KözigazgatásTudomány
DOI: 10.54200/kt.v5i2.97

A 21. SZÁZAD IKT KÖZEGÉNEK FŐ KOCKÁZATAI, MŰKÖDÉSÉNEK IMMANENS GYENGESÉGEI ÉS A JOG (FÉL)MEGOLDÁSAI

Vikman László*

* Egyetemi tanársegéd, Széchenyi István Egyetem. Tudományos segédmunkatárs, Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet. E-mail: Vikman.Laszlo@uni-nke.hu

Absztrakt

A tanulmány a 21. századi kiberbiztonság komplex kihívásait vizsgálja, túllépve a hagyományos, tisztán technológiai megközelítésű fenyegetéselemzéseken. Az elemzés kísérleti módszertanként a katonai műveletervezésben alkalmazott PMESII-PT (Politikai, Katonai, Gazdasági, Társadalmi, Információs, Infrastrukturális, Fizikai környezet és Idő) modellt adaptálja a digitális tér kockázatainak rendszerezésére. Az elemzés rámutat, hogy a szabályozási környezet jelenleg kényszerpályán mozog és reaktív, miközben a technológiai szektor gyors fejlesztési ciklusai és a geopolitikai feszültségek növelik a sérülékenységet. A dolgozat kritizálja a nemzetközi jogi keretek hiányát és a tech-óriások túlzott befolyását az állami szuverenitással szemben. A konklúzió – reflektálva a 2025-ös új nemzeti stratégiára – paradigmaváltást sürget: a biztonsági felelősségi teher fokozottabb áthelyezését a felhasználókról a gyártókra (security by design), valamint egy integrált, önálló nemzeti kiberbiztonsági hatóság felállítását javasolja a hatékonyabb állami koordináció érdekében.

Kulcsszavak

kiberbiztonság, stratégia, kockázatelemzés, PMESII

Abstract

The study examines the complex challenges of cybersecurity in the 21st century, going beyond traditional, purely technological approaches to threat analysis. As an experimental methodology, the analysis adapts the PMESII-PT (Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time) model used in military operations planning to systematize the risks of the digital space. The analysis points out that the regulatory environment is currently on a collision course and reactive, while rapid development cycles in the technology sector and geopolitical tensions are increasing vulnerability. The paper criticizes the lack of an international legal framework and the excessive influence of tech giants over state sovereignty. The conclusion, reflecting on the new national strategy for 2025, calls for a paradigm shift: it recommends shifting the burden of security responsibility from users to manufacturers (security by design) and establishing an integrated, independent national cybersecurity authority for more effective state coordination.

Keywords

cyber security, strategy, risk analysis, PMESII

1. Bevezetés

A hatékony kiberbiztonság kereteinek megteremtése nem működhet tisztán jogi eszközökkel, mint alapvetően műszaki terület, elsősorban technológiai oldalról determinált, de többek közt társadalmi, üzleti, politikai aspektusok is erősen hatnak rá.[1] A kiberbiztonság szabályozása, és különösen a megvalósítását célzó egyéni és szervezeti tevékenységek és folyamatok során ezeket a szempontokat is mérlegelni és értékelni kell (lásd fenyegetettség- és kockázatelemzés), a jogalkotónak már „stratégiai szinten" a szabályozás hatályát, a jogintézményeket, jogosultságokat és kötelezettségeket is ezek ismeretében érdemes kialakítani (ide értendők különösen a nemzeti stratégiák, a kiberbiztonságra vonatkozó jogi normák, a hatáskörrel rendelkező hatóságok és az érintettek feladatai). A kiberbiztonságot megteremteni célzó szervezeti tevékenységek „hadműveleti szintjén" (szervezeti kockázatelemzés, erőforrások allokálása, belső képzések és tudatosság kialakítása stb.) és „harcászati szintjén" (ideértve a konkrét informatikai biztonsági, üzletmenetfolytonossági, katasztrófaelhárítási szabályzatok és tervek, és a belső kiberbiztonsági architektúra kialakításának minden momentumát és a napi tevékenységet) is a képességeket, eljárásokat úgy kell kialakítani, hogy azok illeszkedjenek a konkrét szervezet fenyegetettségi profiljához, jelentősebb kockázataihoz.

Ha felvezetésként szeretnénk néhány fontos, a 21. századi digitális ökoszisztémát fenyegető tényezőt felsorolni, akkor mindenképp érdemes azzal kezdenünk, hogy a jelenleg alkalmazott technológiák jelentős része eddig is ingatag lábakon állt, a biztonság tipikusan nem volt elsődleges szempont ezek fejlesztésénél és bevezetésénél, a legjobb példa, hogy az internet működését meghatározó alapelvek, protokollok kidolgozása katonai céllal (a hálózatosan kialakított vezetés-irányítás képességének megőrzése nukleáris támadást követően is) indult az ARPANET projekt keretében, és nem volt tervben annak globális, határokon átívelő rendszerré fejlődése, ami alapvetően formálta át a társadalmi, üzleti, kereskedelmi, média és igazgatási viszonyokat.

Fontos az is, hogy az interneten az egyes aktorok anonimitása az egyre gyakoribb ellenőrzési mechanizmusok mellett is számos megoldással továbbra is kis szakértelemmel egyszerűen megoldható (hamis vagy lopott profilok, VPN-ek, proxy-szerverek, TOR-böngésző, kriptovaluták, stb.), ami mind az online ügyletek hitelességét, mind az információk biztonságát megkérdőjelezhetővé teszi.

A digitális közegben tipikus 1-2 éves gyártói fejlesztési ciklusok hardverek és szoftverek vonatkozásában is folyamatos fejlesztési kényszert idéznek elő, ami bizonyos szervezetek és felhasználói csoportok által racionálisan egyszerűen nem lekövethető, ezzel adott esetben már kompromittálódott (számos ismert sérülékenységgel rendelkező) rendszert kénytelenek üzemeltetni. Ennek a fonákja is hordoz veszélyeket, hisz azok, akik tartják a lépést, hogy mindig a legkorszerűbb, leggyorsabb eszközöket használják kiteszik magukat az esetleg kevésbé letesztelt, gazdasági érdekek miatt esetleg túl gyorsan leszállított, még számos lehetséges és kihasználható hibát hordozó termékekből származó üzemeltetési vagy sérülékenységi problémáknak.

[1] A kibertér, a digitális technológiák szabályozás témájához bővebben lásd pl.: Farkas és Kelemen (2023), Farkas és Kelemen (2024a), Farkas és Kelemen (2024b), Susskind (2021).

Szintén alapvetően technológiai kérdés azoknak a diszruptív hatású fejlesztéseknek a folyamatos megjelenése, ami várhatóan számos szabályozási, biztonsági intézkedést tesz hatástalanná, és formál át akár egész iparágakat, üzleti modelleket és szolgáltatásokat. Az egyelőre elsősorban a nagy nyelvi modellekben populárissá váló mesterséges intelligencia fejlesztések mellett a kvantumszámítás és -kommunikáció lesz az, ami az eddig használt titkosítási rendszereket meghaladottá teszi. A forgalom biztonsága jogi értelemben is függ azoktól az aszimmetrikus kulcsú titkosítási rendszerektől, amelyek az új számítástechnikai eszközökkel feltörhetőkké válnak, ezzel nem csak az államok minősített adatait, de a pénzügyi tranzakciókat, az internetes kommunikáció titkosításait is kompromittálva.

A technológiai iparra jellemző globális szervezettség és egymásra épülő munkafolyamatokból álló komplex ellátási láncok szempontjából nem csak a szállítók kiberbiztonságot prioritásként kezelő hozzáállása fontos, de a jelen geopolitikájára jellemző multipoláris tendenciák, gazdasági vagy védelmi érdekekből származó vámok és exportkorlátozások bevezetése is okozhat jelentős – akár regionális szintű – lemaradást, és a korábban partnerségre törekvő szereplők között versengést és blokkosodást. Ahogy láttuk, akár egy pandémia, vagy olyan lokálisnak tűnő problémák, mint a jemeni húszi lázadók vörös-tengeri kereskedelmet fenyegető lépései is súlyos késéseket okozhat a szállításokban, még jelentősebb fenyegetés, ha a szállítói láncon keresztül érkezik támadás.

Orwell „1984” című regénye után az állami szereplőt a 90-es években és az ezredfordulón a személyes adatok védelmét szem előtt tartók gyakran „Nagy Testvér”-nek nevezték, annak büntetőjogi és titkosszolgálati eszköztára, kiterjedt igazgatási adatbázisai és az ezekben található információk integrációja miatt érzett aggodalomból fakadóan. A gazdasági folyamatok, és a média jelentős részének internetre költözésével és különösen az interneten elérhető korábban nem létező, személyes adatok gyűjtésén alapuló üzleti modellekkel működő szórakoztató, kommunikációs platformok, és a közösségi média kialakulásával, valamint a tájékoztatásban egyre komolyabb szerepével elmondhatjuk, hogy a 2000-es években még csak egyszerű törzsvásárlói kártyarendszerekkel induló professzionális és pszichológiai eszköztárat is felvonultató marketing mára már a specializált applikációkkal, és a tömeges adatgyűjtéssel maximálisan kiszolgáltatottá teszi a felhasználókat. A továbbra is jogi alapelvként megkövetelt tájékozott beleegyezés, mint kritérium „checkboxok” kipipálásával teljesítése pedig nem igazán vehető komolyan. A „Kis Testvér” gyakran sokkal szélesebb körben fér hozzá a magánszemélyek privátszférájához, mint a titkosszolgálatok valaha, és a gyűjtött információkat pedig egy globális információ-bróker iparág értékesíti a maximális értékesítési hatékonyság és a fogyasztói viselkedés befolyásolása érdekében.

