# CRITICAL INFRASTRUCTURE FOR FUTURE-PROOFNESS

# A JÖVŐBIZTOS KRITIKUS INFRASTRUKTÚRA

PÁL Anita[1]

**Abstract**

In recent years, critical infrastructures such as energy supply, water supply and transport networks have increasingly become dependent on IT systems and digital communication, which has significantly increased their vulnerability to cyber threats and technological errors. The application of AI in critical infrastructure cancer opens up new opportunities for increasing operational efficiency, early detection of threats and rapid response, but at the same time it also raises ethical dilemmas, such as autonomous decision-making and the lack of human supervision. The article highlights that the protection of critical infrastructure requires not only national, but also international cooperation in the fight against cyber threats, and that the stability and security of modern societies is closely related to the effective protection of critical infrastructures, which is essential for future challenges in treatment..

**Keywords**

Artificial Intelligence (AI), Critical Infrastructure Protection, Cyber Security, Industry 5.0, Digital Dependence, Security-Political Instability

**Absztrakt**

Az elmúlt években a kritikus infrastruktúrák, mint az energiaellátás, a vízellátás és a közlekedési hálózatok, növekvő mértékben váltak függővé az informatikai rendszerektől és a digitális kommunikációtól, ami jelentősen növelte ezek sérülékenységét a kiberfenyegetésekkel és technológiai hibákkal szemben. Az MI alkalmazása a kritikus infrastruktúrákban új lehetőségeket nyit meg az operatív hatékonyság növelésére, a fenyegetések korai felismerésére és a gyors válaszadásra, ugyanakkor etikai dilemmákat is felvet, mint az autonóm döntéshozatal és az emberi felügyelet hiánya. A cikk kiemeli, hogy a kritikus infrastruktúra védelme nem csupán a nemzeti, hanem a nemzetközi összefogást is igényli a kiberfenyegetések elleni küzdelemben, valamint hogy a modern társadalmak stabilitása és biztonsága szorosan összefügg a kritikus infrastruktúrák hatékony védelmével, ami elengedhetetlen a jövő kihívásainak kezelésében.

**Kulcsszavak**

Mesterséges intelligencia (MI), Kritikus infrastruktúra védelme, Kiberbiztonság, Ipar 5.0, Digitális függőség, Biztonságpolitikai instabilitás

[1] pal.anita@phd.uni-obuda.hu | ORCID: 0000-0003-4750-193X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

# A JÖVŐBIZTOS KRITIKUS INFRASTRUKTÚRA: AZ MI SZEREPE A VÉDELEMBEN ÉS STABILITÁSBAN

A 21. század küszöbén az infrastruktúrák biztonsága és sebezhetősége kiemelkedő fontossággal bír a modern társadalmakban. Az egyre összetettebbé váló infrastruktúrák digitális függősége növeli a kibertámadások és technológiai hibák kockázatát, amelyek visszafordíthatatlan gazdasági, társadalmi és biztonságpolitikai instabilitást okozhatnak. A kritikus infrastruktúra védelme kulcsfontosságú a biztonsági percepció működésének szempontjából. A mesterséges intelligencia és az új kibertéri fegyverek megjelenése új dimenziókat nyitottak a kiberbiztonságban és a védelemben. A digitális támadások aszimmetrikus jellege és pusztító ereje arra sarkall, hogy prioritásként kezeljük a kritikus infrastruktúra elleni védelmet és a megelőzést.

## Az informatikai forradalom hatása a kritikus infrastruktúrára

Az informatikai forradalom, különösen az elmúlt évtizedekben, forradalmi változásokat hozott a társadalmainkban és gazdaságainkban. Az információs technológia térnyerése és az internet elterjedése gyökeresen átalakította a világ működését. Az információs forradalom ugyanakkor létrehozta az infrastruktúra sebezhetőségeinek új dimenzióját is. Az egyre összekapcsoltabbá váló és kölcsönös függőségen alapuló világban a kritikus infrastruktúra elemei fokozottan függenek az informatikai rendszerektől és az adatoktól. Ezáltal a digitális fenyegetések és a kiberbiztonság kérdései létfontosságúvá váltak. Így ebben a kontextusban, a mesterséges intelligencia megjelenése új lehetőségeket kínál a kritikus infrastruktúra működésének javítására, valamint a veszélyek korai felismerésére. Ugyanakkor alkalmazása új kihívásokat vet fel az adatvédelem, az etika és az emberi beavatkozás kérdéseiben.

A globalizáció és a technológiai fejlődés erőteljesen összefonódott, és ezek közös hatásaiban létrejöttek a hálózat és az Ipar 5.0 koncepciói. Az 5G (ötödik generációs) hálózat a legújabb és leggyorsabb mobilkommunikációs technológia, amely kiemelkedő sebességet, alacsony késleltetést és nagy adatkapacitást kínál. A globális összekapcsoltság és az adatok gyors és nagy mennyiségű átvitele révén az 5G lehetővé teszi az új technológiák, mint például a dolgok internete (IoT) széleskörű alkalmazását. Az Iparban megjelent 5.0 egy paradigmaváltást jelent, amely elmossa a határokat a digitális és a fizikai világok között. Az 5G és az Ipar 5.0 egymást erősítik, mivel az 5G kiterjedt hálózati kapacitása és az alacsony késleltetés lehetővé teszi a gyors és pontos adatátvitelt, amely elengedhetetlen az Ipar 5.0 alkalmazásaihoz. Komplexitása miatt ezen hálózatok kezelése nem képzelhető el kognitív funkciók és a mesterséges intelligencia használata nélkül.[1]

