HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 19–48.
DOI: 10.32567/hm.2025.1.2

Bor Olivér[1]

Szabályozási szemléletváltás

A NIS2 hatása a magyar kiberbiztonsági szabályozásra

A Shift in Regulatory Approach

The Impact of NIS2 on Hungarian Cybersecurity Regulation

Absztrakt

A tanulmány a magyar kiberbiztonsági szabályozás fejlődését vizsgálja a 2013. évi L. törvény és a 2024. évi LXIX. törvény összehasonlításán keresztül, különös tekintettel az Európai Unió NIS2 irányelvének hatására. A kutatás bemutatja, miként alakult át a szabályozás szemlélete az állami elektronikus információbiztonság védelmét célzó megközelítéstől egy átfogóbb, kockázat- és incidenskezelésre épülő kiberbiztonsági ökoszisztéma irányába. Részletes elemzés tárja fel a jogszabályi szövegek strukturális, terminológiai és stratégiai változásait, rávilágítva arra, hogy a szabályozási környezet hogyan igazodott a digitalizációval járó fenyegetések gyors evolúciójához. A tanulmány rámutat, hogy a digitalizációval összefüggő új kihívások szükségessé tették a jogszabályok kibővítését és aktualizálását, ami technológiai, szervezeti és hatósági szinten egyaránt megfigyelhető. A kutatás eredményei azt hangsúlyozzák, hogy a modern kiberbiztonsági szabályozás nemcsak a technológiai védelmi intézkedésekre, hanem az ellenálló képesség növelésére, a kockázatalapú szemléletre és a nemzeti szintű koordináció megerősítésére is kiemelt figyelmet fordít, ezzel hozzájárulva az Európai Unió egységes kiberbiztonsági szintjének megteremtéséhez.

Kulcsszavak: kiberbiztonság, trendek, fenyegetések, NIS2, szabályozás

[1] Kiberbiztonsági és kommunikációs szakértő, okleveles kommunikációs és nemzetközi tanulmányok szakértő, e-mail: oliver.bor@protonmail.com

Abstract

The study examines the development of Hungarian cybersecurity regulation through a comparison of Act L of 2013 and Act LXIX of 2024, with particular attention to the impact of the European Union's NIS2 directive. The research presents how the regulatory approach evolved from a focus on the protection of state electronic information security towards a more comprehensive cybersecurity ecosystem based on risk management and incident handling. A detailed analysis reveals structural, terminological, and strategic changes in the legislative texts, highlighting how the regulatory environment has adapted to the rapid evolution of threats associated with digitalization. The study emphasizes that the new challenges related to digital transformation necessitated the expansion and updating of legislation, a trend observable at technological, organizational, and regulatory levels alike. The findings underline that modern cybersecurity regulation not only focuses on technological protective measures but also places significant emphasis on strengthening resilience, adopting a risk-based approach, and reinforcing national-level coordination, thereby contributing to the creation of a unified level of cybersecurity across the European Union.

Keywords: cybersecurity, trends, threats, NIS2, regulation

Bevezetés

„Kétféle cég létezik a világon: azok, amelyeket már meghackeltek, és azok, amelyeket meg fognak hackelni" – szól az információbiztonsági és kiberbiztonsági szakma által gyakran idézett mondat, amelyet a legtöbben Robert Muellernek, az FBI egykori igazgatójának tulajdonítanak 2012-ből. Valójában azonban Dmitri Alperovitch, a McAfee akkori vezető szakértője a Shady RAT elnevezésű jelentésében már 2011-ben megfogalmazta a mára híressé vált gondolatot: „Kétféle vállalat létezik: azok, amelyeket már feltörtek, és azok, amelyek még nem tudják, hogy feltörték őket." Ezzel gyakorlatilag a világ egyik vezető kiberbiztonsági cégének munkatársaként már 2011-ben világossá tette, hogy a kibertámadások szinte minden vállalatot érintenek, és a vállalatoknak folyamatosan készülniük kell az ilyen jellegű fenyegetésekre. 2012-ben Robert Mueller, az FBI akkori igazgatója egy San Franciscó-i kiberbiztonsági konferencián továbbfejlesztette ezt az üzenetet, amikor beszédében azt mondta: „Már nem az a kérdés, hogy megtörténik-e, hanem hogy mikor. Kétféle cég létezik a világon: azok, amelyeket már meghackeltek, és azok, amelyeket meg fognak hackelni." Ez a kijelentés egyértelműen jelezte, hogy a kibertámadások elkerülhetetlenek a modern digitális világban, és minden vállalat számára csak idő kérdése, hogy mikor válik támadás áldozatává. Mueller hangsúlyozta, hogy a vállalatoknak fel kell készülniük az újabb és újabb kibertámadásokra, mert ezek elkerülhetetlenek a digitális világban. Ha az idézet evolúcióját nézzük, akkor megkerülhetetlen a legújabb változatot is megemlíteni, amely 2015-ben John Chamberstől, a Cisco vezérigazgatójától hangzott el, aki ismét előhozta az idézetet egy beszédében: „Kétféle vállalat létezik: azok, amelyeket már feltörtek, és azok, amelyek még nem tudják, hogy feltörték őket." Beszédében Chambers a kiberbiztonság alapvető

fontosságát hangsúlyozta az üzleti életben, álláspontja szerint a kiberbiztonság már nélkülözhetetlen egy sikeresen működő cég mindennapi tevékenysége során.[2]

A fentieket különösen annak fényében érdemes vizsgálni, hogy az elmúlt években a digitalizáció és az innováció életünk megkerülhetetlen részévé vált, amely képességek nélkül egy szervezet, egy vállalat elveszítheti versenyképességét. A digitalizáció és a digitális transzformáció olyan átfogó folyamat, amely minden iparágra hatással van, és jóval túlmutat a termék- és folyamatfejlesztés határain. Érinti az üzleti modellek kialakítását, a szervezeti és irányítási elveket, valamint az ellátási lánc működését, komoly kihívások elé állítva ezzel a vállalatokat. Másképp fogalmazva: a digitális szolgáltatások és a digitalizáció nem csupán a fizikai termékekre gyakorolnak hatást, hanem alapvetően befolyásolják az üzleti működés természetét, a szervezeti struktúrát és a vállalati stratégiát is, így egy összetett kihívással állunk szemben.[3]

Ugyanakkor elengedhetetlen figyelmet fordítani a biztonsági szempontokra is. A digitalizáció kínálta lehetőségek akkor hozhatnak valódi előnyt a szervezetek számára, és akkor járulhatnak hozzá az ország gazdasági fejlődéséhez, ha a fejlesztések és az innovációk mellett megjelenik a megfelelő szintű, valós kockázatelemzést tükröző, a fenyegetésekre adekvát válaszokat nyújtó kiberbiztonsági felkészültség is. Az átfogó védelem hatékonyságát egy széles körű, kiterjedt biztonsági megközelítés szavatolhatja, amely magában foglalja a technológiai innovációkat, a jól definiált kiberbiztonsági szabályozás bevezetését és felügyeletét, a hatékony incidenskezelést, a proaktív védelmi rendszerek alkalmazását, valamint a következetes és rendszeres kiberbiztonsági tudatosság növelését is. Az elmúlt évek kibertámadási mintáinak elemzése rámutat, hogy a kiberbűnözők számára gyakran a felhasználók a legkedveltebb célpontok. A támadóknak ugyanis sok esetben könnyebb egy szervezet informatikai rendszerébe bejutni a felhasználók révén, így okozva károkat vagy végrehajtva egyéb jogsértő cselekményeket, minthogy közvetlenül a célként kijelölt rendszer technikai gyengeségeit aknázzák ki.[4]

Az Európai Unió az elmúlt években számos kezdeményezést indított annak érdekében, hogy szabályozási eszközökkel és minimális követelmények előírásával csökkentse a tagállamok és a szervezetek kiberbiztonsági kitettségét. A kiberbiztonsági politika fejlődése a digitális infrastruktúra jelentőségének felismerésével indult, amelynek első mérföldkövei a 2013-as kiberbiztonsági stratégia és a 2016-os NIS irányelv[5] voltak. Ezeket a 2017-es, majd a 2019-es intézkedések, például az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) megerősítése és a tanúsítási keretrendszer bevezetése követték. A 2022-ben elfogadott NIS2[6] irányelv már átfogóbb megközelítést alkalmaz, amely a technológiai védekezés mellett a kockázatkezelést, az együttműködést, az ellenőrzést és a társadalmi tudatosság növelését is előírja. Az EU kiberbiztonsági szabályozása egyre inkább holisztikus szemléletet követ, amely technológiai, stratégiai és társadalmi szinten is az ellenálló képesség növelésére törekszik.

[2] Bejtlich 2018.
[3] Horváth–Szabó 2019.
[4] Bor 2024.
[5] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.
[6] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve 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.

Kutatási célok és módszertan

A kutatás középpontjában a magyar kiberbiztonsági szabályozás fejlődésének vizsgálata áll, különös tekintettel a 2013. évi L. törvény[7] (Ibtv.) és a 2024. évi LXIX. törvény[8] (Kibertv.) összehasonlítására. A két jogszabály tartalmi és nyelvi elemzése – beleértve a szógyakorisági mintázatokat, bigramok és trigramok előfordulását, valamint a tematikus klaszterek változásait – azt a célt szolgálja, hogy feltárjuk, miként alakult át a szabályozás szemlélete, struktúrája és terminológiája az elmúlt évtizedben.

Kiemelt kutatási cél annak bemutatása, hogyan módosult a szabályozási fókusz a korábbi, elsősorban állami és önkormányzati elektronikus információs rendszerek védelmét célzó megközelítésről egy szélesebb spektrumot átfogó, incidenskezelésre, szolgáltatásfolytonosságra és tanúsításra épülő kiberbiztonsági ökoszisztéma irányába. A kutatás külön hangsúlyt fektet az EU NIS2 irányelvének hatására, amely alapvetően formálta a 2024. évi LXIX. törvény szemléletét és szerkezetét.

A vizsgálat során megfogalmazott kutatási kérdés így a következő: *Hogyan változott meg a magyar kiberbiztonsági szabályozás szemlélete és nyelvezete a 2013. és 2024. évi törvények tükrében, és milyen hatással volt minderre az Európai Unió NIS2 irányelve?* E kérdés lehetőséget teremt arra, hogy feltárjuk a jogalkotás mögött álló logikai és intézményi átrendeződéseket, a szabályozás mélyülését, valamint a fogalmi és tartalmi gazdagodást, amely egy modern, harmonizált, kockázatérzékeny kiberbiztonsági környezet kialakítását célozza.

A kutatás a 2013. évi L. törvény és a 2024. évi LXIX. törvény közötti szabályozási, tartalmi és nyelvi különbségek feltárására irányult, amelyhez kvantitatív és kvalitatív módszertani megközelítést egyaránt alkalmaztunk. A cél az volt, hogy feltérképezzük, miként tükröződnek a jogalkotási szemléletváltások a törvényi szövegek nyelvi szerkezetében, tematikus fókuszában és terminológiai változásaiban.

A vizsgálat első lépéseként szógyakoriság-elemzést végeztünk, amely a két törvényben leggyakrabban előforduló szavak statisztikai alapú összehasonlítását tette lehetővé. Ezáltal láthatóvá váltak a szabályozási fókusz eltolódásai: például a „kiberbiztonság", „hatóság" vagy „tanúsítás" szavak ugrásszerű növekedése a 2024-es törvényben azt jelezte, hogy a szabályozás technológiai, szervezeti és hatósági szempontból is mélyebbé és részletesebbé vált.

A szógyakoriság mellett n-gram-elemzést is alkalmaztunk – különösen bigramok és trigramok formájában –, amely a gyakran együtt előforduló szókapcsolatokat azonosította. Ez a módszer segített az intézményi és tematikus összefüggések megértésében, például olyan kulcsfontosságú szerkezetek révén, mint a „kiberbiztonsági hatóság" vagy az „incidenskezelő központ".

A kvantitatív módszertani blokk zárásaként klaszterelemzést végeztünk, amely a szóhasználati minták alapján tematikus klasztereket hozott létre. Ez tette lehetővé annak mélyebb megértését, hogy a 2013-as törvény szövege az infrastruktúra és a rendszerbiztonság köré, míg a 2024-es törvény az állami hatósági szerepvállalás, incidenskezelés, kockázatelemzés és auditálás témái köré szerveződik.

