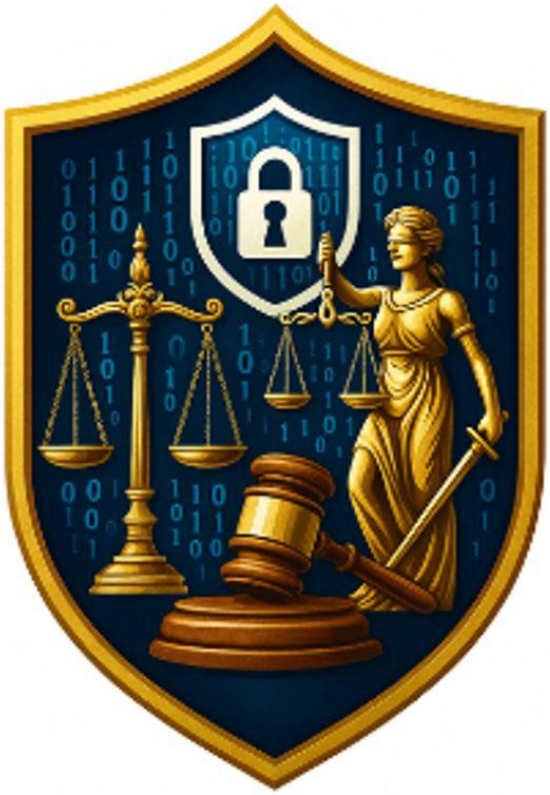

SZÉCHENYI ISTVÁN EGYETEM

Deák Ferenc Állam- és Jogtudományi Kar

Jogi szakokleveles kiberbiztonsági szaktanácsadó

SZÉCHENYI ISTVÁN EGYETEM

Deák Ferenc Állam- és Jogtudományi Kar

Modern Technológiai és Kiberbiztonsági Jogi Tanszék

Jogi szakokleveles kiberbiztonsági szaktanácsadó

DIPLOMAMUNKA

A kibertér mint társadalmi- és konfliktustér

A jogi szabályozás, a biztonságpolitikai kihívások és a digitális nyilvánosság vizsgálata

Készítette: Angyal János

Neptun-kód: UC4HL1

Konzulens: Németh Richárd, egyetemi tanársegéd

Győr, 2026.

DIPLOMAMUNKA
KONZULTÁCIÓS ÉS FELADATKIÍRÓ LAP

Hallgató neve: Angyal János **Neptun-kód:** UC4HL1 **Szak:** Jogi kiberbiztonsági szaktanácsadó

Feladatkiíró tanszék: Modern Technológiai és Kiberbiztonsági Jogi Tanszék

Diplomamunka típusa (aláhúzandó): dolgozat publikáció portfólió

Diplomamunka címe (témája): A kibertér mint társadalmi- és konfliktustér A jogi szabályozás, a biztonságpolitikai kihívások és a digitális nyilvánosság vizsgálata

Dátum: 2026.02.01
(legkésőbb az első konzultáció dátuma)

.....
konzulens(ek) aláírása

Dátum	Tevékenység	Aláírás
2026.02.01.	Előzetes egyeztetés, témakör átbeszélése	
2026.03.07.	Tartalomjegyzék küldése átnézésre, jóváhagyásra	
2026.04.03.	95%-os verzió bemutatása, hiányosságok átbeszélése	
2026.04.24.	Végleges verzió bemuatása, egyeztetés	

A diplomamunkát ellenőriztem: védésre beadható védésre nem adható be

A konzultációs munka értékelése: *(csak a védésre beadható munka értékelhető,ötfokozatú osztályzattal)*	Jeles (5)

(Az értékelés eredménye a leckekönyv féléves adataiban kerül rögzítésre)

Dátum: 2026.04.27.

.....
konzulens(ek) aláírása

NYILATKOZAT

Alulírott Angyal János (Neptun-kód: UC4HL1) kijelentem, hogy ezt a diplomamunkát magam készítettem, és abban csak a megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Győr, 2026.05.01.

Angyal János
hallgató

Tartalomjegyzék

REZÜMÉ

Jelen diplomamunka célja annak vizsgálata, hogy a kibertér miként vált a 21. században társadalmi- és konfliktustérré, valamint hogy ebben a közegben hogyan kapcsolódik össze a jogi szabályozás, a biztonságpolitikai kihívások és a digitális nyilvánosság kérdésköre. A dolgozat abból a feltevésből indul ki, hogy a kibertér ma már nem értelmezhető pusztán technológiai háttérként, hanem olyan összetett működési közegként, amely egyszerre befolyásolja a társadalmi kommunikációt, a gazdasági folyamatokat, az állami működést és a modern konfliktusok természetét.

A kutatás módszertanát tekintve a dolgozat elsősorban leíró és elemző jellegű, szekunder forrásokra épülő elméleti vizsgálat. A feldolgozás során hazai és nemzetközi szakirodalmat, stratégiai dokumentumokat, valamint a témához kapcsolódó legfontosabb magyar és európai uniós jogforrásokat használtam fel. A dolgozat multidiszciplináris megközelítésben vizsgálja a kibertér fogalmát és fejlődését, társadalmi és gazdasági hatásait, az állami szuverenitással való kapcsolatát, konfliktustéri jellegét, továbbá a kapcsolódó jogi szabályozás főbb területeit.

A kutatás eredményei alapján megállapítható, hogy a kibertér mára a társadalmi nyilvánosság, a gazdasági működés és a biztonságpolitikai versengés egyik meghatározó terévé vált. A közösségi média, az online platformok, az elektronikus kereskedelem, valamint a kibertámadások, információs műveletek és hibrid fenyegetések egyaránt azt mutatják, hogy a digitális térben zajló folyamatok közvetlen hatással vannak a fizikai világ működésére is. A dolgozat arra a következtetésre jut, hogy a kibertér kihívásai csak összetett módon kezelhetők: technikai védelemre, megfelelő jogi szabályozásra, szervezeti felkészültségre és tudatos társadalmi jelenlétre egyaránt szükség van.

ABSTRACT

The aim of this thesis is to examine how cyberspace has become both a social space and a space of conflict in the 21st century, and how digital publicity, legal regulation and security policy challenges are interconnected within it. The thesis is based on the assumption that cyberspace can no longer be understood merely as a technological background, but rather as a complex operational environment that simultaneously influences social communication, economic processes, state functioning and the nature of modern conflicts.

From a methodological perspective, the thesis is primarily a descriptive and analytical theoretical study based on secondary sources. The research relies on Hungarian and international academic literature, strategic documents, as well as the most relevant Hungarian and European Union legal sources related to the topic. Using a multidisciplinary approach, the thesis examines the concept and development of cyberspace, its social and economic effects, its relationship with state sovereignty, its role as a space of conflict, and the main areas of its legal regulation.

The findings show that cyberspace has become a key arena of public communication, economic activity and security-related competition. Social media, online platforms, electronic commerce, cyberattacks, information operations and hybrid threats all demonstrate that processes taking place in the digital sphere have direct consequences for the functioning of the physical world as well. The thesis concludes that the challenges of cyberspace can only be addressed in a complex manner, requiring technical protection, adequate legal regulation, organisational preparedness and conscious social engagement.

1. Bevezetés

A 21. század egyik legmeghatározóbb folyamata a digitalizáció. A mindennapi élet, a gazdaság, az állami működés és a társadalmi kommunikáció egyre több területe kötődik digitális rendszerekhez. Ezzel párhuzamosan a kibertér is egyre nagyobb jelentőséget kapott. Ma már nem csupán technikai háttérként tekintünk rá, hanem olyan közegként, amelyben információáramlás zajlik, szolgáltatások működnek, közösségek szerveződnek, és egyre gyakrabban konfliktusok is megjelennek.

A kibertér jelentőségét az adja, hogy a digitális rendszerek mára a társadalmi és gazdasági működés alapvető részévé váltak. A közösségi média átalakította a nyilvánosság szerkezetét, az online kereskedelem új lehetőségeket teremtett, a digitális ügyintézés pedig a közigazgatásban is mindennapossá vált. Ugyanakkor ezekkel a folyamatokkal együtt új kockázatok is megjelentek. Az adatlopás, az online megtévesztések, a dezinformáció, valamint a különböző kibertámadások ma már nem kivételes jelenségek, hanem a digitális működés velejárói.

1.1. A témaválasztás indokoltsága

A téma aktualitása abban rejlik, hogy a kibertér már nemcsak társadalmi és gazdasági, hanem biztonságpolitikai szempontból is kiemelt jelentőségű. A kritikus infrastruktúrák, az állami rendszerek, a pénzügyi szolgáltatások vagy akár az egészségügyi ellátás is erősen függ a digitális háttértől. Emiatt a kibertérben bekövetkező zavarok vagy támadások a fizikai világban is kézzelfogható következményekkel járhatnak. A kibertér emellett az államok és nem állami szereplők közötti versengés egyik új színterévé is vált, ahol az információs műveletek, a kibertámadások és a hibrid fenyegetések egyre nagyobb szerepet kapnak.

A dolgozat témája azért indokolt és különösen aktuális, mert a kibertér ma már nem értelmezhető pusztán informatikai kérdésként. Társadalmi, jogi és biztonságpolitikai szempontból is olyan összetett jelenség, amelynek vizsgálata a jelenlegi digitális környezetben kiemelten fontos. A témaválasztásomat szakmai hátterem is indokolja, hiszen informatikai és információbiztonsági területen szerzett végzettségem, valamint jelenlegi IT vezetői munkaköröm miatt a kibertérhez kapcsolódó kockázatok és szabályozási kérdések a mindennapi szakmai gyakorlatomban is közvetlenül megjelennek.

1.2. A kutatás célja és fő kérdései

A dolgozat célja annak bemutatása, hogy a kibertér miként vált társadalmi és konfliktustérré, valamint hogy ebben a közegben hogyan kapcsolódik össze a digitális nyilvánosság, a jogi szabályozás és a biztonságpolitikai kihívások kérdésköre. A célom nem az, hogy a kibertér minden részterületét teljes mélységében feldolgozzam, hanem az, hogy áttekinthető módon bemutassam a legfontosabb összefüggéseket.

A dolgozat központi kérdése, hogy a kibertér hogyan alakult át az internet és a digitalizáció terjedésével, és miként vált a társadalmi működés egyik meghatározó közegévé. Ehhez kapcsolódóan vizsgálja azt is, hogy a közösségi média és a digitális nyilvánosság milyen hatást gyakorol a társadalmi kommunikációra, milyen új lehetőségeket teremtett az online gazdaság és az elektronikus szerződéskötés, illetve milyen veszélyek jelentek meg az adatlopások, megtévesztések és más digitális visszaélések formájában.

A dolgozat további kérdése, hogy a kibertér milyen módon érinti az állami szuverenitást, és hogyan vált a modern konfliktusok egyik új terévé. Ennek keretében külön figyelmet kapnak

a kibertámadások, az információs műveletek, az OSINT, valamint a hibrid fenyegetések. A dolgozat emellett arra is keresi a választ, hogy a fenti jelenségekre milyen jogi szabályozási válaszok alakultak ki.

1.3. A kutatás módszertana és forrásai

A dolgozat alapvetően elméleti jellegű, és leíró, valamint elemző módszerre épül. A téma feldolgozása során a kibertér technikai, társadalmi, jogi és biztonságpolitikai dimenziói egyaránt megjelennek, de a dolgozatban a terjedelmi korlátok miatt nem törekszem minden részterület teljes körű feldolgozására. Inkább a főbb összefüggések bemutatására helyezem a hangsúlyt.

