.3.7

[49] HAIG Zsolt: Információs műveletek a kibertérben. Budapest: Dialóg Campus Kiadó, 2018.

[50] HAIG Zsolt: Kibertéri kognitív befolyásolás az információs műveletekben. Hadtudományi Szemle, 15. évf. 2. sz. (2022). DOI: 10.32563/hsz.2022.2.7. Elérhető: https://doi.org/10.32563/hsz.2022.2.7

[51] KRASZNAY Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. Nemzet és Biztonság, 10. évf. 3. sz. (2017), 38–53. Elérhető: https://folyoirat.ludovika.hu/index.php/neb/article/view/3718

[52] MAGYAR Sándor: Tudás vagy attitűd? Az emberi tényező fejlesztésének dilemmái a kiberbiztonságban. Előadás, HTE Információbiztonsági Szakosztály – EIVOK, 2025.

[53] GYEBNÁR Gergő – MAGYAR Sándor: Consumption of Technical Threat Intel Indicators. In: 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), 177–182. IEEE, 2025. DOI: 10.1109/SAMI63904.2025.10883294. Elérhető: https://doi.org/10.1109/SAMI63904.2025.10883294

[54] NÉGYESI Imre – TÓTH András (szerk.): International Scientific Conference on Military Information Security 2024. Budapest: University of Public Service, Signal Department, 2024. HU ISSN 2061-9499. Elérhető: https://comconf.hu/kiadvany/International%20Scientific%20Conference%20on%20Military%20Information%20Security_2024.pdf

[55] BALOGH Péter: Technológiai reziliencia a digitális és kritikus infrastruktúrák védelmében. Elméleti keretek, módszertani megközelítések és stratégiai implikációk. Hadtudományi Szemle, 2027/1., megjelenés alatt. Budapest: Nemzeti Közszolgálati Egyetem – Ludovika Egyetemi Kiadó. ISSN 2060-0437 (online).

[56] HOLLNAGEL, Erik: Prologue: The Scope of Resilience Engineering. In: HOLLNAGEL, Erik – PARIÈS, Jean – WOODS, David D. – WREATHALL, John (eds.): Resilience Engineering in Practice: A Guidebook. Farnham: Ashgate, 2011, 3–16.

[57] LEVESON, Nancy G.: Safeware: System Safety and Computers. Reading, MA: Addison-Wesley, 1995.

[58] LINKOV, Igor – EISENBERG, Daniel A. – BATES, Matthew E. – CHANG, Derek – CONVERTINO, Matteo – ALLEN, James H. – FLYNN, Stephen E. – SEAGER, Thomas P.: Measurable Resilience for Actionable Policy. Environmental Science & Technology, 47. évf. 18. sz. (2013), 10108–10110. DOI: 10.1021/es403443n. Elérhető: https://doi.org/10.1021/es403443n

[59] LENGNICK-HALL, Cynthia A. – BECK, Tammy E.: Adaptive Fit Versus Robust Transformation: How Organizations Respond to Environmental Change. Journal of Management, 31. évf. 5. sz. (2005), 738–757. DOI: 10.1177/0149206305279367. Elérhető: https://doi.org/10.1177/0149206305279367

[60] NATO: Resilience, Civil Preparedness and Article 3. North Atlantic Treaty Organization, 2024. Elérhető: https://www.nato.int/cps/en/natohq/topics_132722.htm

[61] ROEPKE, Wolf-Diether – THANKEY, Hasit: Resilience: The First Line of Defence. NATO Review, 27 February 2019. Elérhető: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

[62] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – ENISA: Smart Grid Threat Landscape and Good Practice Guide. Heraklion: ENISA, 2013. Elérhető: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

[63] EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA: ENISA Transport Threat Landscape. ENISA, 21 March 2023. Elérhető: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

[64] EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA: ENISA Threat Landscape 2023. ENISA, 19 October 2023. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[65] EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA: ENISA NIS360 2024: A Comprehensive Look at Cybersecurity Maturity and Criticality of NIS2 Sectors. ENISA, 5 March 2025. Elérhető: https://www.enisa.europa.eu/publications/enisa-nis360-2024

[66] EUROPEAN PARLIAMENT AND COUNCIL: Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333, 27 December 2022, 1–79. Elérhető: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[67] EUROPEAN COMMISSION: Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. Official Journal of the European Union, 2024/1366, 24 May 2024. CELEX: 32024R1366. Elérhető: https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj

[68] YIN, Robert K.: Case Study Research and Applications: Design and Methods. 6th ed. Thousand Oaks, CA: SAGE Publications, 2018.

