DETERMINATION OF THREATS TO THE WORLD'S ENERGY SUPPLY THROUGH THE CONCEPT AND OBJECTIVES OF INFOCOMMUNICATION STRATEGIES

A VILÁG ENERGIAELLÁTÁSA VESZÉLYEINEK MEGHATÁROZÁSA INFOKOMMUNIKÁCIÓS STRATÉGIÁK FOGALMÁN ÉS CÉLJAIN KERESZTÜL

DÉR Attila Tibor[1]

Abstract

An observable phenomenon nowadays is the rise of increasingly complex systems not only in our own lives, but also in our industrial infrastructures. Moreover, for the sake of manageability and comfort, these systems were connected to each other through various channels. This increased their Vulnerability, so much so that terrorism moved more and more towards attacking critical infrastructure. Terrorists realized that with relatively few resources and from a distance, how great a blow could be inflicted on a selected country's most important objects. The article highlights the strategies and ideologies of the dominant countries in cyberspace. Furthermore, it provides a comparison of these countries, but with particular attention to the forward-looking regulations between European Union and Hungary. Finally, the courses of action that can be used to reduce the risk factors of the energy supply of European Union and Hungary as a member country are determined at a strategic level.

Keywords

Strategy, cybersecurity, Information security, legal regulation, critical infrastructure

Absztrakt

Napjainkban megfigyelhető jelenség az egyre bonyolultabb rendszerek térhódítása nem csak saját életünk területén, hanem az ipari infrastruktúráinkban is. Sőt irányíthatóság és a kényelem érdekében ezek a rendszerek egymással különféle csatornákon keresztül összeköttetésbe kerültek. Ezzel Sebezhetőségük megnövekedett, olyannyira, hogy a terrorizmus egyre jobban a kritikus infrastruktúrák támadása felé tolódott. Terroristák felismerték, hogy viszonylag kevés forrásból és távolról, milyen nagy csapást lehet mérni egy kiszemelt ország kiemel fontosságú objektumaira. A cikk kiemeli a kibertérben meghatározó országok stratégiáit és eszmerendszereit. Továbbá összehasonlítást ad ezen országok, de különös tekintettel az Európai Unió és Magyarország közötti jövőbe mutató szabályozásai kapcsán. Végül meghatározásra kerülnek azok a cselekvési irányok, amelyekkel az Unió és tagországaként Magyarország energiaellátásának rizikó faktorai csökkenthetők stratégiai szinten.

Kulcsszavak

Stratégia, kiberbiztonság, információbiztonság, jogi szabályozás, kritikus infrastruktúra

[1] der.attila@uni-obuda.hu | ORCID: 0009-0008-9547-102X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A kiberbiztonság fontosságát a mai fejlet civilizációnkban nem szükséges kifejteni több száz oldalas könyvben, csak egyszerű logikus tapasztalással megérthető, milyen befolyásoló tényezővel rendelkezik a mai fejlett társadalmainkban. Az emberiség történetében már régóta kulcsfontosságú szerepet töltenek be a kritikus infrastruktúrák, mint a szállítás, víz-, olaj-, gáz-, áram-ellátás stb. lehetne még sorolni. Ezek között az infrastruktúrák között ráadásul sokszor szoros kapcsolat van egymástól jelentősen függhetnek, egyi a másik nélkül már elvesztheti eredeti rendeltetését, illetve funkcióját. Ezen kritikus rendszerek között több prioritási csoportosítást is megtalálhatunk a szakirodalomban fontosságuk sorrendjében. Nyilván függ ez az osztályzás, hogy melyik kontinensről vagy országról beszélünk. Az országok társadalmi és technikai adottságai mennyire befolyásolják a kritikus infrastruktúrák kiépítettségét és bonyolultságát. Természetesen rengeteg féle befolyásoló tényezőt még fel lehetne sorakoztatni, de általánosságban kimondható globálisan, hogy az egyik legveszélyeztetettebb infrastruktúra a villamosenergia-ellátást kiszolgáló rendszerek. Erre a megállapításra még ráerősít az elektronikai és az információs technológiai eszközök térhódítása és kölcsönös egymásrautaltsága.