A dolgozat forrásai közé a hazai és nemzetközi szakirodalom, stratégiai dokumentumok, valamint a témához kapcsolódó fontosabb jogszabályok tartoznak. A jogi részben elsősorban az adatvédelemre, az elektronikus kereskedelemre, az online platformok működésére és a kiberbiztonságra vonatkozó szabályozás jelenik meg. A módszertani megközelítés célja az, hogy a kibertér különböző oldalait ne különálló témákként, hanem egymással összefüggő jelenségekként jelenítsem meg.

1.4. A dolgozat felépítése

A szakdolgozat alapstruktúráját a Széchenyi István Egyetem által közölt szakdolgozat minta adja. A terjedelmi korlát e szerint, illetve a konzulensemmel, Németh Richárddal folytatott konzultáció alapján került meghatározásra. A dolgozat szerkesztése során a jobb áttekinthetőség érdekében a bekezdések között térközöket alkalmazok.

A dolgozat felépítése során arra törekedtem, hogy a kibertér társadalmi, jogi és biztonságpolitikai dimenziói logikus, egymásra épülő szerkezetben jelenjenek meg. A fejezetek sorrendjét úgy alakítottam ki, hogy az olvasó a fogalmi alapoktól fokozatosan jusson el a komplexebb társadalmi, konfliktus- és szabályozási összefüggésekig.

A dolgozat második fejezetében a kibertér fogalmának kialakulását és fejlődését mutatom be. Ebben a részben röviden áttekintem a fogalom történeti hátterét, a technológiai fejlődés főbb állomásait, valamint azt, hogy a kibertér miként vált a modern társadalmi és állami működés meghatározó közegévé. A fejezet célja, hogy megalapozza a későbbi társadalmi, jogi és biztonságpolitikai értelmezéseket.

A harmadik fejezetben a kibertér társadalmi és gazdasági dimenzióit vizsgálom. Ebben a részben külön hangsúlyt kap a digitális nyilvánosság, a közösségi média szerepe, az online szólásszabadság kérdése, valamint az online gazdaság és az elektronikus szerződéskötés jelentősége. Ugyanitt mutatom be azokat a kockázatokat is, amelyek a digitális működésből fakadnak, különösen az adatlopások, az online megtévesztések és az egyéb digitális visszaélések területén.

A dolgozat negyedik fejezetében a kibertér és az állami szuverenitás kapcsolatát elemzem. Ennek keretében bemutatom, hogy a digitális környezet miként alakítja át a klasszikus szuverenitás-fogalmat, hogyan jelenik meg a digitális szuverenitás kérdése, valamint milyen jelentősége van a technológiai függőségnek, az adatok feletti kontrollnak és a nemzetközi együttműködésnek.

Az ötödik fejezet a dolgozatom egyik központi része, amelyben a kibertér konfliktustérré válását vizsgálom. Ebben a fejezetben a kibertámadások, az információs

műveletek, a dezinformáció, az OSINT, a hibrid fenyegetések, valamint a mesterséges intelligenciához kapcsolódó automatizált megtévesztési formák kerülnek előtérbe. A fejezet célja annak bemutatása, hogy a kibertér ma már nem csupán technikai infrastruktúra, hanem a modern konfliktusok és biztonságpolitikai versengés egyik meghatározó tere.

A hatodik fejezetben a kibertérhez kapcsolódó jogi szabályozási kérdéseket tekintem át. Ebben a részben a személyes adatok védelme, az online platformok működésének szabályozása, az elektronikus kereskedelem jogi háttere, valamint a kiberbiztonsági és büntetőjogi összefüggések kerülnek bemutatásra. A fejezetben kitérek a felhőszolgáltatások, az IoT és az új technológiai kockázatok szabályozási kihívásaira is. A célom itt nem a teljes joganyag részletes ismertetése, hanem a dolgozat témájához közvetlenül kapcsolódó legfontosabb szabályozási területek áttekintése.

A hetedik fejezetben a kutatás korlátait foglalom össze. Ebben a részben röviden bemutatom azokat a tartalmi és terjedelmi kereteket, amelyek meghatározták a dolgozat felépítését, valamint azt, hogy a téma multidiszciplináris jellege miatt mely területek igényelnének további, önállóan is részletesebb vizsgálatot.

A nyolcadik fejezet az összegzést tartalmazza, amelyben röviden összefoglalom a kutatás legfontosabb megállapításait, és levonom a kibertér társadalmi, jogi és konfliktustér-jellegére vonatkozó főbb következtetéseket.

A dolgozatot az irodalomjegyzék, valamint a rövidítések és fogalmak jegyzéke zárja, amelyek a felhasznált szakirodalom, jogforrások és a gyakran alkalmazott fogalmak áttekinthetőségét segítik.

2. A kibertér fogalma és fejlődése

A kibertér fogalma a modern információs társadalom egyik alapfogalma, amely azonban nem egyetlen lépésben alakult ki, hanem több évtizedes technológiai és elméleti fejlődés eredménye. A jelenlegi értelmezés mögött egyszerre állnak technikai, tudományos és kulturális hatások.[1]

A fogalom egyik legkorábbi elméleti alapja a kibernetika, amelyet Norbert Wiener a 20. század közepén az irányítás és kommunikáció tudományaként határozott meg.[2] Ez a megközelítés már előrevetítette azt a rendszerszintű gondolkodást, amely ma az információbiztonságban és a kockázatkezelésben is megjelenik.

A „kibertér" kifejezés ugyanakkor nem a tudományos, hanem a science fiction irodalomból származik. William Gibson az 1980-as években használta először, egy olyan hálózati tér leírására, ahol az emberek digitálisan kapcsolódnak egymáshoz.[3] A fogalom később a valós technológiai fejlődés hatására fokozatosan bekerült a szakmai és politikai diskurzusba.

A kibertér tényleges kialakulása a számítógépes hálózatok fejlődéséhez köthető. Az ARPANET létrejötte és a csomagkapcsolt hálózatok elterjedése megteremtette az alapját annak a globális infrastruktúrának, amelyre a mai internet épül.[4] A hálózati működés egyik kulcseleme a decentralizáció volt, amely a mai napig meghatározza a kibertér működését és biztonsági kihívásait is.

Az 1990-es évektől kezdve az internet tömeges elterjedésével a kibertér kilépett a szűk technikai közegből, és a mindennapi élet részévé vált. A hangsúly fokozatosan eltolódott az infrastruktúráról a szolgáltatások és a felhasználói interakciók irányába. Ez a változás IT és információbiztonsági szempontból is jelentős, mivel a támadási felület már nem csupán technikai rendszerekhez, hanem teljes üzleti és társadalmi folyamatokhoz kapcsolódik.

A 2000-es évektől a kibertér értelmezése tovább bővült a felhőszolgáltatások, a mobil eszközök és a közösségi platformok megjelenésével. A digitális és fizikai világ közötti határ egyre inkább elmosódott, így egy kibertérben bekövetkező esemény közvetlen hatással lehet a valós működésre is.

Szakmai -különösen információbiztonsági és kockázatkezelési- nézőpontból ez a fejlődés jól leírható egyfajta érettségi folyamatként: a rendszerek összekapcsoltságának növekedésével párhuzamosan nőtt a komplexitás, a függőség és ezzel együtt a sérülékenység is. Ennek következtében a kibertér ma már nem csupán technológiai infrastruktúra, hanem olyan működési környezet, amelynek biztonsága közvetlenül befolyásolja a szervezetek és az államok működését.

Összességében a kibertér fogalmának fejlődése jól mutatja, hogy egy kezdetben elméleti és részben fiktív koncepció hogyan vált a modern társadalom egyik legfontosabb működési terévé, amelynek megértése elengedhetetlen a további társadalmi, jogi és biztonságpolitikai elemzésekhez.

---

[1] Dodge, Martin – Kitchin, Rob: Mapping Cyberspace. Routledge, London, 2003, 1-3. o.

[2] Wiener, Norbert: Cybernetics: Or Control and Communication in the Animal and the Machine. MIT Press, Cambridge, 1948, 11-15. o.

[3] Gibson, William: Neuromancer. Ace Books, New York, 1984, 51-53. o.

[4] Russell, Andrew L.: Rough Consensus and Running Code: Documents and the History of the Internet. Sloan Foundation, New York, 2006, 22-26. o.

2.1. A kibertér technológiai fejlődésének főbb állomásai

A kibertér technológiai fejlődésének első meghatározó állomása a hálózatba kapcsolt számítógépes rendszerek megjelenése, majd az internet tömeges elterjedése volt. Ezt követte a mobilkommunikáció és az okoseszközök térnyerése, amely a digitális jelenlétet a mindennapi élet állandó részévé tette. A következő jelentős lépcsőt a felhőszolgáltatások és a platformalapú működés kialakulása jelentette, amely már a vállalati és állami rendszerek működését is alapvetően átalakította.[5]

Ezek a fejlődési pontok nemcsak hatékonysági ugrásokat hoztak, hanem a támadási felület jelentős növekedését is. A technológiai fejlődés minden új szintje új sérülékenységeket, beszállítói függőségeket és üzletmenet-folytonossági kockázatokat eredményezett, ezért a kibertér fejlődése ma már szorosan összekapcsolódik a reziliencia és a kockázatkezelés kérdésével.

2.2. A kibertér mint multidiszciplináris jelenség

A kibertér sajátossága, hogy nem értelmezhető kizárólag technológiai közegként. Egyszerre jelenik meg informatikai infrastruktúraként, társadalmi kommunikációs térként, gazdasági működési környezetként, valamint jogi és biztonságpolitikai szabályozási területként is.[6] Ez a többdimenziós jelleg különösen jól látható abban, hogy ugyanaz a digitális esemény – például egy adatszivárgás vagy szolgáltatás-kiesés – egyszerre vet fel technikai, adatvédelmi, üzleti, reputációs és akár szuverenitási kérdéseket.

IT-biztonsági szemmel ez a multidiszciplináris jelleg a napi gyakorlatban is meghatározó. Az üzletmenet-folytonosság, az incidenskezelés, a megfelelőség, valamint a reziliencia ma már csak akkor kezelhető hatékonyan, ha a technológiai, jogi és szervezeti szempontok egységes irányítási keretben jelennek meg.

2.3. A kibertér társadalmi és politikai jelentőségének megerősödése

A kibertér társadalmi jelentősége az internet tömeges elterjedésével erősödött meg. A közösségi média, az online platformok és a digitális gazdaság átalakították a kommunikáció, a nyilvánosság és a gazdasági kapcsolatok működését.[7]

Politikai és biztonságpolitikai szinten ez azt eredményezte, hogy a kibertér az állami szuverenitás, a társadalmi stabilitás és a konfliktusok új színterévé vált. A digitális függőség miatt egy kibertámadás vagy információs művelet ma már közvetlen hatással lehet a fizikai működésre és a társadalmi bizalomra is, ami a szervezeti irányítás, a megfelelőség és a kockázatkezelés szintjén is új elvárásokat teremtett.

[5] Manuel Castells: The Rise of the Network Society. Wiley-Blackwell, Oxford, 2010, 407-412. o.
[6] Manuel Castells: The Rise of the Network Society. Wiley-Blackwell, Oxford, 2010, 469-472. o.
[7] Joseph S. Nye Jr.: The Future of Power. PublicAffairs, New York, 2011, 153-158. o.

3. A kibertér társadalmi és gazdasági dimenziói

A kibertér fejlődése nemcsak technológiai, hanem jelentős társadalmi és gazdasági átalakulást is eredményezett. A digitális platformok, az online kommunikáció és az elektronikus kereskedelem ujjászervezték a nyilvánosság, a társadalmi kapcsolatok és a gazdasági működés hagyományos kereteit.