[69] EISENHARDT, Kathleen M.: Building Theories from Case Study Research. Academy of Management Review, 14. évf. 4. sz. (1989), 532–550. DOI: 10.5465/amr.1989.4308385. Elérhető: https://doi.org/10.5465/amr.1989.4308385

[70] FLYVBJERG, Bent: Five Misunderstandings About Case-Study Research. Qualitative Inquiry, 12. évf. 2. sz. (2006), 219–245. DOI: 10.1177/1077800405284363. Elérhető: https://doi.org/10.1177/1077800405284363

[71] EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA: Railway Cybersecurity – Good Practices in Cyber Risk Management. ENISA, 25 November 2021. Elérhető: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

[72] EUROPEAN UNION AGENCY FOR RAILWAYS – ERA: Report on Railway Safety and Interoperability in the EU 2026. Valenciennes: European Union Agency for Railways, 2026. Elérhető: https://www.era.europa.eu/content/report-railway-safety-and-interoperability-eu-2026

[73] NEMZETI MÉDIA- ÉS HÍRKÖZLÉSI HATÓSÁG – NMHH: Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2025 – üzleti felmérés. Budapest: NMHH, 2026. június 23. Elérhető: https://nmhh.hu/cikk/260213/Az_elektronikus_hirkozlesi_piac_fogyasztoinak_vizsgalata_2025__uzleti_felmeres

[74] NATO STANDARDIZATION OFFICE: AJP-3.2, Allied Joint Doctrine for Land Operations. Edition B, Version 1. Brussels: NATO Standardization Office, 2022.

[75] NATO STANDARDIZATION OFFICE: ATP-3.2.2, Command and Control of Allied Land Forces. Brussels: NATO Standardization Office.

[76] SIMON, Herbert A.: The Architecture of Complexity. Proceedings of the American Philosophical Society, 106. évf. 6. sz. (1962), 467–482.

[77] HOLLAND, John H.: Studying Complex Adaptive Systems. Journal of Systems Science and Complexity, 19. (2006), 1–8. DOI: 10.1007/s11424-006-0001-z. Elérhető: https://doi.org/10.1007/s11424-006-0001-z

[78] GYEBNÁR Gergő – HEGEDŰS Ferenc – NÉGYESI Imre – MAGYAR Sándor: Network Security Monitoring for the Electric Sector. Acta Polytechnica Hungarica, 23. évf. 8. sz. (2026).

[79] SOBER, Elliott: Ockham's Razors: A User's Manual. Cambridge: Cambridge University Press, 2015.

[80] BALDWIN, Carliss Y. – CLARK, Kim B.: Design Rules, Volume 1: The Power of Modularity. Cambridge, MA: MIT Press, 2000.

[81] OECD: Recommendation of the Council for Agile Regulatory Governance to Harness Innovation. OECD/LEGAL/0464. Paris: Organisation for Economic Co-operation and Development, 2021. Elérhető: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464

[82] BRUNEAU, Michel et al.: A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra, 19(4), 2003, 733–752. DOI: 10.1193/1.1623497. Elérhető: https://doi.org/10.1193/1.1623497

[83] FRANCIS, Royce – BEKERA, Behailu: A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems. Reliability Engineering & System Safety, 121, 2014, 90–103. DOI: 10.1016/j.ress.2013.07.004. Elérhető: https://doi.org/10.1016/j.ress.2013.07.004