Ennek a közegnek a jogi szabályozási keretei is egyre összetettebbek, értelmezhető technikai (specifikációk, szabványok, üzemeltetési rendek – ezek átszivárgása a jogba egyre jelentősebb, lásd NIST 800-53A[2] szabvány szerepe a magyar jogban[3]), általános jogági (alapjogok, adatvédelem, nemzetközi jog, szerzői jog, kereskedelmi/média szabályozás, büntetőjog) és különös (EU:

[2] A NIST 800-53A szabvány az USA szövetségi kormányzati szervezeteire nézve kötelező kiberbiztonsági szabvány, szabadon elérhető, így világszerte sokan tekintik irányadónak. Online: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

[3] A kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I. 31.) SZTFH rendelet 5. melléklet 1.1.1. pontja szerint: „Az audit módszertan a NIST Special Publication 800-53A Revision 5 dokumentum alapján került kialakításra.”

NIS2,[4] CER,[5] CRA,[6] DMA,[7] DSA,[8] adatrendeletek,[9] nemzeti: Kibertv.[10]) szinteken, amelyek között jelentős eltérések lehetnek az egyes országok közt, ami a joghatóságokon bőven túlnyúló internetes szolgáltatásoknak nem minden esetben tud igazán hatékony és kikényszeríthető kereteket biztosítani. Jogi oldalról is értékelhető a már említett multipoláris versengés, ami a kibertéri folyamatok nemzetközi szabályozási hátterének viszonylagos szabályozatlansága mellett, a szintén már felhozott exportkorlátozási szabályokban is megnyilvánul. Nem szabad elmenni amellett sem, hogy egyelőre nem megoldott kérdés az sem, hogy milyen – jogállami megközelítésben értelmezhető – módszerekkel lesznek kezelhetők a hibrid fenyegetések körében jelentkező információs műveletek és dezinformációs kampányok (Vikman, 2024), amelyek súlyos biztonsági fenyegetést jelenthetnek akár demokratikus folyamatok, pl. választások megzavarásával, akár összehangolt fellépést igénylő járványügyi intézkedések hitelességének megkérdőjelezésével.

Az alábbiakban a jelen tanulmányban használt katonai műveletervezésben tipikusan használt elemzési PMESII-PT módszertan ismertetését és alkalmazásának indoklását követően, az információs és kommunikációs közeg, vagy kicsit korszerűbben a digitális technológiák tervezésének, fejlesztésének, beszerzésének és főleg alkalmazásának főbb kockázatait szeretném katalogizálni a választott elemző modell felhasználásával, mindegyik aspektusnál a releváns jogi vonatkozások említésével. A digitális technológiák egyes ismert gyengeségeit is röviden elemzem – ahol ez releváns – az ezekre adott jogi válaszokkal, amelyek hatékonyságára is kitérek. Ezeknek a folyamatoknak a kordában tartására az EU a digitális korszak korszerű szabályozási kereteinek kialakítását a személyes adatok védelmét szavatolni hivatott GDPR-rendelettel[11] kezdte meg, amit egy teljes rendeleti és irányelvi generációváltás követett, amelyek implementációja fontos tagállami feladat. Az összegzésben az aktuális hazai legfontosabb stratégiai szintű teendőkkel kapcsolatos gondolatokkal kívánom zárni az áttekintést.

[4] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv).

[5] 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.

[6] Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet).

[7] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. december 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály).

[8] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet).

[9] Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet); az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet).

[10] Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény.

[11] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

2. Módszertan: a PMESII-PT modell, és példák kiberbiztonsági fenyegetettségről szóló átfogó jelentésekre, elemzésekre

A PMESII-PT analízis[12] egy stratégiai helyzetértékelésben alkalmazott, komprehenzív elemző megközelítés, nevét a módszerben vizsgált tényezők kezdőbetűiből megalkotva kapta: Political, Military, Economic, Social, Information, Infrastructure és a kiegészítő további két elem Physical, Time. Jelentőségét katonai közegben annak köszönheti, hogy a NATO átfogó összhaderőnemi művelettervezési módszertana, a COPD[13] (Comprehensive Operations Planning Directive), és az USA művelettervezési doktrínája[14] is alkalmazza egy konkrét tervezési folyamat elején egy válsághelyzet, vagy konfliktus műveleti területének, állami vagy nem-állami szereplőjének részletes értékelésére.

Ez a komplex szemlélet a katonai közegen kívül is alkalmassá teszi ezt az elemzői módszert arra, hogy részletes képet adjon jelentős egymásrautaltságot, interdependenciákat is magában hordozó helyzetekről, rendszerekről. Emiatt, mint stratégia-alkotási segédeszköz alkalmas lehet rendszerezni azokat a fenyegetéseket, amelyeknek listába rendezését időnként az aktuális trendek, tipikus előfordulások, vagy adott esetben sajátos érdekek alakítják. A PMESII modellben a jogi értékelést jellemzően a Social kategóriában szokták elvégezni,[15] én mindegyik elem kapcsán igyekszem majd megvilágítani a legfontosabb jogi kérdéseket is.

Jelen tanulmányban a modell szerinti elemzést a következő fejezetben a 21. századi digitális technológiai környezetre és kiberbiztonsági kihívásaira kívánom elvégezni, kifejezetten állami szemszögből, a gyakorlatból ugyan ismert, de absztrakt fenyegetésekkel. Tekintsük át röviden, hogy az egyes elemzési fókuszpontokban – katonai közegben – milyen jelenségeket kell azonosítani:

Politikai: az értékelt szereplő ellenséges vagy baráti attitűdje, a hatalmi központok, a kormányzás típusa, annak hatékonysága és legitimációja, legfontosabb befolyásos politikai csoportok;

Katonai: az erők/képességek jellege, állami és nem állami kategóriában, esetleges nem-fegyveres kombattánsok, nem-katonai fegyveresek, a katonai funkciók jellemzői (vezetés, manőver, információs hadviselés);

Gazdasági: gazdasági sokszínűség, fontos iparágak, a foglalkoztatottság szintje, a gazdasági aktivitás legalitása, illegális aktivitás jellege, a pénzügyek fejlettsége;

Szociális: demográfiai összetétel, szociális volatilitás, képzettségi szint, etnikai összetétel, vallási sokszínűség, lakosság mobilitása, közös nyelvek, bűnözés, emberi jogok érvényesülése;

Információs: média (internet, TV, rádió, print, telefon, posta, szóbeszéd), információs hadviselés (kibertérben pl. a dezinformáció, deep fake egyik oldalról, a médiafelügyelet és annak hatékonysága másik oldalról), információszerzés lehetőségei (OSINT, social engineering, hackertevékenység), információmenedzsment (adatok védelme, ennek fejlettsége);

Infrastruktúra: fejlettség, reziliencia, beépítettség, városi területek, közművek, energiaellátás és ezek szintje, szállítási architektúra (műhold, mobil, vezetékes);

[12] A módszertan bővebb kifejtéséhez lásd pl.: Jurevicius (2025), Ducote (2010), Affleck et al. (2015).

[13] A COPD fejlődéséhez és tartalmához lásd részletesen: Fazekas (2022). A nyilvánosan is elérhető 2.0-es verziót lásd: Allied Command Operations, Comprehensive Operations Planning Directive, COPD INTERIM V2.0. 04. October 2013. Online: https://www.cmdrcoe.org/download.cgf.php?id=9

[14] Nyilvánosan elérhető verzió: Joint Publication 5-0, Joint Planning. 16. June 2017. Online: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/18-F-1152_JP_5-0_Joint_Planning_2017.pdf

[15] A művelettervezés jogi feladataihoz lásd: Vikman (2021).

Fizikai környezet: az adott földrajzi terep és ennek hatásai, a jelentkező természeti veszélyek (áradás, földrengés, erdőtüzek, viharok), klíma, időjárás (hőmérséklet, csapadék);

Időtényező: talán a legabsztraktabb, de mégis igen jelentős értékelési szempont, ide kell érteni a rendelkezésre álló időt a megszerzett ismeretek vonatkozásában a műveleti területről (kevés-sok), ami utalhat az értékelés pontosságára, információk rendelkezésre állásának szintjére, az ellenérdekeltek idő-érzékenysége, illetve az időtényező taktikai kihasználása (kibertérben pl. a zero-day sebezhetőségek), az adott műveleti tér kiszámíthatósága, az események előreláthatósága, tervezhetősége, végül egyes kulcs dátumok, időperiódusok, események (pl. egy online fogadásokkal foglalkozó szolgáltatás esetén egy futball-vb).

