HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 1. szám 125–135.
DOI: 10.32567/hm.2026.1.8

Kocsis Zoltán,[1] Vass Gyula[2]

A kritikus szervezetek rezilienciája különös tekintettel az EU–USA szabályozási keretek összehasonlítására

The Resilience of Critical Organisations with Special Emphasis on the Comparative Analysis of EU and US Regulatory Frameworks

Absztrakt

A kritikus szervezetek rezilienciája az elmúlt évtizedben a katasztrófavédelem, a közigazgatás és a nemzetbiztonság egyik központi kérdésévé vált. A tanulmány célja annak bemutatása és összehasonlító elemzése, hogy az Európai Unió (EU) és az Amerikai Egyesült Államok (USA) milyen szabályozási és intézményi megközelítéseket alkalmaz a kritikus szervezetek ellenálló képességének erősítésére. Jelen cikkben a szerzők áttekintik a reziliencia fogalmát és jelentőségét a társadalmi és gazdasági folyamatok, a környezet és a védelmi képességek stabil fenntartásában, valamint a lakossági alapvető szolgáltatások biztonsága szempontjából. Ezt követően részletesen összehasonlítják az Európai Unió és az Amerikai Egyesült Államok jogi és stratégiai szabályozási kereteit a kritikus infrastruktúrák és szervezetek rezilienciájának, azaz ellenálló képességének erősítése terén. A tanulmány rámutat, hogy míg mindkét térségben növekvő hangsúlyt kap az összveszély megközelítésű reziliencia a természeti katasztrófák, járványok és egyéb krízisek kezelésében, addig az EU szabályozása inkább jogilag kötelező erejű irányelvekkel és átfogó stratégiákkal igyekszik növelni a létfontosságú szolgáltatást nyújtó entitások ellenálló képességét, míg az USA szabályozása hosszú ideig önkéntes

[1] Iparbiztonsági szakértő; tulajdonos, ECIP Kft.; oktató, Pannon Egyetem Mérnöki Kar Fenntarthatósági Megoldások Kutatólaboratórium, e-mail: kocsis.zoltan@ecip.hu
[2] Tanszékvezető egyetemi docens, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi Műszaki Tanszék, e-mail: vass.gyula@uni-nke.hu

együttműködésre és irányelvekre épített, amelyet a legújabb stratégiák már kötelezőbb elemekkel egészítenek ki. A tanulmány megállapítja, hogy a két megközelítés fokozatos közeledése egy hibrid rezilienciamodell irányába mutat, amely releváns tanulságokkal szolgál a közigazgatás és a katasztrófavédelem fejlesztése számára.

Kulcsszavak: reziliencia, kritikus szervezetek, közigazgatás, ellátásbiztonság, Európai Unió, Amerikai Egyesült Államok

Abstract

The resilience of critical organisations has become a key issue in disaster management, public administration, and national security over the past decade. The aim of this study is to provide a comparative analysis of the regulatory and institutional approaches adopted by the European Union (EU) and the United States of America (USA) to strengthen the resilience of critical organisations. In this article, the authors review the concept of resilience and its significance in the stable maintenance of social and economic processes, the environment and defence capabilities, and the security of essential services for the population. This is followed by a detailed comparison of the legal and strategic regulatory frameworks of the European Union and the United States of America in terms of strengthening the resilience of critical infrastructures and organisations. The study shows that while both regions are increasingly focusing on all-hazards resilience in managing natural disasters, epidemics and other crises, EU regulation tends to focus on legally binding guidelines and comprehensive strategies to increase the resilience of entities providing essential services, while USA regulation has long been based on voluntary cooperation and guidelines, which are supplemented by more mandatory elements in recent strategies. The study concludes that the gradual convergence of these approaches points toward a hybrid model of resilience, offering valuable lessons for the development of public administration and disaster management.

Keywords: resilience, critical organisations, public administration, security of supply, European Union, United States of America

Bevezetés

A modern társadalmak egyre összetettebb kihívásokkal néznek szembe, ideértve a természeti katasztrófákat, pandémiákat, gazdasági válságokat és akár szándékos támadásokat is. E kihívások közepette kulcsfontosságú, hogy a kritikus szervezetek reziliensek legyenek, beleértve a közszféra intézményeit és az alapvető szolgáltatásokat nyújtó infrastruktúrákat, azaz képesek legyenek a váratlan eseményeket kezelni és működésüket gyorsan helyreállítani. A reziliencia fogalma eredetileg az ökológiában jelent meg, de mára interdiszciplináris megközelítésben alkalmazzák a kormányzás és válságkezelés területén is.[3]

[3] Pálné Kovács 2023.