[7] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[8] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

A kvantitatív adatok értelmezését kvalitatív elemzéssel egészítettük ki, amely a kulcsfogalmak jelentéstartalmának, a szabályozási logikák eltolódásának és a szemléletváltás mögötti narratíváknak az értelmezésére összpontosított. Ehhez nemcsak a két törvény teljes szövegét elemeztük, hanem kiegészítő dokumentumokat is bevontunk: összehasonlító jelentéseket, kulcsszavas összefoglalókat, új fogalmak listáit és klaszterelemzési eredményeket.

A szövegek feldolgozása során előfeldolgozási lépéseket végeztünk: eltávolítottuk az úgynevezett *stop-wordöket* (például kötőszók, névelők, jogszabályi struktúrára vonatkozó szavak stb.), és létrehoztuk a magyar nyelvi sajátosságokat figyelembe vevő egyedi *stop-word* listát, amely lehetővé tette a finomabb klaszterezést és a pontosabb n-gram-modellezést. Ezzel párhuzamosan kulcsszavakat kategorizáltunk, összevetve azok megjelenését, jelentését és kontextusát az egyes évek törvényeiben.

A kvantitatív és kvalitatív módszerek együttes alkalmazása révén lehetőség nyílt arra, hogy a szövegek mögött meghúzódó szabályozáspolitikai és szemléleti változások is értelmezhetővé váljanak. Ez nemcsak a nyelvi struktúrák, hanem az intézményi és stratégiai irányváltások értelmezéséhez is hozzájárult, így a kutatás túlmutatott a szimpla jogszabályi szöveg-összehasonlításon, és hozzájárult a kiberbiztonsági szabályozás fejlődési ívének mélyebb megértéséhez. A módszertani kombináció révén lehetőség nyílt arra, hogy a törvényi szövegek nyelvi struktúrája mögött rejlő szabályozáspolitikai szemléletváltás is értelmezhetővé váljon, és a változások ne csak számszerűen, hanem tartalmilag is értékelhetők legyenek.

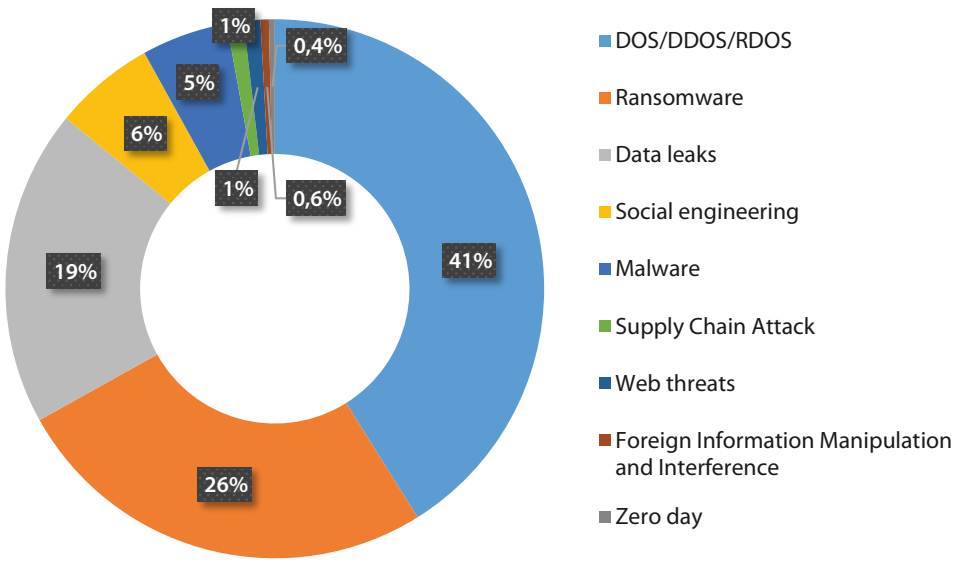
Kiberbiztonsági trendek

A vizsgált hazai szabályozási változások megértéséhez nem elegendő kizárólag a jogszabályi szövegek belső logikájára és szerkezetére koncentrálni. A kiberbiztonsági törvények alakulását alapvetően meghatározta az a fenyegetettségi környezet, amelyre válaszul születtek: a támadások jellege, technikai kivitelezése, célpontjai és azok gyors ütemű változása. A szabályozás fókuszváltása – például az incidenskezelés, a szolgáltatásfolytonosság vagy a kritikus infrastruktúrák védelmének megerősítése – közvetlen összefüggésben áll a kiberfenyegetések fejlődő metodikáival. Ezért a továbbiakban áttekintjük azokat a főbb kiberbiztonsági trendeket, amelyek az elmúlt évtizedben alakították a fenyegetettségi térképet, és amelyek lényeges befolyást gyakoroltak a magyar jogalkotás irányváltására is.

A digitális átalakulás gyors üteme és az új technológiák fejlődése, valamint a kibertámadások növekvő kifinomultsága oda vezet, hogy a szervezetek folyamatosan egyre nagyobb volumenű és súlyosabb kiberbiztonsági fenyegetésekkel találkoznak. Ezek alapján érdemes megvizsgálni az ENISA 2024-es kiberbiztonsági fenyegetettségi jelentését,[9] amely átfogó képet ad az Európai Unióban megfigyelt főbb támadási formákról és azok előző évhez viszonyított változásairól. A jelentés szerint a legkiemelkedőbb fenyegetések továbbra is a szolgáltatásmegtagadással járó támadások (*distributed denial-of-service,* más néven DDoS) és a zsarolóvírusok *(ransomware)* voltak.

[9] Lella et al. 2024.

A zsarolóvírusok ugyan még stabilan magas számban fordulnak elő, ám egyre inkább megfigyelhető, hogy a támadók többfokozatú, úgynevezett „kettős zsarolás" taktikát alkalmaznak, amely az áldozatok ismételt fenyegetésére vagy különböző célokra történő adatfelhasználásra irányul. (A támadástípusok szerinti incidensmegosztást az 1. ábra mutatja be részletesen.) A támadások gyakorisága és mérete – Európa-szerte – jelentősen megnőtt: az előző, 2023-as évhez képest 85%-os növekedést mutat. Ezek a támadások egyre komplexebbek, és gyakran más támadások „füstfüggönyeként" szolgálnak, ami azt a célt szolgálja, hogy a kiberbűnözők eltereljék a biztonsági csapatok figyelmét más, párhuzamosan zajló, komolyabb támadásokról.



1. ábra: Az elemzett incidensek fenyegetéstípus szerinti bontása (2023. júliustól 2024. júniusig)
Forrás: a szerző szerkesztése Lella et al. 2024 alapján

Az előző évhez képest a mesterséges intelligenciát (AI) alkalmazó eszközök használatában változás figyelhető meg: a támadók egyre gyakrabban használják a mesterséges intelligenciát különféle adathalász-e-mailek vagy káros szoftverek létrehozására. Az olyan AI-eszközök, mint például a FraudGPT,[10] lehetővé teszik a támadók számára azt is, hogy gyorsan és hatékonyan hozzanak létre célzott támadásokat.

A *fake news* és a különféle információmanipulációs technikák szintén jelentős szerepet töltenek be a kibertérben, különösen az orosz–ukrán konfliktus kontextusában, ahol dezinformációs kampányok és egyéb információs támadások figyelhetők meg. A jelentés megemlíti, hogy a hacktivista csoportok egyre gyakrabban kerülnek

[10] A FraudGPT egy mesterséges intelligencián alapuló eszköz, amelyet kifejezetten kiberbűnözési célokra hoztak létre. Lehetővé teszi a támadók számára, hogy automatikusan generáljanak adathalász-e-maileket, rosszindulatú programokat és más, csalárd tevékenységekhez szükséges tartalmakat. Gyorsasága és kifinomultsága miatt a kiberbűnözés új dimenzióját képviseli.

kapcsolatba állami háttérrel rendelkező támadókkal vagy akár közvetlenül egy-egy állammal, így ezek az incidensek még inkább átláthatatlanok és bonyolultak.

Összességében az ENISA jelentése szerint az EU-ban a kiberfenyegetések folyamatosan fejlődnek, és az új technológiák, mint a mesterséges intelligencia és a felhőalapú szolgáltatások, egyszerre nyújtanak lehetőséget a támadók számára és jelentenek kihívást a biztonsági és védelmi szakemberek számára. Az előző évhez képest növekvő tendenciák és új fenyegetettségek felhívják a figyelmet arra, hogy a kiberbiztonság erősítése, az adatvédelem és a tudatosság növelése kiemelten fontos az Európai Unió számára.

Ahogyan a mondás tartja, minden lánc olyan erős, mint a leggyengébb láncszeme – a kiber- és információbiztonság területén pedig ez a leggyengébb láncszem gyakran maga az ember. A PurpleSec 2024-es kiberbiztonsági riportjának adatai szerint[11] a kibertámadások 98%-a valamilyen *social engineering* technikát alkalmaz, ami kiemeli az emberi tényező központi szerepét a kiberbiztonság fenyegetései között. A *social engineering*, vagyis a pszichológiai manipuláció olyan módszerek és technikák összessége, amelyek az emberi hibák vagy viselkedésminták kihasználásával célozzák meg a felhasználók bizalmas információinak megszerzését. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet egy, a 2023-as évre vonatkozó jelentése alapján[12] a *social engineering* technikák továbbra is a legelterjedtebb támadási formák közé tartoznak, különösen az adathalászat terén, ahol az e-mail, az SMS és a telefonos megkeresések kombinációja új szintre emelte a fenyegetettséget.

A *social engineering* támadások azért is különösen veszélyesek, mert gyakran rejtve maradnak: az áldozatok sok esetben nem is tudják, hogy támadás érte őket, de sok esetben azért hallgatnak a történtekről, mert attól tartanak, hogy hibáik negatív következményekkel járhatnak. Ez a láthatatlanság jelentősen megnehezíti a pontos statisztikai elemzések készítését, és a védekezést is korlátozza.

A *social engineering* támadások központi eleme az emberi sebezhetőség, amely számos módon kihasználható. Az alkalmazottak közvetlenül hozzáférnek a szervezetek védett eszközeihez és adataihoz, így különösen értékes célpontokká válnak. Például ők telepítik és frissítik (vagy mulasztják el frissíteni) a szükséges szoftvereket, szállítanak és kezelnek hardvereszközöket, valamint hozzáférnek belső fájlokhoz, rendszerekhez és adatokhoz. Ezen túlmenően olyan belső információk birtokában vannak, amelyek értékesek lehetnek a támadók számára. Az emberi tulajdonságok, mint például a segítőkészség, a bizalom és az információhiány, különösen kihasználhatóvá teszik őket, főleg, ha nem részesülnek megfelelő képzésben és tudatosításban.[13]

Az adathalászat a *social engineering* legelterjedtebb formája, amely különféle technikákat foglal magában. Az e-mailes adathalászat során a támadók hivatalosnak tűnő üzenetekkel próbálják meg rávenni az áldozatokat arra, hogy érzékeny adatokat, például jelszavakat vagy bankkártyaadatokat adjanak meg. Az SMS-alapú adathalászat hasonló elven működik, és gyakran csomagátvételi értesítésekkel vagy előfizetés-megújítási figyelmeztetésekkel álcázzák magukat a támadók. A telefonos adathalászat

[11] PurpleSec [é. n.].
[12] Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet 2024.
[13] Oroszi 2023.

pedig közvetlen emberi interakcióra épít, ahol a támadók pszichológiai nyomást alkalmaznak, hogy érzékeny információk kiadására bírják az áldozatokat. Mindegyik adathalászmódszerben közös, hogy az emberi sebezhetőségre épít, és a támadók hivatalosnak tűnő kommunikációt alkalmaznak, például bankok, közműszolgáltatók vagy egyéb szervezetek nevében keresik meg a leendő áldozatokat, továbbá éles helyzetet felvázolva, sürgető hangnemet alkalmazva késztetik arra a másik felet, hogy érzékeny adatokat adjon meg valamilyen módon.[14]

Az utóbbi években a mesterséges intelligencia és a *deepfake* technológiák megjelenése új szintre emelte a *social engineering* támadásokat. Az ENISA jelentése rámutat, hogy az AI által generált adathalász-e-mailek már szinte hibátlan nyelvezetet és formázást alkalmaznak, ami megnehezíti azok felismerését. A hangklónozás és a *deepfake* videók alkalmazása pedig lehetővé teszi, hogy a támadók akár valós idejű videóhívások során is manipulálják az áldozatokat. Noha ezek a technológiák a 2020-as évek elején még gyerekcipőben jártak, gyors fejlődésük manapság jelentős kiberbiztonsági kockázatokat hordoz.[15]

A *social engineering* támadások elleni védekezés elsődleges eszköze a munkavállalók képzése és tudatosítása. Az Európai Unió NIS2 irányelve hangsúlyozza, hogy a szervezeteknek kiemelt figyelmet kell fordítaniuk az alkalmazottak oktatására, különös tekintettel az adathalászat felismerésére és elkerülésére. Ezen túlmenően a technológiai védelmi megoldások, például a multifaktoros hitelesítés, a biztonsági szűrők és az adathalászatot szűrő rendszerek bevezetése jelentősen csökkentheti a támadások sikerességét.