[84] LABAKA, Leire – HERNANTES, Josune – SARRIEGI, Jose M.: A Holistic Framework for Building Critical Infrastructure Resilience. Technological Forecasting and Social Change, 103, 2016, 21–33. DOI: 10.1016/j.techfore.2015.11.005. Elérhető: https://doi.org/10.1016/j.techfore.2015.11.005

[85] LABAKA, Leire – HERNANTES, Josune – SARRIEGI, Jose M.: Resilience Framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant. Reliability Engineering & System Safety, 141, 2015, 92–105. DOI: 10.1016/j.ress.2015.03.009. Elérhető: https://doi.org/10.1016/j.ress.2015.03.009

[86] LAUGÉ, Ana – HERNANTES, Josune – SARRIEGI, Jose M.: Critical Infrastructure Dependencies: A Holistic, Dynamic and Quantitative Approach. International Journal of Critical Infrastructure Protection, 8, 2015, 16–23. DOI: 10.1016/j.ijcip.2014.12.004. Elérhető: https://doi.org/10.1016/j.ijcip.2014.12.004

[87] CURT, Corinne – TACNET, Jean-Marc: Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. Risk Analysis, 38(11), 2018, 2441–2458. DOI: 10.1111/risa.13166. Elérhető: https://doi.org/10.1111/risa.13166

[88] BHAMRA, Ran – DANI, Samir – BURNARD, Kevin: Resilience: The Concept, a Literature Review and Future Directions. International Journal of Production Research, 49(18), 2011, 5375–5393. DOI: 10.1080/00207543.2011.563826. Elérhető: https://doi.org/10.1080/00207543.2011.563826

[89] BURNARD, Kevin – BHAMRA, Ran: Organisational Resilience: Development of a Conceptual Framework for Organisational Responses. International Journal of Production Research, 49(18), 2011, 5581–5599. DOI: 10.1080/00207543.2011.563827. Elérhető: https://doi.org/10.1080/00207543.2011.563827

[90] WHITMAN, Zach R. et al.: Short-form Version of the Benchmark Resilience Tool (BRT-53). Measuring Business Excellence, 17(3), 2013, 3–14. DOI: 10.1108/MBE-05-2012-0030. Elérhető: https://doi.org/10.1108/MBE-05-2012-0030

[91] ILSEVEN, Ekin – PURANAM, Phanish: Measuring Organizational Resilience as a Performance Outcome. Journal of Organization Design, 10, 2021, 127–137. DOI: 10.1007/s41469-021-00107-1. Elérhető: https://doi.org/10.1007/s41469-021-00107-1

[92] FALEGNAMI, Andrea et al.: Resilience Analysis Grid–Rasch Rating Scale Model for Measuring Organizational Resilience Potential. Applied Sciences, 15(4), 2025, 1695. DOI: 10.3390/app15041695. Elérhető: https://doi.org/10.3390/app15041695

[93] DOMÍNGUEZ-ORTEGA, Juan Manuel – MARYNISSEN, Hugo – ERREA RODRÍGUEZ, María: Development and Early Validation of the Organisational Resilience Assessment Survey (ORAS): A Tool to Measure Organisational Resilience. Journal of Contingencies and Crisis Management, 2026. DOI: 10.1111/1468-5973.70164. Elérhető: https://doi.org/10.1111/1468-5973.70164

[94] KARIMI, Mohammad Hossein – SMITH, Doug – SALEHI, Vahid: Resilience Measurement in Socio-Technical Systems: A Systematic Review. Reliability Engineering & System Safety, 275, 2026, 112816. DOI: 10.1016/j.ress.2026.112816. Elérhető: https://doi.org/10.1016/j.ress.2026.112816

[95] STEINMANN, Patrick – TOBI, Hilde – VAN VOORN, George A. K.: Resilience Metrics for Socio-Ecological and Socio-Technical Systems: A Scoping Review. Systems, 12(9), 2024, 357. DOI: 10.3390/systems12090357. Elérhető: https://doi.org/10.3390/systems12090357

[96] PETTIT, Timothy J. – FIKSEL, Joseph – CROXTON, Keely L.: Ensuring Supply Chain Resilience: Development of a Conceptual Framework. Journal of Business Logistics, 31(1), 2010, 1–21. DOI: 10.1002/j.2158-1592.2010.tb00125.x. Elérhető: https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