A Covid–19-járvány különösen ráirányította a figyelmet az ellenálló képességre építő szakpolitikák fontosságára, hiszen világossá vált, hogy a közigazgatási és a gazdasági szereplők felkészültsége és alkalmazkodóképessége alapvetően befolyásolja a válságkezelés sikerét. Ennek nyomán mind globális, mind nemzeti és helyi szinten kihívásként jelent meg a reziliencia intézményesítése a közigazgatásban és a létfontosságú szolgáltatások biztosításában.

A bevezető célja, hogy meghatározza a reziliencia, azaz az ellenálló képesség fogalmát, és keretet adjon a későbbi elemzésnek. A rezilienciát általánosan egy rendszer azon kapacitásaként definiálják, hogy képes megbirkózni a külső sokkokkal, alkalmazkodni a változásokhoz, és megőrizni alapvető struktúráit és funkcióit.[4] Ez nem pusztán a „visszapattanást" jelenti a kiinduló állapotba, hanem gyakran „előre pattanást" is. A rendszer tanul a krízisből és akár egy új, jobb egyensúlyi állapotba fejlődik tovább. A közigazgatásban a reziliencia fogalma sok tekintetben szembemegy a hagyományos bürokratikus jellemzőkkel, a merev hierarchiával és szabályorientáltsággal, és rugalmasabb, adaptívabb működésmódot követel meg a váratlan helyzetek kezelésére.[5]

A reziliencia fogalma az elmúlt évtizedekben több tudományterületen is megjelent, eltérő értelmezési keretek között. Eredetileg az ökológia és a pszichológia területén használták, ahol a rendszerek és egyének alkalmazkodóképességét, illetve a sokkhatások utáni helyreállítás képességét írta le.[6] A biztonságpolitika és a közigazgatás területén a reziliencia ennél összetettebb jelentéstartalmú, mivel nem csupán a helyreállítás, hanem a megelőzés, az alkalmazkodás és az átalakulás képességét is magában foglalja.[7]

A szakirodalom a rezilienciát gyakran négy alapvető dimenzió mentén értelmezi: ellenállás, alkalmazkodás, helyreállítás és tanulás. E megközelítés szerint a reziliens rendszer nemcsak túléli a válsághelyzeteket, hanem képes azokból tanulságokat levonni, és működését ennek megfelelően módosítani. A kritikus szervezetek esetében ez különösen fontos, mivel működésük zavara közvetlen hatással van a társadalom alapvető funkcióira. A közigazgatási és biztonságpolitikai értelmezésekben a reziliencia egyre inkább kormányzási paradigmává válik.[8] Nem kizárólag technikai védelemként jelenik meg, hanem olyan szervezeti és intézményi képességként, amely a komplex és kiszámíthatatlan kockázati környezethez való alkalmazkodást segíti elő. A reziliencia e felfogásban nem helyettesíti a klasszikus védelemfogalmakat, hanem kiegészíti azokat, hangsúlyt helyezve a rugalmasságra és a hálózatos együttműködésre.[9]

A szerzők által alkalmazott kutatási módszertan kvalitatív módszertanon alapul, dokumentumelemzés és összehasonlító szakpolitikai elemzés alkalmazásával. Jelen cikk a reziliencia jelentőségét tárgyalja a közigazgatásban és a gazdasági szereplők működésében, különös tekintettel arra, miként járul hozzá a lakosság alapvető ellátásbiztonságához és a katasztrófavédelmi felkészültséghez. Ezt követően a szerzők

[4] Gunderson 2010.
[5] Profiroiu–Nastacă 2021.
[6] Székely 2015.
[7] Kádár–Keszely 2025.
[8] Mógor – Baloghné Pruha 2025.
[9] Ambrusz–Vásárhelyi 2025.

összehasonlítják az Európai Unió és az Amerikai Egyesült Államok szabályozási kereteit e területen, rávilágítva a megközelítésbeli különbségekre és hasonlóságokra.