Annak alátámasztására, hogy a kibertéri fenyegetések stratégiai megközelítésében hozhatnak új szemléletet, nézzük, hogyan épülnek fel más mértékadónak tekinthető fenyegetéselemzések.

Az ENISA[16] 7 fő fenyegetési formát (ransomware, malware, social engineering, adatok elleni fenyegetések, DDoS-támadások, információ manipulációk, ellátási láncok elleneni támadások) és 4 fő fenyegetési vektor kategóriát (állami szereplők, szervezett bűnözők és hackerek, üzleti/magánszektorbeli támadók, hacktivisták) határoz meg (ENISA, 2024).

A Sophos[17] 2024-es fenyegetettség jelentésének vezetői összefoglalójában is első helyen a zsarolóvírusok szerepelnek, ezt követik az adatlopás, a malware-ek, a védtelen, nem megfelelően menedzselt, vagy már nem támogatott technikai eszközökből származó sérülékenységek szervezett bűnözők által kihasználása, a visszaélések az egyes hardvereszközöket meghajtó ún. driver-programok rosszindulatú módosításával, az egyre szofisztikáltabb e-mail-támadások, végül a kifejezetten mobil-felhasználókat célzó közösségi médiát és social engineering-et kombináló, egyes esetekben kriptovaluta-pénztárcákat célzó támadások (Sophos, 2024).

Ha az Europol[18] 2024-es, internetes szervezett bűnözésre fókuszáló értékelését nézzük meg, itt ismét más hangsúlyok jelentősek. Öt fő jelenségcsoportot emeltek ki: a kriptovaluták és dark web növekvő jelentősége a kiberbűnözésben, a ransomware és malware támadások, kiskorúak szexuális kizsákmányolása (amiben növekvő szerepe van az MI felhasználásának), az online és fizetési rendszerekkel elkövetett visszaélések (ideértve a phishing-et, az account-lopást, a befektetési és romantikus csalásokat, az ATM-ek támadását, az online visszaéléseket és a pénzmosást), végül a jövőben várható trendeket, mint pl. diszruptív technológiák felhasználásával összefüggő bűncselekményeket, de ideértve az MI rossz szándékú alkalmazását, a szervezett bűnözés szolgáltatási szintek szerinti tagolódását (ransomware-as-a-service), a pénzügyi rendszerek fokozott védelmét, a tiltott tartalmak szűrését (Europol, 2024).

A fentiek alapján két fontos következtetés mindenképpen levonható. Elsőként természetes, hogy minden elemzést végző szervezet saját perspektívából, küldetéséhez, feladatrendszeréhez illeszkedően határozza meg a vizsgálat fókuszát, témáit, ezeket gyakran dominálják az éppen aktuális, divatos trendek és témák. Ezekhez igazítva prezentálják aztán az eredményeiket is, időnként toplistás megközelítésben, a figyelem megragadására koncentrálva, ezért bármely elemzés kritika nélküli átvétele semmilyen szervezet számára nem javasolt, a saját szempontok szerint elvégzett analízist a saját stratégia felépítése előtt nem lehet elhagyni. A második konzekvencia, hogy a kiberbiztonsági szféra természetéből fakadóan műszaki-technikai szemlélet, nyelvezet és kultúra által dominált, az azonosított jelenségek, ezek leírása is gyakran a technológiai részletekre koncentrál, politikai vagy stratégiai szintű döntéshozatalt kevésbé képes közvetlenül informálni további interpretáció nélkül.

[16] Az Európai Unió kiberbiztonsági ügynöksége (https://enisa.europa.eu/).

[17] Globális kiberbiztonsági szolgáltató cég (https://www.sophos.com/en-us/company).

[18] Az Europol az EU belső rendészeti koordinációért felelős szervezete (https://www.europol.europa.eu/).

Mindezek miatt – legalább gondolatkísérlet szintjén – nem hiábavaló egy a kockázatokat szélesebb társadalmi kontextusban értékelő elemzési megközelítés elvégzése a következő fejezetben, amire egy jó példa lehet a PMESII-PT modell. A tényezők kifejtésében a terjedelmi korlátok miatt is inkább néhány kiemelt, akár már a fentiekben említett témakörre koncentrálok, azok jogi vonatkozásait is megemlítve, de szándékom szerint jobban – ezeket kicsit másképpen csoportosítva, rendezve – kidomboríthatóak a fenyegetések által befolyásolt össztársadalmi érdekek, amelyek a jogalkotás, jogalkalmazás szintjén is jelentős feladatokat jelentenek már most is.

3. A 21. század IKT közegének fő kockázatai, a digitális technológiák működésének immanens gyengeségei és a jog (fél)megoldásai – PMESII-PT elemzési szempontok mentén

3.1. Politikai

A teljes kibertér működése, tartalma és felhasználói felett nincs egyetlen igazán szuverén hatalom. Egyes domainjei és szegmensei felett, jobban kontrollált, és körülhatárolt hálózatok felett tudnak kialakítani állami szereplők viszonylagos fennhatóságot, de ennek szintjét magasabbra tolni exponenciálisan növekvő költségekkel és restriktív szabályozással lehetséges, és a totalitás sem garantálható.

Globálisan a legkomolyabb problémát a nemzetközileg elfogadott nemzetközi jogi és etikai keretek hiánya okozza. A számítógépes bűnözés elleni nemzetközi küzdelem fontos kezdőpontjának tekintett Budapesti Egyezmény óta átfogó specifikus szabályozás nem született. A NATO-EU országok tipikus álláspontja a hatályos nemzetközi jogi és humanitárius jogalapként és háttérként kezelése,[19] Oroszország, Kína és Irán és a hozzájuk igazodó országok megközelítése ezt nem elismerve, az ENSZ keretei közt egy teljesen új jogi rezsim, „lex specialis" egyezményi környezet kialakítása lenne, ami bár évek óta folyamatban van (UN, 2021), de sok eredménnyel középtávon sem kecsegtet. Érdekesek és a kibertérben játszott szerepük miatt nem elhanyagolható jelentőségűek azok a kezdeményezések, amelyek a techszektor szereplőihez köthetők, és szintén egyfajta közös nevező megteremtését célozzák.

A büntetőjog vonatkozásában akár a nemzeti büntető törvénykönyvek további harmonizálásával és a szintén az ENSZ keretei között 2024 végére elkészült új kiberbűnözés elleni egyezmény[20] széles körű ratifikációja is alkalmas lenne előrelépést elérni, amit már a Budapesti Cybercrime Egyezmény[21] elkezdett, de a 2001-es elfogadása óta bizonyos vonatkozásaiban már bizonyosan meghaladottá vált, hiszen sem a mesterséges intelligencia, sem a közösségi média, sem deepfake-technológiák nem voltak akkor még meghatározók.

[19] Hadijogi és humanitárius jogi szempontból ennek egyfajta összefoglalója az ún. Tallinn 2.0 kézikönyv (Schmitt, 2017), de emellett fontos iránymutatást ad az államok kibertérre vonatkozó nemzetközi jogi értékelésére az elmúlt időszakban kiadott ún. nemzeti álláspontok különböző formákban való közzététele (amivel hazánk egyelőre még adós maradt): https://cyberlaw.ccdcoe.org/wiki/Category:Common_and_national_positions

[20] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (New York, 24 December 2024), Online: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en

[21] Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény.

A nemzetközi jog területén a jelenlegi multipolaritás felé mozduló nemzetközi környezetben és különösen a folyamatban lévő orosz-ukrán háború alatt nem várható lényegi előrelépés, mivel az anyagi érdekek mentén motivált szervezett bűnözés és az állami érdekeket kiszolgáló kibertámadások nagyon gyakran össze is kapcsolódnak, határaik elmosódnak. Mindenesetre hosszabb távon szükséges lenne arra – némi redukcionista szarkazmussal –, hogy például egyfajta szokásjogi, meglévő nemzetközi normákat értelmező kompendiumon[22] és a Nemzetközi Jogi Bizottság államfelelősség-koncepcióján (ARSIWA)[23] túl más, és stabilabb kapaszkodó és világszerte elfogadott, követett és adott esetben kikényszeríthető minimum-standard is legyen annak megítélésére, hogy mi számít tilosnak a nemzetközi jogban.

A kibertér mellett ugyanígy nincsenek globálisan egységes vezérelv-egyezmények a diszruptív technológiákra vonatkozóan, mint amilyen az MI,[24] vagy a kvantumszámítás, pedig az ezekhez való hozzáférés, alkalmazási kereteik, kereskedelmük várhatóan alapvetően formálja majd a jelen évszázadot.

Politikai síkon szintén egyre erősödő jelentősége van a digitális térben, a big data-elemzéseken alapuló és különösen az MI felhasználásával megnövelt hatékonyságú propagandának, információs műveleteknek, amelynek alkalmazásában állami és nem-állami szereplők egyaránt kiveszik a részüket.[25] A szintén növekvő digitális eszközöknek való mindennapi kiszolgáltatottság emeli a megfigyelés, és adott esetben a cenzúra esélyeit is, amelyek kapcsán – gazdasági érdekekből akár – fejlett demokráciákból származó vállalkozások kompromisszumokra is képesek lehetnek az emberi jogok érvényesülése vonatkozásában.