Az Internet of Things (IoT) egy dinamikus globális információs hálózat, amely olyan eszközökből áll, amelyek mind rendelkeznek internetkapcsolattal. Ezek az eszközök olyan rádiófrekvenciás azonosítókból, érzékelőkből és hajtóerőkből állnak, amelyek az internet elválaszthatatlan részét képezik. Így az elmúlt évek során egyre több olyan megoldás jelent meg az iparági piacokon amelyek között széles körben alkalmazták a kontextus-érzékeny technológiai szempontokat. A kontextus-érzékeny technológiai szempontok olyan faktorok és elemek, amelyek figyelembe veszik és reagálnak a környező kontextus vagy környezet változásaira, hogy javítsák a rendszer teljesítményét, alkalmazkodhassanak a körülményekhez és növeljék a felhasználói élményt.[2]

Az ipari szolgáltatások prioritásának megváltozásával felgyorsult az IoT (Internet of Things) bevezetése a COVID-19 járvány idején. A kedvezőtlen körülmények hatására bekövetkezett digitalizáció rugalmasabbá és változatosabbá tette az életfontosságú infrastruktúrák fontosságát.[3]

Azonban ezek a technológiai fejlesztések, különösen az 5G, egyben sérülékenyebbé is tehetik a kritikus infrastruktúrát. A nagyobb függőség az 5G és az Ipar 5.0 terjedésével, növeli a digitális támadások iránti kockázatok lehetőségét. A kritikus infrastruktúrák, mint például az energiaellátás, a víz- és élelmiszer-ellátás, az egészségügyi rendszerek, az adatközpontok stb., szorosan kapcsolódnak az informatikai rendszerekhez és az 5G-hez. A támadók kihasználhatják a sebezhetőségeket azáltal, hogy az 5G és az Ipar 5.0 rendszereket célzottan támadják, ami komoly következményekkel járhat a társadalom és a gazdaság számára, mint ahogy azt a Stuxnet esetében is láthattuk, ahol egy célzott ipari támadásról volt szó, amely főként a nukleáris erőművek vezérlőrendszereit célozta meg. A megfelelő védelem és kiberbiztonsági intézkedések elengedhetetlenek az ilyen típusú fenyegetések leküzdéséhez és a kritikus infrastruktúra biztonságának megőrzéséhez.

**Mi számít kritikus infrastruktúrának?**

Az infrastruktúrák, különösen a kritikus infrastruktúrák, a társadalmunk meghatározó pillérjeit képezik. A szóban forgó rendszerek és létesítmények, mint például az energiaellátás, vízellátás, közlekedési hálózatok és kommunikáció, nem csupán a mindennapi életünk zavartalan működéséhez szükségesek, hanem az országok gazdasági stabilitását és nemzetbiztonságát is alapvetően meghatározzák. Ha ezek a rendszerek meghibásodnak vagy támadás éri őket, akár az élet és halál kérdése is felmerülhet.

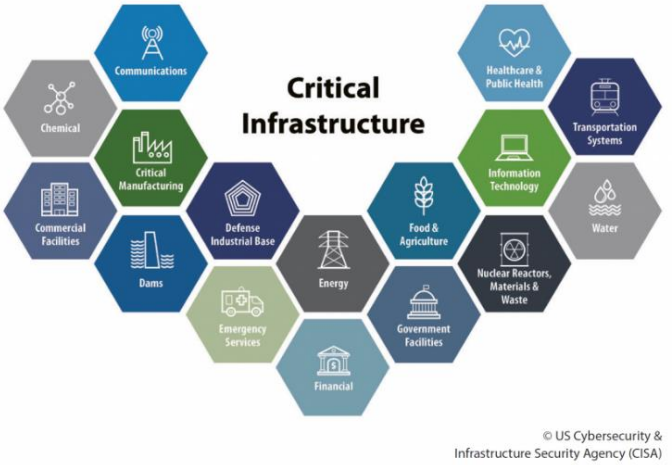
A kritikus infrastruktúra különböző ágazatokat ölel fel, például az energiaellátást (villamosenergia-termelés, gáz- és olajellátás), a víz- és hulladékgazdálkodást, a közlekedést (vasút, közút, légi közlekedés), az információs és kommunikációs rendszereket, valamint a pénzügyi és egészségügyi szektorokat. Nem csak a mindennapi élet alapvető pillérei, hanem az országok gazdasági stabilitásának és nemzetbiztonságának is kulcsfontosságú elemei. Ezeknek a rendszereknek a meghibásodása vagy támadás alá kerülése komoly veszélyeket jelent a társadalom számára.

A kritikus infrastruktúrák meghatározása és védelme bonyolult feladat, különösen a technológiai fejlődés és a digitális világ folyamatos változása miatt. Kihívást jelent meghatározni, hogy mely rendszerek és létesítmények számítanak létfontosságúnak, és hogyan kezeljük az új típusú kihívásokat, mint az aszimmetrikus hadviselés és a kibertér adta fenyegetések.