A reziliencia jelentősége a közigazgatásban, önkormányzatokban és ellátásbiztonságban

A közigazgatási intézmények rezilienciája kulcsfontosságú a társadalom egésze szempontjából, mivel a kormányzati szerveknek válsághelyzetek idején is biztosítaniuk kell az alapvető közszolgáltatásokat és a rend fenntartását.[10] Rámutatnak, hogy a közintézményeknek erősíteniük kell képességeiket a rendkívüli események kezelésére, vagyis a különféle külső és belső váratlan hatásokkal szemben ellenállóvá kell válniuk. Ez magában foglalja a kockázatok folyamatos értékelését, vészhelyzeti tervek kidolgozását, a személyzet képzését és a szervezeti rugalmasság fejlesztését. Az intézményi reziliencia növelése azért létfontosságú, mert a merev, centralizált rendszerek nehezebben reagálnak gyorsan a krízisekre, míg a tanuló szervezetek és a hálózatos együttműködések hatékonyabbak a válságok során. Empirikus tapasztalat, hogy a kormányzatok minősége és felkészültsége nagymértékben hozzájárul a válságok sikeres kezeléséhez vagy kudarcához. A krízisekre való felkészülést ezért rendszerszinten be kell építeni a kormányzati működésbe. Így elkerülhető, hogy vészhelyzetben kizárólag improvizatív, rendkívüli eszközökre kelljen támaszkodni. Önkormányzati szinten a reziliencia még közvetlenebb módon érződik a lakosság mindennapi biztonságában. A települési önkormányzatok felelnek számos alapvető közszolgáltatásért, mint az ivóvíz, helyi közlekedés, hulladékkezelés, alapegészségügyi ellátás vagy a közbiztonság, ezért válsághelyzetben elsődleges, hogy e szolgáltatások fenntartása biztosítva legyen. A 2020–2021-es pandémiás tapasztalatok rámutattak, hogy ahol az önkormányzatok megfelelő autonómiával, erőforrásokkal és krízistervekkel rendelkeztek, ott a helyi közösségek jobban átvészelték a járványt, míg a centralizációs intézkedések és az erőforráshiány sok helyen gátolták a hatékony reagálást.[11] Az önkormányzati ellenálló képesség fejlesztése ezért kiterjed a helyi szintű kockázatértékelésre, a közösségi tervezésre és a civil szektor bevonására is a vészhelyzeti előkészületekbe.

A közigazgatási intézmények rezilienciája ennek megfelelően a modern állam működőképességének egyik alapfeltétele. Válsághelyzetek idején – legyen szó természeti katasztrófáról, járványról vagy technológiai eredetű zavarokról – a közigazgatás feladata nem csupán a rend fenntartása, hanem az alapvető közszolgáltatások folytonosságának biztosítása is. A reziliens közigazgatás ezért olyan intézményi és szervezeti képességekkel rendelkezik, amelyek lehetővé teszik a gyors döntéshozatalt, az erőforrások rugalmas átcsoportosítását és a hatékony koordinációt.

Végül, a reziliencia kritikus a lakosság ellátásbiztonsága szempontjából is. Ide tartozik mindazon kritikus infrastruktúrák és alapvető szolgáltatások köre, mint az energiaellátás, ivóvíz- és élelmiszer-ellátás, az egészségügyi rendszer, pénzügyi szolgáltatások, hírközlés, közlekedés stabil működtetése, amelyek nélkül a mindennapi

[10] Profiroiu–Nastacă 2021.
[11] Pálné Kovács 2023.

élet megbénulna. Az Európai Bizottság megfogalmazása szerint „megbízható energiaellátás, biztonságos ivóvíz, egészségügyi szolgáltatások, banki és pénzügyi szolgáltatások, infokommunikációs szolgáltatások, valamint kiszámítható közlekedés nélkül modern életformánk lehetetlen lenne", ezért a kritikus infrastruktúrák védelme és a kritikus entitások rezilienciája alapvető a társadalom számára. Ebben a relációban kiemelt szerepe van a kibertér védelmének, amely tovább erősíti azt, hogy a kritikus infrastruktúrákon belüli kiberbiztonság megvalósítása elemi érdeke kell hogy legyen minden infrastruktúra-tulajdonosnak és üzemeltetőnek.[12]

A lakossági ellátásbiztonság rezilienciája azt jelenti, hogy e rendszerek képesek ellenállni a természeti katasztrófáknak (árvíz, földrengés, viharkárok), a technológiai meghibásodásoknak (hálózati üzemzavarok), az emberi eredetű fenyegetéseknek (terrorizmus, kibertámadás), valamint esetleges szolgáltatáskimaradást követően gyorsan helyre tudnak állni. Az ellátásbiztonság érdekében kulcsfontosságú a kockázatok azonosítása, elemzése és értékelése, a katasztrófavédelmi tervezés és gyakorlatok végzése, a redundáns kapacitások kialakítása (tartalék rendszerek, alternatív ellátási útvonalak), valamint a lakosság tájékoztatása és bevonása az önvédelmi képességek fejlesztésébe. Összességében tehát a reziliencia elősegíti, hogy a kritikus szervezetek és infrastruktúrák a lehető legkisebb fennakadással vészeljék át a krízíseket, biztosítva ezzel a közszolgáltatások folytonosságát, a társadalmi és gazdasági folyamatok fenntartását.