Az EU kiberbiztonsági politikájának rövid áttekintése, különös tekintettel a NIS2-re

Az Európai Unió kibervédelmi szakpolitikájának fejlődése az elmúlt két évtizedben jól nyomon követhető az uniós stratégiai dokumentumokon, rendeleteken és irányelveken keresztül. Az alapok már a 2000-es évek elején, röviden és csekély mértékben ugyan, de kirajzolódtak, amikor az illetékesek felismerték, hogy a digitális infrastruktúra biztonsága a gazdaság és a társadalom versenyképességének alapvető eleme. Az első releváns dokumentum, a 2003-as európai biztonsági stratégia, amelynek végrehajtásáról szóló dokumentum[16] is még csak áttételesen említi a kiberbiztonságot, főként a terrorizmus kontextusában.[17]

A 2005-ös *i2010: Európai Információs Társadalom a növekedésért és foglalkoztatásért*[18] elnevezésű stratégiai dokumentum már konkrétabban foglalkozik az információs társadalom biztonságával, a digitális gazdaság fejlesztésével, az IKT szerepének erősítésével, és felveti egy átfogó biztonsági stratégia szükségességét. A 2003-ban

[14] Nemzeti Kibervédelmi Intézet 2023.
[15] Veszelszki 2023.
[16] Az Európai Unió Tanácsa 2009.
[17] Molnár 2019.
[18] A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – „i2010: európai információs társadalom a növekedésért és a foglalkoztatásért".

elfogadott európai biztonsági stratégia 2008-as módosítása már külön szakaszban foglalkozott az informatikai biztonság alapvető vonatkozásaival. Az átdolgozott változat kiemeli, hogy a korszerű gazdaságok működése szoros kapcsolatban áll az alapvető infrastruktúrák – többek között az internet – zavartalan működésével. A dokumentum arra is rámutat, hogy az interneten keresztül elkövetett bűncselekmények kérdését már tárgyalta a 2006-ban elfogadott, az európai információs társadalom biztonságát célzó stratégia.[19]

Az EU 2010-es belső biztonsági stratégiája[20] már kiemeltebben foglalkozott a számítástechnikai bűnözés jelentette veszélyekkel. Ugyanebben az évben indult az Európa 2020 stratégia, amely a versenyképesség fokozása mellett – többek között – már a digitális sérülékenységek csökkentését is célul tűzte ki. Ennek részeként született meg az európai digitális menetrend,[21] amely az IKT-központú fejlődést helyezte előtérbe, valamint ráirányította a fókuszt a kiberbűnözés gyors ütemű terjedésére. Az Európai Bizottság és a tagállamok döntéshozói számára hamar nyilvánvalóvá vált, hogy a kitűzött célok csak akkor érhetők el teljes mértékben, ha biztosított a kibertér védelme.[22]

A 2010-es évek elején az EU felismerte, hogy noha a meglévő szabályozások előrelépést jelentettek, nem biztosítanak átfogó védelmet, mivel a tagállamok felkészültsége jelentős különbségeket mutat. Ennek orvoslására az Unió célul tűzte ki egy egységes kiberbiztonsági politika megalkotását, amely erősíti a bűnüldözést, ösztönzi a nemzetközi együttműködést, és közös szabályozási, fogalmi, intézményi alapokat hoz létre. Ennek kiindulópontját képezte az EU első kiberbiztonsági stratégiája, amelyet 2013-ban fogadtak el *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* címmel.[23] A dokumentum kulcspontjai között említhető a kibertér biztonságának uniós szintű biztosítása, a kritikus infrastruktúrák védelme, a kibertámadások elleni védekezés, valamint az alapjogok – különösen a magánszféra védelmének – megerősítése a digitális térben. A stratégia öt prioritása között szerepel az ellenálló képesség növelése, a kiberbűnözés visszaszorítása, a közös védelempolitikai képességek fejlesztése, valamint a nemzetközi együttműködés elmélyítése. Intézményi szinten a stratégia meghatározta az Európai Bizottság, az ENISA és az Európai Külügyi Szolgálat szerepét is.[24]

A stratégia eredményeként – hároméves jogalkotási folyamat végén – született meg az első uniós szintű, kötelező kiberbiztonsági politika, a 2016-os NIS irányelv.[25] Az irányelv célja, hogy egységes biztonsági szintet biztosítson a hálózati és információs rendszerek védelmében, kiemelten az alapvető szolgáltatásokat nyújtó szektorokra (például energia, vízellátás, közlekedés, egészségügy). Az irányelv kötelezővé tette a nemzeti szintű kiberstratégiák kidolgozását, a CSIRT-ek[26] létrehozását, valamint a tagállami együttműködést biztosító szervek – például az Együttműködési

[19] Jelentés az Európai Biztonsági Stratégia végrehajtásáról. A biztonság megteremtése a változó világban.
[20] Az Európai Unió Tanácsa 2010.
[21] Európai Bizottság, Európai Digitális Menetrend 2010.
[22] Kovács 2018.
[23] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.
[24] Kovács 2018.
[25] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[26] CSIRT: Computer Security Incident Response Team (számítógépes biztonsági eseményelhárítási csoport).

Csoport – részvételét. Az irányelv jelentőségét az adta, hogy ez volt az első átfogó, uniós szintű kiberbiztonsági jogszabály, amely kötelező előírásokat és minimum biztonsági követelményeket határozott meg tíz, különösen fontos ágazat számára.[27]

2017 szeptemberében az Európai Bizottság a NIS irányelv végrehajtásával párhuzamosan kiadta a 2017/1584. számú ajánlást[28] a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról. Az ajánlás az EU-n belüli kiberbiztonsági együttműködés megerősítésére törekszik, mivel a NIS irányelv nem szabályozta a válságkezelés kereteit. Az ajánlás úttörő jelentőségű volt, hiszen először határozta meg uniós szinten, mit tekintünk kiberbiztonsági eseménynek. A definíció egy olyan, gyorsan terjedő, előre nem látható válsághelyzetet ír le, amely nem korlátozódik egy adott területre, és jelentős fennakadásokat okozhat az uniós gazdaságban, társadalomban és a demokratikus működést biztosító digitális infrastruktúrában. Mindezek mellett az ajánlás kiemeli a tagállami felelősség elsődlegességét, ugyanakkor szükség esetén uniós szintű politikai koordinációt is előír. A válságkezelésben a CSIRT-hálózat, az ENISA és más uniós szervek közreműködése kulcsfontosságú, míg a stratégiai iránymutatást a NIS irányelv alapján létrejött Együttműködési Csoport biztosítja. Az ajánlás hangsúlyozza a kockázatmenedzsment, a rendszeres kiberbiztonsági gyakorlatok és egy uniós válságreagálási keret kialakításának fontosságát.[29]

A 2013-as stratégia célkitűzéseinek részleges teljesülése és az új típusú fenyegetések – például a WannaCry[30] vagy a NotPetya[31] támadások – szükségessé tették a stratégia felülvizsgálatát. Az EU *Ellenálló képesség, elrettentés, védelem*[32] című 2017-es közleménye új eszközöket javasolt, mint például az ENISA megerősítése, gyorsreagálási protokollok kidolgozása. A kibertámadásokkal szembeni védekező képesség erősítése érdekében elengedhetetlennek mutatkozott a NIS irányelv teljes körű, határidőre történő tagállami végrehajtása. A bizottság útmutatással és bevált gyakorlatok megosztásával segíti ezt a folyamatot, különös figyelemmel az alapvető szolgáltatásokra. Kiemelt cél a köz- és magánszféra közötti bizalom és információcsere elmélyítése.[33]

A 2017-es stratégia kapcsán érdemes kiemelni az ENISA szerepének megerősítését, a digitális termékek és szolgáltatások védelmét támogató, önkéntes uniós tanúsítási rendszer kialakítását, valamint egy olyan terv kidolgozását is, amely lehetővé teszi a gyors és összehangolt reagálást nagyszabású kiberbiztonsági események és válsághelyzetek esetén. A 2017. szeptember 13-án bemutatott kiberbiztonsági csomag részeként elkezdődött a kiberbiztonsági rendelet megalkotása, amely a digitális egységes piac stratégiai célkitűzései közé tartozott. Az Európai Bizottság 2018 szeptemberében javaslatot tett egy európai kiberbiztonsági kompetenciaközpont

[27] Tikos 2019.
[28] A Bizottság 2017/1584 ajánlása.
[29] Bonnyai 2019.
[30] WannaCry: egy 2017 májusában felbukkant zsarolóvírus, amely közel 250 000 számítógépet fertőzött meg világszerte, összesen 99 országban és 28 nyelven hozott létre zsarolóoldalakat.
[31] NotPetya: egy 2017 júniusában felbukkant zsarolóvírus, amelyet főleg ukrán állami szervezetek, bankok és az energiaszektor ellen vetettek be.
[32] Közös közlemény az Európai Parlamentnek és a Tanácsnak: *Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése.*
[33] Krasznay 2022.

és annak hálózatának létrehozására, valamint a kutatásra és innovációra szánt források hatékonyabb felhasználása érdekében. A kiberbiztonsági rendelet javaslata többek között az ENISA megbízatásának állandósítását, erőforrásainak bővítését, valamint a tagállamok támogatását célozza a kibertámadások elleni fellépésben. Cél volt, hogy a 2005 óta működő ENISA hatékonyabban támogassa a tagállamok kapacitásépítését, a tudatosság növelését, valamint az uniós intézmények és tagállamok szakpolitikai munkáját. A rendelet további célja volt egy uniós szintű tanúsítási keret létrehozása, amely javítja a hálózatra kapcsolt eszközök, a kritikus infrastruktúrák és a dolgok internetéhez kapcsolt eszközök biztonságát, akár már a fejlesztések korai szakaszában is.[34]

Az eddigi jogszabályi keretrendszer 2019-ben egy összetett jogi aktussal vált teljessé: a 2019. április 9-én elfogadott rendelettel, amely az ENISA-ról és az információs és a kommunikációs technológiák kiberbiztonsági tanúsításáról szólt, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről.[35] A rendelet egy uniós szintű kiberbiztonsági tanúsítási keretrendszert vezetett be, amely lehetővé teszi a hálózathoz csatlakozó eszközök tanúsítását[36] az EU egész területén. Ez elősegíti a fogyasztói bizalom növekedését, valamint megkönnyíti a vállalkozások számára az innovatív termékek forgalmazását. A tanúsítási rendszerek három megbízhatósági szinten működnek, és habár jellemzően önkéntesek, egységes szabályozási keretet teremtenek az IKT-termékek és -szolgáltatások számára. A rendelet emellett jelentősen megerősíti az Európai Hálózat- és Információbiztonsági Ügynökség szerepét, amely ettől kezdve állandó uniós kiberbiztonsági ügynökséggé vált. Az Ügynökség központi szerepet kapott a tanúsítási rendszerek kidolgozásában, a tagállamokkal és az uniós intézményekkel való együttműködésben, valamint a kiberbiztonsági gyakorlatok szervezésében. Az ENISA ezáltal nemcsak szakmai támogatást nyújt, hanem a kiberbiztonsági politika végrehajtásának egyik fő koordinátorává is vált az Európai Unión belül. (Fontos megemlíteni, hogy az ENISA már a 2016-os, a hálózati és információs rendszerek biztonságáról szóló NIS irányelv végrehajtásában is központi szerepet kapott mint a tagállami intézkedések támogatásának fő uniós szereplője.)[37]

„Ez az a pont, ahol ki kell hangsúlyozni, hogy az EU kezdeti törekvései (2009–2015) az információbiztonságot kifejezetten a kibertámadások szemszögéből közelítették meg. A legtöbb dokumentum preambuluma azokkal az eseményekkel támasztotta alá az intézkedések szigorításának, vagy következetesebbé tételének szükségességét, amelyek kibertámadásokként kerültek a köztudatba. 2016 után – már a NIS irányelvben – azonban változott ez a szinte kizárólagosnak tűnő trend, és egyre nagyobb figyelmet kapnak a technológiai, illetve humán erőforrás eredetű kockázatok, így azok kezelésének igénye is. A kiberbiztonsági jogszabály által megteremtett, a kiberbiztonsági tanúsítási keretrendszer is kifejezetten ezt a célt szolgálja."[38]

[34] Molnár 2019.
[35] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete.
[36] A tanúsítás igazolja, hogy az eszköz megfelel a meghatározott kiberbiztonsági követelményeknek, növeli a felhasználói bizalmat, és elősegíti a piacra jutást.
[37] Az Európai Unió Tanácsa 2018.
[38] Bonnyai 2019: 70.

