HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 3. szám 105–117.
DOI: 10.32567/hm.2026.3.7

Földes Tibor[1]

A működésfolytonosság mint stratégiai képesség a kritikus infrastruktúrák védelmében

Continuity of Operations as a Strategic Capability for the Protection of Critical Infrastructures

Absztrakt

A kritikus infrastruktúrák védelme azért vált kiemelt biztonsági feladattá, mert például az energia-, a közlekedési és az informatikai rendszerek közötti függőségek ma már közvetlen, gyorsan terjedő zavarokat eredményezhetnek. A digitalizáció, a globális ellátási láncok sérülékenysége és a hibrid fenyegetések olyan környezetet teremtettek, ahol a működésfolytonosság biztosítása stratégiai jelentőségű. A működésfolytonosság-tervezés és annak kormányzati-honvédelmi megfelelője, a működés folytonossága olyan vezetési és operatív rendszerek összessége, amelyek biztosítják, hogy a kritikus szolgáltatások jelentős zavar esetén is fennmaradjanak. A NATO doktrínái a katonai működés biztonságos tervezési elveit határozzák meg, míg a NIST-keretrendszerek a civil és kiberbiztonsági folytonosság technikai standardjait rögzítik. A tanulmány bemutatja, hogyan egészítik ki egymást a NATO doktrinális iránymutatásai és a NIST technikai keretrendszerei a működésfolytonosság megteremtésében. Rámutat, hogy a működésfolytonosság-tervezés és a működés folytonossága nem kizárólag adminisztratív tevékenységként értelmezhető, hanem a szervezeti működés irányításának egyik alapvető eleme, amely a megelőzés, észlelés, reagálás és helyreállítás egységes rendszerére épül.

Kulcsszavak: biztonság, kritikus infrastruktúra, működésfolytonosság, stratégia

[1] Okleveles kiberbiztonsági szakértő, doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: foldestibor252@gmail.com

Abstract

The protection of critical infrastructures has become a priority security task because the dependencies between systems such as energy, transportation, and information technology can now result in direct and rapidly spreading disruptions. Digitalisation, the vulnerability of global supply chains, and the rise of hybrid threats have created an environment in which ensuring continuity of operations has strategic significance. Business continuity planning and its governmental–military counterpart, continuity of operations, represent a set of leadership and operational systems that ensure critical services remain functional even under significant disruption. NATO doctrines define the planning principles required for the secure continuation of military operations, while NIST frameworks establish the technical standards for civil and cybersecurity continuity. This study demonstrates how NATO's doctrinal guidance and NIST's technical frameworks complement each other in building resilience. It emphasises that business continuity planning and the continuity of operations cannot be interpreted solely as an administrative activity, but rather as a fundamental element of organisational governance, built on an integrated system of prevention, detection, response, and recovery.

Keywords: security, critical infrastructure, continuity of operations, strategy

Bevezetés

A kritikus infrastruktúra fogalma alatt a tanulmány azokat az állami, gazdasági és társadalmi szempontból alapvető szolgáltatásokat és rendszereket érti, amelyek működésének zavara jelentős hatással lenne az állami működésre, a közbiztonságra vagy a társadalom alapvető szükségleteinek kielégítésére. A fogalom értelmezése az Európai Unió kritikus szervezeteinek rezilienciájáról szóló irányelvére, valamint annak nemzeti megfelelőire támaszkodik, kiegészítve a NATO rezilienciamegközelítésével. A kritikus infrastruktúrák (KI) védelme a 21. századra kiemelten kezelendő szakterületté vált, védelme egyre nagyobb figyelmet kap.[2] A modern társadalmak működését biztosító kritikus infrastruktúrák egyre szorosabb kölcsönhatásban állnak egymással.[3] A KI-k – például energia-, víz-, közlekedési, egészségügyi és információs rendszerek – olyan mértékben épülnek egymásra, hogy működésük zavara nem csupán egy adott ágazat problémája, hanem rövid időn belül társadalmi és nemzetbiztonsági következményekkel járhat. A tudományos felfedezések, az innovációban rejlő képességek és lehetőségek szinte folyamatosan változtatták és változtatják a biztonsági környezetet.[4] A technológiai gyorsulás és a digitalizáció mellett a globális ellátási láncok sérülékenysége és a hibrid fenyegetések[5] terjedése együtt alakítja ki azt a környezetet, amelyben a KI-k védelme már rendszerszintű kihívássá vált. Ebben

[2] Szénási 2024: 19.
[3] Bakos–Kovács 2025: 111.
[4] Földes 2025: 146.
[5] Hibrid fenyegetés: a katonai, információs, kiber-, gazdasági és politikai eszközök összehangolt alkalmazása, amelynek célja a társadalmi működés megzavarása vagy befolyásolása. A fizikai és digitális támadások egyszerre, egymást erősítve jelenhetnek meg.