A közigazgatás és az ellátásbiztonság rezilienciájának erősítése ezért olyan átfogó megközelítést feltételez, amely integrálja a jogi szabályozást, az intézményi kapacitásfejlesztést és a társadalmi együttműködést. E komplex szemlélet képezi azt a keretet, amelyben értelmezhető az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási rendszereinek összehasonlítása. Az összehasonlító elemzés részletes eredményeit a következő fejezet mutatja be.

Az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási kereteinek összehasonlítása

Az Európai Unió megközelítése

Az EU-ban az elmúlt két évtizedben fokozatosan épült ki a kritikus infrastruktúrák védelmének és rezilienciájának átfogó keretrendszere. Kezdetben a hangsúly a kritikus infrastruktúrák védelmén volt (*critical infrastructure protection,* CIP), különösen a 2000-es években meghozott 2008/114/EK irányelvben, amely az európai kritikus infrastruktúrák azonosítását, kijelölését és védelmét célozta meg főként az energia- és közlekedési ágazatban.[13] Az utóbbi években azonban az EU stratégiája jelentős paradigmaváltáson ment keresztül, áthelyezve a hangsúlyt a védelemről a reziliencia növelésére.[14] E szemléletváltást tükrözi az új, 2022-ben elfogadott kritikus entitások

[12] Kovács 2018a.
[13] European Commission 2026.
[14] Tierney 2015.

rezilienciájáról szóló irányelv *(Directive on the Resilience of Critical Entities, 2022/2557 EU Directive),* amely 2023 januárjában lépett hatályba.[15]

Az új szabályozás olyan összveszély *(all-hazards)* megközelítést alkalmaz, amely nemcsak a terrorcselekmények vagy szándékos károkozás ellen kíván védelmet nyújtani, hanem a természeti veszélyek, járványok, káresemények és egyéb fenyegetések ellen is erősíti az alapvető szolgáltatásokat nyújtó szervezetek ellenálló képességét.

Az irányelv előírja, hogy a tagállamok fogadjanak el nemzeti stratégiát a kritikus entitások rezilienciájára, és rendszeresen végezzenek nemzeti kockázatértékelést, amelyek alapján az ellenálló képesség fokozására stratégiai célkitűzéseket és prioritásokat állapítsanak meg, valamint támogassák a kritikus szervezetek kockázatértékelését és ezáltal az ellenálló képességi intézkedéseit.

Az Európai Bizottság közös uniós alapvető szolgáltatás lista alapján segíti ezt a munkát, amely meghatározza az érintett ágazatokat és szolgáltatásokat. Az irányelv tizenegy kulcságazatot sorol fel, köztük az energiát, a közlekedést, a banki szolgáltatásokat, a pénzügyi piaci infrastruktúrát, az egészségügyet, az ivóvíz- és szennyvízszolgáltatást, a digitális infrastruktúrát, az élelmiszer-ellátást, valamint a közigazgatást és az űrinfrastruktúrát is. Újdonság, hogy a „kritikus entitás" fogalma alá már nemcsak a hagyományos értelemben vett infrastrukturális üzemeltetők tartoznak, hanem például állami hivatalok vagy kulcsfontosságú hatóságok is, vagyis minden olyan szervezet, amely nélkülözhetetlen a társadalom és gazdaság működéséhez.[16] A kritikus entitásoknak saját kockázatelemzést kell készíteniük, és megfelelő technikai, fizikai és szervezési intézkedéseket kell bevezetniük a rezilienciájuk fokozása érdekében, beleértve az ellenálló képességi tervek készítését és az incidensek bejelentését a hatóságok felé. A tagállamok kötelesek támogatást nyújtani e szervezeteknek (például képzések, útmutatók, pénzügyi támogatások formájában), míg az Európai Bizottság uniós szinten összehangolja az információcserét, bevált gyakorlatok megosztását, közös kockázatelemzést és akár határokon átnyúló szimulációs gyakorlatokat is szervez. Fontos eleme a keretnek a tagállamok közötti és uniós szintű koordináció, amelynek érdekében hozták létre a Kritikus Entitások Rugalmassági Csoportját (Critical Entities Resilience Group, CERG), amely biztosítja a nemzeti hatóságok képviselőinek és az európai bizottsági szakértőknek az együttműködését. Emellett válaszul az utóbbi évek kritikus infrastruktúrák elleni incidenseire (például gázvezeték-szabotázs), 2022 végén az EU Tanácsa ajánlást fogadott el a tagállamok reziliencianövelő intézkedéseinek összehangolt erősítésére, külön hangsúlyt fektetve a megelőzésre, felkészülésre és reagálásra.