Az elengedhetetlen rendszerek határainak meghatározása a társadalom zavartalan működésének védelmét célozza meg, és folyamatosan változik a technológia fejlődésével.

Az alapvető szükségleteinket kielégítő infrastruktúrák védelme számos tényezőtől függ. Ide tartoznak azok a létesítmények, amelyek biztosítják a hozzáférést az ivóvíz-szolgáltatáshoz, a villamosenergia-ellátáshoz, a digitális szolgáltatásokhoz, a közösségi közlekedéshez, vagy az egészségügyi ellátáshoz. A negyedik ipari forradalom küszöbén az egyik legösszetettebb kérdéskört talán az lengi körbe, hogy a digitalizáció gyors fejlődési üteme által generált új típusú kihívások, az aszimmetrikus hadviselés és a kibertér adta "lehetőségek" közötti határvonal elmosódása miatt hol húzódik meg az a határ, ami garantálni tudja

a mindennapok zavartalanságát biztosító rendszerek védelmét. Felmerül a kérdés, hogy ezeket a határvonalakat milyen szempontok alapján strukturáljuk, vagy hogy szükség van-e szigorúbb előírásokra? A válasz mindig attól függ, hogy mi teszi a társadalom működéséhez nélkülözhetetlen rendszereket valóban elengedhetetlenné, létfontosságúvá vagy kritikussá.[4]




*1. Ábra: Critical Infrastructure Security Guide: Understanding and Securing our Nation's Critical Infrastructure*
*Understanding and Securing our Nation's Critical Infrastructure (valentisinc.com)*

A terminológia kérdése is felmerül, amikor a kritikus infrastruktúráról illetve annak megkülönbözőségéről beszélünk. Az általánosabban elfogadott "kritikus infrastruktúra" mellett vannak olyan fogalmak, mint a "létfenntartó rendszerek elemei," amelyek gyakran országspecifikusak. Amíg a "kritikus infrastruktúra" általánosabban elfogadott, és szélesebb körben használt a nemzetközi tudományos irodalomban, addig a "létfenntartó rendszerek elemei" fogalma inkább az adott ország jogszabályaiban definiált területspecifikus fogalom.[5]

A jelenlegi szakirodalom alapján kiemelkedő figyelmet fordítanak a nemzeti kritikus infrastruktúrák védelmére, ugyanakkor nem szabad elhanyagolni az európai és védelmi kritikus infrastruktúrák szerepét sem. Az infrastruktúra kritikusságát több szempontból is vizsgálhatjuk, például az ország területi szintjén beszélhetünk regionális, területi és lokális (például települési) kritikus infrastruktúrákról. A "kritikusság" dinamikusan változó tulajdonság lehet az adott felhasználói kör számára, és fontos az általános és helyzetfüggő kritikus infrastruktúrák megkülönböztetése.[6]

## A mesterséges intelligencia (MI) térnyerése és szerepe a kritikus infrastruktúra biztonságában

A mesterséges intelligencia (MI) rohamos fejlődése és alkalmazása a kritikus infrastruktúrákban, mint az energiaelosztás, közlekedés és katasztrófaelhárítás, forradalmasítja ezeknek a rendszereknek a működését, növelve hatékonyságukat és rendelkezésre állásukat. Bár az MI kínálta lehetőségek izgalmasak és sokrétűek a kritikus infrastruktúrák működtetésében és védelmében, az új technológiáknak a bevezetése komoly kihívásokat is felvet az

adatvédelem, az etika és a biztonság területén, különösen a kiberfenyegetések és az emberi hibákból eredő problémák tekintetében.

A mesterséges intelligencia olyan tudományág az informatika területén, amelynek célja olyan gépek és rendszerek kifejlesztése, amelyek képesek emberi intelligenciához hasonlóan gondolkodni és döntéseket hozni. Az MI technológiák és alkalmazások robbanásszerű fejlődése az elmúlt években forradalmasította a modern társadalmat és gazdaságot. Fejlődésük olyan területekre is kiterjed, amelyek már hosszú ideje a kritikus infrastruktúra részét képezik. Például, az MI rendszerek részt vesznek az energiaelosztás és hálózatok optimalizálásában, a közlekedési irányításban, valamint a katasztrófák előrejelzésében és reagálásában. Az MI által vezérelt eszközök és algoritmusok hatékonyabbá tehetik ezeknek az infrastruktúráknak a működését és növelhetik a rendelkezésre állásukat.

A mesterséges intelligencia alkalmazása kritikus rendszerekben számos izgalmas lehetőséget rejt magában. Az infrastruktúra, ideértve a villamosenergia-ellátást, adatkommunikációt, víz- és üzemanyagellátást, valamint a légi, szárazföldi és vízi közlekedést, az egy modern társadalom alapvető pillére. Az MI lehetővé teszi ezeknek az átviteli rendszereknek a hatékonyabb működését, csökkentve ezzel az idő-, energia- és anyagpazarlást. Emellett növeli a zavarok elkerülésének és minimalizálásának képességét, például hurrikánok vagy jégviharok esetén.[7]

Az MI sokféle alkalmazási területet kínál a kritikus infrastruktúrában. Ezen területek egyike az előrejelző elemzések és diagnosztika, ahol az MI segíthet a rendszerhibák, energia- vagy vízszivárgások, vagy akár a fogyasztási minták előrejelzésében. Az intelligens rendszerek képesek gyorsan észlelni a rendellenességeket, elősegítve a gyors reakciót és a megelőzést.[8]