a környezetben a biztonság nem statikus állapotként értelmezhető, hanem gyorsan változó, gyakran előre nem jelezhető kockázati környezet. A technológia ma már kettős természetű: egyszerre növeli a hatékonyságot, miközben új, gyakran nehezen felismerhető kockázatokat is létrehoz. A működésfolytonosság-tervezés (BCP[6]), valamint annak kormányzati és honvédelmi megfelelője, a működés folytonossága (COOP) vezetői felelősség és műveleti képesség. Különösen igaz ez azokra az ágazatokra, rendszerekre, ahol a működés elvárt rendelkezésre állása a nap 24 órájában közel teljes, és ahol egy rövid leállás is kárt okozhat. Egy kórház esetében ez konkrétan azt jelenti, hogy egy áramszünet során a sürgősségi ellátás csak akkor biztosítható, ha a tartalék energiaellátás azonnal és megszakítás nélkül átveszi a működést.

Magyarországon a KI-k védelme elsődlegesen állami feladat, amelyet a szövetségesi elvárások és iránymutatások alapján kialakított nemzeti jogszabályok határoznak meg. Tekintettel arra, hogy az alapvető szolgáltatások[7] jelentős részét nem állami, hanem piaci szereplők működtetik, elengedhetetlenné vált a világos és kötelező előírások megfogalmazása. Ez óhatatlanul szoros együttműködést kíván meg az állami, honvédelmi, katasztrófavédelmi és magánszektorhoz tartozó szervezetek között, hiszen az alapvető szolgáltatások folytonossága csak összehangolt módon biztosítható.

A működésfolytonosság egy olyan mechanizmust, intézkedésegyüttest jelent, amellyel egy szervezet vagy rendszer különleges körülmények között, jelentős zavar esetén is elfogadható szinten tud működni, majd tervezetten vissza tud állni a normál üzemre. A jelen publikáció a KI-k védelmének összefüggésrendszerében a működésfolytonosság-tervezés szerepét és módszertani megközelítéseit mutatja be, elsősorban a NATO-doktrínák és a NIST által meghatározott keretrendszerek alapján. A NATO-doktrínák a katonai és stratégiai működésfolytonosság alapelveit rögzítik, míg a NIST-keretrendszerek a civil, technikai és kiberbiztonsági folyamatok részletes követelményeit határozzák meg. A két megközelítés együtt ad teljes képet arról, hogyan tartható fenn a kritikus szolgáltatások működőképessége összetett, többdoménű környezetben.

A BCP olyan szervezeti tervezési és működtetési folyamat, amelynek célja, hogy zavar esetén is fennmaradjanak a kritikus működési képességek. A COOP ugyanezt a megközelítést követi a kormányzati és honvédelmi szervezetek körében. A működésfolytonosság azt jelenti, hogy a rendszer a zavarokat követően gyorsan helyre tud állni. A NATO-doktrínák a katonai műveletek folytonosságát támogatják, míg a NIST-keretrendszerek a civil, szervezeti és informatikai folytonosság technikai szabványait adják. A kutatás módszertana kvalitatív, összehasonlító és normatív elemzésre épül, amely a vonatkozó NATO-doktrínák, NIST-ajánlások és uniós, valamint hazai jogszabályok rendszerszintű feldolgozását végzi el. Az elemzés célja nem új szabályozási elemek létrehozása, hanem annak feltárása, hogy a különböző szabályozási és doktrinális keretrendszerek miként egészítik ki egymást a működésfolytonosság biztosításában. A módszertan lehetővé teszi a stratégiai, szervezeti és technikai szintek közötti összefüggések azonosítását, valamint a működésfolytonosság mint integrált szervezeti képesség értelmezését.

[6] A rövidítések jegyzéke a dokumentum végén található.

[7] A kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. számú melléklet „C" oszlopban meghatározott és a védelmi és biztonsági tevékenységekről szóló 2021. évi XCIII. törvény 5. számú melléklet „C" oszlopban meghatározott szolgáltatások.

A működésfolytonosság stratégiai jelentősége

A KI-k működésfolytonosságának biztosítása multidiszciplináris keretrendszerben értelmezhető. Egyszerre alkalmazandó a NATO katonai doktrínája, a nemzetközi működésfolytonossági és kiberbiztonsági szabványok, valamint az európai és a hazai szabályozás. Ezen három pillér – doktrína, szabvány, jogszabály – teremti meg azt a keretet, amely nélkülözhetetlen az alapvető szolgáltatások folytonosságának fenntartásához.