A 2019 májusában az Európai Unió Tanácsa által kiadott, az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló rendelet[39] célzott korlátozó intézkedések bevezetését teszi lehetővé az EU-t vagy tagállamait érintő, jelentős hatású kibertámadásokkal szemben, különösen akkor, ha azok külső, nem uniós szereplőktől származnak. A rendelet meghatározza, mit ért az EU kibertámadás alatt, és különösen veszélyesnek minősíti azokat az eseteket – többek között –, amelyek kritikus infrastruktúrát, alapvető szolgáltatásokat nyújtó szervezetek, kritikus állami funkciókat vagy uniós intézményeket érintenek. Meghatározza továbbá azon tényezőket, amelyek alapján egy kibertámadás jelentős hatásúnak minősíthető (az előidézett zavar hatóköre, súlyossága, EU-s országok érintettsége stb.). A tagállamok feladata a szankciók végrehajtása, amelyek között beutazási tilalom és vagyonbefagyasztás is szerepelhet.

A rendeletben foglalt meghatározások – különösen a kibertámadás fogalma és annak lehetséges célpontjai, mint a kritikus infrastruktúrák és alapvető szolgáltatásokat nyújtó szervezetek – kulcsszerepet játszanak az Európai Unió kiberbiztonsági szemléletének átalakulásában. E fogalmak nemcsak a szankciópolitika keretében váltak meghatározóvá, hanem a megelőzés és az ellenálló képesség fejlesztése terén is új irányt szabtak. E szemléletváltás nyomán született meg a NIS2 irányelv, amely már nemcsak a fenyegetésekre adott válaszokra, hanem az átfogó kockázatkezelésre, a kritikus szereplők védelmére és az egységes, erősített kiberbiztonsági szabályozásra is hangsúlyt helyez.[40]

Az online tér komplexitása, a gyorsan változó fenyegetési környezet, valamint a globális összekapcsoltság miatt a kiberbiztonság immár nem izolált kérdés, hanem az információs hadviselés, a geopolitikai konfliktusok és a nemzetbiztonsági stratégiák szerves része.[41] Az Európai Unió NIS2 irányelve, amely kiberbiztonsági tudatosságra és felelősségvállalásra ösztönzi a tagállamokat és az érintett szereplőket, ebben az összefüggésben alapvető keretet biztosít, de nem elegendő az egyre kifinomultabb fenyegetésekkel szemben.

Az előzőleg részletezett kockázatok, különösen az aktuális kiberbiztonsági trendek és a társadalmak polarizálása egyértelművé teszik, hogy a digitális világban tapasztalható kihívások mindennapjaink meghatározó elemeivé váltak. Ezek a fenyegetések megkövetelik, hogy az egyének, a vállalatok és az állami szereplők egységes válaszokat adjanak, amelyek technológiai, stratégiai és társadalmi szinten is megállják a helyüket.

Tehát ezen fenyegetésekre válaszul született meg az Európai Unió egyik legfontosabb kiberbiztonsági jogforrása, a NIS2 irányelv. A szabályozás kiemelt jelentőségét az adja, hogy nem pusztán technológiai megoldásokat céloz meg, hanem a társadalmi tudatosságot is alapvető elemmé teszi a kiberbiztonság erősítése érdekében. Ez különösen fontos a közösségi média által nyújtott lehetőségek és veszélyek tükrében, hiszen ezek a platformok egyszerre szolgálnak a tudatosítás eszközeként és a kockázatok forrásaként. A dezinformációval és a manipulációval szembeni ellenálló képesség megteremtéséhez nem elegendők a technikai intézkedések; szükség van

[39] A Tanács (EU) 2019/796 rendelete.
[40] Vandezande 2024.
[41] Farkas–Kelemen 2023.

a felhasználók képzésére, a szervezetek kiberbiztonsági felkészültségének növelésére és a fenyegetések gyors felismerésére. Ebben a kontextusban kulcsfontosságú, hogy a szabályozások és az azokból fakadó intézkedések segítségével növekedjen az egyének és a szervezetek ellenálló képessége. Az ilyen intézkedések egyaránt szolgálják az egyéni és a kollektív biztonságot, miközben hozzájárulnak egy fenntarthatóbb és ellenállóbb digitális ökoszisztéma kialakításához. A kiberbiztonság jövőjének megteremtése érdekében elengedhetetlen, hogy a tudatosítás és a védekezési képességek fejlesztése a társadalmi és gazdasági stabilitás megőrzésének középpontjában álljon.

Az Európai Unió 2022/2555 számú irányelve, közismert nevén a NIS2 irányelv, a hálózati és információs rendszerek kiberbiztonságára vonatkozó átfogó szabályozási keretet határoz meg. Célja, hogy az EU tagállamaiban egységesen magas szintű kiberbiztonságot biztosítson, miközben a tagállamok számára kötelezővé teszi a kiberbiztonsági képességek fejlesztését, a kockázatkezelési mechanizmusok bevezetését, valamint a jelentéstételi kötelezettségek teljesítését. Az irányelv kiterjedt együttműködési keretet hoz létre a tagállamok és az Európai Unió különböző intézményei között, ezzel elősegítve a hatékony információcserét és a kockázatelemzésen alapuló operatív válaszadást a kiberfenyegetésekre.[42]

Az irányelv fő fókuszában a kritikus infrastruktúrák és azon ágazatokban működő szervezetek állnak, amelyek kiemelt szerepet játszanak az európai társadalom és gazdaság működésében. Az I. melléklet alapján a NIS2 szabályai az energia-, a közlekedési, az egészségügyi és a digitális infrastruktúrára, a közigazgatásra vagy a világűrre is kiterjednek. A II. melléklet további ágazatokat határoz meg, például a posta- és futárszolgálatokat, az élelmiszer-termelés, -feldolgozást és -forgalmazást, a gyártást, a digitális szolgáltatókat, valamint a kutatóhelyek kiberbiztonsági védelmét. További fontos kitétel, hogy az irányelvet azon, az I. vagy a II. mellékletben szereplő állami és magánszervezetekre kell alkalmazni, amelyek középvállalkozásnak minősülnek, vagy ennél nagyobb méretűek a 2003/361/EK[43] ajánlás alapján, és az Európai Unión belül nyújtanak szolgáltatásokat vagy végeznek tevékenységeket. Szükséges megemlíteni, hogy az irányelv hatálya bizonyos esetekben a szervezetek méretétől függetlenül is érvényes, többek között nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy nyilvánosan elérhető elektronikus hírközlési, bizalmi szolgáltatók, legfelső szintű doménnév-nyilvántartók és doménnévrendszer-szolgáltatók, vagy az egyetlen szolgáltató egy tagállamban olyan szolgáltatás esetében, amely elengedhetetlen kritikus társadalmi vagy gazdasági tevékenységek fenntartásához.

Az irányelv I. és II. mellékletében szereplő ágazatokban működő szervezetekről, valamint a doménnév-nyilvántartási szolgáltatásokat biztosító szervezetekről minden tagállamnak nyilvántartást kell vezetnie, amit első körben 2025. április 17-ig szükséges megvalósítani és ezt a listát az Európai Unió kijelölt szervei számára megküldeni, majd a meghatározott határidőt követően rendszeresen, de legalább kétévente felül kell vizsgálni ezen nyilvántartást, és szükség esetén aktualizálni.

Az irányelv értelmében minden tagállamnak nemzeti kiberbiztonsági stratégiát kell kialakítania, amely átfogóan szabályozza a releváns érintettek felelősségi köreit,

[42] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve.
[43] Az EU Bizottságának ajánlása – a mikro-, kis- és középvállalkozások meghatározása; Melléklet, I. cím, 2. cikk.

a sérülékenységek kezelését, valamint az ellátási láncok biztonságát. E stratégia szerves része a polgárok és a szervezetek kiberbiztonsági tudatosságának növelése, valamint az oktatás és a képzés fejlesztése. Az irányelv célja, hogy a tagállamok a technológiai innováció és a fenyegetésekre való reagálás szintjén egyaránt egységes kiberbiztonsági keretrendszert valósítsanak meg.

A számítógép-biztonsági eseményekre reagáló csoportok központi szerepet töltenek be a kiberbiztonsági események kezelésében. Az irányelv előírja, hogy a CSIRT-ek biztosítsák a kiberfenyegetések és sérülékenységek valós idejű nyomon követését, valamint a riasztások és előrejelzések közel valós időben történő kiadását. Emellett technikai segítséget nyújtanak a hálózati rendszerek proaktív vizsgálatával és a sérülékenységek azonosításával. A nemzeti CSIRT-ek között létrejött hálózat elősegíti a tagállamok közötti gyors információcserét és az operatív szintű együttműködést. Az ENISA, az EU kiberbiztonsági ügynöksége európai szintű sérülékenység-adatbázist hoz létre, amely biztosítja a kiberbiztonsági események közös értelmezését és a sérülékenységek nyilvános közzétételét.

A stratégiai együttműködést egy külön csoport is támogatja, amely a tagállamok, az Európai Bizottság és az ENISA képviselőiből áll. Ez a csoport koordinálja az uniós szintű információcserét, és részt vesz a nagyszabású kiberbiztonsági események és válságok kezelésében. Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (European Cyber Crisis Liaison Organisation Network, EU-CyCLONe) operatív szintű válságkezelési feladatokat lát el, biztosítva a folyamatos információáramlást az EU tagállamai között.

A NIS2 irányelv átfogó szabályozási keretet biztosít az alapvető és fontos szervezetek kiberbiztonsági kockázatainak kezelésére, különösen a tagállami illetékes hatóságok által végzett célzott ellenőrzések és felügyeleti tevékenységek révén. Az irányelv 32. és 33. cikke részletezi a kiberbiztonsági szabályok betartatásához szükséges mechanizmusokat, amelyek közé a helyszíni vizsgálatok, a célzott biztonsági ellenőrzések és a jogsértések szankcionálása is sorolható. Fontos kiemelni tehát, hogy a tagállamok illetékes hatóságainak hatáskörébe tartozik, hogy az alapvető és fontos szervezeteknél rendszeres és célzott biztonsági ellenőrzéseket végezzenek. Ezeket a vizsgálatokat képzett szakembereknek szükséges lefolytatni, és tartalmazhatnak helyszíni ellenőrzéseket, távoli felügyeleti intézkedéseket, valamint kockázatalapú biztonsági vizsgálatokat. Az ellenőrzések alapját a szervezetek által végzett kockázatelemzések, vagy más rendelkezésre álló kockázati információk adják, amelyek biztosítják az objektivitást és a megkülönböztetésmentes eljárást.

Kiemelésre érdemes információ, hogy a célzott biztonsági ellenőrzéseket független szerv is elvégezheti az egyes tagállamokban. Az ilyen ellenőrzések költségeit általában az ellenőrzött szervezet viseli, kivéve, ha az illetékes hatóság indokolt esetben másként rendelkezik. Az ellenőrzések eredményeit az illetékes hatósághoz kell benyújtani, amely ezek alapján további intézkedéseket kezdeményezhet, például hiányosságok orvoslását, biztonsági szabályzatok frissítését vagy kiberbiztonsági politikák módosítását. Az irányelv szerint a célzott biztonsági ellenőrzések és az illetékes hatóság által végzett felügyeleti tevékenységek kulcsfontosságúak az egységes kiberbiztonsági szint megvalósításában az Európai Unión belül. Ezek az eszközök nemcsak a meglévő hiányosságok azonosítását és megszüntetését teszik lehetővé, hanem

hosszú távon növelik a kritikus infrastruktúrák és szervezetek ellenálló képességét is. Az ilyen mechanizmusok biztosítják, hogy az Unió kiberbiztonsági szabályai minden tagállamban egységesen érvényesüljenek, miközben a társadalmi és gazdasági stabilitást is elősegítik.