A digitális jelenlét erősödésével párhuzamosan ugyanakkor a működési, adatvédelmi és reputációs kockázatok is hangsúlyosabbá váltak. A fejezet célja annak áttekintése, hogy a kibertér miként alakította át a társadalmi kommunikációt és a gazdasági folyamatokat, valamint milyen új típusú kockázatok jelentek meg ezzel összefüggésben.

3.1. A közösségi média megnövekedett szerepe a digitális nyilvánosságban

Az elmúlt évtizedben a digitális nyilvánosság működését alapvetően a közösségi média platformok, a keresőmotorok és a hírportálok formálták át, miközben a profilozás és a mobilinternet révén biztosított, folyamatos hozzáférés jelentősen átalakította az információk elérésének és értelmezésének módját. A hagyományos, egyirányú médiamodellhez képest ezek a felületek lehetővé tették, hogy a felhasználók egyszerre legyenek tartalomfogyasztók és tartalom-előállítók. Ennek következtében a nyilvánosság szerkezete gyorsabbá, interaktívabbá és kevésbé centralizálttá vált.[8]

A közösségi média jelentősége abban áll, hogy a társadalmi diskurzusok, politikai vélemények és gazdasági trendek egyre nagyobb része ezeken a platformokon keresztül formálódik. A nyilvánosság alakításában ma már nem kizárólag a klasszikus médiaszereplők vesznek részt, hanem platformüzemeltetők, influenszerek, szakmai közösségek és automatizált fiókok is. Ez a változás új lehetőségeket teremtett a gyors információmegosztásra, ugyanakkor felerősítette a félretájékoztatás, a polarizáció és az érzelmi alapú tartalomterjedés kockázatait is, amelyhez jelentősen hozzájárulnak a tartalomajánló algoritmusok és a felhasználói profilozás.[9]

A szervezeti és társadalmi működés szempontjából a közösségi média már nem csupán kommunikációs csatorna, hanem reputációs és bizalmi tényező is. Egyetlen valótlan információ, kiszivárgott adat vagy félreértelmezett tartalom rövid idő alatt széles körű társadalmi vagy üzleti következményeket válthat ki. Emiatt a digitális nyilvánosság vizsgálata ma már szorosan összekapcsolódik az információbiztonság, a reputációvédelem és a válságkommunikáció kérdésével is.

3.2. Az online szólásszabadság és annak korlátai

Az online tér a szólásszabadság egyik legfontosabb gyakorlati fórumává vált. A digitális platformok lehetővé teszik, hogy a felhasználók gyorsan és széles körben osszák meg véleményüket, ami jelentősen erősítette a nyilvánosság demokratikus jellegét, ami ugyanakkor torzításokhoz, előítéletekhez és értékítélet befolyásolásához vezet.[10]

Ugyanakkor az online szólásszabadság sajátossága, hogy a jogi keretek mellett a platformok belső moderációs szabályai és algoritmikus döntései is meghatározzák a tartalmak

[8] Manuel Castells: The Rise of the Network Society. Wiley-Blackwell, Oxford, 2010, 355-362. o.
[9] Shoshana Zuboff: The Age of Surveillance Capitalism. PublicAffairs, New York, 2019, 376-382. o.
[10] Koltay András: Az új média és a szólásszabadság. Wolters Kluwer, Budapest, 2019, 41-48. o.

láthatóságát. Emiatt a véleménynyilvánítás szabadsága és a káros tartalmak korlátozása között folyamatos egyensúlykeresés figyelhető meg.[11]

A kérdés jelentőségét növeli, hogy a digitális nyilvánosság ma már közvetlenül befolyásolja a közvéleményt, a társadalmi bizalmat és a szervezeti reputációt is, így a szólásszabadság korlátai egyszerre vetnek fel jogi, társadalmi és működési kérdéseket.

Ebben az összefüggésben a szólásszabadság alapvető értéke gyakran ütközik a platformok tartalommoderálási lehetőségeivel és kötelezettségeivel, különösen a gyűlöletbeszéd, az álhírek és más káros tartalmak kezelésében. Ez a feszültség azt eredményezi, hogy a platformok egyszerre válnak a véleménynyilvánítás tereivé és annak aktív szabályozóivá.

3.3. A platformok hatása a közvéleményre és a társadalmi viszonyokra

A digitális platformok működése ma már közvetlenül befolyásolja, hogy a felhasználók milyen információkkal találkoznak, és hogyan alakul a közvélemény. Az algoritmusok által vezérelt tartalomajánlás elsődleges célja a felhasználói aktivitás növelése, ami gyakran az érzelmileg erős vagy megosztó tartalmak gyorsabb terjedését eredményezi.[12]

Ennek következtében a platformok nem csupán technikai közvetítőként működnek, hanem aktívan formálják a nyilvánosság szerkezetét is. Egyes kutatások szerint az algoritmikus ajánlórendszerek hozzájárulhatnak a véleménybuborékok kialakulásához és a társadalmi polarizáció erősödéséhez, még akkor is, ha a felhasználók úgy érzékelik, hogy sokféle nézőponttal találkoznak.[13]

A jelenség jelentőségét növeli, hogy a közvélemény alakulása ma már közvetlen hatással van gazdasági és politikai folyamatokra is, így a platformok működése a digitális kockázatok értékelésében is kiemelt szerepet kap.

3.4. A kibertér által megteremtett új gazdasági lehetőségek

A kibertér fejlődése a gazdasági működést is alapvetően átalakította. A digitális technológiák elterjedésével új üzleti modellek jelentek meg, amelyek középpontjában az adatok, a platformok és az online szolgáltatások állnak. A vállalatok ma már földrajzi korlátok nélkül érhetnek el piacokat, miközben a digitális infrastruktúra számtalan területen jelentősen csökkenti a működési költségeket.

A digitális gazdaság egyik legfontosabb sajátossága, hogy az adat önálló gazdasági erőforrássá vált. Az adatgyűjtés, az elemzés és az automatizált döntéshozatal versenyelőnyt biztosíthat a szervezetek számára. Emellett a platformalapú működés új piaci kapcsolatokat hozott létre, amelyben a szereplők közvetlenül kapcsolódhatnak egymáshoz. Ugyanakkor ezek az előnyök új függőségeket is teremtenek. A felhőszolgáltatásokra és digitális platformokra

[11] Koltay András: A közösségi média tartalomszabályozásának egyes kérdései. Wolters Kluwer, Budapest, 2022, 73-79. o.
[12] Germano, Fabrizio - Gómez, Vicenç - Sobbrio, Francesco: Ranking for Engagement: How Social Media Algorithms Fuel Misinformation and Polarization. Barcelona School of Economics, Barcelona, 2025, 5-8. o.
[13] Iftikhar, Ifra - Bajwa, Umair Mahmood: Impact of Social Media Algorithms on Polarization Despite Perceived Diversity. Lahore Garrison University, Lahore, 2025, 12-15. o.

épülő működés koncentrált rendszereket eredményez, így egy szolgáltatás kiesése egyszerre több gazdasági szereplőt is érinthet.[14]

3.5. Az online vásárlás és az elektronikus szerződéskötés szerepe

Az online vásárlás mára a gazdasági működés egyik meghatározó elemévé vált. A digitális platformok és webáruházak elterjedésével a szerződéskötés folyamata jelentősen leegyszerűsödött, hiszen a felek jelenléte nélkül, néhány elektronikus nyilatkozattal létrejöhet a jogviszony. Ez a gyorsaság és kényelmi szempont a digitális gazdaság egyik legfontosabb előnye.

Az elektronikus szerződéskötés jogi kereteit Magyarországon több jogforrás együttesen határozza meg. Az online szolgáltatások speciális szabályait a 2001. évi CVIII. törvény rendezi, míg a szerződés létrejöttének általános polgári jogi alapjait a Polgári Törvénykönyv – azaz a 2013. évi V. törvény – tartalmazza. A fogyasztók védelme szempontjából emellett kiemelt jelentőségű a 45/2014. (II. 26.) Korm. rendelet, amely a távollévők között kötött szerződések részletes szabályait rögzíti.[15][16][17]

A digitális környezet sajátossága, hogy a felhasználó gyakran automatizált folyamatokon keresztül, előre kialakított szerződési feltételek elfogadásával lép jogviszonyba. Emiatt különösen fontossá válik az átlátható tájékoztatás, a fogyasztóvédelmi garanciák és az adatkezelési feltételek egyértelmű megjelenítése. Az online vásárlás és az elektronikus szerződéskötés így egyszerre jelent gazdasági lehetőséget és jogi-kockázati kihívást, amely szorosan kapcsolódik a kibertér biztonságos működéséhez.

3.6. A kibertér gazdasági és társadalmi kockázatai: adatlopás, megtévesztések, online csalások

A kibertér gazdasági és társadalmi előnyei mellett egyre jelentősebbek a kapcsolódó kockázatok is. Az adatlopások, az online megtévesztések és a különböző digitális csalási formák ma már a mindennapi működés részei. A működés közben jelen lévő kockázatok nemcsak az egyéni felhasználókat, hanem a vállalati és állami szektort is érintik.

Gazdasági szempontból az egyik legjelentősebb veszély az üzleti és személyes adatok illetéktelen megszerzése, amely közvetlen pénzügyi veszteséget, reputációs károkat és működési fennakadásokat okozhat. A társadalmi oldalon ezzel párhuzamosan az online megtévesztések – különösen az adathalászat, a hamis weboldalak és a manipulált kommunikáció – a digitális bizalom csökkenéséhez vezetnek. Erre tipikus példa, amikor a felhasználó egy banki vagy futárszolgálati értesítésnek látszó adathalász üzenet alapján hamis weboldalra jut, és ott megadja belépési vagy bankkártyaadatait.

A kockázatok jelentőségét növeli, hogy a digitális térben a technikai és emberi tényezők szorosan összekapcsolódnak. Sok esetben nem a technológiai védelem hiánya, hanem a felhasználói figyelmetlenség, a nem megfelelő tudatosság vagy a túlzott bizalom teszi lehetővé

[14] OECD: OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier. OECD Publishing, Paris, 2024, 25-27. o.

[15] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről. Magyar Közlöny, Budapest, 2001, 5-6. o.

[16] 2013. évi V. törvény a Polgári Törvénykönyvről. Magyar Közlöny, Budapest, 2013, 6:63-6:70. §, 412-415. o.

[17] 45/2014. (II. 26.) Korm. rendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól. Magyar Közlöny, Budapest, 2014, 3-6. o.

a visszaéléseket. Emiatt a kibertér kockázatai nem pusztán informatikai problémaként értelmezhetők, hanem a szervezeti kultúra, a tudatosság és a társadalmi bizalom kérdésköréhez is kapcsolódnak.

Ennek megfelelően, a kibertér által teremtett gazdasági lehetőségek csak akkor használhatók ki fenntartható módon, ha a digitális kockázatok kezelése a működés természetes részévé válik.

4. A kibertér és az állami szuverenitás kérdése

A kibertér fejlődése az állami szuverenitás kérdését is új megvilágításba helyezte. A modern állam működése ma már nem választható el a digitális infrastruktúráktól, az adatáramlástól és a hálózatba kapcsolt szolgáltatásoktól. Ennek következtében a szuverenitás hagyományos, területhez kötött felfogása egyre gyakrabban ütközik azokkal a gyakorlati helyzetekkel, amelyek a kibertér határokon átnyúló jellegéből fakadnak. A kérdés ma már nem csupán az, hogy az állam milyen jogokat gyakorol saját területén, hanem az is, hogy mennyiben képes ellenőrizni azokat a digitális folyamatokat, amelyek a működéséhez, a biztonságához és a társadalmi stabilitáshoz kapcsolódnak.