A mesterséges intelligencia fontos szerepet játszik az emberiség néhány legösszetettebb rendszerében, különösen a biztonságkritikus rendszerekben. Ezekben a kulcsfontosságú rendszerekben a szoftver általában felelős az elektromechanikai komponensek viselkedésének irányításáért és azok kölcsönhatásainak felügyeletéért.[9]

Segíthet a kritikus rendszerek működésében olyan területeken, ahol emberi beavatkozásra van szükség, például hibák észlelésére és döntések meghozatalára. Az MI hatékonyabb lehet az embereknél, és csökkentheti az emberi hibákból eredő problémákat.[10]

Alkalmazható továbbá az infrastruktúra optimalizálásában, például az energia- és vízellátás hatékonyabb kezelésében. Az algoritmusok segíthetnek az energiafogyasztás optimalizálásában, a hálózati terhelés szabályozásában, vagy akár az okos közlekedési rendszerekben is, ahol a forgalomirányítás vagy a parkolási rendszerek hatékonyabb működtetése lehetséges az MI által.

A mesterséges intelligencia is szorosan kapcsolódik a kritikus infrastruktúrák védelméhez. Használata lehetővé teszi az infrastruktúrák hatékonyabb és intelligensebb védelmét. Például képes folyamatosan monitorozni az infrastruktúrák működését, azonosítani a rendszert érő fenyegetéseket, és gyorsabban reagálni a biztonsági incidensekre. Emellett az MI alkalmazása a kiberbiztonság terén is segít az azonosítás és az adathalászattal vagy kártékony szoftverekkel szembeni védelemben. Lehetőséget nyújt a prediktív elemzésekre is, amelyek segítenek az infrastruktúraüzemeltetőknek megelőzni a hibákat és a rendszeresedő problémákat. Az adatok elemzésével képes az infrastruktúra karbantartásának optimalizálására is, csökkentve ezzel a kiesési időt és a működési zavarokat. Tehát nemcsak az események utáni reakciókban játszik fontos szerepet, hanem elősegíti a proaktív védelmet

és az infrastruktúra hosszú távú fenntarthatóságát is.[11] Ezen túlmenően, az MI rendszereken alapuló automatizáció lehetővé teszi a folyamatos megfigyelést így a gyors válságreakciót is a potenciális veszélyekre, mint például a kiberfenyegetésekre vagy természeti katasztrófákra. Ezáltal fontos szerepet játszhat a kritikus infrastruktúra biztonságának növelésében és a válságkezelésben.

A védelmi területen a mesterséges intelligencia számos új lehetőséget nyit meg a konvencionális módszerekkel szemben, például a "raj támadások," amelyek célja a célpontok meghatározó rendszereinek elárasztása önálló vagy előszabályozással rendelkező irányítás segítségével. A mesterséges intelligenciát olyan eszközként használják a védelemben, amely felismeri és válaszol az eltérő kibertámadásokra. Az elkövetkező időszakban a hadviselés területén a fő hangsúly a személyzet nélküli rendszerek fejlesztésére fog helyeződni, és a mesterséges intelligencia mind a támadó, mind a védekező feladatokban kulcsszerepet fog játszani, beleértve a kibertámadásokkal összefüggő műveleteket is.[12]

**A mesterséges intelligenciában rejlő etikai kérdések és az infrastruktúra biztonsága közötti összefüggések**

Az MI alkalmazása a kritikus infrastruktúra védelmében etikai kérdéseket vet fel, például az emberi beavatkozás mértékét és az autonóm döntéshozatalt. Az etikai dilemmák közé tartozik az emberi felügyelet hiánya az intelligens rendszerek felett, és az az esetleges képesség, hogy az MI önmagában döntsön válsághelyzetekben. Az etikai alapelveknek és a felelősségi kereteknek azonban meg kell felelni az infrastruktúra biztonságának is. Az egyensúly megtalálása az MI alkalmazása és az etikai elvárások között kulcsfontosságú, hogy megőrizzük a kritikus infrastruktúra biztonságát, miközben tiszteletben tartjuk a magánéletet és az emberi jogokat.[13]

Ezen kihívások és biztonsági megfontolások figyelembevételével az MI alkalmazása a kritikus infrastruktúra védelmében továbbra is egy izgalmas és dinamikus terület marad, ahol a technológia fejlődése és a biztonság előmozdítása közötti egyensúly megteremtése kiemelten fontos kihívás a jövőre nézve.

**Az infrastruktúra sebezhetősége és a biztonság kiemelkedő jelentősége**

Az infrastruktúra sérülékenysége a kiberfenyegetésekkel, technológiai hibákkal és természeti katasztrófákkal szemben kiemelt kockázatokat jelent, ami jelentős gazdasági, társadalmi és politikai instabilitást okozhat. Ez megköveteli az egységes és stratégiai szintű védelmi mechanizmusok kifejlesztését és a különböző országok közötti összehangolt erőfeszítéseket.