A NATO doktrinális rendszere – a vizsgált témát illetően – az AJP-01[8] és az AJP-3-as[9] doktrínacsalád. Az AJP-01 doktrína központi szerepet játszik a hadműveletek tervezésének és végrehajtásának szabályozásában. Ezt egészíti ki az AJP-3 doktrínacsalád, amely részletes útmutatást ad a védelem, logisztikai támogatás, a kommunikációs rendszerek működtetésére és az információmegosztás fenntartására, amely egyben a BCP/COOP-rendszerek alapját is képezi. A műszaki követelményeket részletező AJP-3.12.1[10] doktrína az ideiglenes energiaellátás, a hálózati helyreállítás és a mobil képességek szerepét hangsúlyozza, amelyek a katonai és civil működésfolytonossági megoldások technikai alapját adják, adhatják. Az AJP-3.14[11] lefekteti a haderővédelem alapelveit és működési rendjét. Meghatározza, hogyan kell a fenyegetések, veszélyek és sebezhetőségek elemzését beépíteni a műveleti tervezésbe, és bemutatja, hogy az aktív, passzív és helyreállító védelmi intézkedések együtt hogyan biztosítják a katonai erők folyamatos működőképességét. Az AJP-3.28[12] doktrína a stabilizációs és válságkezelési műveletek[13] során elvárt civil infrastruktúra-támogatási feladatokat határozza meg, kiemelve a kritikus szolgáltatások ideiglenes biztosításának és helyreállításának jelentőségét.

A nemzetközi működésfolytonossági és kiberbiztonsági szabványok – különösen a NIST és az ENISA keretrendszerei – elsősorban azt a célt szolgálják, hogy a szervezetek működése a különféle zavaró események ellenére is fennmaradjon. A NIST SP 800-34 r1[14] egy jól felépített, PDCA-logikára épülő COOP-életciklust kínál, amely segít a felkészüléstől kezdve a válaszadáson át egészen a helyreállításig egységes rendszerben kezelni a folyamatokat. A NIST SP 800-61 r3[15] azt mutatja meg, hogyan érdemes felépíteni és működtetni egy CSIRT-et vagy SOC-ot: milyen protokollok támogatják a kiberincidensek időben történő felismerését, kezelését és koordinált lezárását. A NIST SP 800-53 r5[16] egy átfogó kontrollkatalógust biztosít, amelyben a technikai, szervezeti és folyamatszintű biztonsági és folytonossági intézkedések egy egységes keretrendszerként jelennek meg.

[8] AJP-01: szövetségesi Összhaderőnemi Alap Doktrína.
[9] AJP-3: szövetségi Összhaderőnemi Doktrína a Műveletek Végrehajtásáról.
[10] AJP-3.12.1: szövetségi Összhaderőnemi Doktrína a Katonai műszaki tevékenységekhez.
[11] AJP-3.14: szövetségi Összhaderőnemi Doktrína a Haderővédelemről.
[12] AJP-3.28: szövetségi Összhaderőnemi Doktrína a a Stabilizációhoz való Katonai Hozzájárulásról.
[13] Stabilizációs és válságkezelési műveletek: olyan tevékenységek, amelyek célja az alapvető civil szolgáltatások helyreállítása, fenntartása és a társadalmi rend stabilizálása katonai támogatással.
[14] NIST SP 800-34 r1: Vészhelyzeti és működésfolytonossági tervezési útmutató szövetségi információs rendszerek számára.
[15] NIST SP 800-61 r3: Ajánlások és megfontolások a kiberbiztonsági kockázatkezeléshez kapcsolódó incidenskezeléshez.
[16] NIST SP 800-53 r5: Biztonsági és adatvédelmi kontrollok információs rendszerek és szervezetek számára.

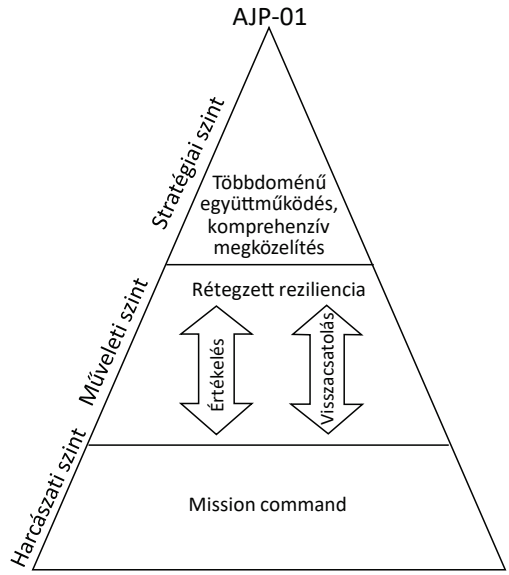
A magyar működésfolytonossági szabályozás az NIS2-[17] és a CER-irányelvekhez[18] igazodva jogszabályi szinten[19] határozta meg a kritikusinfrastruktúra-szereplők szervezeti, jelentési, incidenskezelési és gyakoroltatási kötelezettségeit. A vonatkozó mellékletek egyértelműen nevesítik azokat a szektorokat és alágazatokat, amelyek esetében a BCP/COOP tervezésének és működtetésének megléte elengedhetetlen, továbbá keretrendszert biztosítanak az interdependenciák vizsgálatának standardizált végrehajtásához. A megfelelés így nem pusztán formális jogi kötelezettség, hanem a működésfolytonosság-tervezés minőségének és a szervezeti működésfolytonosság tényleges szintjének egyik legfontosabb meghatározó tényezője.