UKRÁN-OROSZ HÁBORÚ ÁRNYÉKÁBAN

A villamosenergia infrastruktúra, mint a legtöbb kritikus szisztéma, egyre nagyobb mértékben összeköttetésben van az internettel. Ezzel sajnos a kiszolgáltatottsága is egyenes arányban növekszik. Ennek következtében a különféle kibertámadások is megnövekedtek, illetve manapság már vannak kifejezetten olyan szakosodott hacher csoportok, akik csak kizárólag ezeket a villamosipari létesítményeket támadják. Nem is kell messzire menni sajnos szomszédunkban Ukrajnában 2022 februárjában elkezdődött fegyveres konfliktus, amelyet nem csak hagyományos fegyverekkel vívnak meg, hanem a kibertérben is egyre komolyabb és szofisztikáltabb támadások jelentek meg mind a két hadviselő félnél. Oroszország már a háború előtt is támadta Ukrajnát, de csak kiberhadviselés címén. Az első hullámban óriási károkat okozott Oroszország Ukrajnának főként a kritikus infrastruktúrák területén. Nagyon szembetűnő volt Oroszország technikai fölénye és Ukrajna védtelensége, felkészületlensége ezekkel a speciális elektronikai rendszereket érintő agresszor ellen. Itt meg kell jegyeznem, hogy az ENSZ alapokmánya szerint a kibertámadás önmagában nem váltja ki a háború fogalmát, csak ha háborús konfliktussal van kombinálva. Ennek következtében esetünkben Ukrajna nem számíthatott nemzetközi segítségre, hogy a támadót jogilag megállítsa, illetve megfelelő szankciókkal sújtsa. Felismerve ezt a tényt az ukrán vezetés, úgy határozott, hogy nem tétlenkedik és már a tényleges háború kezdete előtt komoly kibervédelmi stratégiát alakított ki. Megerősítették az ország legsérülékenyebb infókommunikációs rendszereit, kiemelt intézményeit, infrastruktúráit. Az ukrán nemzeti adatvagyont felhőbe rejtették el, különféle zombihálózatokat építettek ki, 2022. 02 26.-án felállították az Ukrán Informatikai Minisztériumot stb. Továbbá nem csak a védelemre rendezkedtek be az ukrán politikai elit, hanem a háború bejelentése óta már tudatos kibertámadások sorozata is napirendre került kiemelt orosz létesítmények ellen, amelyek mai napig folyamatban vannak. Korszakalkotó kezdeményezés volt Ukrajnának, hogy megalapította az Ukrán Kiber hacker közösséget, amely több mint 400 000 fős önkéntes nemzetközi hacker háttérrel rendelkezik.

Sőt állami szinten olyan fontosnak tartják ezt a közösséget, hogy a nemzetközi hacker csapatok szervezése már törvénytervezetben jelent meg és hamarosan elfogadhatja az ukrán kormány, amely első ilyen intézkedés lehet a világon. Az ukrán katonai irányítása alatt működő hacker közösség rendkívüli hatékonyságát jól bemutatja - rendelkezésre álló adatok alapján -, hogy Oroszország képtelen volt megvédeni, illetve ellenállni ennek a félelmetes méretű és szaktudású „Armadának". Érdekes az a tény is, hogy az a „nagy" orosz kibervédelem, amelyet évtizedek óta nemzetközi szinten propagál az orosz politikai és szakmai elit, viszonylag rövid idő alatt a porba hullott, az ukrán nemzetközi hackerek által megerősített offenzíva alatt. Ezekkel kibertámadásokkal betörtek a Kremlbe, a Dumába, a titkosszolgálatok adattáraiba és a legfontosabb állami intézményekbe, valamint átlagos adatszivárgás elérte a100GB-ot orosz vállaltonként, ide értve majdnem a teljes kritikus infrastruktúrát is.

STRATÉGIÁK ELEMZÉSE

Nem véletlenül emeltem ki az orosz-ukrán háborút, mivel ez napjainkban is hatással van Magyarországra, mint szomszédos államra és természetesen Európára és közvetlenül vagy közvetetten az egész világra is. Stratégiákat az államok már régóta kialakítottak kezdetben inkább katonai jellegűek voltak, majd később már politikai, gazdasági és társadalmi színezetet is kaptak. Napjainkban pedig minden szakterületnek megvan a maga startégiája, így a nemzeti kibervédelemnek, infókommunikációnak és az energiabiztonságnak is. Természetesen minden állam saját érdekeit veszi alapul és ezeket az érdekeket egyezteti a nemzetközi érdekekkel vagy teljesen sajátos utat követ. A politikai és gazdasági nagyhatalmak ezen a területeken is éreztetik hatásukat illetve befolyásukat. Nagyon szépen követhető a kisebb országok stratégiai dokumentumaiban ezen országok dominanciája.