4.1. A szuverenitás klasszikus fogalma és annak átalakulása

A szuverenitás klasszikus felfogása szerint az állam a saját területén belül gyakorolja a főhatalmat, külső viszonyaiban pedig más államokkal egyenjogú félként jelenik meg. Ez a logika hosszú időn keresztül megfelelő keretet biztosított a politikai és jogi gondolkodásnak, hiszen a hatalomgyakorlás elsődleges tere a fizikai földrajzi tér volt. A kibertér azonban olyan működési közeget hozott létre, ahol a kommunikáció, az adatkezelés és a szolgáltatások jelentős része nem igazodik a klasszikus államhatárokhoz.

Ez a változás azért különösen jelentős, mert a kibertérben zajló műveletek sok esetben egyszerre több országot is érintenek. Egy másik államban működő szolgáltató infrastruktúrája közvetlenül hatással lehet a hazai gazdasági vagy társadalmi működésre, miközben a jogérvényesítés eszközei korlátozottak. A kibertámadásoknál ugyanez még hangsúlyosabban jelenik meg: a műveletek tipikusan több ország hálózatain keresztül zajlanak, ami megnehezíti a felelősség megállapítását – attribúciós probléma – és a válaszlépések megalapozását. A szuverenitás tehát nem szűnik meg, hanem olyan közegbe kerül át, ahol a hagyományos állami kontroll önmagában már nem elegendő.

4.2. A digitális szuverenitás fogalma

A digitális szuverenitás fogalma részben erre a kihívásra adott válaszként jelent meg. Lényege, hogy az állam mennyiben képes érdemi befolyást gyakorolni saját digitális infrastruktúrájára, adataira, kritikus rendszereire és a működéséhez szükséges technológiai környezetre. A fogalom nem feltétlenül jelent teljes technológiai önállóságot, inkább arra utal, hogy az állam ne legyen kiszolgáltatott olyan külső szereplőknek, amelyek válsághelyzetben jelentős működési kockázatot idézhetnek elő.[18]

A digitális szuverenitás kérdése a gyakorlatban elsősorban a technológiai függőségeknél válik láthatóvá. Ide tartozik például az, hogy a kritikus szolgáltatások milyen felhőszolgáltatókra épülnek, hol tárolják az adatokat, milyen beszállítói láncon keresztül működnek, illetve mennyire pótolhatók egy esetleges kiesés esetén. A függőség önmagában nem feltétlenül jelent problémát, de ha egy állam alapvető rendszerei külső technológiai szereplőkre épülnek, akkor a működési kitettség egyben szuverenitási kérdéssé is válik. Ez a függőség részben összefügg a 3.4. alfejezetben bemutatott platformalapú és szolgáltatásközpontú digitális működéssel is. A digitális szuverenitás ezért nem csupán politikai

[18] European Commission: 2030 Digital Compass: the European way for the Digital Decade. European Commission, Brussels, 2021, 2-4. o.

vagy elméleti fogalom, hanem egyre inkább kockázatkezelési, irányítási és biztonsági kérdés is.[19]

4.3. Az állami és nem állami szereplők hatalmi viszonyai a kibertérben

A kibertér egyik sajátossága, hogy az állam mellett nem állami szereplők is jelentős befolyással rendelkeznek. A nagy technológiai vállalatok, platformszolgáltatók, felhőpiaci szereplők és kommunikációs szolgáltatók olyan infrastruktúrák és információs csatornák felett gyakorolnak ellenőrzést, amelyek közvetlenül befolyásolják a nyilvánosság működését, a gazdasági folyamatokat és bizonyos esetekben még a biztonságpolitikai környezetet is. Ez a hatalmi szerkezet eltér a klasszikus állami logikától, mert a befolyás nem kizárólag jogi vagy katonai eszközökkel, hanem technológiai és gazdasági függőségeken keresztül is érvényesül a kritikus infrastruktúrák tekintetében. Ilyen az energiaellátás, a távközlési és internetes hálózatok, a pénzügyi és bankrendszer, a közlekedési infrastruktúra, az egészségügyi ellátórendszer, valamint a vízellátás és egyéb közműszolgáltatások.

A platformok szerepe ebből a szempontból különösen jelentős. Nem csupán technikai közvetítők, hanem a nyilvánosság szerkezetét alakító szereplők is, amelyek algoritmikus döntéseken, moderációs szabályokon és hozzáférési feltételeken keresztül befolyásolják az információ áramlását. Ugyanez igaz a felhőszolgáltatásokra és a digitális infrastruktúra más elemeire is: aki ezek felett ellenőrzést gyakorol, az közvetve jelentős hatással lehet az állami és gazdasági működésre.

A kibertérben így a szuverenitás kérdése összekapcsolódik azzal, hogy az állam mennyiben képes önállóan alakítani saját digitális környezetét, és mennyire válik külső szereplők technológiai döntéseinek kiszolgáltatottjává.

4.4. A nemzetközi együttműködés szükségessége a kibertérben

A kibertér határokon átnyúló jellege miatt a szuverenitás védelme már nem kezelhető kizárólag nemzeti keretek között. A kibertámadások, a platformalapú befolyásolás, az ellátási láncok sérülékenységei és a globális technológiai függőségek olyan kockázatokat jelentenek, amelyekre az államok csak együttműködés útján képesek érdemi választ adni. Ez különösen igaz a hírszerzési, incidenskezelési és kritikus infrastruktúra-védelmi kérdésekre, ahol az információmegosztás és a közös minimumkövetelmények nélkül a védekezés lényegesen gyengébb lenne.

A NATO és az Európai Unió szerepe ebből a szempontból meghatározó, például az EU NIS2 irányelve, valamint a nemzeti CERT/CSIRT rendszerek.[20] A kibervédelem ma már nem csupán technikai kérdés, hanem a kollektív biztonság része is. A közös gyakorlatok, a reziliencia-követelmények, az együttműködési mechanizmusok és a stratégiai koordináció mind azt mutatják, hogy a kibertérben a szuverenitás védelme csak részben értelmezhető önálló nemzeti feladatként. Ugyanakkor ez nem csökkenti a tagállami felelősséget: minden állam saját maga felel a saját rendszereinek alapvető biztonsági szintjéért, kockázatkezeléséért és működési ellenálló képességéért.

[19] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, Brussels, 2022, 80–82. o.
[20] NATO: Cyber defence. NATO, Brussels, 2024, online témalap, letöltés dátuma: 2026. 03. 25.

Fentiek alapján megállapítható, hogy a kibertér újra keretezi az állami szuverenitás fogalmát. A klasszikus területi logika továbbra is fontos marad, de önmagában már nem ad elegendő választ a digitális működésből fakadó kihívásokra. A szuverenitás a kibertérben ma már adatot, infrastruktúrát, technológiai függőséget, információs befolyást és nemzetközi együttműködést is jelent. Ez a változás közvetlenül vezet át a következő fejezethez, ahol a kibertér konfliktustérré válása kerül előtérbe.

5. A kibertér mint konfliktustér és új hadszíntér

A kibertér fejlődésével párhuzamosan a digitális környezet már nem csupán a kommunikáció, a gazdasági működés és az állami szolgáltatások tere lett, hanem a modern konfliktusok egyik meghatározó színterévé is vált. A kibertér sajátossága, hogy benne a versengés, a zavarás, a befolyásolás és a védekezés gyakran a fizikai hadszínterektől részben függetlenedik vagy integrálódok – több műveleti térben zajló hadművelet –, mégis azokkal szoros összefüggésben jelenik meg. A modern államok, gazdasági szereplők és nem állami csoportok számára a digitális infrastruktúrák, az információs rendszerek és a társadalmi kommunikáció befolyásolása ma már stratégiai jelentőségű eszközzé vált. A NATO a kibervédelmet a kollektív védelem részének tekinti, és a kibertér 2016 óta hivatalosan is műveleti doménnek számít a szövetségben.[21]

5.1. A kibertér konfliktustérré válása

A kibertér konfliktustérré válása azzal magyarázható, hogy a társadalmi, gazdasági és állami működés egyre nagyobb mértékben függ a digitális rendszerektől. Minél erősebb ez a függés, annál nagyobb stratégiai jelentősége van annak, hogy ki képes hozzáférni az információkhoz, zavarni a szolgáltatásokat, befolyásolni a kommunikációt vagy gyengíteni a bizalmat. A konfliktusok ezért a kibertérben gyakran nem nyílt háborús cselekményként jelennek meg, hanem alacsony intenzitású, folyamatos műveletek formájában, amelyek célja a működés gyengítése, az információs előny megszerzése vagy az ellenfél döntési képességének befolyásolása.[22]

A kibertér konfliktusjellegének egyik sajátossága, hogy a műveletek sok esetben a béke és a fegyveres konfliktus közötti szürke zónában zajlanak. Ilyen lehet például az adatszerzés, a szolgáltatásmegtagadás, a dezinformáció, a kritikus infrastruktúrák feltérképezése vagy a társadalmi megosztottság erősítése. Ezek a tevékenységek önmagukban nem mindig érik el a klasszikus fegyveres támadás szintjét – amit a támadás hatása, intenzitása és a kritikus infrastruktúrákra gyakorolt következményei együttesen határoznak meg –, mégis hosszú távon jelentős biztonságpolitikai következményekkel járhatnak. A kibertérben ezért a konfliktusok nem kizárólag technikai támadásként értelmezhetők, hanem információs, társadalmi és működési kockázatként is.[23]

Informatikai és kiberbiztonsági szempontból ez azért különösen fontos, mert a konfliktustér logikája nemcsak az állami rendszereket, hanem a vállalati és szolgáltatói infrastruktúrát is érinti. A támadási felület ma már nem szűkíthető le katonai célpontokra: a felhőszolgáltatások, az energetikai rendszerek, a pénzügyi infrastruktúrák, az egészségügyi szolgáltatások vagy akár a médiaplatformok is potenciális célponttá válhatnak. A kibertér konfliktustérré válása tehát nem egy jövőbeli lehetőség, hanem a jelenlegi működési környezet egyik alapvető jellemzője.

[21] NATO: Cyber defence. NATO, Brussels, 2024, online témalap, letöltés dátuma: 2026. 03. 25.
[22] NATO: Washington Summit Declaration. NATO, Washington, 2024, 31–33. pont, letöltés dátuma: 2026. 03. 25.
[23] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, Brussels, 2022, 80-82. o.

5.2. A kibertámadások fogalma, jellemzői és típusai

A kibertámadás fogalma alatt általában olyan szándékos digitális műveletet értünk, amely információs rendszerek, hálózatok, adatok vagy szolgáltatások ellen irányul abból a célból, hogy azok működését megzavarja, megbénítsa, manipulálja vagy jogosulatlanul hozzáférjen az ott tárolt információkhoz. A hackertámadás a kibertámadások egyik, elsősorban jogosulatlan technikai behatoláshoz kapcsolódó formája, ezért a két fogalom nem teljesen azonos. A kibertámadások sajátossága, hogy gyakran aszimmetrikus eszközként működnek: viszonylag alacsony erőforrással is jelentős működési és biztonsági kár okozható, különösen akkor, ha a célpont erősen digitalizált és összekapcsolt rendszerekre épül.

A kibertámadások egyik legfontosabb jellemzője a gyorsaság, a nehéz felismerhetőség és a több szinten jelentkező hatás. Egy támadás egyszerre érintheti az adatok bizalmasságát, a rendszerek sértetlenségét és a szolgáltatások rendelkezésre állását, azaz a CIA elv. három alappillérét. Informatikai szempontból ezért a kibertámadások nem csupán technikai incidensek, hanem üzletmenet-folytonossági, reputációs és adott esetben nemzetbiztonsági kockázatot is jelenthetnek.