A szövetségi rendszerek olyan intézkedéseket hoznak a kritikus infrastruktúrák védelme érdekében, amelyeknek célja, hogy garantálják a környezetünk biztonságát és az önálló védelmünket. Ezen kezdeményezések a védelem célkitűzésén túlmenően azt próbálják elérni, hogy a terrorizmus és a biztonságpolitikai kérdések okozta kihívásokon túl más vészhelyzetekre is tudjanak reagálni. Mivel Európa országai többségükben szövetségek tagjaként élik meg ezeket a fenyegetéseket, fontos hogy egységes és stratégiai szintű védelmi mechanizmusokat fejlesszünk ki. A váratlan események és a sebezhető pontok sokasága miatt össze kell hangolni az erőfeszítéseket. Ehhez szupranacionális iránymutatásra, közös alapokra és hasonló értékrendre szükség van.[14]

Az infrastruktúraelemek egyre inkább függenek az informatikai rendszerektől, a digitális kommunikációtól és az automatizált vezérléstől. Ennek következtében növekszik az

infrastruktúra sérülékenysége a kiberfenyegetésekkel és a technológiai hibákkal szemben, melyek jelentős gazdasági, társadalmi és politikai instabilitást okozhatnak. Emellett a modern társadalomban az infrastruktúra egyre összetettebb és globalizáltabbá válik, ami további kihívásokat teremt a védelemben és az esetleges válságok kezelésében.[15]

A kritikus infrastruktúra biztonságának egyik központi kérdése a sebezhetőség. Az infrastruktúra sebezhetősége azon azonosított és fel nem ismert veszélyek, fenyegetések és sérülékenységek mértékét jelenti, amelyek károkat okozhatnak az infrastruktúrában és annak működésében. Ezek a veszélyek lehetnek emberi eredetűek, mint például a terrorizmus, kiberfenyegetések, vagy természeti jelenségek, mint a földrengés vagy az árvíz.

A mai kritikus infrastruktúra fejlődése egyre inkább az intelligens technológia és a hálózatok integrációján alapul. Ennek következtében a kiberfenyegetésekkel járó sérülékenységek sokasága keletkezik, amelyeknek hatásai súlyos károkat okozhatnak. Ebből kifolyólag a kritikus infrastruktúra terén, a biztonság rendkívül fontos szempont.[16]

A kritikus infrastruktúra védelem célkitűzéseinek konkrét megfogalmazása átalakítja a biztonságról alkotott képünket is. Az alapvető szükségleteinket kielégítő infrastruktúrák védelme fontos szempontokat és kihívásokat vet fel a biztonsági percepciónk és a hétköznapok gördülékenységének fenntartása szempontjából.

Az információs támadások elleni védelem kulcsszerepet játszik a kritikus infrastruktúrák védelmében. A kritikus infrastruktúra kritikussá válásának egyik fő oka a növekvő informatikai szolgáltatásfüggőség a társadalmi, szervezeti és magánélet területén.[17]

A kezelendő kockázatok nem korlátozódnak az államok határaira. Ezért fontos megjegyezni, hogy nem csak környezeti hatások játszanak szerepet, hanem az ellátás és társadalmi hatások is, ami sajátos interdependenciát jelent. Az egymásra gyakorolt kölcsönös függőség rendkívül komplex, és gyakran meghaladja a jogalkotók által meghatározott kereteket. A jogalkotók által kizárt ágazatok esetén nem is ismerik el, hogy az adott infrastruktúra kritikus lehet. Ebből adódóan ajánlatos lenne egy másik megközelítést alkalmazni a besorolási feltételek tekintetében, és meghatározni például egy kezelhető komplex küszöbértéket.[18]

Az infrastruktúra védelmének egyik alapvető feladata az infrastruktúrák azonosítása az adott felhasználói kör vagy alkalmazási terület szempontjából. Ez ágazatonként és szektoronként történhet. A szükséges követelményeket le kell bontani részletesebb, konkrét külső szolgáltatási szintekre, amelyek meghatározzák, hogy az adott szektor vagy infrastruktúra mely elemei minősülnek kritikusnak, és milyen belső szolgáltatási szint követelményeknek kell megfelelniük.[19]

Fontos a kritikus infrastruktúra védelme mind a kormányzati, mind a vállalati szektorban. Még ha eltérés is van a két szektor kritikus elemei között, mindkettőnél létfontosságúak az egészség, biztonság, gazdasági jólét és az ICT (Information and Communications Technology) infrastruktúra folyamatos rendelkezésre állása. Azonosítva és védelmezve ezeket az alapvető elemeket, a veszélyek és fenyegetések kockázatát minimalizálhatjuk. Ennek alapja a Critical Infrastructure Protection (CIP) és a CIP megoldásokra való fókuszálás.[20]

Az elmúlt évtizedek döntő biztonságpolitikai eseményei jelentős hatással voltak a kritikus infrastruktúra védelmének megközelítésére és a globális biztonsági percepcióra. Az 2001. szeptember 11-i terrortámadások, amikor a New York-i Világkereskedelmi Központ

és a Pentagon célpontjai voltak, radikálisan megváltoztatták a nemzetközi biztonsági politikát. Ezek az események rávilágítottak arra, hogy a terrorcsoportok képesek nagy léptékű károkat okozni, ezáltal felhívva a figyelmet a kritikus infrastruktúrák, mint az energiaellátás és a közlekedési hálózatok sebezhetőségére. A madridi vonatok elleni 2004-es merényletek, és a következő évben a londoni metró elleni támadások tovább erősítették a tömegközlekedési rendszerek védelmének szükségességét, mivel ezek a támadások aláhúzták, hogy a városi infrastruktúra különösen kiszolgáltatott a terrorcselekményeknek.