[97] PONOMAROV, Serhiy Y. – HOLCOMB, Mary C.: Understanding the Concept of Supply Chain Resilience. The International Journal of Logistics Management, 20(1), 2009, 124–143. DOI: 10.1108/09574090910954873. Elérhető: https://doi.org/10.1108/09574090910954873

[98] CHRISTOPHER, Martin – PECK, Helen: Building the Resilient Supply Chain. The International Journal of Logistics Management, 15(2), 2004, 1–13. DOI: 10.1108/09574090410700275. Elérhető: https://doi.org/10.1108/09574090410700275

[99] GUNDERSON, Lance H. – HOLLING, C. S. (eds.): Panarchy: Understanding Transformations in Human and Natural Systems. Washington, DC: Island Press, 2002. ISBN 978-1-55963-857-9.

[100] BIGGS, Reinette – SCHLÜTER, Maja – SCHOON, Michael L. (eds.): Principles for Building Resilience: Sustaining Ecosystem Services in Social-Ecological Systems. Cambridge: Cambridge University Press, 2015. DOI: 10.1017/CBO9781316014240. Elérhető: https://doi.org/10.1017/CBO9781316014240

[101] MILLER, Fiona et al.: Resilience and Vulnerability: Complementary or Conflicting Concepts? Ecology and Society, 15(3), 2010, 11. DOI: 10.5751/ES-03378-150311. Elérhető: https://doi.org/10.5751/ES-03378-150311

[102] BAHO, Didier L. et al.: A Quantitative Framework for Assessing Ecological Resilience. Ecology and Society, 22(3), 2017, 17. DOI: 10.5751/ES-09427-220317. Elérhető: https://doi.org/10.5751/ES-09427-220317

[103] LEVESON, Nancy G.: Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge, MA: MIT Press, 2012. ISBN 978-0-262-01662-9. Elérhető: https://mitpress.mit.edu/9780262016629/engineering-a-safer-world/

[104] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev. 1. Gaithersburg, MD: NIST, 2021. DOI: 10.6028/NIST.SP.800-160v2r1. Elérhető: https://doi.org/10.6028/NIST.SP.800-160v2r1

[105] KOTT, Alexander – LINKOV, Igor: To Improve Cyber Resilience, Measure It. arXiv preprint, 2021. arXiv:2102.09455. Elérhető: https://arxiv.org/abs/2102.09455

[106] LIGO, Alexandre – KOTT, Alexander – LINKOV, Igor: How to Measure Cyber Resilience of an Autonomous Agent: Approaches and Challenges. arXiv preprint, 2021. arXiv:2102.00528. Elérhető: https://arxiv.org/abs/2102.00528

[107] SEGOVIA-FERREIRA, Mariana – RUBIO-HERNAN, Jose – CAVALLI, Ana Rosa – GARCIA-ALFARO, Joaquin: A Survey on Cyber-Resilience Approaches for Cyber-

Physical Systems. arXiv preprint, 2023. arXiv:2302.05402. Elérhető: https://arxiv.org/abs/2302.05402

[108] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: ISO [47] 22316:2017 Security and Resilience – Organizational Resilience – Principles and Attributes. Geneva: ISO, 2017. Elérhető: https://www.iso.org/standard/50053.html

[109] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: ISO 22301:2019 Security and Resilience – Business Continuity Management Systems – Requirements. Geneva: ISO, 2019. Elérhető: https://www.iso.org/standard/75106.html

[110] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: ISO 31000:2018 Risk Management – Guidelines. Geneva: ISO, 2018. Elérhető: https://www.iso.org/standard/65694.html

[111] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – INTERNATIONAL ELECTROTECHNICAL COMMISSION: ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva: ISO, 2022. Elérhető: https://www.iso.org/standard/27001

[112] ALYAMI, Saleh H. et al.: Developing a Holistic Resilience Framework for Critical Infrastructure Networks of Buildings and Communities in Saudi Arabia. Buildings, 13(1), 2023, 179. DOI: 10.3390/buildings13010179. Elérhető: https://doi.org/10.3390/buildings13010179

[113] SATHURSHAN, Mathavanayakam – SAJA, Aslam – THAMBOO, Julian – HARAGUCHI, Masahiko: Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. Infrastructures, 7(5), 2022, 67. DOI: 10.3390/infrastructures7050067.Elérhető: https://doi.org/10.3390/infrastructures7050067

[47] ISO: International Organization for Standardization; magyarul: Nemzetközi Szabványügyi Szervezet.