Uniós szabályozás

Az Európai Uniónak is van egy stratégiája, melynek keretrendszerét több szervezet is aposztrofálta, úgy, mint ENISA (European Network and Information Security Agency), amely az Unió egyik legfontosabb kiberbiztonsági szervezete. Tanácsadó szervezetként különféle ajánlásokkal, dokumentumokkal segíti a tagállamokat stratégiáik kialakításában. A gyorsan változó nemzetközi környezetre - ukrán-orosz háború - való rugalmas válaszok elengedhetetlenek az Unió szabályozásaiban. Tisztázni kell a határokon átnyúló fenyegetések határait, hol vannak a NATO vagy az Unió és a nemzeti érdekek közös pontjai, illetve saját elkülönített keretrendszeri. Az ENISA jól rámutatott még régebben, hogy a tagállamoknak elemi érdeke, hogy egymás között egyeztessenek a kardinálisabb kifejezéseken és fogalmakon. Mivel egyáltalán nem mindegy, hogy például Lengyelországban kiberbiztonság, mint fogalom mennyiben hasonlít Magyarországi megfelelőjéhez. A szervezet már akkor felismerte, hogy az állam és a piaci szereplők között kiberbiztonsággal összefüggő kapcsolatokat kell kiépíteni a szükséges védelemhez. Fontos információk nyerhetők a piaci alapon működő vállalkozások infókommunikációs tapasztalataiból és természetesen ez kölcsönös az állami szervek oldaláról is.[1]

Itt megemlíteném Magyarországon a Nemzeti Kibervédelmi Intézetet, amely megalakulása óta egyre hatékonyabban ellátja ezt a híd szerepet az állami szféra és a magánvállalkozások között. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv) 2015. évi módosítása során lett létrehozva a Nemzetbiztonsági Szakszolgálatokon belül. Szakhatósági feladatain kívül eseménykezelési nemzeti

kapcsolattartás Unió határain belül különféle incidensekkel összefüggő adatok elemzése, monitorozása és ezen eredmények megosztása fontosabb Európai incidenskezelő központokkal. Az állami intézményeket és állami tulajdonú vállalatokat kiberbiztonság céljából felügyeli és ajánlásokat küld az illetékes intézmények felé. Fontos, hogy a Nemzeti Kibervédelmi Intézet napra kész információkat oszt meg a honlapján, amelyet bárki elérhet. Sőt incidenseket bárki bejelenthet ezzel segítve a hatóság munkáját. Szolgálatásai kiterjednek incidenskivizsgálásra, eseményészlelésre, sérülékenységvizsgálatra, korai figyelmeztető rendszerre, amelyekkel információs technológiai rendszerek üzemeltetőit nagymértékben támogatják.[2][15]

A NATO Kibervédelmi Kiválósági Központjának kiadott Nemzeti kiberbiztonsági keretrendszer kézikönyve is nagyszerű alapot nyújtott, illetve nyújt a tagok számára, hogy kialakítsák a maguk stratégiáját. A tanulmányban öt kardinális téma kap szerepet, ahol az egyik kritikus infrastruktúra védelme. Érdekes ellentmondás, hogy a veszélyeztetett rendszereket minél jobban korszerűsítik, annál nagyobb sérülékenységet jelentenek egy ország biztonságára. Az sem egy megfelelő gyakorlat főként a villamos iparban, hogy eltérő fejlettségű és típusú eszközöket alkalmaznak. Ezzel az inkompatibilitással és az eltérő biztonsági megoldásokkal kisebb-nagyobb réseket adnak a támadók számára. Nem véletlenül vannak ezekben az ajánlásokban olyan kérdések felvetése, mit például a biztonság vagy versenyképesség legyen a fő mozgatórugó egy adott térségnek illetve országnak. A kérdés egy alapvető megállapításon nyugszik, mint hogy általában információstechnika fejlődése jóval gyorsabb, mint a védelmének fejlődése.[3]