Az Európai Unió a kiberbiztonsági stratégiájában olyan holisztikus megközelítést alkalmaz, amely jóval túlmutat a kibertéren, hiszen az olyan kapcsolódó területek biztonságának növelését is célul tűzte ki, mint a kritikus infrastruktúrák területe. Az ellenálló képesség terén a stratégia kiemeli a kiberbiztonsági tudatosság fejlesztését, amelyben a felhasználók internetes tevékenységeinek minél nagyobb biztonságát hangsúlyozza.[17]

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

[16] Lazari 2022.

[17] Kovács 2018a.

Összességében az EU megközelítését a szabályozási minimumkövetelmények és a jogilag kötelező erejű keretek jellemzik. Az uniós tagállamok számára előírás, hogy a kritikus ágazatokban működő entitásokkal szemben bizonyos biztonsági és üzletmenet-folytonossági követelményeket támasszanak, és ezeket a nemzeti jogba átültetve betartassák. Ugyanakkor az EU felismeri a tagállami szuverenitás és felelősség szerepét, így a keretrendszer rugalmasan alkalmazható a nemzeti sajátosságokhoz, de egy közös minimumszintet garantál a teljes Unió területén.

Az Amerikai Egyesült Államok megközelítése

Az Egyesült Államokban a kritikus infrastruktúrák védelmének és rezilienciájának stratégiája hosszabb múltra tekint vissza, bár jogilag kötelező erejű szövetségi törvény helyett inkább elnöki direktívák és stratégiák formájában fejlődött. Már 1998-ban kiadtak egy elnöki határozatot (*Presidential Decision Directive,* PDD-63), amely először nevezte meg a kritikus infrastruktúra védelmét nemzetbiztonsági prioritásként.[18]

Ezt követően, a 2001. szeptember 11-i terrortámadások hatására és a Belbiztonsági Minisztérium (Department of Homeland Security, DHS) létrehozásával, az USA fokozta erőfeszítéseit a kritikus infrastruktúrák azonosítása és védelme terén. Az amerikai megközelítés sajátossága, hogy a kritikus infrastruktúrák jelentős része magántulajdonban van, ezért a kormányzat a köz- és magánszféra partnerségére épít a védelem és a reziliencia terén.[19]

A 2013-ban kiadott 21. számú Elnöki Politikai Irányelv (*Presidential Policy Directive,* PPD-21) már a kritikus infrastruktúra biztonsága és rezilienciája címet viselte, jelezve, hogy a fizikai védelem mellett hangsúlyt kapott a gyors helyreállítás képessége is.

A PPD-21 deklarálta, hogy az amerikai kritikus infrastruktúráknak „biztonságosnak és képeseknek kell lenniük ellenállni, valamint gyorsan kiheverni minden lehetséges veszélyt", összhangban a nemzeti felkészültségi rendszerrel a megelőzés, a védelem, a mitigáció, a reagálás és a helyreállítás teljes spektrumában. Az irányelv átfogó politikai célként tűzte ki a sebezhetőségek csökkentését, a lehetséges következmények minimalizálását, a fenyegetések felderítését és megzavarását, valamint a reagálási és helyreállítási képességek javítását a kritikus infrastruktúra területén. Emellett hangsúlyozta a nemzeti egységes fellépés szükségességét, amelynek értelmében a felelősség megoszlik a szövetségi, állami, törzsi és helyi kormányzatok, valamint a magánszektorbeli üzemeltetők között. A szövetségi kormányzat feladata a koordináció javítása különösen a Belbiztonsági Minisztérium, DHS révén, az információmegosztás elősegítése a kormányzati szervek és a magánszektor között, valamint az ágazatspecifikus ügynökségek (Sector-Specific Agencies, ma Sector Risk Management Agencies, SRMA) szerepének erősítése. Az USA 16 kritikus infrastrukturális szektort határozott meg (például energia, víz, élelmiszer és mezőgazdaság, egészségügy, vészhelyzeti szolgáltatások, közlekedés, pénzügyi szolgáltatások, kommunikáció,

[18] Lazari 2022.
[19] The White House 2013.

vegyipar), és mindegyikhez kijelölt egy felelős szövetségi szervet, amely az adott szektor kockázatkezelését és védelmi együttműködését irányítja.