A működésfolytonosság jelentősége ma már jóval túlmutat a hagyományos üzletmenet-biztonsági megközelítésen. A kommunikációs, energetikai, logisztikai és – egyre inkább – az informatikai rendszerek olyan szorosan összekapcsolódó hálózatot alkotnak, hogy egyetlen elem meghibásodása vagy kiesése is könnyen láncreakciót idézhet elő. Ez nemcsak technikai fennakadásokat okozhat, hanem a társadalmi működés zavarához, gazdasági károkhoz és komoly reputációs veszteségekhez is vezethet. Míg a piaci szereplők esetében a működésfolytonosság megszilárdítása versenyelőnyt és üzleti stabilitást jelent, addig a kritikus infrastruktúrák terén mindez a közérdek védelméről, a lakosság biztonságáról és az állami működés zavartalanságáról szól – vagyis elengedhetetlen alapfeltétel. Például egy regionális áramszolgáltató esetében egy alállomás kiesése nemcsak az energiaellátást érinti, hanem a távközlési szolgáltatásokat és a közlekedési irányítórendszereket is. Egy ilyen esemény során a BCP-tervnek tartalmaznia kell az alternatív energiaforrások aktiválását és a prioritási sorrendben történő visszakapcsolást.

A működésfolytonosság rendszerszintű megközelítése

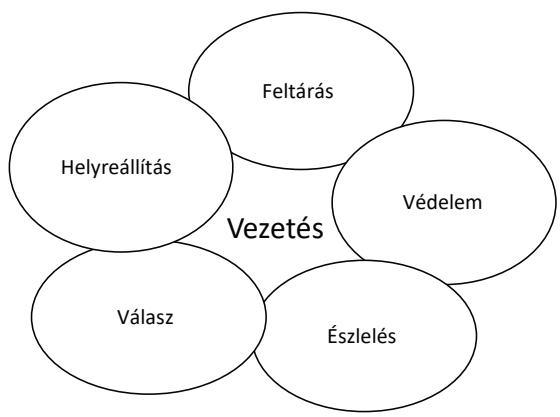
A BCP/COOP-életciklus intézményi nézőpontból mindig a stratégiai keretek kijelölésével indul. A működésfolytonosság nem pusztán a dokumentumok és eljárások együttese, hanem az erők, erőforrások és felelősségi körök olyan rendszere, amely a váratlan helyzetekben is képes fenntartani és helyreállítani a működést. A NATO-doktrínák – kiemelten az AJP-01 – ezt a rendszerszemléletet a komprehenzív megközelítés,[20] a rétegzett működésfolytonosság,[21] a *mission command*[22] és a többdoménű együttműködés alapelveire építik. A gyors regenerációt és döntésképességet az alapelvek mentén összehangolt stratégiai, műveleti és harcászati szintű tervezés, valamint az értékelés és a visszacsatolás biztosíthatja. Az alapelvi összefüggéseket az 1. ábra szimbolizálja.

[17] NIS2: az Európai Parlament és a Tanács 2022/2555 számú irányelve, amely az EU területén egységesen magas szintű kiberbiztonságot ír elő a kritikus és fontos ágazatok számára.
[18] CER: az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról.
[19] Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény, a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény.
[20] Komprehenzív megközelítés: összetett, többdimenziós döntés- és műveletirányítási szemlélet, amely összehangolja a különböző szereplők, szervezetek és képességek tevékenységét.
[21] Rétegzett működésfolytonosság: egy rendszer ellenálló képessége több, egymásra épülő védelmi, működési és helyreállítási komponensből áll.
[22] *Mission command:* küldetésorientált vezetés vagy küldetésalapú irányítás.



1. ábra: Az AJP-01 alapelveinek rendszerszemlélete
Forrás: a szerző szerkesztése

A technikai-szervezeti oldalon a NIST által ajánlott a működésbe integrált állandó visszacsatolás, amelynek keretét a vezetés–feltárás–védelem–észlelés–válasz–helyreállítás hat funkció adja meg. A folyamatok a szerepkörök, a hatáskörök és a felelősségek egyértelmű rögzítésével folytatódik. A folyamatok összefüggéseit a 2. ábra mutatja be.