2013-ban született meg az első komolyabb Európai Unió kiberbiztonsági stratégia, amelynek mottója, mint a címben is utalnak rá nyílt megbízható és biztonságos kibertér. Ez a szabályozás megfelelő alapot jelentett a további intézkedéseknek, de a tagállamok még nem tudták abban az időszakban se gyakorlatban se intézményi szinten kivitelezni ezeket az iránymutatásokat. 2016 nyarán jelent meg az újabb biztonsági direktíva a NIS (Network and Information Systems Directive), amelyben az Európai Unió már geopolitikai alapokon határozta meg az együttműködést egyes tagállamok intézményei számára, sőt közös intézményi háttér kialakítását is előírta. [4]

Időrendben tovább haladva 2020. évben készült el egy ráncfelvarrása az előző digitális stratégiáknak továbbfejlesztett Európai Bizottság javaslata. Ebben a javaslatban röviden a főbb újítások a következők: gyors válaszlépések a kibertámadások ellen; katonai missziók felértékelése; korszerű titkosítás megvalósítása; ellátási láncok megerősítése; növekvő kibertámadások elleni immunitás növelése; közös kiberbiztonsági egység kialakítása; biztonsági műveleti központok hálózatának kiépítése az Unió tagállamaiban [5]

Tavaly év végén az Európai Unió Bizottsága kihirdette a NIS2 Irányelvet. Ennek következtében a legfrissebb és egyben a leghaladóbb szemléletű Uniós szabályozás ez év januárjában került hatályba. Fontos vetülete (később tárgyalja a cikk) ennek az irányelvnek, hogy kiterjeszti és kijelöli a kiberbiztonsági kockázatkezeléseket és bejelentési kötelezettségek körét, kritérium-rendszerét és hatályát a kritikus infrastruktúrák területén is. Sajnos a tagállamok csak közel másfél év múlva fogják saját jogrendjükbe áthelyezni a NIS2-es normatívákat.[6]

USA irányelve

Amerikai Egyesült Államok legfrissebb Kiberbiztonsági Stratégiája 2023 március elején jelent meg. Főbb mozgató rugója ennek az elképzelésnek, hogy az informatikával foglalkozó jelentősebb vállalkozásokra alapozna az ország kibertér védelmével kapcsolatosan. Ezzel szeretné a kormány kisegíteni azokat a szegmenseket (civileket, kisvállalkozásokat, közigazgatási szerveket), akik nem férnek hozzá a megfelelő technológiához, nincs elég forrásuk, hogy egy adekvált védelmet kiépítsenek saját rendszereikben. A megfelelő állami koordináció elengedhetetlen záloga a nemzetbiztonság kézben tartására. A dokumentum tartalma 5 fő részből áll. Az első pillér kiemeli az infrastruktúrák védelmét, egy új szemléletű incidenskezelési politika megalkotásával. A második rész a zsarolóvírusok elleni nemzetközi küzdelem összehangolását célozza meg. A harmadik pillér a megbízható szoftvereket gyártó cégeket helyezni előtérbe. A negyedik meghatározó szegmens nem meglepően a képzés és kutatás elősegítése. Az utolsó pillér általánoságban leírja nemzetközi környezetben, milyen helytállásra van szükség, hogy elkerülje az Amerika a nagyobb kibertámadásokat.[7]

A stratégia elkészítését több előzmény is serkentette, ide értve Amerika Nemzetbiztonsági Stratégiáját, ötös és a tízes számú memorandumokat. Ezeknél az eljárási módoknál már megjelenik egy igen fontos fogalom a zéró bizalom, amely még csak felvetődött biztonsági elvként, de már itt a legújabb kiberbiztonsági dokumentumban tovább lett fejlesztve, mint egy sajátos eszmerendszer. Kiemelném a témámhoz szorosan összefüggő 5. nemzetbiztonsági dokumentumot, ahol kifejezetten a kritikus infrastruktúrák vezérléseinek biztonsági réseinek javításával foglalkozik. Sőt felmerültek lehetőségek, hogy a fontosabb vezérlő rendszereknél kvantumszámítógépek csatasorba állításával jelentősen csökkenthetők a sérülékenységek. A stratégia hangsúlyozza, hogy az állam feladata megvédeni az állampolgárait a kiberbűnözőktől vagy olyan országoktól, amelyek nem tartják be a nemzetközi jog normáit. Számon kérné azon országokat, amelyek a kiberbűnözőket támogatják akár pénzzel, akár technikai eszközökkel. Továbbá rávilágít a különféle kibertámadások okozta károkra, amelyek egyre komolyabbá is válhatnak, ha nincs megfelelő cselekvési terv. A digitális technológiák egyre jobban rátelepednek mindennapi életünkre. Személy adatainkra egyre jobban kell vigyázni, mivel olyan láthatatlan térben vannak ahol sokszor már követni sem lehet.