3.2. Erők, képességek

Katonai közegben ez a pont elsősorban a fegyveres erők leírására szolgál, az IKT közeg vonatkozásában itt elsősorban a kiberbiztonságért felelős állami intézményrendszert, és az EU-ban a NIS2 irányelv és az egyes nemzetek jogharmonizációján keresztül a nemzeti szabályok által megkövetelt szervezeti védelmi intézkedéseket lehet itt felsorolni. Jellemző állami megközelítés a kiberbiztonság állami felügyletére, hogy valamely (technikai jellegű) nemzetbiztonsági szolgálat, vagy egy szakosított szerv kerül felelősként kijelölésre, és az is, hogy a kormányzati szintű koordinációt, a kibertér kapcsán érintett hatóságok összekapcsolására egy koordinációs mechanizmus, platform valósítja meg. Konkrét állam értékelésénél mindenképpen értékelni kell a kiberbiztonságért, a kibertér biztonságáért és még bővebben az információs tér biztonságáért felelős hatóságok – jogállami keretek között maradó, az alapjogokat tiszteletben tartó – megfelelő és hatékony jogköreit, a közöttük kritikus jelentőségű együttműködés csatornáit és formáit, és törekvéseik összkormányzati koordinációját, hogy a szervezetek ne egymással versengjenek erőforrásokért és figyelemért, hanem a kitűzött közös cél megvalósításán dolgozzanak.

Ismert probléma, hogy a kiterjesztett személyi hatály alá tartozó szervezeti kör önmagában egy szabályozási intézkedéstől még nem bővítette feltétlenül a rendelkezésre álló szakemberei körét

[22] Amilyen például a már említett Tallinn 2.0 kézikönyv, de már a szintén drasztikusan fejlődő űrjogra is léteznek ilyen projektek, ld. például az ENSZ UNOOSA gyűjteményét: https://www.unoosa.org/oosa/en/ourwork/spacelaw/nlbcompendium.html

[23] Responsibility of States for Internationally Wrongful Acts (Online: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf). Részleteit lásd pl.: Kajtár (2016).

[24] Az MI szabályozás dilemmáihoz lásd pl.: Rodgers et al. (2023), Erdélyi és Goldsmith (2018), Hacker et al. (2023), Hacker (2023).

[25] Lásd pl.: Dobák és Kenedli (2024).

és ruházott be jelentős mértékben a kiberbiztonságba. Igaz ez ugyanúgy az állami szférára (amely a NIS2-vel került bele általánosan európai szinten a védett körbe, bár hazánkban már korábban is ide tartozott), mint a számos kritikus infrastruktúrát üzemeltető szervezetre, amelyek gyakran elavult, már nem támogatott hardver- és szoftvereszközökkel működő, ún. legacy-rendszereket működtetnek, amelyektől adott esetben fogyasztók tömegeinek energiaellátása is függhet.

A képesség kategóriájában kell említeni a felhasználók gyakran említett kiberhigiéniai felkészültségének hiányosságait is,[26] amit racionálisan azért össze kell mérni azzal a növekvő komplexitással is, amit a növekvő digitalizáció hoz magával (számtalan, növekvő bonyolultságú jelszó, egyre több applikáció, egyre kevesebb „analóg" eszköz, gyakran változó felhasználói felületek stb.), amelyek szintén hordozhatnak magukban akár a tervezésből fakadó, akár a nem megfelelő paraméterezésből/konfigurálásból származó sérülékenységeket (pl. IoT-eszközök biztonsági rései).

A kiberbiztonság szabályozásának fejlődése, az egyes aspektusok egyre szofisztikáltabb igazgatási megközelítése magával hozta a hatáskörök és feladatok töredezettségét és részben inflációját is. A kibertér közege azonban gyors, határozott és hatékony fellépést követel meg, ezért a közösségi harmonizációt követően az első tapasztalatok után érdemes lenne ezen szempontok mentén is konszolidálni az egyre szélesebb szervezeti kört.

3.3. Gazdasági

Ebben a dimenzióban a már bevezetőben említett, és az államok szempontjából is talán egyre inkább nyomasztó techszektor-fölény az első tényező, amit kockázatként azonosíthatunk. A legnagyobb vállalatoknak otthont adó és hagyományosan a szabadpiacot favorizáló Egyesült Államokban hosszú ideje nem jelennek meg olyan fontos területeken sem szövetségi szintű szabályozások, mint a személyes adatok védelme, az általános kiberbiztonság, vagy akár az online platformok és közösségi média tartalomszabályozása, legfeljebb tagállami szintű törvényekről, és egyes részterületekre vonatkozó kezdeményezésekről lehet beszélni. Az EU-ban globális értelemben meghatározó ilyen cégek csak telephelyeket üzemeltetnek, de nem elsősorban honosak, ezen keresztül érvényesül – legalábbis az EU területén nyújtott szolgáltatásaik vonatkozásában – a közösségi jog, ami az IKT-szféra területén a GDPR-tól kezdve egy teljes generációváltáson és a szabályozás spektrumát tekintve meglehetős horizontális bővülésen is keresztülment az elmúlt időszakban (pl. MI rendelet,[27] DSA, CSA, NIS2, CER, DORA[28] rendelet, kiberreziliencia és kiberszolidaritás[29] szabályai).

A techszektor leginkább sikeres cégeire a kezdeti szakaszban különösen jellemző a nagy sebességű termékfejlesztés, ahol a meglévő és hagyományos jogi keretek tiszteletben tartása

[26] Ehhez lásd pl.: Dobák és Babos (2021), Palicz et al. (2010).

[27] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet).

[28] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról.

[29] Az Európai Parlament és a Tanács (EU) 2025/38 rendelete (2024. december 19.) a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról, és az (EU) 2021/694 rendelet módosításáról (a kiberszolidaritásról szóló rendelet).

nem mindig játszik elsődleges szerepet, különösen igaz ez a személyes adatok kezelésére és a szerzői jogokra. A „move fast and break things" megközelítés, a rövid termékciklusok az IKT termékek vonatkozásában mind a hardver, mind a szoftverek esetében jellemző, aminek következménye a nem megfelelő előzetes tesztelés, és általában nem a termékfelelősség, vagy a biztonsági szempontok, hanem a minél gyorsabb piacra kerülés a fő. A félig befejezett termékek utólagos javítócsomagokkal foltozása, vagy éppen a korábbi generációk biztonsági támogatásának néhány éven belüli megszüntetése komoly problémát okoz, még olyan felhasználóknak is, akik telepíteni szokták a frissítéseket. A következő időszak egyik kulcskérdése az EU-ban, hogy a tanúsítási rendszerek, és a kiberreziliencia szabályozás milyen fejlődést hoz.[30]

Szabályozási szempontból a termékfejlesztés olyan vonatkozásokban is problémát okoz az államoknak, hogy az újabb szolgáltatások és megoldások egyre több hagyományos intézmény alapjait kérdőjelezik meg, és további kontrollvesztéshez vezetnek. Ha a kriptovaluták, és a hozzájuk kapcsolódó piac fejlődését vesszük, valamint ezek szerepét a szervezett bűnözésből szerzett bevételek tisztára mosásában, nyilvánvalóvá válik, hogy ezek össztársadalmi hasznossága legalábbis vegyes megítélésű lehet.

Szerzői jog oldaláról okoz gondot az MI fejlesztésekhez felhasznált alapadatok eredetének tisztázottsága, az eredeti szerzők jogainak tiszteletben tartása és a generált eredmények megítélése is, nem is beszélve ezeknek az eszközöknek az akadémiai közegre gyakorolt hatásáról a művek eredetiségét illetően, és az ezekre a rendszerekre még meglehetősen gyakran jellemző, utólag lekövethetetlen belső működéséről, illetve „hallucinációiról". Az MI rendszerekbe betáplált, biztonsági szempontból érzékeny műszaki és személyes adatok kezelése, valamint az ezekre a megoldásokra való jelentős mértékű hagyatkozás egyelőre komoly kockázatokat hordoz magában, de a töretlen fejlődésre törekvést és globális versenyt továbbra sem hűtik megfelelően az etikai és jogi aggályok.

A gazdasági szférát érinti elsősorban a politikai multipolaritásból és bizonyos vonatkozásban high-tech hidegháborúnak is tekinthető az egyre szélesebb körű exportkorlátozási és büntetővám kivetési gyakorlat, ami elsősorban a magasan fejlett, MI-fejlesztéshez és kvantumszámításhoz kapcsolódó félvezető technológiákra, és az ezeken futó szoftvermegoldásokra terjed ki, de ezek mögött közvetlenül egyre jelentősebb a hadiipari és az ún. kettős felhasználású technológiákra irányuló figyelem is, amelyeknek az egyre gyakrabban fellobbanó nyílt fegyveres konfliktusokban is szerep jut.