A kiberbiztonsági fenyegetések növekedése tovább bonyolítja a helyzetet. Ahogy a társadalom egyre inkább függ az informatikai rendszerektől, a kiberbűnözők és más rosszindulatú szereplők által elkövetett támadások súlyos károkat okozhatnak, mind gazdasági, mind társadalmi szinten. A digitális infrastruktúra, mint az adatközpontok és kommunikációs hálózatok elleni támadások rámutatnak a szükséges védelmi intézkedések és stratégiák kiépítésének sürgősségére. Ezen felül a természeti katasztrófák, mint hurrikánok, földrengések és árvizek, amelyek gyakorisága és intenzitása növekszik a klímaváltozás következtében, fokozzák az infrastruktúrák fizikai sérülékenységét, kiemelve a fenntartható és ellenálló infrastruktúra kiépítésének fontosságát.

Ezen kulcsfontosságú események összessége alapvetően formálja át a kritikus infrastruktúrákhoz kapcsolódó biztonsági stratégiákat. A támadások és fenyegetések széles skálája miatt a hatóságoknak és szervezeteknek komplex, többrétegű védelmi rendszereket kell kialakítaniuk, amelyek képesek adaptálódni a változó fenyegetési környezethez. Ennek érdekében a nemzetközi együttműködés és a technológiai innovációk előtérbe helyezése kulcsfontosságú, hogy biztosíthassuk társadalmaink stabilitását és jólétét a jövőben is. Az események által nyújtott tanulságok kulcsfontosságúak a hatékony védelmi politikák kialakításához, melyek központi eleme a kritikus infrastruktúra folyamatos és dinamikus védelme.

**A kritikus infrastruktúra és a kibervédelem**

A mesterséges intelligencia (MI) térnyerése a kiberbiztonság terén lehetővé teszi a fenyegetések korai felismerését és a gyors reakciót, ami alapvetően hozzájárul a kritikus infrastruktúrák védelméhez, különösen az egyre növekvő kiberfenyegetések és technológiai hibák világában. Bár a MI és a kiberbiztonsági technológiák fejlődése jelentős előrelépést jelent a kritikus infrastruktúrák védelmében, a globalizált és összekapcsolt világban a kiberfenyegetések egyre összetettebbé és súlyosabbá válnak az információs hadviselés területén.

A kritikus infrastruktúrák növekvő függősége az informatikai rendszerektől és a globális kiberhálózatoktól jelentős kihívásokat és sebezhetőségeket eredményez a kibervédelemben, amelyeket csak a mesterséges intelligencia (MI) és fejlett kiberbiztonsági megoldások integrált alkalmazásával lehet hatékonyan kezelni.

Az MI hozzájárulhat a fenyegetések korai felismeréséhez és a kiberbiztonsághoz, mivel az algoritmusok és rendszerek képesek az anomáliák észlelésére és az esetleges támadásokra való gyors reagálásra. Az adatok folyamatos monitorozása és elemzése segíthet az azonnali fenyegetések azonosításában, és lehetővé teszi a védelmi intézkedések időbeni bevezetését.

Ahogyan a fejlett infrastruktúrával rendelkező országokban általában, a kibertér sebezhetőnek tekinthető. Ugyan léteznek hatékony védelmi intézkedések, amelyek az egyes

kritikus infrastruktúrákat megfelelően védik, de 21. század által nyújtott globalizáció adta lehetőségek kialakították a határok nélküli és összekapcsolt hálózatok kölcsönös függőségét. Azok a kibertámadások, amelyek veszélyt jelenthetnek egy ország kritikus infrastruktúrájára, egyre összetettebbek és súlyosabbak lehetnek az informatika területén bekövetkező változásoknak köszönhetően.

Az információs hadviselés terén az új évezredben egy paradigmaváltás figyelhető meg. Az informatikai fejlődés új kihívások elé állítja a nemzetek biztonságát. A támadók olyan digitális eszközöket használhatnak, amelyekkel "digitális kőkorszakot" hozhatnak létre a megtámadott országban, anélkül, hogy hagyományos katonai erőket alkalmaznának.[21] Az egyes informatikai rendszerek meghibásodása jelentős károkat okozhat egy ország normális működésében. Azok az országok, amelyek komolyan veszik a had-, biztonság- és informatikai területeket, kritikus információs infrastruktúrájuk védelmét a 21. század egyik legfontosabb kihívásának tekintik.[22]

A kibertér természeténél fogva egy olyan terület, ahol nem alkalmazhatóak azok a hagyományos hadviselési módszerek amelyek az elmúlt évszázadok óta szokásként számítottak. A digitális tér alapjainak a fejlődése jelentős mértékben elősegíti az aszimmetrikus hadviselés lehetőségét, amelyek által a terrorista csoportok is előnyökre és új lehetőségekre tehetnek szert nyújthat.[23]