A stratégia kifejti, hogy egykor jól meghatározott keretek között csak néhány ország volt képes kibertámadások kifejtésére, illetve ehhez szükséges eszközök előállítására. Manapság viszont, már széles körben elérhető a különféle kémprogramok, hacheléshez használt adatok, eszközök és szolgálatások. Ezeknek az eszközöknek a birtokában - általában jóval alacsonyabb költséggel rendelkeznek, mint a hagyományos fegyverek - már olyan országok is vannak, akik messze nem közelítik meg a fejlett országok kiberhatékonyságát. Kiemeli név szerint megemlítve Kínát, Oroszországot, Iránt, Észak-Koreát, ahol agresszíven használnak fejlett kiberképességeket, olyan célok elérésére, amelyek ellentétesek a nemzetközi normákkal és értékekkel. Ezek közül a felsorolt országok között is az amerikai vezetés a Kínai Népköztársaságot tartja a legveszélyesebbnek, amelynek gazdasága, katonai ereje lassan eléri az Egyesült Államokét. Ebben nagy szerepet játszott az elmúlt évtizedekben történt ipari kémkedés, amelyet a kommunista rezsim kifinomult információstechnoló-

giai eszközparkkal véghezvitt USA-ban és más fejlett országokban. A stratégia figyelmeztet, hogy Kína nem csak „importál" kritikus információkat, hanem „exportálja" saját ideológiáját, hogy ezzel átalakítsa a világ demokratikus képét.[8]

Kína startégiája

Nyilván Amerikai szemüvegen nézve teljesen más képet kapunk Kínáról, mint amikor saját dokumentumait kutatjuk. Nem véletlenül ezzel a résszel folytattam a cikkemet, közvetlenül az amerikai álláspont befejezése után. Így jobban érzékelhető az olvasó számára, hogy milyen a két legbefolyásosabb hatalom (Oroszországot még ide lehetne sorolni, de véleményem szerint már leszakadó félben van helyzetével kapcsolatosan) egymás közötti interakciója. Mivel a kínai pártvezetés már több éve megfigyeli állampolgárait totális megfigyelő rendszerein keresztül, ezért óriási információ halmazt gyűjtött össze. Nem is beszélve az infókommunikációs területeket érintő nagyvállalatairól, akik világszínvonalú termékeket és szolgáltatásokat bocsátanak ki szerte a világban. Ezzel Kína úgymond versenyelőnyre tett szert a versenytársakkal szemben. Jellemző a kommunista rezsimre, hogy az ENSZ alapokmányának szabályozásába is beleszólt, sőt beadott egy viselkedési kódexet a következő szövegrészlettel szemben, amely így szól „nem alkalmaznak információs és kommunikációs technológiákat, valamint információs és hírközlési hálózatokat abból a célból, hogy megzavarják más ország belső ügyeit vagy, hogy aláássák annak politikai, gazdasági és társadalmi stabilitását." (United Nations 2015) „ 2003. év óta a Kínai nagy Tűzfal néven felállított megfigyelőrendszerrel totális kontrolt gyakorolnak az állampolgárok felett. Ha azt vesszük, hogy Kínában nagyjából egy milliárd internetes felhasználó van, akkor érzékelhető, hogy megkora tapasztalatot képesek begyűjteni ennyi felhasználóról.[9]

A kínai rendszer folyamatosan szoros együttműködésben van az internet szolgáltató vállalatokkal. Ezzel próbálja megelőzni, hogy bárki is a kormány ellen szervezkedjen vagy agitáljon. Rendszeresen monitorozza az internetet és, ha valami gyanús tartalom kerül előtérbe azt rögtön blokkolásra kerül. Kína kiberbiztonsági stratégiájára teljes mértékben rányomja a bélyegét az előző bekezdések megállapításai és tényei, amelyek természetszerűleg szoros összefüggésben vannak a rezsim ideológiájával is. Stratégiájában jól körvonalazható a katonai szemlélet, amely nem titkolva az Egyesült Államok technikai fölényének legyőzésére is nagymértékben törekszik.