3.4. Társadalmi

A modern IKT közeg vitathatatlanul közvetlen hatással van arra, ahogy a társadalmak szerveződnek, az ideák, nézetek cserélődnek, a közbeszéd alakul. A digitális forradalom vívmányai sajnos egyre többször igazoltan bizonyulnak hatékony eszköznek a társadalmi kohézió megbontására, visszaélésszerű alkalmazása a tisztán üzleti célú marketing mellett a kereső- és ajánló algoritmusok érzelemkiváltó hatására építésével súlyos mellékhatásokkal jár a csoportok és az egyén szintjén is.

A társadalmi szint mellett az egyének mentálhigiénéje is súlyos veszélynek van kitéve, amikor egyes elszigetelődött személyek az interneten keresnek és találnak a saját világlátásukat erősítő tartalmakat és közösséget (nyúlüreg-hatás, echo-chamber effektus), ezzel relativizálva

[30] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály).

a társadalmi normától eltérő nézeteket. Az összeesküvés-elméletek növekvő népszerűsége, a szélsőséges csoportok egymásra találása, megszerveződése vagy akár a magányos és bizonyos esetekben igen súlyos pszichológiai problémákkal küzdő személyek mind jelentős társadalmi kockázatokat hordozhatnak.

A személyes adatok tömeges gyűjtése az egyre több és fejlettebb szenzorral rendelkező eszközökön keresztül, aztán a begyűjtött felhasználói adatok profilozása, kereskedelmi és politikai célú felhasználása szintén komoly probléma. A hosszú szerződési feltételek, amelynek elfogadása nélkül az áhított szolgáltatások nem érhetők el, alkalmasak lehetnek a személyes adatkezelés központjában lévő hozzájárulás kiüresítésére.[31] Hogy mennyire reménytelen dolog egy internetre kikerült információ eltüntetése, azt jól szemlélteti, hogy természetesen már erre is kiterjedt iparág létezik, amelynek szolgáltatói vállalják, hogy az előfizető megbízottjaként törekszenek az érintett magánéletének fokozottabb védelmére.[32]

A PMESII modell a szociális szinten elemzi az általános jogi környezetet, így itt meg kell jegyezni, hogy természetesen érdemes lenne a jog „klasszikus" területein is végiggondolni, hogy mit tehetnénk az IKT technológiák biztonsági minőség-ellenőrzése, terméktámogatása és -fejlesztése színvonalának emelése érdekében (ennek a már meglévő, konkrét specifikus EU szintű szabályozási lépéseit lásd az Infrastruktúra elemzésénél). A szoftvertermékek kellékszavatosságának eddigi, hagyományosan felelősségkizáró/minimalizáló megközelítése helyett egy magasabb szintű és a felhasználói érdekeket jobban figyelembe vevő szabályozás, vagy a szerzői jog egyes megkötéseinek átgondolása (kód-visszafejtés nem csak az interoperabilitás, hanem akár biztonsági szempontok mentén is?) szintén segíthetne egy reziliensebb digitális környezet kiépítésében. Ebben fontos előrelépést hozott a magyar jogban is a Ptk. módosításával harmonizálásra kerülő új EU szabályozás, amit a termékfelelősséget 2026. december 9-től a szoftverekre is kiterjeszti.[33]

3.5. Információs

A hagyományos lineáris médiaszolgáltatásokat, amelyekre az évszázados hagyományokkal rendelkező szabályozási modelleket építettük fel (központi jogi elemei többek közt a cenzúra tilalma, szólásszabadság, sajtószabadság, médiaigazgatás), az internet és a mobilkommunikáció kombinációján alapuló hírportál és közösségi oldalak lassan teljesen kiszorítják. Az ezek hátterében álló felelősségi szabályok viszont korántsem olyan kezelhetők (lásd USA, Section 230[34],

[31] A személyes adatok védelmét a fejlesztés kezdetétől figyelembe vevő privacy-by-design szemlélet bővebb kifejtéséhez lásd: Danezis et al. (2014).

[32] Az adatbrókerek működésének lehetséges kockázataira hívja fel a figyelmet az amerikai Legfelsőbb Bíróság előtti vita, amelyben a brókercég egy 2020-as New Jersey-ben hozott törvény alkotmányosságát vitatja. A törvény lehetőséget ad bizonyos védett csoportoknak (elsősorban az igazságszolgáltatásban dolgozóknak), hogy beperelje a brókert, ha kérés ellenére sem távolítja el személyes adataikat a nyilvánosság elől, illetve az adatbázisaiból. A törvény megalkotására egy rendőr gyermekének megölése miatt került sor. Részletesen lásd: Riley (2024).

[33] Az Európai Parlament és a Tanács (EU) 2023/988 rendelete (2023. május 10.) az általános termékbiztonságról, az 1025/2012/EU európai parlamenti és tanácsi rendelet és az (EU) 2020/1828 európai parlamenti és tanácsi irányelv módosításáról, valamint a 2001/95/EK európai parlamenti és tanácsi irányelv és a 87/357/EGK tanácsi irányelv hatályon kívül helyezéséről; a magyar tervezet társadalmi egyeztetését lásd: https://kormany.hu/dokumentumtar/tarsadalmi-egyeztetes-a-maganjogi-targyu-torvenyek-modositasarol

[34] Communications Decency Act 1996, Section 230: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Nyers fordításban: Az interaktív számítógépes szolgáltatás nyújtója vagy felhasználója nem tekinthető más infor-

az egyes online platformok önszabályozáson alapuló felhasználási feltételei, irányelvei), mint a hagyományos médiától és sajtószervektől megszokott jogilag is szabályozott szakmai és felelősségi színvonal, szerkesztési fegyelem és újságírói etika. A tömeges adatfeldolgozás, az ajánló algoritmusok (és ezek működésének átláthatósága) továbbá az MI fejlesztések eredményeként a 21. század tömegtájékoztatása súlyos belső konfliktusokkal és hitelességi problémákkal terhelt.

A digitális adatok feletti „szuverenitás" társadalmi és egyéni szinten is gyengül, az információáramlás feletti kontrollt a diskurzus kibertérbe és digitális közegbe költözésével a nemzetállamok nagyrészt elvesztették a – többnyire extraterritoriális hatállyal működő – techszektor óriásaival szemben, amelyek képesek lehetnek akár a szabályozási folyamatok befolyásolására, de arra is, hogy költség-haszon elemzés keretében valójában működési kiadásként tekintsenek hatósági bírságokra, amennyiben a kétséges legalitású üzleti gyakorlat nagyobb növekedéssel, piaci részesedés szerzésével vagy nagyobb bevétellel kecsegtet. Az egyes országok kibertérben meghatározott joghatósági szabályai, a „digitális határok" definiálására szintén nem egységes, és kisebb érdekérvényesítő képességgel rendelkező államok esetében kérdéses hatékonyságú. A felhőszolgáltatások, adatközpontok, gyorsító-tárolók, adattárházak valóságos működése nehezen kontrollálható, és a gyakorlatban elsősorban vélhetően az üzemeltető érdekeit szolgálják.

Az EU-ban egyre komolyabban vett platformszabályozás (pl. DSA, DMA, online terrorista tartalmak elleni fellépés[35]) fontos előrelépéseket hozott a közösségi térben, de a globális konszenzus nem csak a mulitpolaritás, a saját információs tér feletti kontroll megőrzése miatt valószínűtlen, de a legnagyobb szereplők maximális önjárósága miatt is. A platformok algoritmusai átláthatatlanok, és manipulatív hatással lehetnek a közvéleményre, politikai döntésekre (pl. Facebook választások alatt). A szintén már érintett „filter bubble" és „echo chamber" jelenségek rontják a nyilvános diskurzus minőségét, az információs tér objektív megbízhatóságát és tájékoztatási hitelességét.

3.6. Infrastruktúra

A korszerű számítástechnikai rendszerek működésének egyik alapvető gyengesége valóban az, hogy a tervezési hibák, túl gyors fejlesztési ciklusok, valamint a rendszerek egyre növekvő komplexitása együtt olyan sebezhetőségeket eredményeznek, amelyeket sem biztonsági, sem minőségbiztosítási folyamatok nem tudnak teljesen kiküszöbölni, és bár a biztonság szerepe nő, de továbbra sem az egyes számú prioritás, alapvetően függ a védeni kívánt infrastruktúra felett diszponálók ún. „kockázati éhségétől".[36]

A mai elektronikus információs rendszerek és hálózatok gyökerei az USA-ban az 1950-es években a védelmi és az akadémiai szférából erednek (ARPA, Berkeley). Az internet gerincét alkotó alapvető protokollok kifejlesztése kapcsán a szakmai szerzőpáros Tanenbaum és Wetherall (2013, 160) így ír:

---

mációtartalom-szolgáltató által nyújtott információk kiadójának vagy közlőjének. Ezzel a „csak" a közzétételhez platformot nyújtó szolgáltató mentesül a felelősség alól, ha nem ő készítette, szerkesztette az adott megkérdőjelezhető tartalmat. Ezt az immunitást az kezdi ki, hogy az ajánló algoritmusok gyakorlati hatása egyre inkább közelíti a szerkesztői tevékenységet, emiatt a Legfelsőbb Bíróság előtt már több eljárás is volt folyamatban, de egyelőre változatlan maradt a szabály, lásd pl.: Quinn (2024).