A konvencionális hadviseléssel párhuzamosan nélkülözhetetlenné váltak a kibertérben elindított parhuzamos támadások indítása a kritikus infrastruktúrák ellen. Ahhoz, hogy blokkolni tudjuk az infrastruktúra elemeit, kellő információ birtokában kell lenni a célpont strukturális felépítéséről és sebezhetőségéről. Sajnos prevenció tekintetében a támadók általában lépéselőnyben vannak, így a válságkezelés csak válaszreakció tud lenni. Mint minden rendszernek vannak biztonsági hézagjai. Ennek okán a biztonság és a támadhatóság szempontjából nem szabad figyelmen kívül hagyni a különböző technológia eszközök használatának és a virtuális térben indított támadásoknak a hadtudományokban betöltött szerepét. A digitális tér alapjait tekintve olyan terület, ahol nem alkalmazható azok a hagyományos hadviselési módszerek, amelyek évszázadok óta bevett szokásnak számítottak. Ez a fejlődés lehetővé teszi az aszimmetrikus hadviselés elterjedését, ami előnyöket biztosíthat a terrorista csoportoknak.

A kibertér és más hadviselési területek közötti egyik kulcsfontosságú különbség az, hogy a kibertérben a rombolás képessége hasonló elvi szempontból az atomfegyverekhez hasonlóan megváltozott. Az új kibertéri fegyverek dimenziókkal nagyobb pusztító erőt képviselnek, mint a hagyományos eszközök. Ez azt jelenti, hogy a kibertérben olyan rombolás és fenyegetettség valósítható meg egy másik országgal szemben, amely akár meghaladhatja a nukleáris fegyverek által nyújtott pusztító erőt is.[24]

Az informatikai területek alapvetően egy elég szenzitív életfázisba értek. Az újonnan zajló változások, új kihívások elé állítják a nemzetek biztonságáról alkotott képünket. A támadók képesek pusztán számítógép-hálózatok segítségével jelentős kárt okozni anélkül, hogy hagyományos hadviselési módszereket alkalmaznának. Ennek következtében a lehető legmagasabb prioritásként kezdték el kezelni a kibertámadások jelentőségét.[25] Míg korábban a kibervédelem főként az ipari kémkedés és adatlopások ellen irányult, most egyre inkább a külföldi kormányok által végrehajtott hálózati támadások kezelése válik prioritássá, különösen Kína hatására. Ennek következtében a hadseregek támadó képességei is

fejlődnek, hogy képesek legyenek kritikus infrastruktúrák megsemmisítésére az ellenséges államok ellen.[26]

A kritikus infrastruktúrák elleni támadások különböző módszerekkel valósulhatnak meg, mind azzal a céllal, hogy az adott infrastruktúra működését zavarják vagy korlátozzák, akár ideiglenesen, akár véglegesen. Ezek közé tartozik a fizikai károkozás, amely kinetikus hatással valósulhat meg. Továbbá az infrastruktúra belső alrendszeri közötti kommunikáció manipulálása vagy blokkolása is egy gyakori támadási módszer. Emellett az egy vagy több alrendszerben történő belső, fizikai károkozás is előfordulhat.[27]

Az elmúlt időszakban a kibervédelem főleg az adatlopások és ipari kémkedés elleni védelemre koncentrált. Kína vezetésével az állami hálózatok elleni támadások növekedése erősítette a hadseregek képességeit a kritikus infrastruktúra támadására. A kibertámadások kezelése kiemelten fontos a biztonságpolitikában, de sokan nem értik teljesen ezt a veszélyt és a szükséges intézkedéseket.

## ÖSSZEFOGLALÁS

Az infrastruktúra biztonsága és védelme kritikus szerepet játszik a társadalmi stabilitás és gazdasági folytonosság fenntartásában. A kihívások folyamatosan növekednek az információs korban, ahol az infrastruktúrák egyre inkább az informatikai rendszerektől függnek és ahol a kiberfenyegetések súlyos veszélyeket hordoznak magukban. Az MI fejlődése, a kibertéri szülte új támadási felületek lehetőségei és az aszimmetrikus hadviselés térhódítása új stratégiai megközelítéseket követel meg a kritikus infrastruktúra védelmében. Mind a kormányzati, mind a vállalati szektorban, a Critical Infrastructure Protection (CIP) keretében való fókuszálás és megelőzés kiemelkedő fontosságú. A kibertámadások súlyosabb pusztítást okozhatnak, mint a hagyományos hadviselési eszközök, így a fenyegetések felismerése és kezelése elengedhetetlen. Az intelligens technológiák és hálózatok fejlődésével nő az infrastruktúrák sebezhetősége, így a kibertér prioritása és az informatikai biztonság kulcsszerepet játszik a megelőzésben és a válságkezelésben. A kritikus infrastruktúrák védelme új kihívások elé állítja a biztonságpolitikát, ahol a nemzetközi közösségnek stratégiai válaszokat kell találnia a jövőbeni veszélyekre. Az együttműködés és a megosztott értékrend alapján történő védelem kulcsfontosságú a globális biztonság fenntartásához.

## FELHASZNÁLT IRODALOM

[1] J. Daniels, *The Internet of Things, Artificial Intelligence, Blockchain, and Professionalism*, IT Professional, 2018, pp. 15-19., DOI: 10.1109/MITP.2018.2875770

[2] V. Mani, S. Lavanya, *Iot based smart energy management system*, International Journal of Applied Engineering Research, 2017, pp. 5455-5462.