EURÓPAI SZINTŰ SZABÁLYOZÁS LÉTFONTOSÁGÚ RENDSZEREKKEL KAPCSOLATOSAN

2005. zöld könyv CIP (Critical infrastructure Protection) irányelvek 2008-as és 2020-as átdolgozása, majd következett a 2020 NIS 2.0 javaslata a CIP továbbfejlesztése. A létfontosságú infrastruktúrák védelmére vonatkozó európai program 2020-as markáns jellegzetesége, hogy bevezette az immunitás képességének korszerűsítését, a bekövetkező problémák gyors és szakszerű kezelését szakítva a korábbi gyakorlattal, miszerint materiális síkon kellene megvédeni a különféle infrastruktúrális elektronikai rendszereket. Kiemeli a kockázatelemzés fontosságát, kritikus elemek azonosítása, entitások hatósági felügyeletét stb. A kritikus entitások ellenálló képességéről szóló irányelv CER (Critical Entity Resilience)-ben egyre jobban bővül az ágazati paletta az évek előrehaladtával például tavaly is

bekerült digitális infrastruktúra, agrárium és a közigazgatás. A dokumentum kifejezett szándéka, hogy a többi rendelkezéssel vagy jogi aktusokkal, ne kerüljön ellentmondásba, ne lehessen kijátszani és ne legyen egy konkrét szabályozás több helyen.[10]

A hálózati és információs rendszerek biztonsága (NIS 2) Uniós szintű szabályozását az Európa tanács elfogadta, de még a tagállamok nem ratifikálták saját jogrendükben. Ebben a tervezetben az Unión belüli országoknak egy hatóságot kellene felállítani kapcsolattartó ponttal és egy eseménykezelő központtal egyetemben. Részletezi a kritikus szervezetek bejelentési és kapcsolattartási kötelezettségit a jövőbeni hatóság felé, ahol a mostani gyakorlatot (több hatóság) felváltja egykapus rendszer. Igy egy hatóság járna el az adatszivárgások kivizsgálásánál, helyszíni ellenőrzéseknél, iratok és adatok átvilágításánál. Fontos felvetése a NIS 2 –nek, hogy az Unióban jelentkező szakemberhiányt, azt valahogyan pótolni kell, úgy hogy a jogilag kiszervezhető szolgáltatásokat még az eddigi szabályozásoknál is markánsabban kellene támogatni. Viszont még ettől is fontosabb, hogy ezeket a külső „alvállalkozókat" legalizálni kellene az új irányelv szerinti. Ugyanis nem mindegy, hogy ezeket a szenzitív adatokkal kapcsolatos munkákat kire illetve kikre bízzák. Továbbá az Uniós jogalkotás még keményebben fellépne, ezen jogi normák megsértőivel szemben. Azok a szervezetek, amelyek az ENISA-nál szerepelnek és 72 órán belül nem jelentik a hatóság felé biztonsági incidensüket, azokat jelentős bírsággal lehetne súlytani.

Magyarországi szabályozás

Magyarországon a Nemzeti Infokommunikációs Stratégia 2014-2020 közötti időszakot ölelte fel. Majd az Európai Unió által szerkesztett iránymutatás digitális iránytű címmel 2030-ig kijelölte az európai tagállamok digitális stratégiáját. Egy újabb szemléletet vezetett be a - régebbi iránymutatásokkal összhangban - digitális készségek fejlesztése, vállalkozások és az infrastruktúrák teljes digitalizációja területén. Ennek a digitális „forradalomnak" magyarországi leképezése a Nemzeti Digitalizációs Stratégia (2022-2030), amely újabb lendületet adhat a hazai digitális gazdaságnak. A Nemzeti Digitális Stratégia inkább általánosságokat fogalmaz meg, mint a szupergyors internet kiépültségének hatása a társadalomra, a digitális ökoszisztéma területén megfogalmazott kezdeményezéseket, stratégiákat, azok fejlesztési irányait, jövőképét, digitális kompetenciákat, SWOT elemzést, eszközrendszereket és átfogó jövőképet.[11]