2. ábra: A NIST biztonsági keretrendszere
Forrás: a szerző szerkesztése

A NATO-műveleti logika szerint a működésfolytonosság feltétele a stabil C2-rendszer, a világos felelősségmegosztás és a *unity of effort,*[23] mert válsághelyzetben a felelősségi zavar vagy a döntések késlekedése önmagában is kockázatnövelő tényező. A NIST-ajánlások ezt már kötelező elvárásként határozzák meg: az incidenskezeléshez kapcsolódó szerepek, jogosultságok, döntési jogok és folyamati utak előre rögzített, egyértelmű dokumentálása teremti meg azt a szervezeti alapot, amelyre a műszaki és üzemeltetési kontrollok biztonsággal épülhetnek. Ez az alap azonban csak akkor működik valódi képességként, ha a szervezeten belüli függőségeket és a kritikus erőforrásokat részletesen ismerjük. Nemcsak a saját folyamataikat és rendszereiket kell feltérképezni, hanem azokat a szolgáltatókat, beszállítókat, közmű- és felhőszolgáltatókat, stratégiai partnereket is, amelyek közvetlenül vagy közvetve befolyásolják a működés folytonosságát. Például egy felhőszolgáltató kiesése esetén egy szervezet működése csak akkor tartható fenn, ha előzetesen kialakított alternatív szolgáltatói kapcsolatokkal vagy több szolgáltatót alkalmazó architektúrával rendelkezik. A reális kockázatértékeléshez ezek aktív bevonása a tervezés alapvető feltétele. A BCP/COOP technikai alapja a kritikus eszközök és erőforrások azonosítása, a rájuk ható fenyegetések és sérülékenységek feltárása – a fizikai, az informatikai és a kommunikációs infrastruktúrák teljes spektrumán –, hogy a releváns kockázatokat időben észleljük és kezelni tudjuk.

A korai észlelés mind a NATO-, mind a NIST-megközelítésben kiemelt jelentőségű. A NATO-doktrínák ezt többdoménű érzékeléssel és egységesen működő hírszerzési-kommunikációs láncokkal támogatják. A NIST ugyanezt műszaki oldalról bontja ki: a folyamatos hálózati és szolgáltatói megfigyelés, a rendellenes mintázatok elemzése, valamint a riasztási és incidensbejelentési feltételek egyértelmű meghatározása teremti meg azt a helyzetképet, amelyre a gyors reagálás épül. Egy zsarolóvírus-támadás során például a szervezet először leválasztja az érintett rendszereket a hálózatról, ezt követően elemzi a naplóállományokat a behatolás azonosítására, majd biztonsági mentésekből állítja helyre a működést, ami jól leképezi az észlelés–válasz–helyreállítás folyamatát.

A NATO-oldali reagálás kockázatközpontú, és erősen támaszkodik a vezetésirányítási rendszerre. Katonai környezetben ez például azt jelenti, hogy egy kommunikációs rendszer kiesése esetén mobil kommunikációs egységeket telepítenek a parancsnoki lánc fenntartása érdekében. A megközelítés lényege a gyors helyzetértékelés, a világos prioritások kijelölése, az erőforrások összehangolása és a kritikus szolgáltatások átmeneti fenntartása, miközben szükség esetén az alternatív megoldások is azonnal aktiválhatók. A NIST ugyanezt részletes, lépésről lépésre követhető folyamatokban írja le: az incidensek első vizsgálatától és továbbításától kezdve a helyzet elemzésén és a bizonyítékok kezelésén át egészen a belső és külső kommunikáció összehangolásáig, a célzott beavatkozások végrehajtásáig. A helyreállítás célja a működőképesség ellenőrzött és biztonságos visszaállítása. Ez a gyakorlatban jelentheti például egy informatikai rendszer fokozatos újraindítását priorizált szolgáltatások mentén, miközben folyamatosan ellenőrzik az adatintegritást és a rendszerbiztonságot. A NATO ezt műveleti követelményként határozza meg, míg a NIST ennek részletes,

[23] *Unity of effort:* erőfeszítések egysége, különböző szervezetek összehangoltan, közös cél irányába dolgoznak.

technikai folyamatleírást ad. Mindkét megközelítés közös eleme, hogy a tanulságok és a bizonyítékok visszacsatolása indítja el a következő életciklusszakaszt, ezáltal válik a működésfolytonosság valóban tanuló és önjavító képességgé.

A kritikus infrastruktúrák működésfolytonosságának gyakorlati értelmezését jól szemlélteti egy olyan forgatókönyv, amelyben egy állami működés szempontjából kiemelt, digitalizált szolgáltatás – például egy központi adminisztratív vagy logisztikai rendszer – külső, felhőalapú szolgáltató infrastruktúrájára támaszkodik. Egy ilyen környezetben egy szolgáltatói oldalon bekövetkező incidens – például kiberbiztonsági esemény, hálózati kiesés vagy ellátási láncot érintő zavar – közvetlen hatással lehet a kritikus szolgáltatás rendelkezésre állására, miközben maga az érintett szervezet objektumszintű védelmi intézkedései változatlanul fennállnak. A működésfolytonosság biztosítása ilyen esetben kizárólag integrált megközelítéssel valósítható meg. NATO-doktrinális szempontból a vezetés és irányítás folyamatossága, a döntési ciklus fenntartása és az erőforrások újrapriorálása biztosítja a szervezeti működőképesség fenntartását. Ezzel párhuzamosan a NIST által meghatározott incidenskezelési életciklus – az észlelés, elemzés, reagálás és helyreállítás egymást követő lépéseivel – a technikai válaszintézkedések végrehajtását strukturálja. A példában a szolgáltatás helyreállításának sikeressége nem kizárólag a technikai redundanciától függ, hanem attól is, hogy a szervezet előzetesen meghatározta-e az elfogadható helyreállítási idő- és adatvesztési célértékeket, valamint képes-e együttműködni a külső szolgáltatóval a válsághelyzet kezelésében. Ez a megközelítés jól szemlélteti, hogy a működésfolytonosság napjainkban nem statikus tervdokumentumként, hanem a szervezeti irányítás, a technikai védelem és a szabályozási megfelelés szerves egységeként értelmezhető.