Az USA-ban sokáig iránymutató, önkéntes jellegű keretrendszer működött. A kritikusinfrastruktúra-üzemeltetők jelentős részére nem vonatkozott egységes szövetségi törvény vagy kötelező sztenderd a reziliencia terén, néhány erősen szabályozott ágazat, például nukleáris létesítmények vagy a villamosenergia-hálózat kivételével. Ehelyett a kormányzat ösztönzőkkel, partnerségi programokkal, mint információcsere-fórumokkal, közös gyakorlatokkal, védelmi tervezési útmutatók kiadásával támogatta a magáncégeket abban, hogy javítsák saját biztonsági és üzletmenet-folytonossági terveiket. Ez a megközelítés rugalmasságot biztosított, de sok szakértő rámutatott a korlátaira is, különösen a kibertámadások és az új típusú fenyegetések korában. Az utóbbi években részben a kiéleződő geopolitikai versengés és az infrastruktúrákat érő kibertámadások hatására az USA stratégiája is változóban van.

2024 áprilisában az amerikai elnök új nemzetbiztonsági memorandumot adott ki (*National Security Memorandum,* NSM-22), amely felülírta a korábbi PPD-21 irányelvet, és átfogó erőfeszítést indított a kritikus infrastruktúrák minden fenyegetéssel és veszéllyel szembeni védelmére. Az új stratégia megerősíti a DHS vezető szerepét a kritikus infrastruktúra rezilienciakoordinációjában a Kiber- és Infrastruktúra-biztonsági Ügynökséget (Cyber and Infrastructure Security Agency, CISA) jelölve ki nemzeti koordinátornak, valamint előírja egy kétévente megújítandó *Nemzeti Kockázatkezelési Terv (National Risk Management Plan)* elkészítését, amely áttekinti a legfőbb fenyegetéseket és a kezelésükre tett intézkedéseket. Mindezek mellett a DHS alárendeltségében működik a Nemzeti Kiberbiztonsági és Kommunikáció Integrációs Központ (National Cybersecurity and Communications Integration Center, NCCIC), amely napi 24 órában, heti 7 napon biztosítja szövetségi szinten az eseménykezelési és irányítási feladatokat. Emellett ez a szervezet kapcsolatot biztosít a szövetségi kormány, a hírszerző közösség és a bűnüldözési hatóságok kiber- és kommunikációs szervezetei között.[20] Az NSM-22 megerősíti a 16 kritikus szektor rendszerét és az azokért felelős szövetségi ügynökségek mandátumát, ugyanakkor kiemeli a minimális biztonsági és rezilienciakövetelmények fontosságát az egyes szektorokban, felismerve, hogy pusztán az önkéntes kockázatkezelés nem elegendő a jelenlegi fenyegetettségi környezetben. Ez a retorika egy szigorúbb, szabályozottabb megközelítés felé mozdulást jelez, különösen a kibervédelmi előírások terén, mint például a kötelező incidensbejelentés vagy alapvető kiberhigiéniai követelmények előírányzása bizonyos infrastruktúráknál. Az új stratégia az „előre építkező reziliencia" elvét hangsúlyozza.

Ennek megfelelően a jelentős szövetségi infrastrukturális beruházások (például az infrastruktúra-fejlesztési törvénycsomag keretében) során eleve olyan projekteket finanszíroznak, amelyek figyelembe veszik a jövőbeli éghajlati és biztonsági kockázatokat, így már tervezéskor beépül a reziliencia a rendszerekbe. Az NSM-22 továbbá elismeri, hogy „a reziliencia a hazai védelem és biztonság sarokköve", mivel ellenálló kritikus infrastruktúra nélkül az ország ellenfelei válság vagy konfliktus idején könnyebben okozhatnak zavart a lakosság bizalmában és az ország haderejének mozgósíthatóságában.

[20] Kovács 2018b: 350.