Az Európai Unió szabályrendszerével összefüggésben 2012. évi CLXVI. törvény (létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről)

majd energia ágazati iránymutatása kiegészült 374/2020 kormányrendelettel. Itt körvonalazódik, hogy a villamosenergia rendszernek magyarországi hatósága a Magyar Energetikai és Közmű-szabályozási Hivatal. Azonosítási jelentés küldése a Magyar Energetikai és Közmű-szabályozási Hivatal részére. Üzemeltetői biztonsági tervnél nevesítette a jogalkotó a rendkívüli eseményeket, sőt a kiemelt ágazatok üzemeltetőinek meg kell adniuk, hogy milyen eljárásrend szerint oldják meg ezeket az incidenseket. A rendkívüli intézkedések részleteit is meghatározta ez a törvény. Megfelelő részletességgel az Európai Uniós normáknak megtartásával segítik ezen előírások a jogalkalmazókat. Itt kiemelném, hogy a létfontosságú ágazatoknak és természetesen az államnak is elemi érdeke, hogy felkészítsék létesítményeiket és vezetőiket a rendkívüli eseményekkel szemben. Ennek érdekében az Országos Katasztrófavédelmi Igazgatóság bevonásával – kötelező gyakorlatot el-

rendelheti, mint hatóság - vagy nélküle tesztelési gyakorlatokat kell elvégezni. A fiktív támadási teszt meglátásom szerint nagyon fontos eleme a védekezésnek, mivel nem éles helyzetben kell kapkodni és a hiányosságokat feltárni, amikor közvetlen vagy közvetett formában emberi illetve anyagi kárt szenved az ország. Továbbá kötelező tartalmi elme lett a biztonsági tervnek a kockázatelemzés, amelynek összhangban kell lennie a törvény mellékletében lévő védelmi intézkedések szintjével és elvárásaival. Ezekhez a táblázatok, tervek kitöltéséhez segítséget nyújtanak a Vármegyei Katasztrófavédelmi Igazgatóságok. A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság éves jelentése is hasznos szakmai alapot adhat a kockázatelemzés szakszerű leírásával kapcsolatosan. [12][14][16]

2013. évi L. tv. Ibtv az állami és önkormányzati szervek elektronikus információbiztonságáról. Ahol a kritikus infrastruktúrák rendszereit és intézményeit törvény által nevesített osztályok szerint kell nyilvántartani. Kötelező ezen szervezetek mindegyikéhez egy-egy kiberbiztonsági felelős szakértőt kijelölni. Leírja a hatóságok szerepét és ellenőrzését államilag fontos intézményeknél.[15]

ÖSSZEFOGLALÁS

A jelen írás megvizsgálta a világ kiberterében meghatározó országainak stratégiáit. Így górcső alá vettem Amerikát különös tekintettel a legújabb kiberbiztonsági dokumentumait, majd Kína, mint vetélytárs követte a sorban. Továbbá Magyarország geopolitikájából kiindulva átrágtam magam az Európai Unió stratégiai elvein, illetve tervezetein és ezzel összefüggésben hazánk szabályozásait és infókommunikációhoz köthető irányelveit is átnéztem.

Ezekből a vizsgálatokból levonható következtetés, hogy még mindig nincs kiberteret érintő garanciális alapokon nyugvó egységes szabályozás a teljes globális világra nézve. Ha van is, mint például ENSZ határozat, akkor sem mindegyik állam ratifikálja. Sőt Kína még saját dokumentumot is benyújtott, hogy saját nézőpontja szerint legyen az ENSZ határozat megváltoztatva. Megjegyezném, hogy ha minden ország a világon aláírna egy ilyen kiberbiztonsági egyezményt, akkor sem biztos, hogy az be is tartanák az aláírók. Sajnos volt már rá példa, hogy egyes országok hacher kalózokat bízott meg titokban, hogy más államok biztonságát és szuverenitását veszélyeztesse. A nagyhatalmakhoz képest az Uniónak van még lemaradása stratégiai szinten, habár a NIS 2 tervezetben már jól körvonalazódnak azok a tendenciák, amelyek már képesek lesznek majd egy fejlett struktúra kialakítására. A hazai szabályozásban is kivehető, hogy az Európai intézmények és a tagországok között nincs az a kohézió, amellyel az elméleti iránymutatásokat megfelelő hatékonysággal át lehetne ültetni a gyakorlatba. Az Amerikai gyakorlatban – nyilván a politikai berendezkedés miatt – nem probléma az államok közötti munkamegosztás és bizonyos központosítás. Megállapítható, hogy a jelenlegi ukrán háborús politikai helyzet, amely jól reprezentálta és reprezentálja a hibrid hadviselés elemeit, igen csak komoly gondokat okozott az Európai Uniós tagországok belbiztonsága szempontjából. Gondolok itt például a nem régen történt ír kórházak elleni kibertámadásra.