A működésfolytonosság és a biztonsági érettség egységes megközelítése

Az ajánlás szerint a biztonsági környezet gyorsan, nem lineáris módon változik, ezért a szervezetnek tudatosan felépített, mérhető és folyamatosan fejleszthető biztonsági szintet kell elérnie és fenntartania. Ez nem egyetlen intézkedésen múlik: a megelőzés, az észlelés, a reagálás és a helyreállítás együtt adhat stabil működést. A cél nemcsak az üzemeltetés és a rendelkezésre állás védelme, hanem az ártó szándékú befolyásolásból eredő incidensek kezelése is. Ez a képesség végigkíséri a teljes tervezési és végrehajtási ciklust, és érdemben erősíti a rendszer BCP/COOP-dokumentációját. Mivel a szervezetüzemeltetési eszközökön kívül számos infokommunikációs eszközt használnak – akár integráltan is –, a kiberbiztonsági kockázatok mellett adatvédelmi, beszállítói láncbeli, hírnévi, technológiai és fizikai kockázatokkal is számolni kell. A kockázatkezelésnek folyamatos – nem kampányszerű – tevékenységnek kell lennie. A folyamatos működés alapja az ajánlás szerint a felelősök kijelölése a hat fő funkció mentén. A szerepek a szervezet méretétől és a kockázati profiltól[24] függően összevonhatók, de a felelősség és az elszámoltathatóság – különösen a jogi kötelezettségek miatt – nem csökkenthető, a szerepek összevonása sem eredményezheti ezeknek a követelményeknek a gyengülését.

[24] Kockázati profil: rendszer vagy folyamat egyedi kockázati jellemzőinek összessége.

- A *vezetés* kialakítja, jóváhagyja és kommunikálja a biztonsági stratégiát, összeköti a funkciókat, és láthatóvá teszi a képességeket, hiányokat, beszállítói kitettségeket és beavatkozási pontokat.
- A *feltárás* a valós kockázati kép vizualizálása: eszköz- és szolgáltatásleltár, az adatáramlás megértése és ábrázolása, kritikussági besorolás, sérülékenységek és fenyegetések azonosítása, az eredendő kockázat becslése és a válaszok rangsorolása.
- A *védelem* az arányos, célzott megelőző és következménycsökkentő intézkedésekről szól: azonosítás- és hozzáférés-kezelés, fizikai védelem, tudatosság és képzés, adatbiztonság, konfigurációkezelés, gondozott szoftver- és hardveréletciklus, szabályozott válaszok a környezeti fenyegetésekre.
- Az *észlelés* a hálózatok, szolgáltatások, a fizikai környezet és – amennyire a beszállítói átláthatóság engedi – a partnerek folyamatos nyomon követése. Feladata az anomáliák értelmezése, a „zaj" kiszűrése és a cselekvésre kész döntési információk előállítása.
- A *válasz* a tényleges lépések összehangolását jelenti, vagyis az incidensek osztályozását és hitelesítését, az objektív belépési pont kijelölését a helyreállítási folyamatba, az eseti elemzések elkészítését a kiváltó okok és a terjedés feltárására, a bizonyítékszintű dokumentálást, a kár és a további események valószínűségének becslését, valamint a belső és külső érintettek időszerű és hiteles tájékoztatását.
- A *helyreállítás* pedig a működőképesség ellenőrzött visszaállítása. A lépések kiválasztása és rangsorolása, a zárási feltételek teljesítése, az esemény- és helyreállítási dokumentáció lezárása, a tanulságok beépítése a terveinkbe és szabályzatainkba. A megvalósítást rendszeres visszamérés és a tanulságok tudatos beépítése követi, így a folyamatos működés egy dinamikus, önmagát erősítő folyamattá válik.