Mindeközben: Magyarország kiberbiztonsága

A nemzeti szintű kiberbiztonsági szabályozás Magyarországon az uniós folyamatokkal párhuzamosan indult el. 2013-ban elfogadták az ország első átfogó stratégiáját a kiberbiztonság területén,[44] amely megalapozta az állami és önkormányzati szervek elektronikus információbiztonságára vonatkozó jogi keretrendszer kialakítását. Ennek részeként jött létre az a törvényi szabályozás, amely nemcsak az érintett szervek kötelezettségeit rögzítette, hanem elindította az információbiztonsági szervezetrendszer kiépítését is.

A szabályozás fejlődésével és a gyakorlati tapasztalatok alapján 2015-ben sor került az intézményrendszer részleges központosítására: megalakult a központi hatóságként működő nemzeti intézmény, a Nemzetbiztonsági Szakszolgálaton belül működő Nemzeti Kibervédelmi Intézet (a továbbiakban: NBSZ NKI), amely az állami és a piaci szereplők számára egyaránt illetékes az információ- és hálózatbiztonság területén. Ez a szerv vette át a korábbi eseménykezelési feladatokat, egyúttal képviseli Magyarországot az uniós kiberbiztonsági együttműködésekben is. A kiberbiztonsági védelem külön területeit további, speciális feladatkörrel rendelkező szervezetek látják el – ilyenek például a honvédelmi rendszerekért vagy az állami létfontosságú infrastruktúrákért felelős egységek. A működésükre vonatkozó részletszabályokat egy külön kormányrendelet rögzíti. A hazai stratégiai gondolkodás a nemzetközi szabályozási környezethez igazodva folyamatosan frissül: a korábbi uniós irányelvek nyomán új, a korszerű fenyegetésekre reflektáló nemzeti stratégiák születtek, amelyek megalapozzák Magyarország hosszú távú kiberbiztonsági célkitűzéseit és cselekvési irányait.

A magyar kibertér jogi szabályozásának első mérföldkövét a 2013. április 15-én elfogadott törvény jelentette, amely az állami és önkormányzati szervek elektronikus információinak védelmét helyezte középpontba.[45] Már elnevezésében is egyértelművé teszi, hogy kizárólag az elektronikus információbiztonság területére vonatkozik, és célzottan az állami intézmények információs rendszereit kívánja védeni. A jogszabály olyan átfogó keretet teremt, amely megelőzésre épülő, rendszerszintű védelmet nyújt a teljes elektronikus információs infrastruktúra számára, különös figyelmet fordítva a fenyegetések azonosítására és a tudatosság növelésére. Az alapelvek mentén a szabályozás célja a biztonsági kockázatok megelőzése, valamint a bekövetkező események szakszerű és tudatos kezelése. Az Ibtv. már a preambulumában hangsúlyt helyez a megelőzésre, a védelemre, a biztonságra és a tudatosság növelésére, amelyek a jogszabály alapelveit képezik. A törvény kiemeli a nemzeti elektronikus adatvagyon, valamint a létfontosságú információs rendszerek biztonságának fontosságát, utalva

[44] 1139/2013. (III. 21.) Korm. határozat.
[45] 2013. évi L. törvény.

arra, hogy ezek védelme társadalmi elvárás. A jogszabály részletesen meghatározza az információbiztonság kulcsfogalmait, mint a bizalmasság, a sértetlenség és a rendelkezésre állás. Ezek az alapelvek biztosítják, hogy az adatokhoz csak jogosultak férhessenek hozzá (bizalmasság), azok hitelesek és eredetük igazolható legyen (sértetlenség), illetve az információs rendszerek folyamatosan elérhetők maradjanak az arra jogosultak számára (rendelkezésre állás). A védelmi intézkedések tervezésénél alapvető elv, hogy azoknak a kockázatokkal arányosan kell megvalósulniuk – vagyis a védelemre fordított erőforrásoknak összhangban kell lenniük a lehetséges károk mértékével. Az Ibtv. ennek megfelelően már a fogalmi keretében is hangsúlyosan kezeli a védelem különböző típusait, és pontosan meghatározza azok tartalmát.[46] Az Ibtv. hozzájárult a 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégiában megfogalmazott kormányzati célok és intézkedések megvalósításához, valamint a kapcsolódó szervezeti feladatok gyakorlati alkalmazásához.

A 2013. évi L. törvény, amely Magyarországon elsőként teremtette meg a kiberbiztonság jogszabályi kereteit, egy adott történeti és technológiai kontextusra reflektált, és elsősorban az állami elektronikus információs rendszerek védelmére fókuszált. Az elmúlt évtized technológiai fejlődése, valamint az Európa-szerte egyre gyakoribb és komplexebb kibertámadások azonban új típusú kihívásokat generáltak, amelyek túlnőttek a korábbi szabályozás keretein. A kiberbiztonság társadalmi, gazdasági és nemzetbiztonsági jelentősége számottevően megnőtt, mindezt pedig az Európai Unió NIS2 irányelve is tükrözi, amely a tagállamoktól átfogó, szektorokon átívelő és egységes szabályozást követel meg. E körülmények tették indokolttá egy új, korszerű és strukturált törvényi szabályozás megalkotását, amelyet a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény testesít meg. Ez a jogszabály a korábbi törvények hatályon kívül helyezésével és az uniós előírások integrálásával új alapokra helyezi Magyarország kiberbiztonsági rendszerét.

A Kibertv. Magyarország új, egységes és korszerű jogszabálya, amely 2025. január 1-jén lépett hatályba, és a nemzeti kiberbiztonság szabályozási kereteit átfogóan újraszabályozta. A jogszabály célja az elektronikus információs rendszerek védelmének megerősítése, különös tekintettel azokra a szervezetekre, amelyek tevékenysége kiemelt jelentőségű az állam, a gazdaság és a társadalom működése szempontjából. A törvény a korábbi kiberbiztonsági jogszabályokat – így többek között az Ibtv.-t és a Kibertantv.-t[47] – hatályon kívül helyezi, és egyetlen átfogó keretbe integrálja a releváns előírásokat, összhangban az Európai Unió NIS2 irányelvével.

A törvény hatályát a szervezetek típusán, tevékenységi körén és méretén alapuló besorolás szerint határozták meg. A hatály alá tartoznak mindenekelőtt az állami szervek és szervezetek, a többségi állami befolyás alatt álló gazdasági társaságok, valamint a NIS2 irányelvben meghatározott ágazatokban működő szervezetek, amennyiben megfelelnek a középvállalkozásokra vonatkozó küszöbértékeknek. Mindezek mellett az NBSZ NKI nemzeti kiberbiztonsági hatóságként jogosult további szervezetek azonosítására és bevonására is, ha azok tevékenysége alapján ez indokolt. A szervezetek

[46] Bodó 2014.
[47] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és kiberbiztonsági felügyeletről.

„alapvető" vagy „fontos" kategóriába sorolása a törvény erejénél fogva történik, a vezetők felelőssége pedig a hatály meghatározása és a kötelezettségek teljesítése.

A kiberbiztonsági hatósági feladatokat a jogszabály hatálybalépésétől kezdve négy intézmény látja el: a közigazgatási ágazat, valamint az állami működés szempontjából kiemelt jelentőséggel bíró szervezetek vonatkozásában az NBSZ NKI; a banki szolgáltatások és a pénzügyi piaci infrastruktúrák, valamint a közigazgatási ágazat kivételével a NIS2 irányelv szerinti ágazatokban a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH); a honvédelmi célú elektronikus információs rendszerek tekintetében a honvédelemért felelős miniszter; a banki szolgáltatások és a pénzügyi piaci infrastruktúrák vonatkozásában a Magyar Nemzeti Bank.

A törvény kulcsszerepet játszik az Európai Unió NIS2 irányelvének hazai implementációjában. Ez az irányelv új szintre emeli a kiberbiztonság uniós szabályozását, kiterjesztve a kötelezettségek körét, megerősítve a felügyeleti mechanizmusokat, valamint szigorúbb biztonsági követelményeket állítva a köz- és a magánszféra számára. A magyar jogalkotó ezt figyelembe véve egy központosított, egységes törvényi keretet alkotott, amely a NIS2 előírásait szervezeti szintre bontja le. A Kibertv. átfogó és strukturált válasz Magyarország részéről az egyre komplexebb kiberbiztonsági fenyegetésekre, és egyben megfelel az uniós elvárásoknak is. A hatálya alá tartozó szervezetek pontos meghatározása és a kijelölt hatóságok szerepének tisztázása elősegíti a hatékony jogalkalmazást és a kibertér védelmének erősítését.

Jogszabályi ív: a 2013. évi L. és a 2024. évi LXIX. törvény összevetése

A digitális környezet gyors átalakulása új kihívások elé állította a kiberbiztonsági szabályozást Magyarországon is. A 2013. évi L. törvény lefektette a nemzeti információbiztonság alapjait, de az elmúlt évtized technológiai és geopolitikai változásai szükségessé tették egy új, komplex szabályozási rendszer bevezetését. Ezt valósítja meg a 2024. évi LXIX. törvény, amely már az egész társadalomra és gazdaságra kiterjedő kiberbiztonsági keretrendszert nyújt.

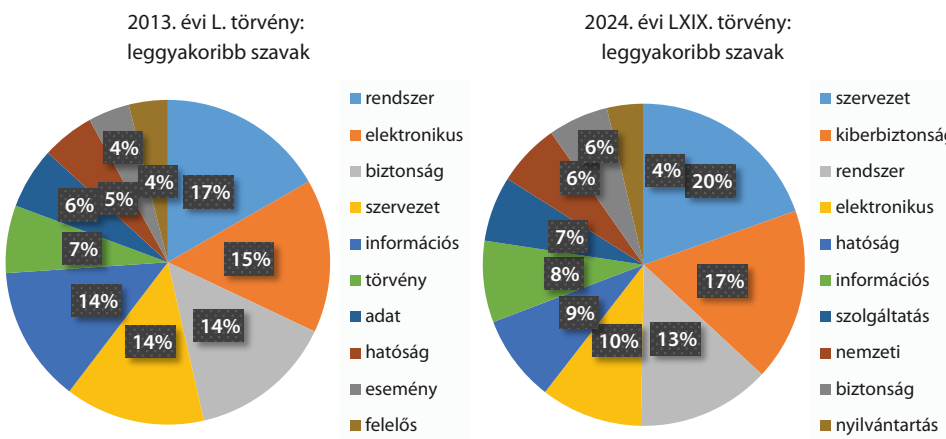
A két szabályozás közötti különbségek nem csupán terjedelmi vagy technikai, hanem strukturális és stratégiai szinten is érzékelhetők. Jelen tanulmány legfőbb célja e két törvény összehasonlító elemzése: feltárni, hogy miként változott a kiberbiztonság definíciója, az alkalmazási kör, a fogalomhasználat, valamint a szabályozás fókusza. Az elemzés kiterjed a kulcsszavak gyakoriságára, a jogszabályok szerkezeti és tematikai klasztereire, valamint a szabályozás mögötti hatósági és auditmechanizmusokra is.

Az Ibtv. jogalkotási célja az elektronikus információs rendszerek védelme volt az állami és önkormányzati szférában. E törvény főként az állami szféra – közigazgatási, igazságügyi és honvédelmi szervek – elektronikus rendszereinek biztonságát kívánta megerősíteni. A jogszabály hatálya szűk, jól körülhatárolt maradt, nem terjedt ki a magánszektor szereplőire vagy a kritikus infrastruktúrákra. Ezzel szemben a Kibertv. hatóköre jelentősen bővült. A szabályozás már nemcsak az állami és önkormányzati szektor intézményeire, hanem gazdasági szereplőkre – így többek között az energia-, víz- és közlekedési szektorra, hírközlési szolgáltatókra, digitális infrastruktúrákra, gyártói tevékenységekre – is kiterjed.