Kritikus infrastruktúra szerepe nem kérdőjelezhető meg egy ország életében sem, ezért is fokozott figyelmet kell fordítani rá, mint Uniós keretszinten és tagállamok „sajátos" szintjén egyaránt. Viszont az Európai Unió nehézkes jogalkotási rendszere nem teszi lehetővé a gyors stratégiai szabályozást és így a védekezés mindig hátrányban lesz a támadók

képességeivel szemben, főként tagállami szinten (lásd NIS 2-es szabályozás 2024 őszén lesz csak a tagállamok jogrendjébe ültetve).

A cikk elemzéseiből levont következtetésem, hogy az Európai Uniónak, így hazánknak is magáncégeket kellene bevonni a kritikus infrastruktúrák védelme szempontjából. Mivel a kormányzati szektoroknak jelenleg nincs akkora anyagi és emberi erőforrása, illetve technikai kompetenciája, hogy egyedül megbirkózzon ezzel a speciális és késlekedést nem tűrő speciális feladattal. Egyébként a digitális magáncégeknek épp úgy érdeke az együttműködés, mint az állami intézményeknek, hiszen egy kívülről jövő agresszív kibertámadás az adott célország teljes nemzetbiztonságát fogja veszélyeztetni. Ehhez kellene erősíteni a felderítést és a védekezést. Nagyobb hangsúlyt kellene fektetni az oktatásra kiberbiztonsági szakemberek képzésére, kvantumszámítógépek és a mesterséges intelligencia fejlesztésére. Kormányzati és magáncégek összefogásával kellene létrehozni egy egységes védelmi rendszert és egy tartalékszolgálatot is, amelyet éles helyzetben vethetnének be a veszély semlegesítésére.

FELHASZNÁLT IRODALOM

[1] Kovács László, *Kiberbiztonság és –stratégia*. Budapest: Dialóg Campusz Kiadó, 2018, pp. 32-44.

[2] https://nki.gov.hu/intezet/tartalom/magunkrol. 2023.05.12.

[3] B Müller Tamás, *Kiberhadviselés és katonai védelem*. infójegyzet 2019. november 15. https://www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf

[4] Bihaly Barbara: *A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában*, Hadtudományi Szemle 2021 XIV. évfolyam 3. szám 45- 55. doi 10.32563 /hsz.2021.3.4

[5] EU Tanácsa: *Kiberbiztonság: a Tanács következtetéseket fogadott el az uniós kiberbiztonsági stratégiáról*. Sajtóközlemény 2021. március 22. https://www.consilium.europa.eu/hu/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

[6] EU Tanácsa: *A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között*. Sajtóközlemény 2022. május 13. https://www.consilium.europa.eu/hu/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

[7] The White House: *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, 2023.03.02. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[8] The White House: *Amerikai Egyesült Államok Nemzeti Kibervédelmi Stratégiája* 2023. március. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[9] Kovács László, *Kiberbiztonság és –stratégia*. Budapest: Dialóg Campusz Kiadó, 2018, pp. 104-105.

[10] SeConSys együttműködés keretében: *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*, Nemzeti Kibervédelmi Intézet, 2022, pp. 42-44. http://www.seconsys.eu/
[11] Miniszterelnöki Kabinetiroda: Nemzeti Digitalizációs Stratégia, 2022.12.05, https://kormany.hu/dokumentumtar/nemzeti-digitalizacios-strategia-2022-2030
[12] https://www.securinfo.hu/szabalyozasok/jogszabalyok/12033-jogszabalyvaltozasok-kritikus-infrastruktura-vedelemben.html

FELHASZNÁLT JOGSZABÁLYOK

[13] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
[14] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[15] 2013. évi L. tv. Ibtv az állami és önkormányzati szervek elektronikus információbiztonságáról.
[16] 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.