[35] Az Európai Parlament és a Tanács (EU) 2021/784 rendelete (2021. április 29.) az online terrorista tartalom terjesztésével szembeni fellépésről.

[36] Hazánk szintjén ennek informált megközelítéséhez lásd pl.: Kovács és Krasznay (2024).

„Végül meg kell említeni, hogy bár az IP- és a TCP-protokollt alaposan átgondolták, és jól implementálták, a többi protokoll nagy részt ad hoc jellegű volt. Ezeket többnyire egy tucat egyetemista készítette ütve-vágva, amíg el nem fáradtak. Mivel a protokoll-implementációk ingyenesek voltak, ezért széles körben elterjedtek, mélyen beépültek a rendszerekbe, és emiatt nehezen lehetett azokat lecserélni, ami még ma is kisebb-nagyobb problémákhoz vezet."

Az információs technológiák és a hálózatok világára jellemző felépítési modell az egymásra épülő réteges szerkezet. (pl. TCP/IP protokoll), az egység erejét a leggyengébb része is képes meghatározni, kompromittálódásával a biztonságát veszélyeztetni, azaz a védekezőnek minden szinten biztosítania kell a naprakész állapotot, a támadóknak viszont továbbra is elegendő egyetlen hiba, legyen az emberi tényező, vagy műszaki alapú.

A hibás vagy nem biztonságos protokollok (Kiswani et al., 2022), az elavult vagy nem biztonságos kriptográfiai algoritmusok (amiket a kvantumszámítás réme már konkrétan fenyeget), és a még mindig meglévő implicit bizalom az architektúrában (amelyek úgy vannak tervezve, hogy a belső hálózat megbízható – és így ellentétesek a korszerűbb zero-trust szemlélettel), a kritikus rendszerek digitális függése, az adatok mozgásából, kezeléséből és tárolásából származó kockázatok napi szinten okoznak problémát. Szintén súlyos következményekkel jár, hogy egyre komplexebb, egymásra épülő rendszereket használunk, amelyekben kompatibilitási problémák, működésbeli időzítési hibák, vagy a folyamatos méretbeli növekedésből származó skálázáshatósági zavarok fordulhatnak elő, nem is beszélve az erőforráshiány, vagy üzemeltetési szempontok miatt ismert hibáktól hemzsegő legacy-rendszerekről.

A gyors fejlesztési ciklusban alkalmazott ún. agilis fejlesztési módszertanok (Turk et al., 2002; Abrahamsson et al., 2002), mint pl. a RAD – Rapid Application Development, elősegítik a gyors piacra jutást, de gyakran kompromisszumokat jelentenek a szoftver minősége és megbízhatósága terén és nem alkalmasak összetett, esetleg hosszú távú projektek kezelésére, amelyekben idővel a felhasználás körülményei is változhatnak.[37] A fejlesztésben felmerülő esetleges komplikációkat tovább növeli az MI megoldások alkalmazása kód írására, amely egy ponton túl már a fejlesztő számára is követhetetlenné válhat (Shafiq et al., 2020).

Túl gyakran fordul elő, hogy új funkcionalitások és technológiák települnek olyan korábban már törékenynek és sérülékenynek bizonyuló megoldásokra és ezzel a biztonság és reziliencia szempontja sérülnek. Ebbe a közegbe érkezik meg egyre nagyobb jelentőséggel a mesterséges intelligencia-kutatások és a kvantumszámítás számos eredménye.

Mindezekkel a negatív tendenciákkal szemben szerencsére szembeállítható a kiberbiztonsági ipar néhány fontos fejlődési trendje, amely a regulatív és financiális ösztönzők megfelelő kalibrálása esetén, széles körben elterjedve komoly biztonsági színvonal-emelkedést hozhatnak. Ilyenek a zero trust, security by design, privacy by default, privacy by design, DevSecOps és más módszertanok,[38] fejlesztői megközelítések, amelyek kiterjedt alkalmazása egyelőre túlzottan idő- és erőforrásigényes, ezért az üzleti érdekek egyelőre gyakran felülírják a biztonsági szempontok mentén történő következetes alkalmazásukat.

Az ellenállóképesség növeléséhez mindenképpen a digitális szféra legjobban pozicionált szereplőinek magasabb szintű felelősségvállalására van szükség, a végfelhasználókra hárított felelősség jelenleg túl nagy, az egyének, a kis- és középvállalkozások, az állami igazgatási szervezetek és különböző közművek üzemeltetői korlátos kiberbiztonsági képességekkel és erőforrásokkal rendelkeznek, döntéseik, tetteik ugyanakkor gyakran messzemenő negatív következményekkel járhatnak.

[37] A szoftverfejlesztési életciklusokhoz lásd pl. Shah (n. d.).

[38] Például a DARPA által finanszírozott és a Michigan Egyetemen fejlesztett speciális chiptechnológia: Halfacree (2021).

3.7. Fizikai környezet

A digitális technológia fizikai oldalról a működtetés előfeltételeként egyrészt a folyamatos (és ideálisan redundáns) elektromos energia-ellátástól,[39] másrészt a nagyobb szolgáltatások hátterében működő szerverparkok vonatkozásában a száraz, tűztől és más haváriáktól védett, klimatizált-hűtött elhelyezéstől függ.

Ezeket feltételeket nem elegendő egy-egy kulcsprojekt vonatkozásában egyszer teljesíteni, a folyamatos fejlesztések, bővítések, az eszközök természetes avulása soha véget nem érő beruházási szükségleteket támaszt az üzemeltetéssel szemben. Azt sem szabad elfelejteni, hogy a kritikus infrastruktúrákra, a Kibertv. hatálya alá tartozó szervezetekre, vagy éppen a DORA rendelet hatálya alatt működő pénzügyi szférára, de a gyakorlatban minden olyan szervezetre, ahol a szolgáltatások fenntartása, a magas rendelkezésre állás prioritás, ott a üzlet-folytonossági tervezés a helyszíni redundáns eszközök és energiaforrások mellett a legrosszabb esetben az alternatív üzemelési helyszínekre is kiterjed, ahonnan annak készültségi szintjétől függően az adott szervezet működés némi átállást, és előkészületeket követően tovább folytatható.

A klímaváltozás kapcsán egyre komolyabb és drágább problémát jelent a mérsékelt, vagy trópusi égövekben lévő országok adattárházai vonatkozásában a folyamatos hűtés és energiaellátás. Az adott ország elektromos energiahálózatának felépítése,[40] a szomszédos országokkal való összeköttetések alapvetően meghatározzák a hálózat rugalmasságát. Az egyenletes és változó termelési kapacitású energiatermelés megfelelő szintje nagyon fontos, tekintettel arra, hogy az ingadozó hozamú megújulók komoly szabályozási nehézségeket tudnak okozni az áramhálózatok szabályozásában, ezért jelentősek azok a törekvések is, amelyek az energiatárolás fejlesztését célozzák.

Kevésbé hétköznapi, de drasztikus következményekkel járhat még az elektromágneses spektrumban működő digitális technológiák vonatkozásában a napkitörések jelensége, amelyek már több alkalommal okoztak jelentős üzemzavarokat,[41] és a védekezés is elég nehéz ellenük, de a legfontosabb infrastruktúrák vonatkozásában ezzel az eshetőséggel is érdemes számolni.

3.8. Időtényező

Az időtényező a digitális technológiák vonatkozásában drámai fontossággal bírhat, mivel teljesen tipikusak az automatizált, vagy fél-automatizált megoldások, amelyek az emberi felfogóképességet jócskán lehagyva törekszenek a maximális hatékonyságra. A gazdasági életből példaként hozhatók fel a hipergyors tőzsdei arbitrázs kereskedő-rendszerek, vagy az infrastruktúra és a fizikai környezet kapcsán már említett SCADA és ipari vezérlőrendszerek az energiaellátásban. A kiberbiztonságban is hétköznapinak számítanak azok az előre paraméterezett, sőt most már

[39] Az energetikai kritikus infrastruktúrák kiberbiztonságához részletesen lásd a SeconSys projekt keretében készült kézikönyvet: Angyal et al. (2023).

[40] Példaként lásd a Spanyolországot, Portugáliát és kisebb részben Franciaországot érintő 2025. április 28-i áramhálózati összeomlást, a feltételezett okokról röviden lásd az Institute for Energy Research előzetes áttekintő anyagát, kommentárját: IER (2025).

[41] Az USA-ban ezt meglehetősen komolyan veszik, és számos tanulmány készült már a témában, ami az elektromos hálózat ellenállóképességét elemzi. Ezek azonosítják is az aktuálisan sérülékenynek számító területeket, amivel segíthetnek megalapozni a rezilienciát növelő fejlesztéseket. Példaként lásd: Lucas et al. (2020).

öntanuló, és MI háttérrel megerősített adatforgalom-ellenőrző megoldások, amelyek szinte valós idejű védekezést tesznek lehetővé.

A szoftver és hardver sérülékenységére vonatkozó információk jelentőségét jól mutatja, hogy ezek feltárására időnként a gyártó cégek is pályázatokat írnak ki, a dark weben szervezett bűnözők kereskednek velük, de nyilván ezek mindaddig őrzik meg „értéküket" amíg az elsők közt, a hatékony javítócsomagok telepítése, vagy más védelmi intézkedések alkalmazása előtt lehet ezeket bevetni. Ezek között is kiemelt szerepet játszanak a teljesen ismeretlen, ún. zero-day sérülékenységek, amelyek a nyilvánosság számára nem ismertek nem csoda, hogy az ilyen tudás számít a legnagyobb értéknek, és nem csupán a bűnözők, de akár a multipolaritásra jellemző kibertéri műveletek kapcsán egyes ellenérdekelt államok, és a számukra technikai megoldásokat, „kiberfegyvereket" fejlesztő és szállító specializált vállalkozások számára is.[42]

Kicsit lassabb, emberközelibb időhorizonton az adott célpont kitettségét növelheti egy-egy különleges, kiemelt időszak. Erre jó példa lehet egy választási eljárást kiszolgáló rendszer a választás napján, egy online szerencsejátékkal foglalkozó weboldal nagyobb sportesemények esetén, vagy egyszerűen csak üzemeltetési szempontokból egy e-közigazgatási felület valamely jogszabályban rögzített kötelező adatszolgáltatási határidő környékén.

Összegezve a fenti szempontok rövid értékelését elmondható, hogy a 21. századi infokommunikációs rendszerek működése mélyen összefonódik a társadalom egészével, és ezáltal a bennük rejlő kockázatok is komplex módon jelentkeznek. A szabályozási környezet már szinte reménytelenül reaktív, ami a legjobb esetben is csak követni tudja a technológiai rendszerekből eredő veszélyeket. Ahhoz, hogy ezeket a kihívásokat kezelni tudjuk, multidiszciplináris, nemzetközi szempontokat mérlegelő, erőforrások vonatkozásában tartalékokat képző és előrelátó stratégiaalkotásra, valamint arra épülő szabályozási megközelítésekre van szükség.

Nem túlfeszítve a PMESII modell kereteit elmondható, hogy akad még értékes eszköz a katonai művelettervezés eszköztárában (pl. a kritikus képességeket, sebezhetőségeket, és követelményeket ábrázoló súlypontelemzés, vagy a stratégiai célkitűzéseket, eljárásokat és alkalmazási rendeket, illetve képességeket kifejtő ends-ways-means modell), ami megfelelő interpretáció mellett logikusan alátámasztott, követhető analízissel tenne levezethetővé fontos szakpolitikai lépéseket. A korlátos erőforrások melletti hibás, vagy nem kellően megalapozott döntések látszatmegoldásokhoz, zsákutcákhoz és a jelenlegi geopolitikai helyzetben növekvő kitettséghez vezethetnek.

4. Összegzés

2025. március 31-én hosszú munkát követően kiadásra került a NIS2 és Kibertv. alapján is szükséges, több mint 12 év után frissített új nemzeti kiberbiztonsági stratégia.[43] Tartalmát nyilván a jogszabályi keretek, elsősorban az EU szabályozási generációváltása és annak horizontjának drasztikus tágulása határozta meg, de ha csak a jelen dolgozatban a stratégia építés egy lépésének tekinthető fő kockázatok meghatározását nézzük, itt is némi ötletszerűséggel és nem feltétlenül átfogó elemzéssel találkozunk, habár vannak a stratégiának ilyen részei is. A stratégia a 3. pontjában azonosítja a legnagyobb kihívásokat, és ezek a válságok megjelenése

[42] Lásd pl. az izraeli NSO Group által fejlesztett és notóriussá vált a Pegasust, háttérhez lásd pl. a Council of Foreign Relations összefoglalóját: Robinson (2022).

[43] 1089/2025. (III. 31.) Korm. határozat, Magyarország Kiberbiztonsági Stratégiájáról.

(máshogy romló biztonsági környezet), az egyén és társadalom összhangjának megzavarása (káros hatások szociális kohézióra), függőség kialakulása (ami szintén szociális elem), ellátási láncok megzavarása (ami értékelhető gazdasági és infrastrukturális problémaként is), valamint az adatbiztonság sérülékenysége (ami képességbeli, gazdasági, szociális kérdés is lehet). A stratégia becsületére legyen mondva, hogy több más fent említett elem azért megjelenik benne a bevezetőben, a fontos szereplők azonosításában, de azért lehet néhány vonatkozásban hiányérzete az olvasónak, ha kifejezetten stratégiakészítési módszertant (Vikman, 2023), logikusan egymásra épített elemeket keres a dokumentumban.

Véleményem szerint a PMESII-PT és más modellek alkalmazása összetettebb képet adhat mint a tisztán technikai szemléletű, aktuális, „divatos" fenyegetésekre koncentráló felsorolások, különösen azzal, hogy egy társadalmat több szempontból közelít meg, így az elemzőt is elsősorban a védendő érdekek irányából gondolkoztatja el, és ezzel a politikai/szakmai döntéshozatalt segítheti az erőforrások vonatkozó döntésekben egyrészt az ország/szervezet prioritásainak és a rendelkezésre bocsátott erőforrások mennyiségének, minőségének és összetételének meghatározásában.

Azzal együtt több fontos elem is megjelent az új stratégiában, ami a szakpolitikában is korszerű szemléletet jelez. Ezek közül, részben ezeket továbbfejlesztve valószínűleg egyet lehet érteni azzal, hogy szüksége lenne már rövid távon is paradigmaváltásra a biztonságért viselt felelősség elosztásában a fogyasztó/ügyfél, gyártó/szolgáltató, szabályozó/felügyelet között, valós és hatékony ellenőrzésre a termékek és szolgáltatások és azok igénybevétele felett (akár harmadik felekkel, garantőrökkel). Konkrét lépéseket kellene tenni közösségi és nemzeti szinten egyaránt az adatok védelme, ellenőrzése feletti kontroll visszaszerzésére, ezek védelmi-biztonsági érdekű megismerésének jogállami garanciákkal körbebástyázott lehetőségével. A minőség-ellenőrzés, terméktámogatás, és -fejlesztés színvonalának emelése, a szoftvertermékek kellékszavatosságának hagyományosan felelősségkizáró/minimalizáló megközelítése helyett, valamint, a szerzői jogi korlátok esetleges lazítása biztonsági érdekből a meglévő interoperabilitási visszafejtés lehetőségének bővítésével szintén praktikus eszközök, amelyek előrelépést jelenthetnének biztonsági szempontból.

A jelenlegi geopolitikai közegben egy ilyen széleskörű konszenzust igénylő témakörben viszont sajnos nem várható egy valóban tartalmi nemzetközi összefogás egy átfogó szabályozás megalkotása a széttartó biztonsági, és gazdasági érdekek miatt, továbbá Európának továbbra is komoly fejtörést okoz majd a technológiai szektorának relatív versenyhátránya, és az Európán kívüli tech-cégek hatékony visszaszorítása a közösségi jog keretei közé.

Nemzeti szinten lehetséges intézkedések, legalábbis állami oldalról praktikusan egyrészt az állami IKT beszerzéseknél minél magasabb és számonkérhető biztonság színvonal megkövetelése, másrészt a digitális technológiák és biztonságos felhasználásuk kapcsán bármely szinten érintett állami szervezetek tevékenységének, fejlesztéseinek, és működésének hatékony összehangolása, akár egy egyesített, dedikált, a nemzetbiztonsági közegből kimozdított (és így kevésbé félelmetes) önálló központi kiberbiztonsági hatóság és incidenskezelő kialakításával, amire jó példákat ismerünk Németországból (Bundesamt für Sicherheit in der Informationstechnik)[44] vagy Nagy-Britanniából (National Cyber Force).[45]

A negatív tendenciákkal szemben szerencsére szembeállítható a kiberbiztonsági ipar néhány fontos fejlődési trendje, amely a regulatív és financiális ösztönzők megfelelő kalibrálása esetén, széles körben elterjedve komoly biztonsági színvonal-emelkedést hozhatnak. Ilyenek a zero trust, security by design, privacy by default, privacy by design, DevSecOps és más mód-

[44] Bővebben lásd: Vikman (2021).

[45] Bővebben lásd: Farkas (2022).

szertanok, fejlesztői megközelítések. Ezek kiterjedt alkalmazása állami szorítás nélkül továbbra sem várható minden esetben, idő- és erőforrásigényük miatt, ezért az üzleti érdekek továbbra is várhatóan felülírják a biztonsági szempontok mentén történő következetes alkalmazásukat[46].

Hivatkozások

Abrahamsson, P., Salo, O., Ronkainen, J., & Warsta, J. (2002). Agile Software Davalopment Methods: Review and Analysis. *VTT Publications, 478*. https://doi.org/10.48550/arXiv.1709.08439

Affleck, R. T., Roningen, J. M., Macpherson, J. S., Tracy, B., & Voyadgis, D. E. (2015). *Analysis of Operational Data*. Engineer Research and Development Center. Online: https://apps.dtic.mil/sti/tr/pdf/ADA624478.pdf

Angyal I., Arató Gy., Bakos B., Baranya Zs., Bocsok V., Bogáncs T. J., Bonnyai T., Buttyán L., Csatár J., Danyek M., Deák V., Faragó J., Görgey P., Gyebnár G., Illés G., Kocsis T., Krasznay Cs., Molnár F., Ölvegyi R., Pfeiffer Sz., Pongrácz P., Sípos R., Szabó-Nyakas Zs. Cs., Szádeczky T., Szent-Királyi B., Winter G., & Zámbó M. (2023). *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági* kézikönyve 2022. SeConSys. Online: https://seconsys.eu/#kezikonyv

Carter, S., King, J., Lothian, J., & Younkers, M. (2023). *Model-Driven DevOps. Increasing agility and security in your physical network through DevOps*. Addison–Wesley.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., & Schiffner, S. (2014). Privacy and Data Protection by Design – from policy to engineering. ENISA. https://doi.org/10.2824/38623

Das, BK S., & Chu, V. (2023). *Security as Code. DevSecOps Patterns with AWS*. O'Reilly.

Dobák I., & Babos S. (2021). A biztonságtudatosítás lehetőségei a 21. századi platformok fényében. *Nemzetbiztonsági Szemle*, 9(4), 18–34. https://doi.org/10.32561/nsz.2021.4.2

Dobák I., & Kenedli T. (2024). Információszerzési tendenciák és kihívások a kibertérben rejlő lehetőségek és a mesterséges intelligencia. In Farkas Á., Kelemen R., & Vikman L. (Szerk.), *Kibertéri műveletek és ellenálló képesség. A kibertéri műveletek egyes állami és jogi kérdései* (pp. 143–188). Gondolat Kiadó.

Ducote, B. M. (2010). *Challenging the Application of PMESII-PT in a Complex Environment*. School of Advanced Military Studies, United States Army Commands and General Staff College. Online: https://apps.dtic.mil/sti/pdfs/ADA523040.pdf

ENISA. (2024). *ENISA Threat Landscape 2024*. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Erdélyi J. O., & Goldsmith, J. (2018). Regulating Artificial Intelligence: Proposal for a Global Solution. *AIES ,18: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 95–101. https://doi.org/10.1145/3278721.3278731

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Online: https://tinyurl.hu/UqXG

Faily, S. (2018). *Designing Usable and Secure Software with IRIS and CARIS.* Springer.

[46] Az elmúlt időszakban az IKT technológia biztonsági aspektusát tárgyaló szakirodalom nagy fejlődést mutat, lásd erre kiragadott példaként: Neumann (2024), Das és Chu (2023), Carter et al. (2023), Saini és Raj (2022), Kohnfelder (2022), Riberio (2021), Merkow (2020), Faily (2018).

Farkas Á. (2022). The UK'S National Cyber Force: Beginning of a Hybrid Trend or New Answer for Cyber Domain. *Military and Intelligence Cybersecurity Research Paper*, 2. Online: https://tinyurl.hu/3ohc

Farkas Á., & Kelemen R. (Szerk.). (2023). *A fejlődés fogságában?.* Gondolat Kiadó.

Farkas Á., & Kelemen R. (Szerk.). (2024a). *Kibertér és biztonság egyes jogtani és államtani kérdései.* Universitas-Győr.

Farkas Á., & Kelemen R. (2024b). *National Security and Cyberspace*. Universitas-Győr.

Fazekas F. (2022). A NATO átfogó műveletttervezési útmutatójának evolúciója. *Hadtudomány*, 32(4), 45–61., https://doi.org/10.17047/Hadtud.2022.32.4.45

Hacker, P., Engel, A., & Mauer, M. (2023). Regulating ChatGPT and other Large Generative AI Models. *FAccT ,23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 1112–1123. https://doi.org/10.1145/3593013.3594067

Hacker, P. (2023). *AI Regulation in Europe: From the AI Act to Future Regulatory Challenges*. https://doi.org/10.48550/arXiv.2310.04072

Halfacree, G. (2021). „Unhackable" MORPHEUS Chip Passes Its First Public Test, DARPA's FETT Bug Bounty, Unhacked. *hackster.io*. Online: https://tinyurl.hu/aLIp

Institute for Energy Research (IER). (2025. április 29.). *What Caused Spain and Portugal's Massive Power Outage?*. Online: https://tinyurl.hu/4DXZ

Jurevicius, O. (2025). PMESII-PT Explained. *Strategic Management Insight*. Online: https://strategicmanagementinsight.com/tools/pmesii-pt

Kajtár G. (2016). Szükséghelyzet vagy önvédelem? Vitatott jogalapok a terrorizmus elleni „háborúban". *Jog – Állam – Politika,* 8(2), 57–74. Online: https://epa.oszk.hu/03000/03010/00002/pdf/EPA03010_jap_2016-02_057-074.pdf

Kiswani, J., Dascalu, S., & Harris, F. (2022). Software Development: Past, Present, and Future. In F. Harris, A. Redei, & R. Wu (Eds.), *Proceedings of 31st International Conference on Software Engineering and Data Engineering*, 88, 1–7. https://doi.org/10.29007/qzrd

Kohnfelder, L. (2022). *Designing Secure Software. A Guide for Developers.* No Starch Press.

Kovács L., & Krasznay Cs. (2024). Digitális Mohács 3.0. *Hadtudomány*, 34(3), 40–55. https://doi.org/10.17047/HADTUD.2024.34.3.40

Lucas, G. M., Love, J. J., Kelbert, A., Bedrosian, P. A., & Rigler, E. J. (2020). A 100-year Geoelectric Hazard Analysis for the U.S. High-Voltage Power Grid. *Space Weather*, 18(2), e2019SW002329. https://doi.org/10.1029/2019SW002329

Merkow, M. S. (2020). *Secure, Resilient, and Agile Software Development.* CRC Press.

Neumann M. (2024). *Bevezetés a kiberbiztonsági projektmenedzsmentbe.* Universitas-Győr.

Palicz T., Bonnyai T., Bencsik B., Pintér L., Dombrádi V., Joó T., Bor O., & Hornyik Zs. (2010). Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei. *Belügyi Szemle,* 70(2), 395–418. https://doi.org/10.38146/BSZ.2022.2.11

Quinn, M. (2024. július 2.). Supreme Court declines to review scope of Section 230 liability shield for internet companies. *CBS News*. Online: https://tinyurl.hu/r3Gt

Ribeiro M. (2021). *Learning DevSecOps*. O'Reilly.

Riley, T. (2024. szeptember 30.). Cops Battle Data Brokersfor Privacy in Constitutional Clash (1). *Bloomberg Law*. Online: https://tinyurl.hu/rnuz

Robinson, K. (2022. március 8.). *How Israel's Pegasus Spyware Stoked the Surveillance Debate*. Council on Foregin Relations. Online: https://tinyurl.hu/nLpC

Rodgers, C. M., Ellingson, S. R. & Chatterjee, P. (2023). Open Data and transparency in artificial intelligence and machine learning: A New Era of Research. *F1000Research*, 12(387). https://doi.org/10.12688/f1000research.133019.1

Shafiq, S., Mashkoor, A., Mayr-Dorn, C., & Egyed A. (2020). Machine Learning for Software Engineering: A Systematic Mapping. *CoRR – Computing Research Repository*, abs/2005.13299. https://doi.org/10.48550/arXiv.2005.13299

Saini, K., & Raj, P. (2022). *Advancing Smarter and More Secure Industrial Applications Using AI, IoT, and Blockchain Technology.* IGI Global.

Schmitt, M. N. (Szerk.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Shah, T. (n. d.). *Software Development Life Cycle*. Online: https://www.academia.edu/35735644/Software_Development_Life_Cycle

Sophos. (2024). *Sophos 2024 Threat Report: Cybercrime on Main Street*. Online: https://www.sophos.com/en-us/content/security-threat-report

Susskind, J. (2021). *Politika a jövőben. Életünk a technológia uralta világban*. Athenaeum.

Tanenbaum, A. S., & Wetherall, D. J. (2013). *Számítógép-hálózatok* (3. kiadás). Panem Könyvek.

Turk, D., France, R., & Rumpe B. (2002). Limitations of Agile Software Processes. In: *Third International Conference on Extreme Programming and Flexible Processes in Software Engineering, XP2002, May 26–30, Alghero, Italy*, 43–46. https://doi.org/10.48550/arXiv.1409.6600

United Nations (UN). (2021). *Open-Ended Working Group on Information and Communication Technologies*. Online: https://tinyurl.hu/bFVV

Vikman L. (2024). Az online dezinformáció jogi kezelésének nemzetközi mintái az internet és az online média szabályozásában. *In Medias Res*, 13(2), 198–212. https://doi.org/10.59851/imr.13.2.13

Vikman L. (2023). Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán. In Farkas Á., & Kelemen R. (Szerk.), *A fejlődés fogságában?* (pp. 97–105). Gondolat Kiadó.

Vikman L. (2021). A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. *Military and Intelligence Cybersecurity Research Paper*, 2. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2_2021_MIC_RP.pdf

Vikman L. (2021). A művelettervezés jogi feladatai. *Honvédségi Szemle*, 149(2), 44–56. https://doi.org/10.35926/HSZ.2021.2.4