Az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási megközelítései közötti főbb különbségeket és hasonlóságokat az 1. táblázat foglalja össze.

1. táblázat: Az EU és az USA rezilienciaszabályozásának összehasonlítása

Szempont	**Európai Unió**	**Egyesült Államok**
Szabályozás jellege	Jogilag kötelező irányelvek	Elnöki irányelvek, stratégiák
Kormányzási modell	*Top-down,* harmonizált	Decentralizált, partneri
Kritikus szervezetek tulajdonosi szerkezete	Vegyes, jelentős állami szerep	Túlnyomórészt magántulajdon
Reziliencia fókusza	Strukturális és intézményi	Funkcionális és operatív
Magánszektor szerepe	Szabályozott, korlátozottabb	Meghatározó
Kötelező követelmények	Egységes minimumkövetelmények minden tagállamban	Ágazatonként eltérő, növekvő tendencia
Rugalmasság	Korlátozottabb	Magas
Innováció ösztönzése	Közvetett	Erőteljes
Jövőbeni trendek	Minimumkövetelmények erősítése	Szabályozás szigorodása

Forrás: a szerzők szerkesztése

Összefoglalva, az amerikai keretrendszer napjainkra közelít az európaihoz abban az értelemben, hogy egyre inkább felismeri a kötelező minimumkövetelmények szükségességét a reziliencia területén (különösen a kibertérben), miközben továbbra is támaszkodik a magánszektor együttműködési hajlandóságára és innovációjára. Mindkét rendszer hangsúlyozza *az all-hazards* megközelítést, vagyis hogy a kritikus infrastruktúrákat és a kritikus szervezeteket egyaránt védeni kell a természeti katasztrófáktól, káreseményektől és a rosszindulatú támadásoktól.

A koordináció és információmegosztás fontossága szintén közös elem. Az EU a tagállami hatóságok és a Bizottság közötti együttműködést formálissá téve (CER irányelv és munkacsoport révén), míg az USA a szövetségi, állami és magánszereplők közötti partnerséget erősítve igyekszik „nemzeti egységben" kezelni a kihívásokat.[21]

Ugyanakkor a megközelítések különböznek a szabályozási kultúra miatt, mivel Európában jogszabály rögzíti, míg Amerikában ezt sokszor inkább ajánlások és iparági standardok határozzák meg – legalábbis mostanáig. A trend mindkét oldalon a reziliencia intézményesülése és integrálása a mindennapi működésbe, nem csupán válsághelyzeti kérdésként kezelve azt.

Következtetés

A kritikus szervezetek rezilienciája mára a katasztrófavédelem és a nemzetbiztonság kiemelt területévé vált, hiszen a társadalom és a gazdaság ellenálló képessége jelentős részben attól függ, hogy e szervezetek miként képesek megbirkózni a váratlan eseményekkel. A szerzők rámutattak arra, hogy a reziliencia nem statikus állapot, hanem

[21] The White House 2013.

állandóan fejlesztendő folyamat, amely magában foglalja a felkészülést a krízisekre, a hatékony reagálást a bekövetkező rendkívüli eseményekre, valamint a tanulást és alkalmazkodást a válságot követően.

A közigazgatásban és a gazdasági szereplők működésében a reziliencia erősítése olyan reformokat és szervezeti kultúraváltást igényel, amelyek a merev bürokratikus működés helyett a proaktív, rugalmas és együttműködésen alapuló megoldásokat helyezik előtérbe. A lakossági ellátásbiztonság szempontjából pedig kulcsfontosságú, hogy a kritikus szervezetek és infrastruktúrák már békeidőben felkészüljenek a lehetséges rendkívüli eseményekre, ami nemcsak technikai kérdés, hanem stratégiai tervezési és kormányzási feladat is.

A tanulmány célja az volt, hogy összehasonlító elemzés keretében bemutassa az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási megközelítéseit a kritikus szervezetek vonatkozásában, valamint feltárja azokat az intézményi és jogi különbségeket, amelyek meghatározzák az ellenálló képesség fejlesztésének módját.

Az Európai Unió és az Egyesült Államok rezilienciakereteinek összehasonlítása rávilágított arra, hogy bár földrajzilag és intézményileg eltérő környezeti viszonyokról van szó, a célkitűzések hasonlók. Ezek elsődlegesen a szolgáltatások folytonosságának biztosítása minden körülmények között, a társadalom biztonságérzetének fenntartása, valamint a károk minimalizálása és a gyors helyreállítás krízisek idején. Az EU az egységes szabályozás és a tagállami végrehajtás kombinációjával igyekszik koordinált rezilienciát teremteni, míg az USA a decentralizált, partneri megközelítést ötvözi újabban erősödő központi iránymutatással.

Mindkét megközelítésből tanulhatnak egymástól a felek. Az EU-nak hasznos lehet az amerikai rugalmasság és innováció ösztönzése, míg az USA számára az európaiak tapasztalata a minimumkövetelmények és nemzeti stratégiák terén szolgálhat iránymutatásul. A két megközelítés közeledése arra utal, hogy a jövőben egy hibrid modell válhat meghatározóvá, amely ötvözi a jogi kötelezettségek és a partnerségen alapuló megoldások előnyeit. Végső soron a kritikus szervezetek rezilienciájának növelése közös társadalmi érdek, amely megköveteli a tudományos ismeretek, a szakpolitikai döntéshozatal és a gyakorlati végrehajtás szoros összefonódását. A reziliens infrastruktúrák kiépítése a jövő kihívásaival szembeni legjobb befektetés, hiszen erősíti a lakosság biztonságát, a társadalom és a gazdaság stabilitását, ezáltal a nemzetek ellenálló képességét a 21. század sokrétű veszélyeivel szemben.

Felhasznált irodalom

Ambrusz József – Vásárhelyi Örs (2025): A kritikus szervezeti reziliencia és a lakosságfelkészítés nemzetbiztonsági jelentősége a modern fenyegetésekkel szemben. *Nemzetbiztonsági Szemle,* 13(2), 74–93. Online: https://doi.org/10.32561/nsz.2025.2.6

European Commission (2026): *Critical Infrastructure Resilience at EU-level.* Online: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

Gunderson, Lance (2010): Ecological and Human Community Resilience in Response to Natural Disasters. *Ecology and Society,* 15(2). Online: https://doi.org/10.5751/ES-03381-150218
Kádár Pál – Keszely László (2024): A nemzeti ellenálló képesség – a Vbö. V. fejezete. In Kádár Pál (szerk.): *A védelmi és biztonsági szabályozás magyarországi reformja.* Budapest: Ludovika, 185–206. Online: https://doi.org/10.36250/01232_07
Kovács László (2018a): *A kibertér védelme.* Budapest: Dialóg Campus. Online: www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf
Kovács László (2018b): *Kiberbiztonság és -stratégia.* Budapest: Dialóg Campus.
Mógor Judit – Baloghné Pruha Mária (2025): A kockázat alapú gondolkodás gyakorlati elemei a kritikus szervezeteknél I. rész. *Védelem Tudomány*, 10(3), 14–25. Online: https://doi.org/10.61790/vt.2025.20648
Lazari, Alessandro (2023): Comparing Policy Frameworks: Critical Infrastructure Security and Resilience in the United States and the European Union. In Evans, Carol V. et al. (szerk.): *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency.* Carlisle PA: USAWC Press, 155–170. Online: https://press.armywarcollege.edu/monographs/955
Pálné Kovács Ilona (2023): Az önkormányzati válságkezelés és/vagy reziliencia: Szakirodalmi szemle. *Tér és Társadalom,* 37(1), 3–22. Online: https://doi.org/10.17649/TET.37.1.3465
Profiroiu, Alina Georgiana – Nastacă, Corina-Cristiana (2021): What Strengthens Resilience in Public Administration Institutions? *Eastern Journal of European Studies,* 12(Special Issue), 100–125. Online: https://doi.org/10.47743/ejes-2021-SI05
Székely Iván (2015): Reziliencia: a rendszerelmélettől a társadalomtudományokig. *Replika,* (94), 7–23. Online: http://real.mtak.hu/id/eprint/110083
The White House (2013): *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience.* Washington, DC: Office of the Press Secretary. Online: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/
The White House (2024): *Fact Sheet: Biden-Harris Administration Announces New National Security Memorandum on Critical Infrastructure.* Washington, DC: Office of the Press Secretary. Online: www.presidency.ucsb.edu/documents/fact-sheet-biden-harris-administration-announces-new-national-security-memorandum-critical
Tierney, Kathleen (2015): Disaster Resilience and the Neoliberal Project: Discourses, Critiques, Practices – And Katrina. *American Behavioral Scientist,* 59(10), 15–36. Online: https://doi.org/10.1177/0002764215591187

Jogi forrás

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