A gyakorlatban több alapvető típust lehet elkülöníteni. Ide tartoznak az adatszerzésre irányuló műveletek, például a jogosulatlan behatolás vagy az adathalászat; a szolgáltatásromboló támadások, mint a DDoS; a zsarolóvírusos műveletek, amelyek titkosítással és váltságdíj-követeléssel bénítják meg a működést; valamint a szabotázs jellegű támadások, amelyek célja egy adott rendszer vagy infrastruktúra tartós károsítása. A modern kibertámadások jelentős része már nem egyetlen technikára épül, hanem több módszert kapcsol össze, például social engineeringet, jogosultságkiterjesztést és adatexfiltrációt.

A konfliktustér logikájában különösen fontos, hogy a kibertámadások nem mindig látványosak. Sok esetben a cél nem az azonnali rombolás, hanem a csendes hozzáférés megszerzése, a későbbi műveletek előkészítése vagy az ellenfél folyamatos gyengítése. Emiatt a kibertámadások értelmezése ma már nem szűkíthető le a technikai események szintjére, hanem a stratégiai szándékot, a célpont működési függőségeit és a várható társadalmi hatásokat is figyelembe kell venni. Ezt a gyakorlatban is tapasztaltam, mivel korábbi munkahelyemet, a Unix Autó Kft.-t 2021-ben kibertámadás érte, és az eset jól mutatta, hogy a támadók már hónapok óta jelen voltak a rendszerben. Egy ilyen incidens nem pusztán informatikai probléma, hanem a működés, a szervezeti koordináció és az üzletmenet szintjén is azonnali következményeket okozhat. A cégvezető beszámolója az esetről itt olvasható: https://www.unixauto.hu/hirlevel/hackertamadas

5.3. A kibervédelem és a reziliencia jelentősége

A kibertér konfliktusjellegéből következik, hogy a védekezés ma már nem merülhet ki kizárólag technikai védelmi megoldások alkalmazásában. A kibervédelem lényege nem csupán a támadások megakadályozása, hanem annak biztosítása is, hogy egy szervezet vagy állami szereplő támadás esetén is képes legyen a működés fenntartására, a károk korlátozására és a helyreállításra. Emiatt a modern kiberbiztonsági szemléletben a reziliencia legalább olyan fontos, mint a megelőzés, valamint a támadások felismerése, illetve a bekövetkezett támadások esetén a kárenyhítés, kárhelyreállítás.

A reziliencia ebben az összefüggésben azt jelenti, hogy a rendszerek nemcsak védettek, hanem ellenállók és helyreállíthatók is. Ez magában foglalja a kockázatok előzetes azonosítását, a megelőző intézkedéseket, az incidenskezelési képességet, a biztonsági mentéseket, a kommunikációs protokollokat és az üzletmenet-folytonosság fenntartását. Konfliktustéri

környezetben különösen fontos, hogy a védelmi szemlélet ne kizárólag az informatikai rendszerekre korlátozódjon, hanem kiterjedjen a szervezeti működésre, a döntéshozatalra és a külső partnerekkel való koordinációra is.

Ezt az irányt az uniós szabályozás is egyértelműen megerősíti. A NIS2 irányelv a magas közös kiberbiztonsági szint elérését célozza, és olyan kockázatkezelési, incidensbejelentési és szervezeti követelményeket ír elő, amelyek a rezilienciát már nem opcionális, hanem kötelező működési elemmé teszik.[24] A kibervédelem így nem pusztán informatikai feladat, hanem irányítási, megfelelőségi és biztonságpolitikai kérdés is.

A konfliktustér szempontjából a kibervédelem jelentősége abban áll, hogy a támadásokkal szembeni teljes sérthetetlenség reálisan nem biztosítható. A reziliencia, a gyors észlelés, a hatékony reagálási képesség és a működés folytonosságának biztosítása viszont garantálható. A valódi különbséget sok esetben nem az jelenti, hogy történik-e incidens, hanem az, hogy a célpont milyen gyorsan képes azt felismerni, elszigetelni, kezelni és a működést helyreállítani. Emiatt a reziliencia a modern kibervédelem egyik központi eleme. Ezt jól mutatta a 2024 nyarán bekövetkezett globális IT-incidens is, amikor egy hibás CrowdStrike-frissítés (egy széles körben használt kiberbiztonsági szoftver) a Microsoft Windows rendszereken világszerte működési zavarokat okozott, és többek között repülőterek, légitársaságok és más kritikus szolgáltatások működését is érintette.[25]

5.4. Az attribúció problémája a kibertérben

A kibertámadások egyik legnehezebben kezelhető sajátossága az attribúció problémája, vagyis annak megállapítása, hogy egy adott művelet mögött pontosan ki áll. A digitális környezetben a támadók gyakran több ország infrastruktúráját, köztes szervereket, anonim hálózatokat vagy kompromittált rendszereket használnak fel, így a technikai nyomok önmagukban sokszor nem elegendők a felelős egyértelmű azonosításához. Ez a folyamat jellemzően OSINT-alapú és attribúciós elemzési módszereket igényel, mivel a támadók infrastruktúrájának összekapcsolása és a felelős azonosítása túlmutat a tisztán technikai (pl. malware-analitikai) vizsgálaton. Emiatt a kibertérben a támadó kilétének megállapítása jóval bonyolultabb, mint a hagyományos fizikai konfliktusok esetében.

Az attribúció nehézsége nemcsak technikai, hanem jogi és politikai kérdés is. Egy állam számára komoly következményekkel járhat, ha egy másik államot vagy szervezetet hivatalosan megnevez egy kibertámadás mögött álló szereplőként. Ha az azonosítás nem kellően megalapozott, a válaszlépések legitimitása is megkérdőjelezhetővé válhat. A kibertérben ezért az attribúció gyakran nem abszolút bizonyosságot, hanem eltérő szintű valószínűséget jelent.[26]

Informatikai szempontból az attribúció azért is nehéz, mert a támadók sok esetben tudatosan törekednek a megtévesztésre – vö. flag false operation. Hamis nyomokat hagyhatnak, más csoportokra jellemző eszközöket használhatnak, vagy olyan technikai megoldásokat alkalmazhatnak, amelyek félrevezethetik az elemzőket. A technikai vizsgálat ezért önmagában

[24] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, Brussels, 2022, 80-82. o.
[25] ENISA (2024): *Cyber resilience and large-scale IT outages – lessons learned from global incidents*, p. 12-15. o.
[26] NATO CCDCOE: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017, 81-85. o.

általában nem elegendő; szükség van hírszerzési, kontextuális és működési információk együttes értékelésére is.

A konfliktustér logikájában az attribúció problémája azért bír különös jelentőséggel, mert közvetlenül befolyásolja az elrettentést, a válaszadás lehetőségét és a politikai kommunikációt is. Ha a támadó kiléte bizonytalan, akkor a védekező fél mozgástere is szűkül, ami kedvez a szürke zónás műveleteknek és az alacsony intenzitású, folyamatos nyomásgyakorlásnak. Emiatt az attribúció a kibertérben nem mellékes technikai részlet, hanem a konfliktuskezelés egyik kulcskérdése.

5.5. OSINT és információszerzés a digitális térben

A kibertér konfliktusjellegének egyik fontos eleme az információszerzés, amelyben a nyílt forrású hírszerzés, vagyis az OSINT egyre nagyobb szerepet kap. Az OSINT lényege, hogy nyilvánosan- és a legálisian elérhető információk – például közösségi média tartalmak, sajtóanyagok, nyilvános adatbázisok, fórumok, domain-adatok vagy technikai metaadatok – elemzésével következtetéseket lehet levonni egy adott szereplő, esemény vagy rendszer működéséről. Konfliktustéri környezetben ez különösen értékes, mert sok esetben már a nyílt információk rendszerezése is jelentős műveleti vagy stratégiai előnyt biztosíthat.

Az OSINT jelentősége abból fakad, hogy a digitális térben rendkívül nagy mennyiségű adat keletkezik, és ezek között sok olyan információ található, amely külön-külön jelentéktelennek tűnhet, összekapcsolva azonban érzékeny következtetésekre adhat alapot. Egy szervezet technológiai környezete, partnerei, földrajzi jelenléte, sőt akár egyes biztonsági gyengeségei is részben feltárhatók lehetnek nyilvános forrásokból. Emiatt az OSINT a kibervédelem oldalán is fontos, hiszen segítheti a fenyegetések felismerését, a kockázatok értékelését és az incidensek elemzését.

Ugyanakkor az OSINT nem pusztán védekezési eszköz. A támadó oldalon is felhasználható célpontkiválasztásra, social engineering műveletek előkészítésére, a szervezeti struktúra feltérképezésére vagy a technikai környezet elemzésére. Ez különösen jól mutatja, hogy a kibertérben az információ önmagában is műveleti jelentőségű erőforrás. Az OSINT ezért tipikus kettős felhasználású terület: ugyanaz az ismeret szolgálhatja a védelmet és a támadást is.

A konfliktustér logikájában az OSINT azért bír kiemelt jelentőséggel, mert összeköti a technikai és az információs dimenziót. Segítségével a nyílt digitális jelenlétből olyan mintázatok rajzolhatók ki, amelyek közvetlenül befolyásolhatják a kockázatkezelést, a kibervédelmet és adott esetben a műveleti döntéshozatalt is.

5.6. Információs műveletek, dezinformáció és befolyásolás

A kibertér konfliktustérré válásának egyik legfontosabb sajátossága, hogy a támadások nem kizárólag rendszerek és infrastruktúrák ellen irányulhatnak, hanem a társadalmi érzékelés, a közvélemény és a bizalom befolyásolására is. Az információs műveletek célja sok esetben nem az azonnali technikai rombolás, hanem az, hogy az ellenfél döntéseit, társadalmi stabilitását vagy politikai mozgásterét közvetett módon gyengítsék. Ebben a környezetben a dezinformáció, a manipulált tartalom és a célzott kommunikáció a konfliktus egyik sajátos eszközévé vált.

A félrevezető információ (misinformation) olyan valótlan vagy pontatlan tartalom, amelyet nem szándékosan terjesztenek, a dezinformáció (disinformation) ezzel szemben

tudatosan előállított és terjesztett hamis információ, míg a fake news olyan, gyakran szenzációhajhász formában megjelenő ál-hírek összefoglaló elnevezése, amelyek célja a közvélemény befolyásolása vagy megtévesztése. A digitális platformok működése, az algoritmikus ajánlórendszerek és a gyors tartalomterjedés különösen kedveznek annak, hogy az érzelmileg erős, megosztó vagy bizonytalanságot keltő üzenetek rövid idő alatt széles körhöz jussanak el. Emiatt az információs műveletek ma már nem pusztán kommunikációs jelenségek, hanem a konfliktustér működésének részei.

A befolyásolás szempontjából különösen fontos, hogy a célpont nem mindig maga az állam vagy annak infrastruktúrája, hanem a társadalom, a választói magatartás, a közintézményekbe vetett bizalom vagy éppen egy szervezet reputációja. Egy jól felépített információs művelet képes lehet a bizonytalanság növelésére, a megosztottság fokozására vagy arra, hogy a valós eseményekről kialakult képet torzítsa. Ez a hatás önmagában is stratégiai jelentőségű lehet, még akkor is, ha nem társul hozzá közvetlen technikai támadás.

A kibertérben az információs műveletek jelentősége ezért abban áll, hogy a konfliktusokat részben áthelyezik a technikai térből a társadalmi érzékelés szintjére. A modern konfliktusokban így a digitális információs környezet védelme legalább annyira fontossá vált, mint maguknak a rendszereknek a technikai védelme.

5.7. A hibrid hadviselés kibertéri dimenziói

A hibrid hadviselés lényege, hogy a szereplők nem egyetlen eszközzel próbálnak előnyt szerezni, hanem a politikai, gazdasági, információs, technológiai és adott esetben katonai nyomásgyakorlást összehangoltan alkalmazzák. A kibertér ebben a működésben különösen fontos, mert olyan rugalmas műveleti teret biztosít, ahol a támadó fél viszonylag alacsony láthatóság mellett tud zavart kelteni, információt szerezni vagy befolyást gyakorolni.

A kibertéri dimenzió a hibrid hadviselésben több formában jelenhet meg. Ide tartozhatnak a kritikus infrastruktúrák elleni támadások, a kommunikációs rendszerek zavarása, az információs műveletek, a dezinformáció, valamint a társadalmi bizonytalanság erősítésére alkalmas digitális kampányok is. Ezek a műveletek önmagukban nem feltétlenül idéznek elő nyílt fegyveres konfliktust, de alkalmasak arra, hogy fokozatosan gyengítsék az ellenfél működését, döntési képességét és társadalmi kohézióját.

A hibrid logika egyik sajátossága, hogy a különböző műveleti elemek egymást erősítik. Egy kibertámadás például összekapcsolódhat dezinformációs kampánnyal, diplomáciai nyomásgyakorlással vagy gazdasági zavarkeltéssel. Emiatt a védekezés sem szűkíthető le technikai szintre. A kibertérben jelentkező hibrid fenyegetések kezeléséhez a technológiai védelem mellett szükség van szervezeti felkészültségre, társadalmi tudatosságra, jogi keretekre és nemzetközi együttműködésre is.

A kibertéri dimenzió tehát azért vált a hibrid hadviselés központi elemévé, mert egyszerre teszi lehetővé a rejtett beavatkozást, a folyamatos nyomásgyakorlást és a széles körű társadalmi hatás kiváltását. Ez jól mutatja, hogy a modern konfliktusokban a digitális tér már nem kiegészítő terület, hanem az összetett versengés egyik alapvető közege.

5.8. A kibertér mint új hadszíntér a NATO és az EU megközelítésében

A kibertér stratégiai jelentőségét jól mutatja, hogy a NATO és az Európai Unió ma már nem pusztán technológiai környezetként, hanem biztonságpolitikai és műveleti szempontból is önálló jelentőségű térként kezeli. A NATO 2016-ban ismerte el a kiberteret műveleti

doménként, vagyis olyan területként, ahol a szövetségnek a szárazföldi, légi és tengeri műveletekhez hasonlóan képesnek kell lennie a működésre és a védekezésre.[27] Ez a megközelítés jól mutatja, hogy a kibertér ma már nem kiegészítő elem, hanem a kollektív védelem egyik lényeges összetevője.

A NATO nézőpontjában a kibervédelem a szövetség alapvető elrettentési és védelmi feladataihoz kapcsolódik. A hangsúly a saját hálózatok védelmén, a tagállami reziliencia erősítésén, a közös helyzetértékelésen és a koordinált válaszadási képességen van. A kiberteret műveleti doménként kezelő logika azért fontos, mert a modern konfliktusokban a hagyományos hadszínterek és a digitális műveleti környezet egyre szorosabban kapcsolódnak össze.[28]

Az Európai Unió megközelítése részben eltér ettől, mivel nagyobb hangsúlyt helyez a rezilienciára, a szabályozási háttérre és a tagállamok közötti koordinációra. Ugyanakkor az EU is egyre erőteljesebben kezeli a kiberteret stratégiai jelentőségű működési térként. Az uniós cyber defence politika célja a védekezési képességek, az együttműködés és az ellenálló képesség erősítése, különös tekintettel a kritikus infrastruktúrákra és a védelmi rendszerekre.[29]

A két megközelítés közös pontja, hogy a kibertérben a védelem már nem pusztán informatikai kérdésként jelenik meg, hanem a biztonságpolitika, a stratégiai tervezés és a válságkezelés részévé vált. A kibertér hadszíntér-jellegét ezért nem kizárólag az adja, hogy digitális támadások történnek benne, hanem az is, hogy a működési, társadalmi és politikai következmények miatt a modern konfliktusok egyik meghatározó műveleti környezetévé vált.

5.9. A mesterséges intelligencia és az automatizált megtévesztés szerepe a modern konfliktusokban

A mesterséges intelligencia (vö.: MI) a modern konfliktusokban egyszerre jelent új védelmi lehetőséget és új fenyegetést. Segítheti az anomáliák felismerését és az incidenskezelést, ugyanakkor alkalmas lehet megtévesztő tartalmak előállítására, célzott adathalász kampányok támogatására és a felhasználói viselkedés befolyásolására is.[30]

A konfliktustérben különösen nagy jelentősége van az automatizált megtévesztésnek. A deepfake videók, mesterségesen generált hangfelvételek – ez is deepfake – és hitelesnek tűnő hamis szövegek – LLM generált tartalmak – nemcsak technikai, hanem társadalmi kockázatot is jelentenek, mert a bizalom gyengítésére és a közvélemény befolyásolására is alkalmasak.

A szabályozás oldaláról ezt a problémát az Európai Unió is felismerte. Az AI Act a mesterséges intelligenciával létrehozott vagy manipulált tartalmak esetében bizonyos átláthatósági kötelezettségeket ír elő, ami különösen fontos a deepfake és más megtévesztő tartalmak kezelésében. Ez ugyan önmagában nem szünteti meg az automatizált megtévesztés kockázatát, de jól mutatja, hogy az MI-hez kapcsolódó fenyegetések már nemcsak technológiai, hanem jogi és biztonságpolitikai kérdésként is megjelennek. [31]

[27] NATO: Cyber defence. NATO, Brussels, 2024, online témalap, letöltés dátuma: 2026. 03. 25.
[28] NATO: Washington Summit Declaration. NATO, Washington, 2024, 31-33. pont, letöltés dátuma: 2026. 03. 25.
[29] Council of the European Union: Cyber defence. Council of the European Union, Brussels, 2025, online tájékoztató, letöltés dátuma: 2026. 03. 25.
[30] ENISA: Threat Landscape 2024. European Union Agency for Cybersecurity, Athens, 2024, 13-18. o.
[31] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union, Brussels, 2024, letöltés dátuma: 2026. 03. 25.

A mesterséges intelligencia konfliktustéri jelentősége ezért abban áll, hogy a technikai és információs műveletek közötti határt tovább csökkenti. Az automatizált megtévesztés eszközei lehetővé teszik, hogy a befolyásolás gyorsabban, szélesebb körben és kisebb költséggel történjen meg, mint korábban. Emiatt a mesterséges intelligencia a modern kibertérben nem pusztán innovációs tényező, hanem a konfliktusok természetét is alakító eszköz.

6. A kibertér jogi szabályozásának főbb területei

A kibertérhez kapcsolódó jogi szabályozás sajátossága, hogy egyetlen jogág vagy egyetlen jogszabály keretében nem kezelhető. A digitális környezet egyszerre vet fel adatvédelmi, elektronikus kereskedelmi, platformszabályozási, büntetőjogi és kiberbiztonsági kérdéseket, ezért a szabályozás szükségszerűen több szinten és több jogterület határán alakul ki. A kibertér jogi megközelítése ezért nem csupán normák felsorolását jelenti, hanem annak vizsgálatát is, hogy a különböző jogi eszközök milyen módon próbálnak reagálni a technológiai fejlődésre, a digitális függőségre és az új típusú kockázatokra.

6.1. A kibertér szabályozásának sajátosságai

A kibertér szabályozásának egyik legfontosabb sajátossága, hogy a digitális működés természetéből adódóan határokon átnyúló, gyorsan változó és erősen technológiafüggő. Míg a klasszikus jogi szabályozás sok esetben területhez, állami joghatósághoz és viszonylag stabil intézményi keretekhez kapcsolódik, addig a kibertérben a szolgáltatások, adatáramlások és platformok működése gyakran több országot és többféle szereplőt érint egyszerre. Emiatt a szabályozásban különösen nagy szerepe van az uniós szintű harmonizációnak és a közös minimumkövetelmények kialakításának. A NIS2 irányelv és a Digitális Szolgáltatásokról szóló rendelet is jól mutatja, hogy az Európai Unió egyre inkább egységes szabályozási keretben kíván reagálni a kiberbiztonsági és platformszintű kihívásokra.[32]

A szabályozás másik sajátossága, hogy a kibertérben a technikai, szervezeti és jogi dimenziók szorosan összefonódnak. Egy adatszivárgás, szolgáltatás-kiesés vagy platformon terjedő jogsértő tartalom egyszerre vethet fel adatvédelmi, fogyasztóvédelmi, megfelelőségi és biztonsági kérdéseket. Ezért a kibertérben a jogi szabályozás nem lehet kizárólag reaktív, hanem egyre inkább megelőző és kockázatalapú megközelítésre épül.

Magyar szempontból a szabályozási környezetet részben a hazai törvények, részben az Európai Unió közvetlenül alkalmazandó rendeletei és átültetendő irányelvei alakítják. Ennek következtében a kibertérhez kapcsolódó jogi keretek egyszerre épülnek nemzeti és uniós szintű normákra, ami különösen igaz az adatvédelem, az elektronikus kereskedelem és a kiberbiztonság területén.[33][34]

6.2. A személyes adatok védelme és az adatbiztonság

A kibertér jogi szabályozásának egyik központi területe a személyes adatok védelme, mivel a digitális működés során a szervezetek és szolgáltatók egyre nagyobb mennyiségű adatot kezelnek. A személyes adatok védelme ma már nem pusztán magánszféra-védelmi kérdés, hanem szorosan kapcsolódik a bizalomhoz, a működési biztonsághoz és a szervezeti felelősséghez is. A 3.6. alfejezet már rámutatott arra, hogy az adatlopás és a digitális visszaélések a kibertér egyik legjelentősebb kockázati területét jelentik.

[32] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, Brussels, 2022, 80-82. o.
[33] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Nemzeti Jogszabálytár, Budapest, letöltés dátuma: 2026. 03. 26.
[34] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Nemzeti Jogszabálytár, Budapest, letöltés dátuma: 2026. 03. 26.

Az uniós szabályozás központi eleme a GDPR, amely a személyes adatok kezelésére vonatkozó alapelveket, az adatkezelői felelősséget, valamint a megfelelő technikai és szervezési intézkedések követelményét is meghatározza. A rendelet alapján az adatkezelőnek olyan védelmi szintet kell biztosítania, amely figyelembe veszi a kockázatokat, az alkalmazott technológia állását és a kezelt adatok jellegét.[35] A személyes adatok védelme így nem választható el az adatbiztonságtól: a jogi megfelelés és a technikai védelem egymásra épül.

Magyarországon az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény egészíti ki a hazai adatvédelmi keretet. A törvény rögzíti az adatkezelés alapelveit, különösen a célhoz kötöttséget, a tisztességes és törvényes adatkezelés követelményét, valamint az érintetti jogok jelentőségét. Ez azért bír különös jelentőséggel, mert a kibertérben a személyes adatok védelme már nem csupán jogi formalitás, hanem a szervezeti működés egyik alapvető megfelelőségi kérdése.

A személyes adatok védelmének gyakorlati súlyát növeli, hogy adatvédelmi incidens esetén nem elegendő kizárólag technikai oldalról kezelni a problémát. A GDPR az adatvédelmi incidensek bejelentésére és kezelésére is kötelezettségeket állapít meg, ami összhangban áll az 5.3. alfejezetben bemutatott reziliencia-szemlélettel is. A kibertérben ezért az adatbiztonság nem szűkíthető le informatikai védelemre: egyaránt magában foglalja a kockázatkezelést, a jogosultságkezelést, az incidenskezelést és a szervezeti felelősségvállalást is.