[3] H. Bangui, B. Buhnova, B. Rossi, *Shifting towards Antifragile Critical Infrastructure Systems*, 2022, Conference: 7th International Conference on Internet of Things, Big Data and Security, pp. 1-10., DOI:10.5220/0011086400003194

[4] T. Bonyai, NKE Kiberbiztonsági Kutatóintézet, *Kritikus infrastruktúrák: célpont, vagy eszköz?* 2021, https://www.ludovika.hu/blogok/cyberblog/2021/01/27/kritikus-infrastrukturak-celpont-vagy-eszkoz/

[5] L. KIRÁLY, *Hadszíntér-előkészítés, befogadó nemzeti támogatás, kritikus infrastruktúra védelem-védelemgazdasági nézőpontból*. Military Science Review/Hadtudományi Szemle 2015. VIII. évfolyam 3. szám, pp. 10-20.
[6] S. MUNK, *Kritikus infrastruktúrák védelme információs támadások ellen*. Military Science Review/Hadtudományi Szemle 2008 XVIII. évfolyam 1-2 szám, pp. 95-106.
[7] K. Bresniker, A. Gavrilovska, J. Holt, Grand challenge: Applying artificial intelligence and machine learning to cybersecurity, Computer, 2019, pp. 45-52., DOI: 10.1109/MC.2019.2942584
[8] C. Perera, C.H. Liu, S. Jayawardena, M. Chen, A survey on internet of things from industrial market perspective. IEEE Access **2**, 1660–1679 (2014), A Survey on Internet of Things From Industrial Market Perspective | IEEE Journals & Magazine | IEEE Xplore
[9] W. WONG, P. LAPLANTE, *Be more familiar with our enemies and pave the way forward: A review of the roles bugs played in software failures*. Journal of Systems and Software, 2017, pp. 68-94.
[10] P. Laplante and B. Amaba, *Artificial intelligence in critical infrastructure systems*, Computer, 2021 1, pp. 4-24
[11] Cs. Kollár, *A mesterséges intelligencia megjelenése a biztonságtudományban*. In: Tibor, János Karlovitz (szerk.) What will our Future be Like? 2 essays in German, 7 in English, 30 in Hungarian language (Német, angol és magyar nyelvű esszék) Grosspetersdorf, Ausztria : Sozial und Wirtschafts Forschungsgruppe (2023) 448 p. pp. 242-256. 15 p.
[12] J. Johnson, *Artificial intelligence & future warfare: implications for international security*. Defense & Security Analysis, 2019, pp. 147-169
[13] I. Négyesi, *A mesterséges intelligencia és az etika*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata 30 (1), 2020 pp. 103-113. http://doi.org/10.17047/HADTUD.2020.30.1.103
[14] Katasztrófavédelmi Tudományos Tanács pályázata, *Kritikus Infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása*, 2011, pp. 01-61
https://www.vedelem.hu/letoltes/anyagok/382-a-kritikus-infrastruktura-vedelem-fogalmi-rendszere-hazai-es-nemzetkozi-szabalyozasa.pdf
[15] *A Proclamation on Critical Infrastructure Security and Resilience Month*, 2021 | The White House, Briefin Room, Presidental Actions
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/10/29/a-proclamation-on-critical-infrastructure-security-and-resilience-month-2021/
[16] J. Sakhin, H Karimipour, A Dehghantanha, *AI and security of critical infrastructure*, Handbook of Big Data Privacy, 2020, pp. 7-36. DOI:10.1007/978-3-030-38557-6_2
[17] S. Munk, *Kritikus infrastruktúrák védelme információs támadások ellen*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata XVIII.:(1-2.), 2008, pp. 95-106.
[18] K. Kralovánszky, *A kibertér fejlődése (második rész)–Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai,* Hadmérnök 16.1, 2021, pp. 145-160.
[19] S. Munk, *Kritikus infrastruktúrák védelme információs támadások ellen*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata XVIII.:(1-2.), 2008, pp. 95-106.
[20] https://www.e-spincorp.com/protect-what-is-critical-to-your-infrastructure/

[21] P. Bányász és Á. Orbók, *A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében.* Hadtudomány, Magyar Hadtudományi Társaság folyóirata 23. szám, 2013, pp. 188-209. ISSN 1215-4121
https://www.mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf
[22] L. Kovács, Cs. Krasznay: *Digitális Mohács, Egy kibertámadási forgatókönyv magyarország ellen*, Nemzet és Biztonság, 2010, pp. 44-56.
https://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf
[23] I. Porkoláb, *Az aszimmetrikus hadviselés adaptációja*. Ludovika Egyetemi Kiadó, 2020,
https://demo.repozitorium.uni-nke.hu/xmlui/bitstream/handle/123456789/15904/576_aszimmetrikus_hadviseles.pdf?sequence=7
[24] K. Kralovánszky, *A kibertér fejlődése (második rész)–Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai*, *Hadmérnök* 16.1, 2021, pp. 145-160.,
DOI: 10.32567/hm.2021.1.9
[25] P. Bányász, Á. Orbók, *A NATO Kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata, 2013, pp. 188-206
[26] *A New Kind of Warfare*, The New York Times-The Opinion Pages, 2012, https://www.nytimes.com/2012/09/10/opinion/a-new-kind-of-warfare.html
[27] K. Kralovánszky, *A kibertér fejlődése (második rész) – Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai*, *Hadmérnök* 16.1, 2021, pp. 145-160.