A 2013-as törvény idején nem volt cél az uniós jogharmonizáció. A szabályozás egyértelműen nemzeti keretek között készült, a belső állami struktúrák megerősítésére irányult. Ezzel szemben a 2024-es törvény megalkotásának egyik alapvető célja az EU-s NIS2 irányelv implementációja volt. A harmonizációval Magyarország egy olyan egységesített, európai szinten elvárt kiberbiztonsági ökoszisztémához csatlakozott, amely megköveteli a kockázatalapú szemlélet, az auditálható működés és az incidensmenedzsment alkalmazását. A törvény immár stratégiai célként határozza meg a kiberfenyegetések elleni nemzeti védekezést, amelynek részei a nemzeti kiberbiztonsági hatóság megerősítése (fogalmi szinten létrehozása), a tanúsítási és megfelelőségi rendszerek bevezetése, valamint a nemzetközi együttműködés szabályozása.

A szógyakorisági elemzés szintén jól tükrözi a két szabályozás fókuszainak és nyelvi karakterének változásait. Az elemzés során külön figyelmet kaptak az úgynevezett stop-word listán szereplők szavak kivételével a leggyakrabban előforduló kulcsszavak, valamint azok n-gram típusú előfordulási mintázatai (például bigramok, trigramok).

A 2013-as törvényben a leggyakoribb szavak csökkenő sorrendben a „rendszer", „elektronikus", „biztonság", „szervezet", „információs" voltak. Ezek a technikai és intézményi védelemre, valamint az állami szervezeti struktúrákra utaltak. Ezzel szemben a 2024-es törvény nyelvezetében erőteljesen dominálnak az alábbi szavak: „szervezet", „kiberbiztonság", „rendszer", „elektronikus", „hatóság", de a szókészlet szempontjából gyakorinak számítanak az olyan szavak, mint a „tanúsítás", „megfelelőség", „incenskezelő" és „szolgáltatás". Ezek a szavak nemcsak gyakoribbak lettek, de új szemléletet is tükröznek: az állami irányítás helyett az auditálható működés, a szolgáltatások folytonossága és a felügyeletre épülő ökoszisztéma került a középpontba (2. ábra).



2. ábra: A 2013. évi L. és a 2024. évi LXIX. törvény leggyakoribb szavai
Forrás: a szerző szerkesztése

A „védelmi" szócsalád (például védelem, védelme, védelmének) előfordulása a 2024-es törvényben több mint háromszoros a 2013-ashoz képest. Ez mutatja, hogy a védekezési mechanizmusok nemcsak gyakoribbak, hanem részletesebben is szabályozottak lettek. Figyelemre méltó a „kiberbiztonság" szó markáns szerepe a Kibertv.-ben, a szó

előfordulása több mint hetvenszeres az Ibtv.-hez képest. Jól látható, hogy a „kiberbiztonság" fogalma és annak hangsúlya jelentősen megnőtt az újabb szabályozásban, az egész törvény fókusza kifejezetten erre a témára épül. Ezzel szemben a 2013-as törvény inkább az elektronikus információs rendszerek biztonságáról szól általánosságban, és a „kiberbiztonság" fogalma kevésbé központi. A „kiberbiztonság" kifejezés gyakoriságának növekedése nem pusztán nyelvi vagy terminológiai változás, hanem egy mélyebb átalakulás jele: a digitális tér védelme stratégiai nemzetbiztonsági és gazdaságpolitikai kérdéssé vált. A 2024-es törvény ezt a paradigmaváltást tükrözi, és célja, hogy strukturáltabb, egységesebb, valamint hatékonyabb választ adjon a 21. század kibertérből érkező kihívásaira. Fontos továbbá, hogy a „kiberbiztonság" kulcsszó dominanciája annak is köszönhető, hogy a törvény célja immár nem pusztán az információbiztonság technikai aspektusainak szabályozása, hanem egy egységes, kockázatalapú, hatóságilag (is) ellenőrzött kiberbiztonsági rendszer létrehozása. A törvény emellett közvetlenül hivatkozik a NIS2-re, ami szintén hangsúlyosabbá teszi a kiberbiztonság stratégiai fontosságát.

Mindezek mellett, ha a szavak gyakoriságát vizsgáljuk, akkor látható, hogy a „szervezet" és a „szerinti" szavak használata szintén ugrásszerűen nőtt a Kibertv.-ben, ami a jogalanyok pontosabb, kategorizált (alapvető/fontos) szabályozására utal. A „nemzeti" és „hatóság" szavak sokkal gyakoribb használata mutatja, hogy 2024-re erőteljesebben és komplexebben jelent meg a nemzeti hatósági struktúra a hazai kiberbiztonsági szegmensben.

Az előzőket figyelembe véve megállapítható, hogy a 2024. évi törvény jóval szélesebb hatókört ölel fel, mint a 2013-as elődje. Míg utóbbi kizárólag az állami és önkormányzati szervek elektronikus információbiztonságát szabályozta, az új jogszabály az egész társadalmi-gazdasági környezetre, beleértve a magánszektort is, kiterjeszti a szabályozást. Ez önmagában indokolja a „szolgáltatás" és „szolgáltató" kifejezések gyakori megjelenését, hiszen a törvény – többek között – a többségi állami befolyással működő és kritikus infrastruktúrákat üzemeltető vállalatok mellett kiterjed számos kiemelten kockázatos (például energetika, egészségügy és hírközlési szolgáltatások) és kockázatos ágazatban (például élelmiszeripar, gyártás, digitális szolgáltatások) működő gazdasági társaságra is.

Összességében tehát a szavak gyakorisági különbségei azt tükrözik, hogy a 2024-es jogszabály nemcsak terjedelmében, hanem komplexitásában és stratégiai célkitűzéseiben is jóval előrébb tart, mint a 2013-as verzió. Ez pedig a kulcsszavak súlyozásában is markánsan megmutatkozik.

A két szabályozás eltérő nyelvezete, fogalomhasználata és tematikus fókusza azt mutatja, hogy miként alakult át az információbiztonság technikai megközelítéséből egy átfogó, stratégiai szemléletű kiberbiztonsági keretrendszerré. Az Ibtv. főként a „bizalmasság, sértetlenség, rendelkezésre állás" hármas védelmi célra épülő, alapvetően információbiztonsági szemléletet tükrözi. A törvény célja a fogalmi keretek meghatározása, a szabályozási alapok lefektetése, a közigazgatási és önkormányzati rendszerek biztonságának megalapozása, az elektronikus információs rendszerek osztályba sorolása, valamint a védelmi szintek szabályozása volt. Az elemzett bigramokban olyan kifejezések domináltak, mint az „elektronikus információs", „információs rendszer" vagy a „biztonsági osztály" (1. táblázat).

Ezzel szemben a Kibertv. szókészlete már egy kiterjesztett, nemzetstratégiai szemléletet tükröz, ahol megjelenik a központosított irányítás, hatósági ellenőrzés és a digitális szuverenitás fogalma is. A 2024-es törvény már nem csupán a technikai védelmet célozza meg, hanem egy szélesebb, nemzetbiztonsági és stratégiai szintre emelt kiberbiztonsági keretrendszert vezet be. A hangsúly a „kiberbiztonság" fogalom köré szerveződik, és – néhány bigram még markánsabb előfordulása mellett – megjelentek olyan új elemek, mint az „incidenskezelő központok", a „tanúsítási rendszerek" vagy a „kiberbiztonsági hatóság". A nyelvezet erősebben utal állami szabályozásra, központosított reakciómechanizmusokra és az EU-s harmonizációra.

A „poszt-kvantumtitkosítás" bigram mind a 2013-as, mind a 2024-es magyar kiberbiztonsági törvényben hasonló gyakorisággal szerepel, ám eltérő funkcióval. A 2013-as törvényben a kifejezés előrelátó módon, jövőorientált technológiai tudatosságként jelenik meg, a kvantumszámítógépek okozta lehetséges fenyegetésekre reagálva. Ezzel szemben a 2024-es törvény már konkrét szabályozási tartalommal ruházza fel: kijelöli az alkalmazásra kötelezett szervezetek körét, meghatározza az intézményi felügyeletet (SZTFH), és részletezi az alkalmazás módját. A bigram statisztikai gyakoriságának hasonlósága mögött tehát tartalmi fejlődés húzódik meg: a korábbi elvi megközelítés mára gyakorlati, intézményesült védelemmé vált, amely a digitális szuverenitás megőrzésének egyik sarokköve lett. A „poszt-kvantumtitkosítás" bigram hasonló gyakoriságú jelenléte tehát nem a technológiai stagnálásra, hanem inkább egy konzisztens, hosszú távú szabályozási gondolkodásra utal. A magyar jogalkotás már 2013-ban érzékelte a kvantumfenyegetés lehetőségét, és a 2024-es törvényben már intézményes szinten szabályozza is azt. Ez egyben azt is jelzi, hogy a kiberbiztonsági szakpolitika nemcsak reaktív, hanem proaktív is: felkészülés történik azokra a technológiai áttörésekre, amelyek jelenleg még nem okoznak tömeges problémát, de a jövőben alapjaiban rengethetik meg a digitális infrastruktúrák biztonságát.

1. táblázat: A leggyakoribb bigramok

Bigram	2013. évi L. tv.	2024. évi LXIX. tv.	Eltérés
elektronikus információs	155	256	+101
információs rendszer	155	241	+86
nemzeti kiberbiztonság	0	175	+175
kiberbiztonsági hatóság	0	149	+149
kiberbiztonsági incidenskezelő	0	114	+114
rendszerbiztonság	36	65	+29
biztonsági osztály	27	64	+37
incidenskezelő központ	0	86	+86
kiberbiztonsági incidens	0	86	+86
poszt-kvantumtitkosítás	28	36	+8
kiberbiztonsági tanúsítás	0	55	+55
Összesen	401	1327	926

Forrás: a szerző szerkesztése

A 2013. évi L. törvény és a 2024. évi LXIX. törvény szövegének kvantitatív tartalomelemzése a bigramok és trigramok gyakoriságának összehasonlításával jól érzékelteti a magyar kiberbiztonsági szabályozás fejlődését. A bigramelemzés eredményei alapján megállapítható, hogy 2024-re jelentősen megnőtt az olyan kifejezések előfordulása, mint az „elektronikus információs" (+101), az „információs rendszer" (+86) és a „rendszerbiztonság" (+29). Emellett új, 2013-ban még nem szereplő, de 2024-re domináns bigramok jelentek meg, például „nemzeti kiberbiztonság" (175 előfordulás) és „kiberbiztonsági hatóság" (149 előfordulás), jelezve a kiberbiztonság önálló szakpolitikai területté válását.

A trigramok összehasonlítása még markánsabban mutatja a tematikai váltást (2. táblázat). A 2013-as törvény kulcsszavai egy még épülő információbiztonsági keretrendszert jeleztek, míg a 2024-es törvény kifejezései egy beérett, stratégiai irányítás alá vont kiberbiztonsági ökoszisztémát rajzolnak ki. 2024-ben a gyakori trigramok között már szerepel a „kiberbiztonság incidenskezelő központ", „nemzet kiberbiztonság hatóság" is.

2. táblázat: A leggyakoribb trigramok

Trigram	2013. évi L. tv.	2024. évi LXIX. tv.	Eltérés
elektronikus információs rendszer	151	240	+89
információs rendszer biztonsága	36	59	+23
kiberbiztonsági incidenskezelő központ	0	86	+86
nemzeti kiberbiztonsági hatóság	0	72	+72
biztonságért felelős személy	19	40	+21
poszt-kvantumtitkosítás alkalmazás	23	30	+7
biztonsági osztályba sorolás	16	34	+18
kiberbiztonsági tanúsítási rendszer	0	37	+37
információs rendszer védelme	15	18	+3
informatikáért felelős miniszter	0	28	+28
ideiglenes hozzáférhetetlenné tétel	11	14	+3
Összesen	271	658	387

Forrás: a szerző szerkesztése

A trigramok elemzése megerősítette a bigramokból levont következtetéseket, ugyanakkor tovább részletezte az eltolódás mértékét. A legnagyobb növekedés a „nemzeti kiberbiztonsági hatóság" típusú összetett kifejezések körében figyelhető meg, amelyek közvetlenül az újonnan létrehozott intézményi és jogszabályi struktúrákra utalnak. A trigramok alapján nemcsak az általános információbiztonsági fókusz erősödése mutatkozik, hanem a kiberbiztonsági incidensek kezelésére, a tanúsítási rendszerek kiépítésére és a poszt-kvantumtitkosítási eljárásokra helyezett hangsúly is. Az új törvény egyik legmarkánsabb újítása a megfelelőségi és auditmechanizmusok bevezetése: míg a 2013. évi L. törvény csupán felügyelő és koordináló szerepkörrel ruházta fel az állami intézményeket, a 2024-es jogszabály részletes, szabványokon alapuló megfelelőségi struktúrát ír elő.