A SZERZŐ TÉMÁVAL KAPCSOLATBAN MEGJELENT PUBLIKÁCI48ÓI

Megjelenés előtt álló közlemény

1. BALOGH Péter: Technológiai reziliencia a digitális és kritikus infrastruktúrák védelmében. Elméleti keretek, módszertani megközelítések és stratégiai implikációk. *Hadtudományi Szemle*, 2027/1. Megjelenés előtt.

Megjelent tudományos közlemények

2. BALOGH Péter: Pilóta nélküli felderítő eszközök Észak-Afganisztán felett II. rész. Haditechnika, 49. évf. 4. sz., 2015, pp. 20–26.

3. BALOGH Péter: A katonai célú technikai információgyűjtés/felderítés sajátosságai a 21. században. In: Boda József – Dobák Imre (szerk.): A nemzetbiztonság technikai kihívásai a 21. században. Budapest: Nemzeti Közszolgálati Egyetem Szolgáltató Kft., 2015, pp. 93–108.

4. BALOGH Péter: Felderítő szenzorok a pilóta nélküli repülésben. Robothadviselés 2015 Tudományos Konferencia, NKE HHK, 2015. november 26.

5. BALOGH Péter: Felderítés-hírszerzés az afganisztáni hadszíntéren. In: Boldizsár Gábor – Wagner Péter (szerk.): A Magyar Honvédség befejezett szárazföldi műveletei Afganisztánban: Tapasztalatgyűjtemény. Budapest: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, 2014, pp. 73–93.

6. BALOGH Péter: Tapasztalatok a NATO hadműveletekben: az Operation Unified Protector (Líbia 2011). Felderítő Szemle, 13. évf. 1. sz., 2014, pp. 142–191.

7. BALOGH Péter: A békefenntartás során szerzett tapasztalatok a harcászati-hadműveleti felderítéssel kapcsolatban. Felderítő Szemle, 13. évf. 4. sz., 2014, pp. 146–164.

8. BALOGH Péter: A SIGINT[49] és ESM kihívásai a Magyar Honvédség 21. századi békefenntartó műveleteiben. In: Kiss Petra (szerk.): A hadtudomány és a

[49] SIGINT: Signals Intelligence; magyarul: jelhírszerzés / rádióelektronikai felderítés.

21. század: Konferenciakötet. Budapest: Doktoranduszok Országos Szövetsége, 2014, pp. 61–78. Az MTMT tudományos konferenciaközleményként tartja nyilván.

9. BALOGH Péter: Az Operation Unified Protector felderítő tapasztalatai. Hadtudomány, 23. évf. 1. sz., 2013, pp. 92–112.

10. BALOGH Péter: Rádióelektronikai (jel)-felderítés. In: Kobolka István (szerk.): Nemzetbiztonsági alapismeretek. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013, pp. 122–144.

11. BALOGH Péter: Az elektronikai támogatás és a SIGINT helyzete a Magyar Honvédségben. Felderítő Szemle, 12. évf. 1. sz., 2013, pp. 58–100. Az MTMT két független hivatkozást is jelez a közleményhez.

12. BALOGH Péter: A Szövetségi felderítőrendszer korszerűsítése, avagy néhány gondolat a NATO földfelszín felderítő rendszerének megteremtéséről. Felderítő Szemle, 12. évf., február, 2013, pp. 126–139.

13. BALOGH Péter: In the Focus: NATO Alliance Ground Surveillance System. Academic and Applied Research in Military and Public Management Science, Vol. 12, No. 2, 2013, pp. 165–179. DOI: 10.32565/aarms.2013.2.1.

14. BALOGH Péter: Repülő robotok a NATO szolgálatában: AGS. Robothadviselés 2013 Tudományos Konferencia, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, 2013. november 27.

15. BALOGH Péter: A Magyar Honvédség ISTAR[50] (ISR) képességei, a fejlesztés lehetséges irányai, különös tekintettel az elektronikai hadviselésre. Hadmérnök, 7. évf. 4. sz., 2012, pp. 75–94.

16. BALOGH Péter: Elektronikai felderítő eszközök: szenzorok, mint a katona egyéni felszerelésének részei. Hadmérnök, 7. évf. 3. sz., 2012, pp. 100–113.

17. BALOGH Péter: Rádiófelderítő (COMINT[51]) tapasztalatok az afgán hadszíntéren. Felderítő Szemle, 8. évf., Titkos szám, 2009, pp. 143–162.

18. BALOGH Péter: A harctéri azonosító rendszerekről. Felderítő Szemle, 5. évf. 1. sz., 2006, pp. 88–109.

[50] ISTAR: Intelligence, Surveillance, Target Acquisition and Reconnaissance; magyarul: hírszerzés, megfigyelés, célfelderítés és felderítés.

[51] COMINT: Communications Intelligence; magyarul: kommunikációs hírszerzés / rádiófelderítés.

Kapcsolódó tudományos konferencia-előadások

19. 1. BALOGH Péter: Felderítő szenzorok a pilóta nélküli repülésben. Robothadviselés 2015 Tudományos Konferencia. Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, 2015. november 26.

20. 1. BALOGH Péter: Egy NATO hadművelet tapasztalatai: Operation Unified Protector. Repüléstudományi Konferencia. Szolnok, 2014. április 10.

21. 13. BALOGH Péter: Repülő robotok a NATO szolgálatában: AGS. Robothadviselés 2013 Tudományos Konferencia. Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, 2013. november 27.

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Teljes megnevezés	Magyar jelentés / értelmezés
5G	Fifth Generation Mobile Network	ötödik generációs mobilhálózat
6G	Sixth Generation Mobile Network	hatodik generációs mobilhálózat
ACT	Allied Command Transformation	Szövetséges Transzformációs Parancsnokság
AI	Artificial Intelligence	mesterséges intelligencia
AI RMF	Artificial Intelligence Risk Management Framework	mesterségesintelligencia-kockázatkezelési keretrendszer
API	Application Programming Interface	alkalmazásprogramozási felület
BATR	Balogh Adaptive Technological Resilience Cycle	Balogh-féle Adaptív Technológiai Reziliencia Ciklus
BCM	Business Continuity Management	üzletmenet-/működésfolytonosság-menedzsment
C2	Command and Control	vezetés és irányítás
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance	vezetés, irányítás, kommunikáció, számítástechnika, hírszerzés, megfigyelés és felderítés
CAS	Complex Adaptive System	komplex adaptív rendszer
CER	Critical Entities Resilience Directive	a kritikus szervezetek rezilienciájáról szóló uniós irányelv
CERT	Computer Emergency Response Team	számítógép-biztonsági incidenskezelő csoport
CI	Critical Infrastructure	kritikus infrastruktúra
CIP	Critical Infrastructure Protection	kritikus infrastruktúra-védelem
COMINT	Communications Intelligence	kommunikációs hírszerzés / rádiófelderítés
CRA	Cyber Resilience Act	kiberrezilienciáról szóló uniós rendelet
CSF	Cybersecurity Framework	kiberbiztonsági keretrendszer
CSIRT	Computer Security Incident Response Team	számítógép-biztonsági incidenskezelő csoport
DDoS	Distributed Denial of Service	elosztott szolgáltatásmegtagadási támadás
DORA	Digital Operational Resilience Act	digitális működési rezilienciáról szóló uniós rendelet
DR	Disaster Recovery	incidens vagy katasztrófa utáni helyreállítás
EC	European Commission	Európai Bizottság
ENISA	European Union Agency for Cybersecurity	az Európai Unió Kiberbiztonsági Ügynöksége
ERA	European Union Agency for Railways	az Európai Unió Vasúti Ügynöksége
ESM	Electronic Support Measures	elektronikai támogató intézkedések
EU	European Union	Európai Unió
EW	Electronic Warfare	elektronikai hadviselés
GDPR	General Data Protection Regulation	általános adatvédelmi rendelet
GNSS	Global Navigation Satellite System	globális műholdas navigációs rendszer
GPS	Global Positioning System	globális helymeghatározó rendszer
HMI	Human–Machine Interface	ember–gép interfész
HRO	High Reliability Organization	magas megbízhatóságú szervezet
ICT	Information and Communication Technology	információs és kommunikációs technológia
ICS	Industrial Control System	ipari irányítórendszer
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IIoT	Industrial Internet of Things	ipari dolgok internete

Rövidítés	Teljes megnevezés	Magyar jelentés / értelmezés
IoT	Internet of Things	dolgok internete
IP	Internet Protocol	internetprotokoll
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
ISR	Intelligence, Surveillance and Reconnaissance	hírszerzés, megfigyelés és felderítés
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance	hírszerzés, megfigyelés, célfelderítés és felderítés
IT	Information Technology	információtechnológia
IT/OT	Information Technology / Operational Technology	információtechnológiai és műveleti/üzemirányítási technológiai rendszerek
K+F	Kutatás és fejlesztés	Research and Development
KPI	Key Performance Indicator	kulcsfontosságú teljesítménymutató
MDO	Multi-Domain Operations	többdoménes műveletek
MI	Mesterséges intelligencia	Artificial Intelligence
NATO	North Atlantic Treaty Organization	Észak-atlanti Szerződés Szervezete
NIS2	Directive on Measures for a High Common Level of Cybersecurity across the Union	az Európai Unió magas közös kiberbiztonsági szintjének biztosításáról szóló NIS2 irányelv
NIST	National Institute of Standards and Technology	az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete
NTRGF	National Technological Resilience Governance Framework	Nemzeti Technológiai Reziliencia Irányítási Keretrendszer
OECD	Organisation for Economic Co-operation and Development	Gazdasági Együttműködési és Fejlesztési Szervezet
OT	Operational Technology	műveleti/üzemirányítási technológia
PNT	Positioning, Navigation and Timing	helymeghatározás, navigáció és pontos időszolgáltatás
R&D	Research and Development	kutatás-fejlesztés
RPO	Recovery Point Objective	helyreállítási pont célértéke; az elfogadható adatvesztés időbeli határa
RTO	Recovery Time Objective	helyreállítási idő célértéke; a szolgáltatás helyreállításának elvárt maximális időtartama
SATCOM	Satellite Communications	műholdas kommunikáció
SCADA	Supervisory Control and Data Acquisition	felügyeleti irányító és adatgyűjtő rendszer
SFA	Strategic Foresight Analysis	stratégiai előretekintő elemzés
SIGINT	Signals Intelligence	jelhírszerzés / rádióelektronikai felderítés
SLA	Service Level Agreement	szolgáltatási szint megállapodás
SoS	System of Systems	rendszerek rendszere
STO	Science and Technology Organization	NATO Tudományos és Technológiai Szervezete
T–O–R	Technological–Organizational–Regulatory/Governance	technológiai–szervezeti–szabályozási/irányítási dimenziórendszer
TRI	Technological Resilience Index	Technológiai Reziliencia Index
TRMM	Technological Resilience Maturity Model	Technológiai Reziliencia Érettségi Modell
TRL	Technology Readiness Level	technológiai érettségi szint
UEBA	User and Entity Behavior Analytics	felhasználói és entitásviselkedés-elemzés
UPS	Uninterruptible Power Supply	szünetmentes tápegység
WEF	World Economic Forum	Világgazdasági Fórum

ÁBRÁK JEGYZÉKE

Összesen: 30 ábra.

TÁBLÁZATOK JEGYZÉKE

Összesen: 12 táblázat.