Mindez arra utal, hogy a személyes adatok védelme a kibertérben egyszerre alapjogi, megfelelőségi és működésbiztonsági kérdés. A GDPR és a hazai adatvédelmi szabályozás közös logikája alapján az adatkezelés jogszerűsége és az adatbiztonság megfelelő szintje nem választható el egymástól.

6.3. Az online platformok és közösségi média jogi kérdései

Az online platformok és a közösségi média jogi megítélése a kibertér szabályozásának egyik legösszetettebb területe. A 3.1. alfejezet már bemutatta, hogy a közösségi média alapvetően átalakította a digitális nyilvánosságot, míg a 3.3. alfejezet arra mutatott rá, hogy a platformok algoritmikus működése közvetlenül hat a közvéleményre és a társadalmi viszonyokra. Ebből következik, hogy működésük nem kezelhető pusztán technikai vagy piaci kérdésként, hanem jogi és felelősségi oldalról is vizsgálni kell.

E területen kiemelt jelentőségű az Európai Unió Digitális Szolgáltatásokról szóló rendelete (DSA), amely az online közvetítő szolgáltatók és platformok felelősségi, átláthatósági és kockázatkezelési kötelezettségeit határozza meg.[36] A rendelet külön hangsúlyt helyez az illegális tartalmakkal szembeni fellépésre, valamint arra, hogy a platformok átlátható eljárásokat biztosítsanak a felhasználók számára.

A kérdés szorosan kapcsolódik a 3.2. alfejezetben bemutatott online szólásszabadsághoz, hiszen a platformok moderációs gyakorlata ténylegesen befolyásolja a véleménynyilvánítás határait. Emellett az 5.6. alfejezet is rámutatott arra, hogy a digitális platformok az információs műveletek és a dezinformáció egyik legfontosabb közegei. Emiatt a

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Official Journal of the European Union, Brussels, 2016, 49. és 83. cikk, letöltés dátuma: 2026. 03. 27.

[36] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services. Official Journal of the European Union, Brussels, 2022, letöltés dátuma: 2026. 03. 27.

platformok szabályozása ma már nemcsak piaci vagy fogyasztóvédelmi, hanem társadalmi és biztonságpolitikai jelentőségű kérdés is.

A platformok szabályozó szerepe abban áll, hogy saját tartalommoderációs és közösségi irányelveiken keresztül meghatározzák a közzétehető tartalmak kereteit, és ezzel közvetetten a véleménynyilvánítás határait is befolyásolják, miközben tevékenységükre egyre erősebben hatnak az olyan külső szabályozások, mint az EU digitális szolgáltatásokról szóló rendelete (DSA).

6.4. Az online szólásszabadság és a jogi korlátok

Az online szólásszabadság a digitális nyilvánosság egyik alapvető kérdése, ugyanakkor a kibertérben ez a szabadság nem korlátlan. Jogi szempontból a kiindulópontot a magyar Alaptörvény IX. cikke és az Emberi Jogok Európai Egyezményének 10. cikke adja, amelyek a véleménynyilvánítás szabadságát alapjogként ismerik el, de lehetőséget adnak annak törvényben meghatározott korlátozására is.[37][38]

A digitális térben ez azért különösen érzékeny kérdés, mert a jogsértő vagy káros tartalmak gyorsan és széles körben terjedhetnek. Ilyen lehet például a gyűlöletkeltő tartalom, a személyiségi jogokat sértő közlés vagy a félrevezető információ. A szabályozás ezért egyensúlyt keres a véleménynyilvánítás szabadsága és más jogok, illetve társadalmi érdekek védelme között. Az online szólásszabadság gyakorlati érvényesülése ma már a platformok működésétől is függ, ezért a kérdés szorosan kapcsolódik a platformszabályozáshoz és a moderációhoz is.

6.5. Az elektronikus kereskedelem és az elektronikus szerződéskötés szabályozása

Az elektronikus kereskedelem és az elektronikus szerződéskötés szabályozása a kibertér gazdasági működésének egyik alapvető jogi területe. Az online vásárlás és a digitális szolgáltatások elterjedésével a szerződéses kapcsolatok jelentős része ma már elektronikus úton jön létre, ezért a jogi környezetnek a hagyományos polgári jogi elveket a digitális működéshez kellett igazítania.

Magyarországon az elektronikus kereskedelem speciális szabályait a 2001. évi CVIII. törvény tartalmazza, míg a szerződés létrejöttének általános polgári jogi kereteit a Polgári Törvénykönyv adja. A fogyasztói jogviszonyokban ehhez kapcsolódik a 45/2014. (II. 26.) Korm. rendelet, amely a távollévők között kötött szerződések részletes szabályait határozza meg. Az EU-s fogyasztóvédelmi szabályozás közvetlen hatással van a magyar jogra, mivel az irányelvek harmonizációs kötelezettsége révén a hazai szabályozás (pl. e-kereskedelmi és távollévők között kötött szerződésekre vonatkozó előírások) nagymértékben uniós jogharmonizáció eredménye, így biztosítva az egységes fogyasztóvédelmi minimumszintet a tagállamok között.

A szabályozás jelentősége abban áll, hogy az elektronikus szerződéskötés során a felek személyes jelenléte hiányzik, ezért különösen fontos az átlátható tájékoztatás, a szerződési feltételek egyértelműsége és a fogyasztói jogok megfelelő védelme. A digitális környezetben a jogbiztonság szempontjából nemcsak az számít, hogy a szerződés létrejön-e, hanem az is, hogy a felek jogai és kötelezettségei világosan meghatározhatók legyenek. Az elektronikus

[37] Magyarország Alaptörvénye. Nemzeti Jogszabálytár, Budapest, IX. cikk, letöltés dátuma: 2026. 03. 27.
[38] European Convention on Human Rights. Council of Europe, Strasbourg, Article 10, letöltés dátuma: 2026. 03. 27.

kereskedelem szabályozása azt a célt szolgálja tehát, hogy a digitális gazdaság működése jogilag is kiszámítható és biztonságos keretek között történjen.

6.6. A kibertámadásokkal, digitális visszaélésekkel kapcsolatos büntetőjogi vonatkozások

A kibertámadások és digitális visszaélések büntetőjogi megítélése azért bír különös jelentőséggel, mert a kibertérben megjelenő jogsértések nem minden esetben kezelhetők kizárólag adatvédelmi, polgári jogi vagy megfelelőségi kérdésként. Bizonyos magatartások már olyan súlyú beavatkozást jelentenek az információs rendszerek működésébe vagy az adatok biztonságába, amelyek büntetőjogi felelősséget alapozhatnak meg. A büntetőjogi szabályozás ezért a kibertérben a jogi védelem egyik végső eszközének tekinthető.

A magyar szabályozásban e körben kiemelt jelentőségű a 2012. évi C. törvény a Büntető Törvénykönyvről, amely több olyan tényállást is tartalmaz, amelyek közvetlenül kapcsolódnak az információs rendszerekhez és a digitális visszaélésekhez. Ide sorolhatók különösen az információs rendszer vagy adat megsértésével, az információs rendszer felhasználásával elkövetett csalással, valamint az adatokhoz való jogosulatlan hozzáféréssel összefüggő magatartások.[39] A szabályozás jelentősége abban áll, hogy a digitális térben elkövetett jogsértések nem maradnak „láthatatlan" technikai események, hanem adott esetben büntetőjogi szankciót is maguk után vonhatnak.

A büntetőjogi megközelítés ugyanakkor a kibertérben sajátos nehézségekkel jár. Az 5.4. alfejezet már bemutatta, hogy az attribúció problémája miatt a támadó személyének azonosítása sok esetben bonyolult, ami a büntetőjogi felelősségre vonást is megnehezíti. Emiatt a jogi szabályozás önmagában nem elegendő: a büntetőjogi védelem tényleges érvényesüléséhez technikai felkészültségre, megfelelő naplózásra, incidenskezelésre és hatósági együttműködésre is szükség van.

6.7. A kiberbiztonság és a kritikus infrastruktúrák védelmének jogi keretei

A kiberbiztonság és a kritikus infrastruktúrák védelme a kibertér szabályozásának egyik legfontosabb területe, mert a digitális rendszerek sérülése már nemcsak technikai vagy gazdasági, hanem közvetlen társadalmi és állami működési kockázatot is jelenthet. A kritikus szolgáltatások, különösen az energetika, a közlekedés, a pénzügyi rendszerek, az egészségügy és a digitális infrastruktúra fokozott védelmet igényelnek – CIA elv alkalmazása –, mivel kiesésük széles körű következményekkel járhat.

Európai Uniós szinten e terület egyik legfontosabb jogforrása a NIS2 irányelv, amely a magas közös kiberbiztonsági szint megteremtését célozza. A szabályozás a kockázatkezelési intézkedésekre, az incidensbejelentésre, a vezetői felelősségre és a felügyeleti követelményekre helyezi a hangsúlyt.

A hazai szabályozásban kiemelt jelentőségű a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról, amely a magyar kiberbiztonsági követelményrendszer fontos eleme, mivel egységes kockázatkezelési, incidensbejelentési és szervezeti megfelelőségi követelményeket vezet be a kritikus és fontos szervezetek számára, összhangban az EU NIS2 irányelvi elvárásaival. Emellett a kritikus entitások rezilienciájáról szóló uniós irányelv is azt erősíti, hogy a fizikai és digitális ellenálló képesség ma már nem választható el egymástól.

[39] 2012. évi C. törvény a Büntető Törvénykönyvről. Nemzeti Jogszabálytár, Budapest, letöltés dátuma: 2026. 03. 30.

A szabályozás lényege tehát abban áll, hogy a kiberbiztonság ne pusztán technikai feladat legyen, hanem a szervezeti működés, a felkészültség és a reziliencia részeként jelenjen meg.

6.8. A magyar és európai uniós szabályozás főbb irányai

A kibertér szabályozásában a magyar és az európai uniós megközelítés közös vonása, hogy egyre erősebben a kockázatalapú, rezilienciára épülő és felelősségi szemléletű szabályozás felé mozdul el. Az uniós jogalkotás célja elsősorban az, hogy a tagállamok között egységesebb keretek jöjjenek létre a kiberbiztonság, az adatvédelem, a digitális szolgáltatások és a platformok működése terén. Ezt mutatja a GDPR[40], a DSA és a NIS2 szabályozási logikája is.

A magyar szabályozás ehhez részben nemzeti sajátosságokkal, részben az uniós normák átvételével kapcsolódik. A hazai jogi környezetben az adatvédelem, az elektronikus kereskedelem, a büntetőjogi védelem és a kiberbiztonság egymással összefüggő területekként jelennek meg. Ebből következően a kibertér szabályozása ma már nem egyetlen jogterület feladata, hanem több szabályozási szint összehangolt működését igényli.

A jelenlegi szabályozási irányok alapján jól látható, hogy a hangsúly egyre kevésbé a pusztán utólagos jogérvényesítésen, és egyre inkább a megelőzésen, az átláthatóságon, a szervezeti felelősségen és az incidensekre való felkészülésen van. Ez a szemlélet illeszkedik ahhoz a változáshoz, amelyben a kibertér már nem csupán technológiai közeg, hanem társadalmi, gazdasági és biztonságpolitikai jelentőségű működési tér.

6.9. A felhőszolgáltatások, az IoT és az új technológiai kockázatok szabályozási kihívásai

A felhőszolgáltatások, az IoT-eszközök és más új technológiák terjedése tovább növeli a kibertér összetettségét. Ezek a megoldások jelentős hatékonysági előnyöket biztosítanak, ugyanakkor új sérülékenységeket, beszállítói függőségeket és szabályozási kérdéseket is felvetnek. A probléma lényege, hogy a technológiai fejlődés gyorsabb, mint a részletes jogi reagálás, ezért a szabályozás sok esetben általános kockázatkezelési és biztonsági követelményeken keresztül próbál alkalmazkodni.

A felhőszolgáltatások esetében különösen fontos kérdés az adatok helye, a szolgáltatói függőség, a rendelkezésre állás és az incidenskezelés. Az IoT területén pedig az jelent kihívást, hogy nagyszámú, eltérő biztonsági szintű eszköz kapcsolódik a hálózatra, ami növeli a támadási felületet. A szabályozás ezért egyre inkább arra törekszik, hogy ne egyes technológiákat külön-külön kezeljen, hanem az általuk okozott kockázatokat integrált módon, a reziliencia és a biztonság szemszögéből közelítse meg, tehát egyre inkább a NIS2, a DORA és a reziliencia-alapú megközelítések mentén, a technológiák helyett az azokból eredő kockázatok integrált kezelésére és a rendszerek ellenálló képességének erősítésére fókuszál.

Ez a szabályozási irány jól mutatja, hogy a kibertérben az új technológiák jogi kezelése ma már nem pusztán innovációs vagy piaci kérdés, hanem a biztonságos és kiszámítható működés feltétele is.

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Official Journal of the European Union, Brussels, 2016, letöltés dátuma: 2026. 04. 04.

7. A kutatás korlátai

A dolgozat elkészítése során fontos szempont volt számomra, hogy a kibertér témája rendkívül összetett, és egyszerre kapcsolódik technológiai, társadalmi, jogi és biztonságpolitikai kérdésekhez. Ebből következően nem törekedhettem arra, hogy a témakör minden részterületét teljes mélységben feldolgozzam. A vizsgálat célja elsősorban a főbb összefüggések bemutatása volt, különös tekintettel a digitális nyilvánosságra, a konfliktustér-jellegre és a jogi szabályozás főbb irányaira.

A kutatás egyik korlátját a dolgozat hosszára vonatkozó keret jelentett, így a korlát szükségessé tette az egyes részterületek tudatos szűkítését. Emiatt több kérdéskört – például a technikai kibervédelmi megoldások részletes bemutatását, a nemzetközi jog mélyebb elemzését vagy az egyes platformok működésének önálló vizsgálatát – csak a téma szempontjából indokolt mértékben érintettem.

További korlátot jelentett, hogy a kibertér gyorsan változó terület, ahol a technológiai fejlődés, a fenyegetések és a szabályozási környezet is folyamatosan átalakul. Ez különösen igaz a mesterséges intelligenciához kapcsolódó kockázatokra, az online platformok működésére és a kiberbiztonsági megfelelőségi követelményekre. A dolgozatban ezért elsősorban a jelenlegi állapot főbb tendenciáit és összefüggéseit vizsgáltam, nem pedig minden részterület kimerítő feldolgozására vállalkoztam.

A dolgozat elméleti jellege szintén meghatározta a kutatás kereteit. A vizsgálat nem empirikus kutatásra vagy esettanulmányok széles körű elemzésére épül, hanem elsősorban szakirodalmi, jogi és stratégiai források feldolgozására. Ebből következően a téma több eleme – különösen a konfliktustér gyakorlati működése és az egyes incidensek szervezeti hatása – további, önálló kutatás tárgya is lehetne.

8. Összegzés

Dolgozatomban arra kerestem a választ, hogy a kibertér miként vált a 21. században társadalmi és konfliktustérré, valamint hogy ebben a közegben hogyan kapcsolódik össze a digitális nyilvánosság, a jogi szabályozás és a biztonságpolitikai kihívások kérdésköre. A vizsgálat során arra a következtetésre jutottam, hogy a kibertér ma már nem értelmezhető pusztán technológiai háttérként, hanem olyan összetett működési közegként, amely egyszerre alakítja a társadalmi kommunikációt, a gazdasági folyamatokat, az állami működést és a modern konfliktusok természetét.

A dolgozat első felében bemutattam, hogy a kibertér fogalma technológiai fejlődés, társadalmi átalakulás és politikai jelentőség erősödése révén nyerte el jelenlegi tartalmát. Ezt követően vizsgáltam a digitális nyilvánosság, a közösségi média, az online szólásszabadság és a platformalapú gazdaság kérdéseit, amelyek jól mutatják, hogy a kibertér már a mindennapi társadalmi és gazdasági működés egyik meghatározó terévé vált. Ezzel együtt azt is megállapítottam, hogy az adatlopások, az online megtévesztések és a digitális visszaélések a kibertér kockázati oldalát is egyre hangsúlyosabbá teszik.

A diplomamunka központi részében arra jutottam, hogy a kibertér konfliktustér-jellege ma már nem elméleti lehetőség, hanem gyakorlati valóság. A kibertámadások, az információs műveletek, a dezinformáció, az attribúció problémája, az OSINT, valamint a hibrid hadviselés kibertéri dimenziói mind azt igazolják, hogy a digitális tér a modern versengés és befolyásolás egyik meghatározó közege lett. E körben különösen fontosnak tartom, hogy a konfliktustér logikája nemcsak az állami szereplőket érinti, hanem a vállalati és szolgáltatói környezetet is, így a kiberbiztonság ma már a működésbiztonság és a szervezeti ellenálló képesség alapvető része.

A jogi szabályozás vizsgálata alapján arra a megállapításra jutottam, hogy a kibertérben jelentkező problémák nem kezelhetők egyetlen jogterület keretében. Az adatvédelem, az online platformok működése, az elektronikus kereskedelem, a büntetőjogi védelem és a kiberbiztonsági követelmények egymással összefüggő szabályozási területeket alkotnak. A magyar és európai uniós szabályozás fő iránya egyértelműen a kockázatalapú, rezilienciára épülő és felelősségi szemlélet erősödése felé mutat. Ez jól illeszkedik ahhoz a felismeréshez, hogy a kibertér biztonsága nem pusztán technikai, hanem jogi és intézményi kérdés is.

Mindezek alapján arra a következtetésre jutottam, hogy a kibertér ma már a társadalmi működés, a gazdasági kapcsolatok, az állami szuverenitás és a biztonságpolitikai versengés egyik meghatározó tere. A kibertérhez kapcsolódó kihívások kezelése ezért csak több szempont együttes figyelembevételével lehetséges: szükség van technikai védelemre, megfelelő jogi szabályozásra, szervezeti felkészültségre és tudatos társadalmi jelenlétre is. A kibertér jövőbeli jelentősége várhatóan tovább erősödik, ezért a témakör vizsgálata a jövőben is indokolt és aktuális marad.

9. Irodalomjegyzék

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

2012. évi C. törvény a Büntető Törvénykönyvről.

2013. évi V. törvény a Polgári Törvénykönyvről.

45/2014. (II. 26.) Korm. rendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól.

CASTELLS, Manuel (2010): The Rise of the Network Society. Wiley-Blackwell, Oxford.

Council of the European Union (2025): Cyber defence. URL (letöltés dátuma: 2026. március 25.)

DODGE, Martin - KITCHIN, Rob (2003): Mapping Cyberspace. Routledge, London.

ENISA - European Union Agency for Cybersecurity (2024): Threat Landscape 2024. URL (letöltés dátuma: 2026. március 25.)

European Commission (2021): 2030 Digital Compass: the European way for the Digital Decade. URL (letöltés dátuma: 2026. március 25.)

Council of Europe (1950): European Convention on Human Rights. URL (letöltés dátuma: 2026. március 27.)

GERMANO, Fabrizio - GÓMEZ, Vicenç - SOBBRIO, Francesco (2025): Ranking for Engagement: How Social Media Algorithms Fuel Misinformation and Polarization. Barcelona School of Economics, Barcelona.

GIBSON, William (1984): Neuromancer. Ace Books, New York.

IFTIKHAR, Ifra - BAJWA, Umair Mahmood (2025): Impact of Social Media Algorithms on Polarization Despite Perceived Diversity. Lahore Garrison University, Lahore.

KOLTAY András (2019): Az új média és a szólásszabadság. Wolters Kluwer, Budapest.

KOLTAY András (2022): A közösségi média tartalomszabályozásának egyes kérdései. Wolters Kluwer, Budapest.

Magyarország Alaptörvénye.

NATO (2024): Cyber defence. URL (letöltés dátuma: 2026. március 25.)

NATO (2024): Washington Summit Declaration. URL (letöltés dátuma: 2026. március 25.)

NATO CCDCOE (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge.

NYE JR., Joseph S. (2011): The Future of Power. PublicAffairs, New York.

OECD (2024): OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier. OECD Publishing, Paris.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

RUSSELL, Andrew L. (2006): Rough Consensus and Running Code: Documents and the History of the Internet. Sloan Foundation, New York.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

WIENER, Norbert (1948): Cybernetics: Or Control and Communication in the Animal and the Machine. MIT Press, Cambridge.

ZUBOFF, Shoshana (2019): The Age of Surveillance Capitalism. PublicAffairs, New York.

10. Rövidítések és fogalmak jegyzéke

adatexfiltráció - adatok jogosulatlan kimentése vagy kiszivárogtatása.

AI (Artificial Intelligence) - mesterséges intelligencia.

AI Act - az Európai Unió mesterséges intelligenciára vonatkozó rendelete.

CCDCOE (Cooperative Cyber Defence Centre of Excellence) - a NATO Kibervédelmi Kiválósági Központja.

CER (Critical Entities Resilience) - a kritikus entitások rezilienciájára vonatkozó uniós szabályozási megközelítés.

CISA (Cybersecurity and Infrastructure Security Agency) - az Egyesült Államok kiberbiztonsági és infrastruktúravédelmi ügynöksége.

DDoS (Distributed Denial of Service) - elosztott szolgáltatásmegtagadásos támadás.

deepfake - mesterséges intelligenciával előállított vagy manipulált hamis kép-, hang- vagy videótartalom.

DSA (Digital Services Act) - az Európai Unió digitális szolgáltatásokról szóló rendelete.

dual use - kettős felhasználás; olyan eszköz vagy tudás, amely polgári és támadó célra is alkalmazható.

EDPB (European Data Protection Board) - Európai Adatvédelmi Testület.

ENISA (European Union Agency for Cybersecurity) - az Európai Unió Kiberbiztonsági Ügynöksége.

GDPR (General Data Protection Regulation) - az Európai Unió általános adatvédelmi rendelete.

influenszer - közösségi médiában aktív véleményformáló személy, aki követőire befolyást gyakorol.

IoT (Internet of Things) - dolgok internete; hálózatra kapcsolt intelligens eszközök összessége.

IT (Information Technology) - információtechnológia.

LLM (Large Language Model) - mesterséges intelligencián (MI) alapuló rendszer, amely hatalmas mennyiségű szöveges adat alapján tanul.

MI - mesterséges intelligencia.

multi-stakeholder - több szereplő együttműködésére épülő megközelítés.

NATO (North Atlantic Treaty Organization) - Észak-atlanti Szerződés Szervezete.

NIS2 (Network and Information Security 2) - az Európai Unió hálózati és információs rendszerek biztonságára vonatkozó irányelve.

OECD (Organisation for Economic Co-operation and Development) - Gazdasági Együttműködési és Fejlesztési Szervezet.

OSINT (Open Source Intelligence) - nyílt forrású hírszerzés, nyilvánosan elérhető információk elemzése.

platform - digitális közvetítő felület vagy szolgáltatási környezet.

Ptk. - Polgári Törvénykönyv.

reziliencia - ellenálló és helyreállításra képes működés.

social engineering - emberi befolyásoláson alapuló támadási módszer.