Összességében mind a bigram-, mind a trigramszintű kvantitatív elemzés azt bizonyítja, hogy a magyar kiberbiztonsági szabályozás a 2013–2024 közötti időszakban jelentős mértékben bővült, mélyült és specializálódott. Az új kifejezések számossága és előfordulási gyakorisága tükrözi a kiberfenyegetésekre adott szabályozási válaszok komplexitásának növekedését, valamint az európai uniós szabályozási harmonizáció hatását.

A dokumentumok tartalmi vizsgálata alapján mindkét törvény jól elkülöníthető klaszterekbe sorolható tematikusan (3. táblázat). Ezek a klaszterek nemcsak a jogszabályok szerkezetét, hanem azok szabályozási logikáját is tükrözik. A bigramok és trigramok elemzése különösen fontos volt a tematikus klaszterek azonosításában, mivel az egyszerű szavak szintjén nehezen megragadható fogalmi összefüggések – mint például az „eseménykezelő központ" vagy a „kiberbiztonsági incidenskezelő központ" – kizárólag a kifejezéspárok szintjén mutatták meg a jogszabályok hangsúlyeltolódását. Míg a 2013. évi szabályozás a szervezeti szintű felkészültség és védelem köré szerveződött, a 2024. évi törvény a kiberfenyegetésekre adott központi válaszok és a nemzeti hatósági struktúrák kiépítését állítja középpontba.

A 2013. évi L. törvény klaszterezési eredményei alapján három meghatározó tematikai egység rajzolódik ki. Az első klaszter a szervezeti hatály és alkalmazás témakörét öleli fel, amely a jogi szövegezés hagyományos logikáját követi: középpontjában az érintett szervezetek körének kijelölése, a különböző típusú állami és önkormányzati szervek beazonosítása, illetve az alkalmazási kör bekezdések szerinti strukturált bemutatása áll. A szöveg itt szigorúan normatív, a szereplők körének meghatározásán keresztül biztosítja a jogszabály érvényesülését. A második klaszter a kulcsfogalmak és rendszer-definíciók világára koncentrál, ahol az „elektronikus információs rendszer", „adatkezelő" és „adatfeldolgozás" fogalmai kiemelt jelentőséget kapnak. Ez a rész biztosítja a törvény technológiai és fogalmi alapjait, nélkülözhetetlen keretet adva a szabályozás többi részéhez. A harmadik klaszter a biztonsági események és osztályozás területét fedi le, amelyben a biztonsági események felismerése, osztályozása és kezelése kap hangsúlyt. Itt a cél az, hogy a rendszerbiztonság fenntartása érdekében a különböző típusú fenyegetésekre arányos és megfelelő válaszreakciók szülessenek.

A 2024. évi LXIX. törvény klaszterstruktúrája ehhez képest jelentős tematikus eltolódást mutat, ami a kiberbiztonság új dimenzióinak megjelenését tükrözi. Az első klaszter, a fogalmi alapok és technológia, továbbra is az elektronikus információs rendszerek jelentőségét emeli ki, ugyanakkor sokkal hangsúlyosabban jelenik meg a digitális szolgáltatások hálózati alapú értelmezése, valamint a szolgáltatási modellek átalakulása. A második klaszter egyértelműen az állami kontroll, incidenskezelés és tanúsítás köré épül: itt már nemcsak rendszereket, hanem intézményes mechanizmusokat szabályoznak, például a nemzeti kiberbiztonsági hatóság, valamint egy új hatósági szereplő, az incidenskezelő központok és a tanúsítási rendszerek kiemelésével. A harmadik klaszter új tematikai súlypontként a kockázatkezelés és audit témáját fejleszti ki, amely a megfelelőségértékelési rendszerek, szervezeti auditok és kiberkockázatok tudatos kezelését állítja középpontba. Ez a változás a nemzetközi szabályozási környezet fejlődésével is összhangban van, és a kockázatalapú megközelítés elterjedését tükrözi.

3. táblázat: Tematikus klaszterek

Jogszabály	A klaszter neve	Kulcsszavak	Leírás
2013/L.	szervezeti hatály és alkalmazás	szervezet, szerinti, bekezdés, meghatározott, vonatkozó	hatálymeghatározás, szervezeti kör
2013/L.	alapfogalmak és rendszerdefiníció	elektronikus, információs, rendszer, rendszerek, adatkezelő	fogalmi alapok és technológiai keret
2013/L.	biztonsági események és osztályozás	biztonsági, esemény, osztályba, szint, kezelés	rendszerbiztonság és eseménykezelés
2024/LXIX.	fogalmi alapok és technológia	elektronikus, információs, rendszer, rendszerek, szolgáltatás	digitális infrastruktúra, szolgáltatási modell
2024/LXIX.	hatóság, incidenskezelés és tanúsítás	kiberbiztonsági, nemzeti, hatóság, incidenskezelő, tanúsítás	szabályozás, incidenskezelés
2024/LXIX.	kockázatkezelés és audit	kockázat, szolgáltató, megfelelőség, audit	kockázatmenedzsment, megfelelőségértékelés
Mindkét jogszabály esetén 3-3 klaszter határozható meg.			

Forrás: a szerző szerkesztése

A 2024-es kiberbiztonsági törvény jelentős tematikus elmozdulást tükröz a korábbi szabályozáshoz képest, amit a klaszterezési elemzés is világosan kirajzol. Míg a 2013-as törvény főként a szervezeti felkészültségre és a rendszerbiztonság általános irányelveire fókuszált, addig a 2024-es szabályozás központi elemei között a hatósági struktúrák kiépítése, az incidenskezelés intézményesítése és a tanúsítási mechanizmusok formalizálása szerepel.

Az új törvény alapján bevezetett auditálási rendszer előírja, hogy a meghatározott szolgáltatóknak független, akkreditált szervezetek által végzett kötelező auditokon kell átesniük, összhangban a „Kockázatmenedzsment, megfelelőségértékelés" klaszter tartalmával. Ezzel párhuzamosan létrejön egy központosított nemzeti kiberbiztonsági hatóság és egy további hatóság, amelyek a „Hatóság, incidenskezelés és tanúsítás" klaszter logikájának megfelelően széles jogosultságokkal felügyelnek, végeznek hatósági ellenőrzéseket, koordinálnak és szükség esetén szankcionálhatnak. Emellett a törvény immár részletesen szabályozza az incidenskezelési ciklust – a megelőzés, észlelés, reagálás és helyreállítás fázisait –, ami szintén tematikus súlypontot képez az új klaszterstruktúrában.

Összehasonlítva a két törvényt, megállapítható, hogy a magyar kiberbiztonsági szabályozás fejlődése során a kezdeti, technológiai alapú, rendszerközpontú megközelítést egy komplexebb, átfogóbb és szervezeti szintű kockázatmenedzsment-alapú modell váltotta fel. A klaszterezés eredményei azt mutatják, hogy míg 2013-ban az információbiztonsági rendszerek integritása és bizalmassága volt a központi kérdés, 2024-re a fókusz az incidenskezelés, a szabályozó hatóságok, a nemzeti ellenálló

képesség és az auditfolyamatok megerősítése irányába tolódott el. A szabályozási fejlődés nemcsak a technológiai környezet változását tükrözi, hanem az Európai Unió közös irányelveinek, valamint a globális kiberfenyegetettségre adott válaszoknak is megfelel. Összességében tehát a szabályozási fejlődés – ahogyan azt a klaszterelemzés is megerősíti – egyértelműen a kiberbiztonság átfogóbb, rendszerszintű megközelítése felé mutat, amely a nemzeti ellenálló képesség és a megfelelőség központi szerepét hangsúlyozza a globális fenyegetettségi környezet változásainak tükrében.

A 2013. évi L. törvény és a 2024. évi LXIX. törvény összehasonlítása világosan rávilágít a magyar kiberbiztonsági szabályozás fejlődési ívére: a technikai és szervezeti alapú védelemtől eljutottunk egy EU-konform, stratégiai szinten szervezett, teljes digitális ökoszisztémát lefedő szabályozási keretrendszerig.

Az Ibtv. célja az állami rendszerek alapvető információbiztonságának megteremtése volt. A fókusz elsősorban az elektronikus információs rendszerek fizikai és logikai védelmére, valamint az adatkezelési szabályozásra helyeződött. A fogalomhasználat stabil, de szűk spektrumú volt, kevésbé reagált az akkor már nemzetközileg is megjelenő új típusú fenyegetésekre és szolgáltatási modellekre. A Kibertv. ezzel szemben paradigmaváltást képvisel. Az EU NIS2 irányelvének implementálásával egy olyan korszerű, incidensalapú, auditálható és a nemzetközi követelményekhez illeszkedő szabályozási rendszert vezet be, amely már nem csupán az állami szférát, hanem a gazdasági szereplők és a kritikus infrastruktúrák teljes spektrumát lefedi. A 2024-es dokumentum retorikája és szókincse is változást tükröz: a „kiberbiztonság", „szolgáltató", „tanúsítás", „hatóság" és „incidens" kulcsszavak gyakorisága mutatja, hogy immár nemcsak a védelem hangsúlyos, hanem a kontroll, a reagálás, a megfelelőség és a stratégiai felügyelet is.

Összességében elmondható, hogy a 2024. évi LXIX. törvény egy modern, rugalmas, de egyben szigorú szabályozási eszköztárat ad a magyarországi kiberbiztonság intézményesített védelmére. Az összehasonlító elemzés jól demonstrálja, hogy a változások nemcsak tartalmi és jogi szinten, hanem a szabályozási filozófiában is érvényesülnek. Ennek értelmében a magyar kiberbiztonsági szabályozás fejlődése jól mutatja a digitális fenyegetésekre adott jogalkotói válaszok dinamikáját. Míg a 2013. évi L. törvény az információbiztonsági alapok lefektetését szolgálta, a 2024. évi LXIX. törvény már egy komplexebb, szektorokon átívelő, integrált megközelítést képvisel. Az SZTFH szerepe pedig azt mutatja, hogy a jövőbiztos technológiai megoldások alkalmazása központi elemévé vált a nemzeti kiberstratégiának. Ez a fejlődési ív jól tükrözi a nemzetközi trendeket és Magyarország digitális szuverenitás iránti elkötelezettségét.

Összegzés és diszkusszió

A magyar kiberbiztonsági szabályozás fejlődése világosan tükrözi azt az átalakulást, amelyet a globális digitalizáció és az Európai Unió szabályozási törekvései váltottak ki. A 2013. évi L. törvény egy korai szabályozási modellként szolgált, amely az állami és önkormányzati szervek elektronikus információinak védelmére koncentrált, szűk, infrastruktúra-központú megközelítést alkalmazva. Ezzel szemben a 2024. évi LXIX. törvény – szoros összhangban a NIS2 irányelv célkitűzéseivel – már egy integráltabb,

incidens- és kockázatkezelés-orientált, nemzeti és uniós szintű együttműködésre épülő rendszert valósít meg.

A kutatási kérdésre adott válasz során megállapítható, hogy a magyar kiberbiztonsági szabályozás szemlélete alapvetően megváltozott: az állami rendszerek szűk védelmétől egy olyan átfogóbb kiberbiztonsági ökoszisztéma irányába mozdult el, amelyben az állami és magánszektor szereplői egyaránt érintettek. A kockázatérzékenység, az incidensek gyors és hatékony kezelése, a szolgáltatásfolytonosság biztosítása, valamint a fenyegetések megelőzése váltak a szabályozás központi elemeivé.

A nyelvezetben szintén markáns elmozdulás figyelhető meg: míg a 2013. évi törvény terminológiája a technikai biztonsági intézkedésekre, rendszerleírásokra és az állami felelősségi körökre helyezte a hangsúlyt, addig a 2024-es törvény már a kockázatértékelés, incidenskezelés, kiberreziliencia, auditálhatóság és tanúsítás fogalmait állítja középpontba. A fogalmi gazdagodás a szabályozás mélyülését is tükrözi, hiszen az új szövegben megjelennek az ellátási lánc biztonságára, az emberi tényezőre, a folyamatos felügyeletre és az uniós szintű adatmegosztásra vonatkozó előírások is.