Az AJP-01 szemlélete szerint a szervezet működőképességének fenntartása nemcsak technikai vagy eljárási kérdés, hanem vezetési és együttműködési gyakorlat, amely a teljes életciklust átszövi. A gyorsan változó környezetben a vezetőknek nemcsak irányt kell mutatniuk, hanem olyan bizalmi és együttműködési kultúrát is teremteniük, amelyben minden szereplő tisztán látja a saját feladatát, hatáskörét és az együttműködés kereteit. Ez teremti meg azt a működési alapot, amelyre a folytonossági és helyreállítási képességek épülhetnek. A tevékenységek koordinációját támogatja a helyzetértékelés folyamatos, több forrásból történő frissítése: az információk hitelességének vizsgálata, a működési képességek állapotának értékelése és a rendelkezésre álló erőforrások valós idejű átlátása. Az ajánlás hangsúlyozza, hogy a megelőzés, a felkészülés, a reagálás és a helyreállítás nem elszigetelt funkciók, hanem egymást erősítő, ciklikusan ismétlődő tevékenységek, amelyeknek a parancsnoki döntések és a végrehajtó szintek között zavartalanul kell áramolniuk. A dokumentum rámutat, hogy a folyamatos működés nem tartható fenn pusztán erőforrásoldalról, szükség van a kommunikáció, a feladatmegosztás, a felelősségi viszonyok és a partnerségi kapcsolatok összehangolt, átlátható kezelésére is. A működésfolytonosság humán oldala ugyanilyen meghatározó: a szerepek, a felelősségek és az együttműködési szabályok

egyértelmű meghatározása, valamint a feladatellátás személyi feltételeinek biztosítása döntően befolyásolja, hogy egy válsághelyzetben a tervek valóban végrehajthatók-e. Ez különösen fontos olyan helyzetekben, amikor a szervezet egyszerre több működési területen tevékenykedik, és a feladatok összehangolásához több beszállítóval és számos érintett féllel kell együttműködnie. Amennyiben ez az összhang működik, a folytonosság nem külön gyakorlat, hanem a mindennapi vezetés részévé válik, amely a BCP/COOP-dokumentációt élővé, a döntéseket következetessé, a helyreállítást pedig gyorsabbá és bizonyítékokon nyugvóvá teszi.

Ezek a vezetési és együttműködési alapok teremtik meg azt a ritmust, amelyben a folytonosság és a helyreállítás már nem külön feladat, hanem a szervezet működésének szerves része. Ez a működés természetes ritmusa a BCP/COOP-életciklusnak, ahol a stratégiai irányok és a műszaki-eljárási kontrollok kölcsönösen támogatják egymást, és a szervezet kritikus képességei folyamatosan finomodnak a tervezés, a végrehajtás, az ellenőrzés és a beavatkozás köré épülő gyakorlatnak köszönhetően. Ebben a keretben a NATO-szemlélet stratégiai és műveleti megközelítése összhangba kerül a NIST részletes végrehajtási nyelvével. A NATO oldaláról érkezik a több szintre és doménre kiterjedő, felelősségalapú együttműködés iránya, míg a NIST biztosítja a gyakorlati megvalósítás eszközeit. A NATO–NIST összehasonlító kereteit az 1. táblázat mutatja.

1. táblázat: A NATO–NIST összehasonlító keretei

NATO: Stratégia, művelet	**NIST: Technika, eljárás**
C2, együttműködés	Detektálás, válasz, kontrollok
Mission command	Életciklus
többdoménű működés	CSIRT-, SOC-folyamatok

Forrás: a szerző szerkesztése

Összegzés

Amennyiben ez a két megközelítés valóban találkozik, akkor a működésfolytonosság gyakorlati értelemben azt jelenti, hogy egy szervezet egy esemény után módosítja az eljárásait, például frissíti a helyreállítási terveit vagy átalakítja a beszállítói struktúráját. A szervezet képes érzékelni a helyzeteket, értelmezni az összefüggéseket, döntéseket hozni, cselekedni és helyreállítani, mindezt bizonyítékokra támaszkodva és a saját valós kitettségeihez igazítva. A NATO stratégiai gondolkodásmódja és a NIST részletes végrehajtási logikája egymás mellett nem kettős terhet jelentenek, hanem közösen létrehoznak egy olyan keretet, amelyben a vezetők és a végrehajtó szereplők egyaránt tisztán látják, hogy mikor, mivel és hogyan kell beavatkozni. Ebben a modellben a működésfolytonosság nem egyszeri projekt, nem kampányszerű feladat, hanem a szervezet kollektív tanulási folyamata, amelyben a hibákból nyert tapasztalat, a visszajelzések elemzése és az előretekintő tervezés egyaránt helyet kap.

Ez a megközelítés lehetővé teszi, hogy a szervezet ne csupán reagáljon a zavarokra, hanem előre felismerje a gyenge pontokat, és még az események bekövetkezése előtt

kialakítsa a megfelelő alternatívákat. A felkészültség és a gyors alkalmazkodóképesség így nemcsak technikai, hanem kulturális tényezővé válik. A döntéshozók és a működtetésben érintettek közösen alakítanak ki egy olyan működési környezetet, ahol a problémák nyíltan felszínre kerülhetnek, és a megoldások keresése nem büntetéshez, hanem fejlődéshez kapcsolódik.

Ennek eredményeképpen a BCP/COOP nem különálló dokumentum vagy „külön dosszié" lesz, hanem a vezetési és üzemeltetési gyakorlat szerves része, ahol a stratégiai elvek a műszaki kontrollokon és az operatív rutinokon keresztül tényleges túlélőképességgé formálódnak. A működésfolytonosság így válik valódi szervezeti kompetenciává. Olyan képességgé, amely nemcsak válsághelyzetben véd, hanem a mindennapi működés stabilitását, a szolgáltatások minőségét és a társadalmi bizalom fennmaradását is támogatja.

A két megközelítés összeérése tehát nem adminisztratív kötelezettség teljesítését jelenti, hanem azt a felismerést, hogy az ellenálló képesség egy olyan befektetés, amely mérhetően csökkenti az üzemszünetek idejét és a helyreállítás költségeit. A bemutatott megközelítés egy integrált működésfolytonossági modellt körvonalaz, amely egyaránt illeszkedik a katonai-doktrinális, a technikai-eljárási és a szabályozási követelményekhez.

Felhasznált irodalom

Jogszabályok és uniós dokumentumok

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (2022). Brüsszel, Az Európai Unió Hivatalos Lapja, L 333/164, 2022. december 27. Online: https://publications.europa.eu/resource/cellar/c4d36f49-85bc-11ed-9887-01aa75ed71a1.0012.01/DOC_1

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózat- és információbiztonságról (2016). Brüsszel: Az Európai Unió Hivatalos Lapja, L 194, 2016. július 19. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve a hálózat- és információbiztonságról (2022). Brüsszel: Az Európai Unió Hivatalos Lapja, L 333, 2022. december 27. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022L2555

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Online: https://mkogy.jogtar.hu/jogszabaly?docid=a1200166.TV

NATO-doktrinális dokumentumok

North Atlantic Treaty Organization – NATO Standardization Office (2021): AJP-3.14 Allied Joint Doctrine for Force Protection. Online: www.coemed.org/files/stanags/01_AJP/AJP-3.14_EDA_V1_E_2528.pdf

North Atlantic Treaty Organization – NATO Standardization Office (2022. december 19): NATO Standard AJP-01 Allied Joint Doctrine (Edition F, Version 1). Online: www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf

North Atlantic Treaty Organization – NATO Standardization Office (2020): AJP-3 Allied Joint Doctrine for Operations. Online: www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf

North Atlantic Treaty Organization – NATO Standardization Office (2021): AJP-3.28 Allied Joint Doctrine for Stability Policing. Online: https://assets.publishing.service.gov.uk/media/63d7b111e90e0773d50c7530/AJP-3.28_web_accessible.pdf

NIST- és technikai keretrendszerek

National Institute of Standards and Technology (2018): Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD.

National Institute of Standards and Technology (2012): Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). Gaithersburg, MD.

National Institute of Standards and Technology (2018): Risk Management Framework for Information Systems and Organizations (NIST Special Publication 800-37 Revision 2). Gaithersburg, MD.

Szabványok és módszertani források

International Organization for Standardization (2019): ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements. Geneva: ISO.

International Organization for Standardization (2022): ISO/IEC 27001:2022 – Information security management systems – Requirements. Geneva: ISO.

Folyóiratcikkek

Bakos Tamás – Kovács Ferenc (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány,* 35(3), 106–119. Online: https://doi.org/10.17047/HADTUD.2025.35.3.106

Földes Tibor (2025): A biztonság szerepe és fontossága a szövetségesi kritikus infrastruktúra szabályozásának kialakításában. *Szakmai Szemle,* 23(1), 146–163. Online: https://ojs.knbsz.gov.hu/index.php/szakmai/article/view/234/130

Szénási Imre (2024): Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme; *Nemzetbiztonsági Szemle,* 12(2), 18–37. Online: https://doi.org/10.32561/nsz.2024.2.2

Rövidítések jegyzéke

Rövidítés	**Angol megnevezés**	**Magyar jelentés**
AJP	Allied Joint Publication	Szövetséges összhaderőnemi kiadvány
ATP	Allied Tactical Publication	Szövetséges harcászati (taktikai) kiadvány
BCP	Business Continuity Planning	Üzletmenet-folytonosság tervezése
BIA	Business Impact Analysis	Üzleti hatáselemzés
C2	Command and Control	Vezetés és irányítás
COOP	Continuity of Operations	A szervezeti működés folytonossága
CI	Critical Infrastructure	Kritikus infrastruktúra
CSIRT	Computer Security Incident Response Team	Informatikai Biztonsági Incidens-kezelő Csapat
CER	Critical Entities Resilience	Kritikus szervezetek ellenállóképessége
NIS / NIS2	Network and Information Security Directive	Hálózat- és információbiztonsági irányelv / NIS2
NIST	National Institute of Standards and Technology	Amerikai Nemzeti Szabványügyi és Technológiai Intézet
IR	Incident Response	Incidenskezelés
SOC	Security Operations Center	Információbiztonsági Műveleti Központ
RTO	Recovery Time Objective	Helyreállítási időcél
RPO	Recovery Point Objective	Helyreállítási pontcél
PDCA	Plan–Do–Check–Act	Tervezés, végrehajtás, ellenőrzés, beavatkozás