A szabályozási logika szintjén is jelentős átrendeződés történt: míg a 2013-as törvény inkább a szabályozott alanyok kötelezettségeire és az állami védelem fenntartására koncentrált, addig a 2024-es jogszabály egy proaktív, kockázatalapú megközelítést követ, amely a megelőzésre, a korai észlelésre, a gyors incidensreagálásra és a nemzeti szintű koordináció megerősítésére épít. A szabályozás immár nemcsak a technológiai eszközök védelmét célozza, hanem egy átfogó társadalmi reziliencia megteremtését is.

A jogalkotási átrendeződések mögött az intézményi szereplők is differenciálódtak és specializálódtak: míg korábban egyetlen központi szereplő, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet dominált, addig ma már több hatóság – az NBSZ NKI mellett a Szabályozott Tevékenységek Felügyeleti Hatósága, a Magyar Nemzeti Bank és a honvédelemért felelős minisztérium – feladatmegosztása biztosítja a szektorok közötti differenciált felügyeletet. Ez a logikai és intézményi mélyülés a kiberbiztonsági ökoszisztéma komplexitásának felismerését tükrözi, továbbá ezen felügyeleti rendszer biztosítja, hogy az egyes ágazatok sajátosságainak megfelelő, szektorspecifikus kiberbiztonsági követelmények érvényesüljenek.

Az Európai Unió NIS2 irányelve volt az a katalizátor, amely nemcsak a magyar szabályozás átfogó modernizációját eredményezte, hanem azt is kikényszerítette, hogy a nemzeti szabályozási modell szervesen illeszkedjen az egységes európai kiberbiztonsági architektúrába. A harmonizált követelmények révén Magyarország nemcsak a belső piac védelmét erősíti, hanem saját gazdasági és társadalmi stabilitását is növeli.

A NIS2 irányelv az Európai Unió kiberbiztonsági stratégiájának központi pillére, amely a digitalizációval járó fenyegetések kezelésére és az Unió kiberrezilienciájának növelésére irányul. Az irányelv célja az egységes és magas szintű kiberbiztonság megteremtése a tagállamok között, különös tekintettel a kritikus infrastruktúrák és ágazatok védelmére. Az irányelv sikeressége a tagállamok és a társadalom minden szereplőjének együttműködésén múlik. A kiberbiztonság nem csupán technológiai kérdés, hanem közös társadalmi felelősség is, amelyhez elengedhetetlen a tudatosság növelése és az együttműködés erősítése. Az emberi tényező védelmére és a technológiai

innovációk összehangolt alkalmazására alapozott megközelítés biztosíthatja, hogy az Európai Unió – és így Magyarország is – hatékonyan szálljon szembe a kiberfenyegetésekkel. A NIS2 irányelv és a 2024. évi LXIX. törvény által meghatározott keretek és intézkedések kulcsfontosságúak a digitális tér biztonságának és fenntarthatóságának megőrzésében, elősegítve a társadalmi és gazdasági stabilitás hosszú távú fenntartását.

Összességében megállapítható, hogy a 2013–2024 közötti szabályozási evolúció során a magyar kiberbiztonsági jogalkotás logikai, intézményi és tartalmi értelemben is érettebbé vált. A kutatás eredményei alátámasztják, hogy a modern, harmonizált és kockázatérzékeny kiberbiztonsági környezet kialakítása nemcsak technológiai, hanem társadalmi és stratégiai szinten is elengedhetetlenné vált. A jövő kihívásai közé tartozik, hogy a törvényi keretek gyakorlati alkalmazása is képes legyen lépést tartani a folyamatosan változó kiberfenyegetésekkel – ezt pedig további empirikus kutatások és folyamatos hatékonyságértékelések segítségével kell megerősíteni.

Felhasznált irodalom

Ambrus Éva (2023): *Kiberhadviselési képességek a jelen tükrében.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

Barna Bianka Rita et al. (2023): A *social engineering* helye az információbiztonsági auditban. *Biztonságtudományi Szemle,* 5(1), 25–41. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/317/258

Bányász Péter et al. (2019): A *social engineering* jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Bejtlich, Richard (2018): The Origin of the Quote „There Are Two Types of Companies". *TaoSecurity Blog,* 2018. december 18. Online: https://taosecurity.blogspot.com/2018/12/the-origin-of-quote-there-are-two-types.html

Bihaly Barbara (2021): A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában. *Hadtudományi Szemle,* 14(3), 45–55. Online: https://doi.org/10.32563/hsz.2021.3.4

Bodó Attila Pál (2014): *Információbiztonsági jogi ismeretek vezetőknek.* Budapest: Nemzeti Közszolgálati Egyetem. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/10084/Inform%E1ci%F3biztons%E1gi%20jogi%20ismeretek.pdf?sequence=2

Bodó Attila Pál – Joó Tamás – Palicz Tamás (2020): *Az Ibtv. gyakorlata. Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020.* Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/20.500.12944/18029

Bonnyai Tünde (2019): Kritikus információs infrastruktúrák védelme. In Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 56–83.

Bor Olivér (2024): Egységesen magas kiberbiztonság az Európai Unióban. *Szakmai Szemle,* 22(1), 177–196.
Castells, Manuel (2005): *A hálózati társadalom kialakulása. Az információ kora. Gazdaság, társadalom, kultúra. I. kötet.* Budapest: Gondolat–Infonia.
Deák Veronika (2023): Hírszerzés a kibertérben. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó, 87–114.
ENISA: EU Cybersecurity Index: Framework and Methodological Note (2024). Online: www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf
Európai Tanács – Az Európai Unió Tanács (2024): Az EU kiberbiztonságának megerősítése. Online: www.consilium.europa.eu/hu/policies/cybersecurity/?__cf_chl_tk=ddeADBDrnMIodjybZUhgCRVV76GXde13WCOyblKwLzc-1744563582-1.0.1.1-Gm9pFfeRocYZZORBZ94xJeGYG11Vs_GQW1_ye7tPNaI
Falyuna, Nóra et al. (2024): Against Disinformation: Bridging Science and Public Discourse. *Információs Társadalom,* 24(2), 68–84. Online: https://doi.org/10.22503/inftars.XXIV.2024.2.4
Farkas Ádám – Kelemen Roland (2023): *Nemzeti biztonság és kibertér.* Budapest: Médiatudományi Intézet. Online: https://mtmi.hu/files/7ddaa0c7-9a10-4123-af9c-e2d86c49cf30.pdf
Ghaib, Arkan A. (2024): Future Trends in Cybersecurity: Exploring Emerging Technologies and Strategies. *International Research Journal of Modernization in Engineering Technology and Science,* 6(2). Online: www.doi.org/10.56726/IRJMETS49530
Horváth, Dóra – Szabó, Zs. Roland (2019): Driving Forces and Barriers of Industry 4.0: Do Multinational and Small and Medium-Sized Companies Have Equal Opportunities? *Technological Forecasting and Social Change,* 146, 119–132. Online: https://doi.org/10.1016/j.techfore.2019.05.021
Kelemen Roland (2020): A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 148(4), 65–81. Online: https://doi.org/10.35926/HSZ.2020.4.5
Kis Márton – Bódi Antal – Számadó Róza (2024): A NIS2 hazai bevezetésének folyamata és kockázatai. *Hadmérnök,* 19(3), 165–182. Online: https://doi.org/10.32567/hm.2024.3.10
Kovács László (2018): *Kiberbiztonság és -stratégia*. Budapest: Dialóg Campus Kiadó.
Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika Egyetemi Kiadó.
Krasznay Csaba (2022): *Kiberbiztonsági a XXI. században.* Budapest: Katonai Nemzetbiztonsági Szolgálat.
Krasznay Csaba (2023): A *deepfake*-technológia kiberbiztonsági vonzatai. In Aczél Petra – Veszelszki Ágnes (szerk.): *Deepfake: a valótlan valóság.* Budapest: Gondolat Kiadó, 104–118.
Legárd Ildikó (2020): A barát és ellenség megkülönböztetése a kibertérben. *Jog – Állam – Politika,* 12(3), 125–140.
Legárd Ildikó (2023): A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintése. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó, 11–40.

Lella, Ifigeneia et al. (2024): *ENISA Threat Landscape 2024.* Online: https://doi.org/10.2824/0710888

Mäkelä, Jarmo (2019): Countering Disinformation: News Media and Legal Resilience. *Hybrid CoE Paper,* (1), 1–25. Online: www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf

Molnár Anna (2019): Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége. In Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 35–55.

Nemzeti Kibervédelmi Intézet (2023): *Adathalász csalások, visszaélések a bankok nevében.* Online: https://nki.gov.hu/it-biztonsag/elemzesek/adathalasz-csalasok-visszaelesek-a-bankok-neveben/

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (2024): *Éves kiberbiztonsági jelentés.* Online: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf

Nyári Gábor (2023): Elrettentés a kibertérben: elérhető cél vagy ábránd? In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó, 61–86.

Oroszi Eszter Diána (2023): *A biztonságtudatossági szint mérésének és fejlesztésének lehetősége.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2024.023

Pintér István (2016): *A virtuális tér geopolitikája.* Budapest: Geopolitikai Tanács Közhasznú Alapítvány.

PurpleSec [é. n.]: *2024 Cybersecurity Statistics. The Ultimate List Of Cybersecurity Stats Data, & Trends.* Online: https://purplesec.us/resources/cybersecurity-statistics/

Tikos Anita (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 8–34.

Trellix 2024 Threat Predictions. *Trellix,* 2023. október 30. Online: www.trellix.com/blogs/research/trellix-2024-threat-predictions/

Vandezande, Niels (2024): Cybersecurity in the EU: How the NIS2-directive Stacks up Against Its Predecessor. *Computer Law & Security Review,* 52, 105890. Online: https://doi.org/10.1016/j.clsr.2023.105890

Veszelszki Ágnes (2021): deepFAKEnews: Az információmanipuláció új módszerei. In Balázs László (szerk.): *Digitális kommunikáció és tudatosság.* Budapest: Hungarovox Kiadó, 93–105.

Veszelszki Ágnes (2023): Deepfake: kételkedés a kételyben. In Aczél Petra – Veszelszki Ágnes (szerk.): *Deepfake: a valótlan valóság.* Budapest: Gondolat Kiadó, 13–31.

Jogi források

A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról. C/2017/6100. 2017. szeptember 13. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32017H1584

A Bizottság Közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – „i2010: Európai információs társadalom a növekedésért és a foglalkoztatásért". COM/2005/0229 végleges. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52005DC0229

A Tanács (EU) 2019/796 rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32019R0796

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32016L1148

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). 2019. április 17. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32019R0881

Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve 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 (NIS 2 irányelv). Online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/hun

Az Európai Unió Tanácsa (2009): *Európai Biztonsági Stratégia. Biztonságos Európa egy jobb világban.* Luxembourg: Az Európai Unió Kiadóhivatala. Online: https://doi.org/10.2860/15719

Az Európai Unió Tanácsa (2010): *Az Európai Unió belső biztonsági stratégiája. Az európai biztonsági modell felé.* Luxembourg: Az Európai Unió Kiadóhivatala. Online: https://doi.org/10.2860/89974

Az Európai Unió Tanácsa (2018): Javul az EU kibervédelme: a Tanács támogatja a közös tanúsításról és a megerősített ügynökségről létrejött megegyezést. *Consilium.europa.eu,* 2018. december 19. Online: www.consilium.europa.eu/hu/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

Európai Bizottság (2010): A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az európai digitális menetrend. COM(2010)245 végleges. 2010. május 19. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex:52010DC0245

Jelentés az európai biztonsági stratégia végrehajtásáról. A biztonság megteremtése a változó világban. S407/08. Brüsszel, 2008. december 11. Online: www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/HU/reports/104644.pdf

Közös közlemény az Európai Parlamentnek és a Tanácsnak. Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése. JOIN/2017/0450 final. 2017. szeptember 13. Online: https://eur-lex.europa.eu/legal-content/hu/ALL/?uri=CELEX:52017JC0450

Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. JOIN/2013/01 final. 2013. február 2. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex%3A52013JC0001

A Bizottság ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (az értesítés a C(2003) 1422. számú dokumentummal történt)

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról