Magyarország Kiberbiztonsági Stratégiája

1. Vízió

Magyarország célja – a változó világ kihívásának kezelése a fenyegetésekkel és kihívásokkal szemben ellenálló kiberbiztonság elérésén, az emberek kiberbiztonsági tudatosságának folyamatos fejlesztésén, az állami szervek és a gazdaság egyéb szereplői hatékony digitalizációján és az ezzel összefüggő biztonsági célú együttműködésén, valamint a védelmi és biztonsági célú állami-társadalmi együttműködés fokozásán keresztül – a digitális jólét és a nemzeti kiberbiztonsági ellenálló képesség erősítése és fenntartása.

2. Bevezető

Magyarországon a korábbi kiberbiztonsági stratégiák és a kiberbiztonság erősítésére való törekvések eredménye a kiberbiztonság meghonosodásával párhuzamosan egyre inkább láthatóvá vált, a kibertérből érkező fenyegetésekkel szembeni ellenálló képesség nőtt, azonban ez a képesség – a változó kihívásokra való reagálások érdekében – további hangsúlyos fejlesztést igényel, folyamatosan új megoldások bevezetését teszi szükségessé.

A digitalizáció szerves része a mindennapi életnek, kulcsfontosságú hajtóerő a társadalom fejlődésében, a jólét megteremtése és fenntartása érdekében. Mindezen kiemelt célokat felismerve Magyarország Kormánya elfogadta a Nemzeti Digitalizációs Stratégiát, valamint a digitalizáció középtávú irányait kijelölő Nemzeti Digitális Állampolgárság Programot (a továbbiakban: NDÁP), illetve megszületett a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (a továbbiakban: DÁP tv.), amelyek jelen kiberbiztonsági stratégia készítésekor is figyelembevételre kerültek.

A digitalizáció kiemelt gazdasági fejlődési lehetőséget, ugyanakkor hatalmas fenyegetettséget is jelent. A magyar társadalom tagjai egyre több esetben digitális szolgáltatásokat vesznek igénybe ügyeik intézéséhez, így ehhez kell igazítani a kibertámadásokkal szembeni védelmi képességet is. A kibertérből érkező fenyegetéseknek kitett, a kibertéren keresztül összekapcsolt elektronikus információs rendszerek, IKT termékek és szolgáltatások, a kibertérben elkövetett bűncselekmények, honvédelmi és nemzetbiztonsági vonatkozású események és a kiberbiztonsági incidensek száma hazánkban folyamatosan emelkedik. Magyarország feladata, hogy biztosítsa a hatékony védekezéshez szükséges jogszabályi környezetet, képességeket, és hozzájáruljon a tudatosság növeléséhez, valamint olyan védelmi rendszert működtessen, amely alkalmas az állami támogatású kiberbiztonsági tevékenység elleni, illetve a dezinformációs célú támadások, a kiberbűnözés, valamint – a Nemzeti Katonai Stratégiával összhangban – az ellenérdekű katonai kibertér műveletek lehetséges bekövetkezése és hatásai elleni hatékony fellépésre.

Magyarországon a lehetőségek kihasználásában és a veszélyek elhárításában mindenkinek van feladata. A DÁP tv.-ben és az NDÁP-ban előírt, továbbá a Nemzeti Elektronikus Közigazgatási Stratégiában (a továbbiakban: NEKS) kiegészített feladatrendszer végrehajtásának köszönhetően a digitális fejlesztések ütemezetten haladnak, az ország digitális adatvagyona dinamikusan növekszik, az állampolgárok digitális jelenléte egyre szélesebb körűvé válik, azonban a kritikus infrastruktúrák számának növekedésével, és az egyre változatosabb fenyegetések megjelenésével arányosan a kibertérben jelentkező kitettség is folyamatosan nő.

Magyarország megfelelő alapokkal rendelkezik, hogy a megkezdett folyamatokban a digitális fejlődés irányával és sebességével lépést tartson, sőt egyes területeken irányt is mutasson, és a jelentkező veszélyekre felkészüljön, valamint azokat elhárítsa, és ezáltal biztonságos környezetet biztosítson az állami, a társadalmi, a gazdasági szereplők és az állampolgárok számára.

Hazánk a negyedik ipari forradalom és az átalakuló biztonsági környezet jelentette kiberbiztonsági kihívásokat az Európai Unió és a NATO-tagországok átlagánál jobban kezelheti, ha a változás jelentette gazdasági lehetőségeket kihasználja. E vonatkozások kölcsönhatásos kiaknázása mellett alapvető fontosságú a kibertér sokrétű, különösen életviteli, társadalmi, képzési, kommunikációs és kulturális kibontakozásának és hatásainak megfelelő elemzése, értékelése és hasznosítása, ideértve e területeken is a tudományos és gyakorlati tapasztalatok, valamint a kutatások fokozását és összhangjának erősítését. Egy nemzet sikere annak tagjainak együttműködésén és egymás iránti bizalmán is múlik, ezért a biztonságos kibertér megteremtése önmagában stratégiai és gazdasági előnyt jelent. A kiberbiztonság garantálása ezáltal közös érdekké és közös felelősséggé válik.

Magyarország kiberbiztonsági stratégiája illeszkedik az európai uniós és NATO-tagságából fakadó kötelezettségeihez, a környező országok és a világ fejlődésének irányt mutató országok stratégiáihoz is. Ezen stratégiák többségének közös pontja, hogy a fejlődés érdekében a digitális társadalom működéséhez elengedhetetlen biztonságos közeg megteremtését, a kritikus szervezetek és infrastruktúrák védelmét, az egyéni és a szervezeti tudatosság fenntartását, valamint a fokozott nemzetközi együttműködést célozza meg. A digitalizáció egy globális folyamat, elszigetelten nem lehetséges a biztonságos fejlődés megteremtése: az nemzetek közötti összefogást igényel.

Magyarország szuverenitásának védelme a kibertérben is nemzeti érdek. Magyarország a Nemzeti Biztonsági Stratégiában és a Nemzeti Katonai Stratégiában megfogalmazott célok támogatása érdekében jelen stratégiában is megerősíti, hogy hazánk biztonsági és katonai céljainak megvalósításához kiemelten szükség van a biztonságos kibertér által nyújtott szolgáltatásokra és az értékteremtésre, valódi hozzáadott értékkel rendelkező termékek és szolgáltatások létrehozására és működtetésére. Magyarország a kibertér szabad, demokratikus jogállami és biztonságos működését alapvető értéknek és érdeknek tekinti. Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósul meg.

A kiberbiztonság keretrendszerének, alapvető szervezeti feltételeinek biztosítása és az elektronikus információs rendszerek biztonságának megteremtése és fenntartása elsősorban az egyes kormányzati és nem-kormányzati intézmények döntéshozóinak, de leginkább az első számú vezetőinek a felelőssége. A kiberbiztonsági kockázatokat nem lehet egyszerűen biztonsági kockázatnak tekinteni, ezek komplex szemléletű, össztársadalmi kockázatot is jelentenek, amelyek kezelésében kiemelt szerepe van a komplex biztonság szavatolásának, továbbá a védelmi és biztonsági tevékenységek összehangolásának.

3. A kibertérben jelentkező legnagyobb kihívások

A különféle válságesemények, a hagyományos és az új típusú, katonai és nem katonai elemeket együttesen magába foglaló biztonsági kihívások és fenyegetések dinamikus váltakozása, eddig nem látott mértékben növelték meg a kiberbiztonsági kockázatokat. A fennálló fenyegetettségek

kölcsönös megjelenési formái, valamint az állami és nem állami szereplők fokozott online jelenléte növeli az államok kitettségét. Magyarország tekintetében a jelenlegi turbulens világban a kiberteret fenyegető veszélyek közül az alábbi kiemelt kockázatok azonosíthatók:

3.1. Válságok megjelenése: A 21. században is jelen lévő háborúk és az ezek által megváltozott biztonsági és geopolitikai viszonyok tovább formálják a kibertér védelméről alkotott elképzeléseket. A tapasztalatok ráirányították a figyelmet arra, hogy a kibertérből érkező fenyegetések és támadások – függetlenül attól, hogy állami vagy egyéb, nem állami szereplők, akár közvetlen vagy közvetett módon idézik elő –, valós hatással járnak az ország politikai, gazdasági, társadalmi folyamataira, nemzetbiztonsági és honvédelmi helyzetére, illetve jelentős zavarokat, illetve károkat okozhatnak.

3.2. Egyén és társadalom összhangjának megzavarása: A digitalizáció a modern világban magas szinten állt már korábban is, de az egyéni életvitelre, a társadalmi gondolkodásra, a kultúrára és az információszabadság működésére gyakorolt hatását teljesen átalakította a pandémia és kísérő jelenségei. Ennek eredményeként a kibertér egyszerre jelent a társadalmi dimenzióban újszerű kockázati halmazt és felerősítő erőt a hagyományos biztonsági kihívások és fenyegetések viszonylatában. A fentieket kiegészítendő kiemelést érdemel a társadalom információs csatornáinak veszélyeztetése, mint az egyik legnagyobb kockázat. Ide tartoznak az olyan ártó szándékú információs kampányok, amelyek digitális eszközök és módszerek alkalmazásával, mérnöki determináltsággal képesek elérni a célul kitűzött tudatállapotot, közvetve vagy közvetlenül hatást gyakorolva a társadalom alapvető döntési folyamataira. Mellékhatásként az információs csatornákba vetett bizalom megkérdőjelezésével a társadalom alapvető morálját támadják, figyelembe véve, hogy a társadalom egyénekre vagy kis közösségekre eshet szét hiteles kommunikációs csatornák nélkül, illetve hogy a befolyásolás hatására a társadalom elbizonytalanodik.

3.3. Függőség kialakulása: A digitális technológiától és elsősorban az internettől való nagyfokú függőség számos új működési modellt eredményezett mind a köz-, mind a magánszféra esetében, ahol külön figyelmet érdemelnek a kiskorúakat érő sajátos hatások. A függőségekből adódó fokozott sebezhetőségek olyan megnövekedett támadási felületet kínálnak a rossz szándékú szereplők számára, amelyeket folyamatosan szem előtt kell tartani.

3.4. Ellátási láncok megzavarása: Az ellátási láncok fenyegetettsége az elmúlt években kiemelt veszélyforrássá vált, mivel az azokhoz kapcsolódó, többnyire előre nem látható események kölcsönhatásai súlyos társadalmi, gazdasági és politikai következményekkel járhatnak.

3.5. Adatbiztonság sérülékenysége: A más állami és nem állami rosszindulatú szereplők a kiberteret egyre inkább az érzékeny és személyes adatok, információk, valamint állami, ipari és üzleti titkok illegális megszerzésére, kritikus infrastruktúrák működésébe történő beavatkozásra, az elektronikus információs rendszerekben történő károkozásra, a katonai és nemzetbiztonsági képességek befolyásolására, megzavarására vagy üzemelésének blokkolására, rombolására, a gazdasági és társadalmi szereplők megtévesztésére és manipulálására is használják. Külön kiemelést érdemel a fentieket kiegészítendő a zsarolóvírus-támadások növekedése által felvetetett problémák és a károk megszüntetését, minimalizálását szolgáló intézkedések.

Megjegyzendő, hogy a kibertérben veszélyként azonosított technológiák többsége a védelem oldalán is alkalmazható. Az eredményes kiberbiztonság kialakításához szükséges, hogy a

céljainkat szolgáló technikai eszközöket attól függetlenül alkalmazzuk, hogy azokra a támadó oldal már korábban rátalált.

A külső és egyéb fenyegetések mellett további kockázatot jelent, hogy a kibertér alkotóelemeiként szolgáló elektronikus információs rendszerek szabályozása nem elég széles körű, túlságosan decentralizált. A dinamikusan megjelenő és terjedő technológiák – mint például a mesterséges intelligencia alapú technológiák, az Internet of Things (a továbbiakban: IoT) eszközök, az 5G-vel megjelenő új technológiák és eszközök – újabb biztonsági kockázatok folyamatos kialakulásához vezetnek, a felhasználók technológiai kitettsége folyamatosan növekszik, így elengedhetetlen annak elvárása, hogy az új technológiák bevezetésének elsődleges feltétele a biztonságos környezet kialakítása.

A kibertér biztonságos használatát támogató felkészültség és információbiztonsági tudatosság számos esetben még további fejlesztésre szorul. Emellett a védelmi képességek megerősítése érdekében kiemelt jelentőséggel bír a kiberbiztonsági és informatikai területeken a szakemberek körének bővítésére erőfeszítések megtétele.

A digitális átalakulás, az internet globális természete és az erősödő kölcsönös függőségek országhatárokon átívelővé tették a kiberbűnözést, valamint a kiberbiztonsági fenyegetéseket és kockázatokat. A kibertér ezen túlmenően alkalmas a hagyományos kihívások és fenyegetések közvetítésére, felerősítésére, mely szintén részét képezi a védelmi és biztonsági feladatoknak. Mindezekre tekintettel a kiberbiztonsági események, a kiberbűnözés elleni fellépéshez erős és hatékony nemzetközi együttműködés szükséges.

4. Kritikus szereplők azonosítása

A kiberbiztonság közös érdek és felelősség, a társadalom minden rétegének kötelessége és feladata tenni a kiberbiztonság erősítése érdekében. A kiberbiztonság magas szinten tartásának egyik lényegi eleme a fenyegető szereplők azonosítása, amely kulcsfontosságú mind a megelőzés, mind a reagálás, az elhárítás szempontjából.

A kiberbiztonság erősítésének elsődleges feladata az állampolgár online jelenlétének és adatvédelmének kiberbiztonsági célú hatékony szavatolása. A teljes kiberbiztonsági ökoszisztéma elsődleges célja, hogy a társadalom kibertámadásoknak való kitettségét a lehető legalacsonyabb szinten tartsa.

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) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelv implementációja keretében 2025. január 1-jén hatályba lépett Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.), valamint végrehajtási rendeletei határozzák meg a kibervédelmi szervezetrendszer kereteit. A kibervédelmi szervezetrendszer – beleértve az irányítási keretrendszert, a felelős intézményeket és szerveket, valamint a jogszabályokat – felkészülési, védelmi és koordinációs szerepe kiemelkedő a kiberbiztonság stratégiai és operatív rétegében is.

4.1. Fontos szerep hárul az alábbi kiemelt stratégiai szintű szereplőkre:

4.1.1. a védelmi és biztonsági igazgatási rendszerre, mint Magyarországot és annak lakosságát veszélyeztető fenyegetésekkel és támadásokkal szembeni fellépésre létrehozott, illetve jogszabályban ilyen feladatra kijelölt állami szervek központilag összehangolt tervező, végrehajtó és rendelkező tevékenysége,

4.1.2. a kiberbiztonságért felelős biztos által vezetett Nemzeti Kiberbiztonsági Munkacsoportra, amely a Kormány javaslattevő, véleményező szerve,

4.1.3. a Nemzeti Kiberbiztonsági Fórumra, mint nem kormányzati szereplőkkel való együttműködésnek keretet biztosító szerv,

4.1.4. az Európai Unió és a NATO és egyéb nemzetközi szervezetek kiber ügyekkel foglalkozó illetékes szakértői csoportjai, bizottságai magyar képviselőinek mandatálásáért felelős hazai szakértői csoportok.

4.2. Fontos szerep hárul továbbá az alábbi kiemelt operatív szereplőkre:

4.2.1. a kiberbiztonsági incidenskezelő központokra (CSIRT) különösen:

4.2.1.1. a nemzeti kiberbiztonsági incidenskezelő központra,

4.2.1.2. a honvédelmi kiberbiztonsági incidenskezelő központra és

4.2.1.3. az ágazaton belüli kiberbiztonsági incidenskezelő központra,

4.2.2. a kiberbiztonsági hatóságokra,

4.2.3. az egyedüli kapcsolattartó pontra (SPOC),

4.2.4. az (EU) 2021/887 európai parlamenti és tanácsi rendelet szerinti, a kiberbiztonsági kompetenciaközösséggel való kapcsolattartásra kijelölt nemzeti koordinációs központra,

4.2.5. a Magyar Honvédség kibervédelmi erőire,

4.2.6. a Rendőrség információs rendszerekkel összefüggő bűncselekmények megelőzésére, felderítésére hivatott szervezeteire, mint a kiberbűncselekmények felderítésére és nyomozására feljogosított szervezet,

4.2.7. az operatív kiberbiztonsági központokra (SOC),

4.2.8. az információmegosztó és elemző szervezetekre (ISAC),

4.2.9. a szakágazati egyetemekre, kutatóintézetekre,

4.2.10. az érintett állami és gazdasági szereplőkre.

Ezen stratégiai és operatív szereplők egymással szorosan – a koordináció és adatmegosztások keretében kidolgozott szabályok alapján – együttműködve végzik a kiberbiztonságot erősítő feladataikat, amelyekbe beletartozik az információs csatornák biztosítása, az

információmegosztás és annak jogi szabályozása, a rendszeres találkozók, valamint az információcsere fenntartása a fenti szereplők, illetve a kiberbiztonság valamennyi releváns szereplője között.

A kritikus szervezetek és infrastruktúrák kiberbiztonsága kiemelt feladat az általuk nyújtott szolgáltatások jellege és Magyarország szuverenitása szempontjából, ugyanakkor egyes ipari, nagyvállalati elektronikus információs rendszerek, közműszolgáltatók által használt, hálózatba kötött nélkülözhetetlen eszközök, berendezések (ipari irányítási rendszerek – ICS) az egyes ipari területeken természetszerű, hosszabb technológiai ciklusokból adódó kiberbiztonsági lemaradás miatt kiemelt és folyamatos figyelmet követelnek.

Magyarország digitális felkészültségének érdekében átfogó megközelítés szükséges az újonnan felmerülő technológiai, biztonsági és fenntarthatósági kihívásokra. A technikai fejlődéssel párhuzamosan a kormányzat és a közigazgatás folyamatosan igyekszik megfelelni a modern kor elvárásainak. Az állami szolgáltatások egyre inkább a kibertérben jelennek meg, a hatékony működés érdekében az információs és kommunikációs technológiák használata megkerülhetetlen. A társadalom számára nyújtott digitális szolgáltatások tekintetében kiemelt jelentőségű a DÁP tv., az NDÁP és a NEKS megvalósítása, amelyek egységes alapon biztosítanak széles körű digitális szolgáltatásokat. Ennek érdekében kiemelt szerep jut az állami elektronikus információs rendszerek kiberbiztonságáért felelős szakembereknek. E szakemberek felkészültségének fenntartása és feladatuk szakszerű ellátásához szükséges információkkal való ellátása kiemelt feladat.

A kiberbiztonság fejlődését nagymértékben támogatják az oktatási és tudományos szféra innovatív megoldásai. Ezek megvalósításában kulcsszerepe van a legalacsonyabb oktatási szintektől kezdődő tudatosságra nevelésnek, valamint a humánerőforrás-utánpótlás biztosításának, mely alapul szolgálhat a kiberbiztonság általános szintjének emeléséhez. Fontos hozzájárulás a nem állami szereplők (egyesületek, szervezetek) kiberbiztonság javításáért tett erőfeszítése, és ezekre egyfajta szektoriális önkéntes társadalmi tevékenységként kell tekinteni. Az infokommunikációs társadalom kulcsfontosságú szereplői a szolgáltatások és az állampolgárok összekapcsolását biztosító digitális szolgáltatók.

Magyarország és gazdaságának alappillérei a gazdasági növekedést serkentő termelés, a szolgáltató és ez utóbbin belül kiemelten az infokommunikációs szféra, amelynek folyamatos, zavartalan működésének biztosítása a kiberbiztonság szempontjából kiemelt feladat.

5. Magyarország pozíciójának erősítése a nemzetközi kibertérben

Magyarország elkötelezett a kibertérben tanúsított felelős állami magatartás elismert önkéntes normáinak betartása és az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ), valamint egyéb regionális szervezetek keretei között történő konszenzusos továbbfejlesztése iránt. Magyarország elismeri a nemzetközi jog alkalmazhatóságát a kibertérre, és fontosnak tartja – a NATO és az Európai Unió által meghatározott keretek között – a témával kapcsolatos saját nemzeti értelmezés kialakítását. Kiáll a globális, nyitott, biztonságos és szabad internet, valamint az internet több érdekelt fél bevonásán alapuló (multi-stakeholder) kormányzási modelljének megőrzése mellett. Magyarország a nemzetközi szervezetek (különösen ENSZ, Európai Biztonsági és Együttműködési Szervezet, a továbbiakban: EBESZ), multilaterális, valamint a többi nem-kormányzati szereplőt magában foglaló kezdeményezések keretében hozzájárul a bizalomerősítő intézkedések gyakorlati alkalmazásának előmozdításához, amely

fontos szerepet játszik a nem szándékos kiberbiztonsági események megelőzésében és a konfliktusok deeszkalálásában.

Magyarország az Európai Unió tagjaként a kiberbiztonság területén együttműködik a tagállamokkal, aktívan részt vesz a közös helyzetismeret és kapacitások kialakításában, valamint szükség esetén a kölcsönös segítségnyújtásban. A NATO Magyarország biztonságának alapvető garanciája, így a kiberteret érő, harmadik országok és általuk támogatott csoportok által végrehajtott támadások elhárításában és a közös kibervédelmi képességek fejlesztésében szorosan együttműködik a NATO-tagállamokkal. A hazai digitális szuverenitás erősítése érdekében a kiberbiztonság magas szintjéhez elengedhetetlen a biztonságos, korszerű, a velük kapcsolatosan felmerülő kiberbiztonsági kockázatokat azonosító, követő és kezelő termékek és szolgáltatások fejlesztése és elterjedése.

Magyarország törekszik arra, hogy az állami szervek, a magyar vállalatok és szakértők a lehető legnagyobb mértékben részesüljenek a kiberbiztonság növelését célzó támogatásokból, és ezáltal aktív részesei legyenek az európai innovációnak.

Magyarország támogatja az állami szervezetek, magyar vállalatok és szakértők részvételét a kiberbiztonsággal és kiberbűnözés elleni harccal kapcsolatos, illetve egyes kiemelt partnerországaink kiber képességépítését célzó nemzetközi és európai uniós kapacitásépítési projektekben.

Magyarország aktívan részt vállal mind szakpolitikai, kiberdiplomáciai és operatív szinten az Európai Unió, a NATO, valamint a multilaterális és bilaterális kiberbiztonsági együttműködésekben és törekvésekben a magyar érdekek és célkitűzések hatékony képviselete mellett. Magyarország kiberdiplomáciai és szakpolitikai szinten, a magyar érdekek mentén aktívan részt vesz az Európai Unió és a NATO kiberbiztonsággal és kibervédelemmel kapcsolatos stratégiai célkitűzéseinek alakításában, a közös törekvések formálásában, végrehajtásában és harmadik felek irányába történő képviseletében. Ösztönzi az EBESZ keretében a bizalomerősítő intézkedések kidolgozását és végrehajtását, valamint hozzájárul az ENSZ a kibertérben tanúsított felelős állami magatartás normáinak tovább fejlesztésével, a kiberbiztonsággal és a kiberbűnözés elleni fellépéssel kapcsolatos munkafolyamataihoz, képviselve a fejezet elején rögzített alapvetéseket. Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye (röviden: Budapesti Egyezmény) részes államaként hazánk támogatja az egyezményben lefektetett standardok szélesebb körben történő elterjesztését, valamint biztosítja az egyezményen alapuló hatékony bűnügyi együttműködést a kiberbűnözés, illetve az elektronikus bizonyítékok gyűjtése és átadása terén. Emellett hazánk is nyomon követi a kiberbűnözés elleni új, univerzális ENSZ-egyezmény elfogadását célzó tárgyalások kimenetelét.

A kibertér, az európai és magyar alapvető és kritikus szolgáltatók védelméhez és a kiberválságok megelőzéséhez, koordinált kezeléséhez elengedhetetlen az uniós szintű műveleti együttműködés, ezért Magyarország aktívan hozzájárul a nemzeti számítógép-biztonsági eseményekre reagáló csoportok európai uniós hálózatában (CSIRT-hálózat) és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatában (EU-CyCLONe) folytatott információcseréhez együttműködéshez és nemzetközi gyakorlatokhoz. Különösen fontos az uniós munka során a közös helyzetismeret, a műveleti eljárások és a biztonságos információcserét lehetővé tevő platformok szükségtelen párhuzamosságok nélküli fejlesztése. Figyelmet érdemel a NATO, az EU és egyéb releváns nemzetközi szervezet (pl. EBESZ, ENSZ) keretei között folytatott gyakorlatokban való előkészített és koordinált magyar részvétel is.

Bűnüldöző hatóságaink támogatják a kiberbűnözők elleni fellépést szolgáló Europol és Interpol kezdeményezéseket, információcserét és műveleteket, és készek együttműködni más nemzetek hatóságaival a határon átnyúló kiberbűnözői csoportok felszámolása és az elkövetők felelősségre vonása érdekében. Ezen együttműködés részeként Magyarország csatlakozott az Amerikai Egyesült Államok javaslatára létrehozott nemzetközi zsarolóvírus-elleni kezdeményezéshez.

A kiberbiztonságot érintő két- és többoldalú tárgyalások során törekedni kell egy stratégiaibb, a szakdiplomáciai csatornákat egyaránt használó megközelítésre, kölcsönösen vizsgálva a multilaterális fórumokon folytatott együttműködés kétoldalú keretek között történő erősítését, partnerségek kialakítását, illetve fordítva a kétoldalú, regionális keretek között kidolgozott kezdeményezések multilaterális keretek között történő népszerűsítésére. A kibertér kölcsönösen függő tulajdonságából adódóan a sikeres védelemhez elengedhetetlen egyes versenypiaci szereplők egymással, valamint az állami szereplőkkel történő együttműködése, hiszen jelentős és meghatározó technológiai képességek ezen szereplők felügyeletében, birtokában vagy tulajdonában vannak. A piaci szereplőkkel való szoros együttműködés elengedhetetlen a nemzetbiztonság folyamatos fenntartása érdekében, hiszen az általuk birtokolt tudás és képesség erősíti a digitalizált társadalom és állam működését.

Hangsúlyosan meg kell jeleníteni Magyarországon is a nemzetközi téren egyre nagyobb teret nyerő ún. „Rule-based Order" koncepciót, azaz a meglévő nemzetközi szabályozók betartását a kibertérben, mely megfelelő alkalmazás mellett közelebb vihet a hibrid konfliktusok eszkalálódásának csökkentéséhez vagy – jó esetben – megakadályozásához.

A fenti elvek érvényesítéséért valamennyi releváns szereplő köteles minden tőle telhetőt megtenni. Különleges és kiemelt felelősség az egyes szervezetek első számú vezetőié, akik megfelelő eszközök birtokában vannak a célok elérésének támogatásához.

6. Általános stratégiai megállapítások

Jelen stratégia célja, hogy az Alaptörvény elveivel összhangban – figyelemmel a Nemzeti Biztonsági Stratégiában és a Nemzeti Katonai Stratégiában megfogalmazottakra, – az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, prioritásokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben.

A kiberbiztonság erősítése nemcsak védelmi feladat, hanem gazdasági lehetőség is. Ennek kiaknázása érdekében a jövőbe mutató kihívásokra úgy érdemes felkészülni, hogy ne csak finanszírozandó területként, hanem gazdasági, társadalmi és pénzügyi forrásként tekintsünk a kiberbiztonságra, mert a kiberbiztonság fejlesztésében nemcsak védelmi szempontok érvényesülése játszik szerepet, hanem egyedülálló gazdasági potenciál is rejlik benne. Magyarország elkötelezett olyan innovatív kiberképességek kutatása, fejlesztése és kiépítése iránt, amelyek önálló szellemi termékként vagy erre épülő magas minőségi szintű szolgáltatásként jelenhetnek meg határainkon túl is. Hazánk célja mindezek mellett a kibertérben rejlő lehetőségek, az abból következő komplex hatások és a biztonsági vonatkozások tekintetében is kutatásokkal és elemzésekkel vizsgálni a társadalmi, kulturális, állami működési kapcsolódásokat, és kiaknázni ezek eredményeit a kiberbiztonság fokozása terén is.

A kiberbiztonság közös felelősség, amely megköveteli az együttműködést. A kiberbiztonság erősítése közösen valósítható meg, mivel így az információk és tapasztalatok összeadódnak. Ennek biztosítása érdekében a kiberbiztonság különböző területeire a lehető legtöbb szereplőt kell bevonni. Magyarországon számos szektor, többek között a pénzügyi és energiaszektor kiberbiztonságának fokozása érdekében példaértékű tevékenységek zajlanak.

Ezen minták alapján a lehető legtöbb szektorban hasonló kezdeményezések támogatásával is fokozni kell a kiberbiztonság szakmai fejlődését.

A kibertérből érkező fenyegetések megakadályozása, hatékony elhárítása és kezelése érdekében cél a magyar információs és kommunikációs technológiai (IKT) hálózatok (és ennek részeként a termékek és szolgáltatások), a gazdaság és társadalom szempontjából alapvető és fontos feladatokat ellátó ágazatok rezilienciájának növelése és az operatív kapacitásépítés. Ennek tükrében átlátható szabályozási, beruházási és szakpolitikai eszközök szükségesek annak érdekében, hogy az állampolgárok, valamint a vállalati és kormányzati szektor a magyar nemzeti kibertérben megtalálható szolgáltatásokat biztonsággal használhassa.

A biztonságtudatosság kialakítása kiemelt fontosságú minden ágazat esetében, így a közigazgatásban munkát vállaló emberek között is, mivel az állami és önkormányzati szerveket növekvő számú és egyre kifinomultabb kibertámadás éri. A felhasználók megfelelő kiberbiztonsági tudatossága az incidensek megelőzésének egyik kulcseleme, ezért e terület folyamatos fejlesztése, képzési programok kidolgozása szükséges.

Minden szereplőnek meg kell teremtenie a kiberhigiénia alapjait, mely többek között az alábbi intézkedéseket és eljárásokat tartalmazza: rendszeres szoftver- és hardverfrissítések, a már biztonsági frissítésekkel nem támogatott komponensek mihamarabbi kivezetése a rendszerekből, biztonságos jelszóházirendek létrehozása, az új telepítések biztonságos kezelése, a rendszergazda-szintű hozzáférési fiókok korlátozása és az adatmentés. Lehetővé kell tenniük a proaktív felkészültségi keretet, valamint az aktív és általános biztonságot és védelmet kiberbiztonsági incidensek vagy kiberfenyegetések esetén. Törekedni kell olyan technológiai és szervezeti megoldások alkalmazására, melyek az aktív kiberbiztonságot mozdítják elő, ezen belül kiemelten gyors és hatékony, a lehetőségekhez képest automatizált megelőzést, incidenskezelést és adatmegosztást.

A szabályozás naprakészségéhez szükséges a kapcsolódó szakmai elemző és tudományos kutató kapacitások erősítése, (pályázati) támogatási lehetőségeinek fokozása és e körben a tudományterületeken átívelő, illetve a biztonsági fókuszú kutatások erősítése, lehetőleg a szabályozási környezet fejlesztését segítő kutatási eredményekkel párosulva.

Az ellenálló képesség fokozása érdekében a kiberbiztonságot integrálni kell a digitális beruházásokba már a tervezés fázisában, a köz- és magánszférában egyaránt („security-by-design”). Folyamatosan vizsgálni kell és szükség szerint be kell vezetni a legújabb kiberbiztonsági kockázatkezelési intézkedéseket és módszereket.

A hardver és szoftver beszerzések tekintetében elengedhetetlen felülvizsgálni a jelenleg érvényes szabályozókat, mivel kiemelten fontos, hogy a közbeszerzési rendszeren keresztül a legújabb biztonsági technológiák beszerzése, különösen a felhőalapú, valamint a mesterséges intelligenciát használó megoldások, ne ütközzön akadályba.

Szükséges fenntartani egy átfogó, nemzeti kiberbiztonsági képesség kiépítését és folyamatos magas szinten tartását. Ezen képesség garantálja a nemzetközileg hozzáférhető kiberbiztonsági szolgáltatások nemzeti felhasználásának magas szintjét.

Kiemelést érdemel, hogy a kritikus infrastruktúra szereplők, ezen belül is az állampolgárok vonatkozásában leghangsúlyosabban a pénzügyi és az energetikai szektorok, kiberbiztonsági szempontból különleges helyet foglalnak el.

Ezek a szektorok komolyan kitettek a kibertámadásokból eredő károkozásnak, és nagyban kihatnak a lakosság napi biztonságra. Ezen szereplők kiberbiztonságára különleges hangsúlyt kell fektetni, és kiemelten kell kezelni, hogy valamennyi szektorban minél egységesebb elvek szerint valósuljon meg a kiberbiztonság növelése.

Az összes szereplő kiberbiztonság javítása érdekében hozott intézkedésének meg kell teremtenie a hálózati és információs rendszerek infrastruktúrája, hardver-, szoftver- és online alkalmazásbiztonsága, valamint a szervezetek által felhasznált üzleti és végfelhasználói adatok védelmének alapjait.

7. Védelmi és biztonsági kérdések

Magyarország kiberbiztonságát nem csak a védelmi képességeinek erősítése biztosítja, hanem azon – szövetségi elköteleződésből is levezethető – törekvése is, hogy fejlessze elrettentő erejét, és különös figyelmet fordítson kibertere biztonságára, a szuverenitására veszélyt jelentő szereplők beazonosítására, felkutatására és felelősségre vonására, összehangolt védelmi és biztonsági fellépésbe illeszkedő kibervédelmi és kiberbiztonsági tevékenység által, továbbá fenyegetés-, illetve válságspecifikus működési megoldásokkal válsághelyzetek és különleges jogrend idejére. Ez elsődlegesen a magyar kormány felelőssége, azaz nemzeti hatáskör, ugyanakkor Európai Unió- és NATO-tagállamként számíthatunk szövetségeseink támogatására. A kiberműveletek elkövetőit jelenleg nehéz egyértelműen azonosítani, így a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezek bevonásával, a nemzeti mellett a nemzetközi jog alkalmazásával.

A hazánk ellen irányuló ellenséges kibertevékenységek kumulatív hatása elérheti a fegyveres támadás szintjét, vagy egy olyan küszöböt, ami – az Észak-Atlanti Tanács döntése alapján – a Washingtoni Szerződés V. cikk életbe léptetését vonhatja maga után. Ilyen esetben – a helyzet alapos, technikai, jogi és politikai értékelését követően – a nemzeti és a nemzetközi jog előírásainak megfelelő, eseti politikai elbírálás alapján akár katonai erővel – a fizikai vagy a kibertérből – történő válaszadás is indokolt lehet.

A kibertérben jelentkező feladatok rendkívül összetettek. Ezek megoldása érdekében a részfeladatok összehangolása és a kiberbiztonsági szempontok magas szintű egyenszilárdságú érvényesítése szükséges. A folyamatok stratégiai összehangolása, az új hazai védelmi és biztonsági szabályozási és működési környezettel összhangban álló keretrendszerben történő irányítása kiemelt cél.

8. Speciális célok és prioritások megfogalmazása

Magyarország, igazodva a kibertér jelentette technikai kihívásokhoz és azok folyamatos fejlődéséhez, valamint a támadások nemzetközi szinten tapasztalható növekvő tendenciájához és egyre nagyobb kifinomultságához, a bizalomépítés mellett jelen stratégiában a kibertér

használatához kapcsolódóan alapvető védelmi elveket és cselekvési irányokat az alábbi négy speciális célkitűzésben határozza meg úgy, hogy egyszerre ad iránymutatást az állami és a piaci szektor kibervédelmi feladatainak megoldásához:

8.1. A hazai kiberbiztonsági szervezetrendszer megszilárdítása és állami kiberbiztonság

Magyarország egyik legfőbb célja a kiberbiztonság terén illetékes kormányzati és nem-kormányzati szereplőket tömörítő stratégiai szintű fórumokból (Nemzeti Kiberbiztonsági Munkacsoport, Nemzeti Kiberbiztonsági Fórum), valamint operatív szereplőkből (nemzetbiztonsági szolgálatok, a Magyar Honvédség kibervédelmi erői, valamint a Rendőrség információs rendszerekkel összefüggő bűncselekmények megelőzésére, felderítésére hivatott szervezetei) álló szervezetrendszer megszilárdítása a kiszámíthatóság és a hatékonyság növelése érdekében. További feladatként jelenik meg a folyamatosan fejlődő vonatkozó uniós joganyag hatékony és maradéktalan átültetése a hazai jogrendszerbe.

A nemzetközi sztenderdeknek és irányelveknek történő megfelelés részeként vizsgálni kell a Nemzeti Kiberbiztonsági Munkacsoport és a tevékenységét támogató formációk (Operatív Törzs, kiberbiztonsági almunkacsoportok) működésének gyakorlati hatékonyságát, és ez alapján feladat- és hatásköreik pontosabb meghatározásának lehetőségét, hogy az hatékonyabban járulhasson hozzá a kiberbiztonság területén illetékes szervezetek közötti nemzeti szintű együttműködéshez, koordinációhoz, a kiberfenyegetésekkel kapcsolatos információk megosztásához (nemzeti kiberbiztonsági elemzések végrehajtása egységes szempontrendszer szerint, amelynek eredménye egy rendszeres értékelés Magyarország és az Európai Unió kiberbiztonsági fenyegetettségi és érettségi helyzetéről a szükséges összkormányzati intézkedések megalapozása érdekében).

Az ország kiberbiztonságát célzó együttműködésekben nem csak a közszféra szereplőire lehet és kell támaszkodni. Ebből a célból alkalmas fórumként kiemelendő a Nemzeti Kiberbiztonsági Fórum, amely a kormányzaton kívüli szereplők bevonására is hivatott.

A hatékonyság fokozása érdekében, az új nemzeti védelmi és biztonsági szabályozáshoz igazodva vizsgálni kell a 2025. január 1-jével felállt kiberbiztonsági szervezetrendszer működésének hatékonyságát, ezáltal is hozzájárulva kiberbiztonsági válsághelyzetek hatékonyabb kezeléséhez. A legjobb nemzetközi gyakorlatokból kiindulva vizsgálni kell az Európai Unió- és NATO-tagállamok kiber nagyköveteinek és koordinátorainak részvételével zajló találkozókon részt vevő magyar képviselő (jelenleg a Külgazdasági és Külügyminisztérium kibertér koordinátora), valamint a Kiberbiztonsági tv. által létrehozott kiberbiztonságért felelős biztos és Operatív Törzs feladat- és hatáskörei pontosabb meghatározásának lehetőségét, valamint az ezek ellátásához szükséges eszközök hozzárendelésének kérdését. Fokozni kell a különböző kiberbiztonsági kommunikációs és egyeztető fórumok működését, annak érdekében, hogy az információáramlás és tapasztalatcsere még hatékonyabb legyen, szem előtt tartva a párhuzamosságok elkerülését.

A követő, védelmi célú, monitorozás alapú kiberbiztonság folyamatos fejlesztésével, a jelenlegi eszközök horizontális és vertikális szélesítésével párhuzamosan és a nemzetközi jogi kötelezettségeinkre figyelemmel meg kell szilárdítani a proaktív kiberképességeket, azaz a potenciális támadások előrejelzését, megelőzését, valamint az aktív támadások megszakítását a támadók ellehetetlenítését a szféra összes szereplőjének bevonásával. Ezzel párhuzamosan törekedni kell arra, hogy egy komplex esemény esetén is a helyzetértékelési és helyreállítási

képességek a lehető legrövidebb idő alatt érvényre jussanak, az utólagos értékelést támogató incidens adatok megőrzése, utólagos kiértékelése és visszaható hasznosítása mellett.

Több módon is ösztönözni szükséges ágazaton belüli kiberbiztonsági incidenskezelő központok (CSIRT), operatív kiberbiztonsági központok (SOC), információmegosztó és -elemző szervezetek (ISAC) létrehozását, fejlesztését és az ehhez kapcsolódó adminisztratív és költségvetési háttér kialakítását. Állami keretekből támogatni kell működésüket, és külön fejlesztési kereteket kell biztosítani a folyamatos fejlődésük érdekében. Az ágazati kiberbiztonságot támogató szervezeti elemek létrehozásánál a kialakítás tervezésének pillanatától kezdve biztosítani kell a nemzeti kiberbiztonsági incidenskezelési struktúrába történő integrálást, a működésük kereteit, valamint a jó gyakorlatok megosztásának lehetőségét. Támogatni szükséges tovább azt is, ha több ágazat kíván egy ilyen központot létrehozni.

A fentiekre figyelemmel kiemelkedő fontosságú a nemzeti kiberbiztonsági incidenskezelő központ, a honvédelmi kiberbiztonsági incidenskezelő központ, illetve a kormányzati/közigazgatási SOC kialakítása és működtetése, hiszen ebben a szektorban ezek a biztonsági elemek járulhatnak hozzá leginkább a kiberbiztonsági szint általános emeléséhez. Kiemelést érdemel, hogy a különböző kiberbiztonsági incidenskezelő központok kerüljenek bevonásra a különböző egyeztető, stratégia és kommunikációs fórumokba, annak érdekében, hogy az információáramlás és tapasztalatcsere még hatékonyabb legyen, és csökkenjenek a párhuzamosságok. Az állampolgári bizalom megerősítése az e-közigazgatási intézményekkel és szolgáltatásokkal szemben alapvető stratégiai cél, ehhez pedig elengedhetetlen a biztonságos kormányzati elektronikus szolgáltatások biztosítása.

Egyre nagyobb hangsúlyt kapnak Magyarországon is az okosváros projektek. Nyomon kell követni az összekapcsolt vagy intelligens városok fejlődését és azok társadalomra gyakorolt lehetséges hatásait, valamint ezek kiberbiztonsági aspektusát, kihívásait, és amennyiben szükséges, úgy cselekvési tervet kell kidolgozni ezen projektek egységesen magas szintű kiberbiztonságának megteremtése érdekében.

8.2. Együttműködés és az innováció fokozása

A kiberbiztonság magasabb szintű megteremtésének egyik legfontosabb záloga, hogy Magyarország hazai és nemzetközi szinten is törekedjen az együttműködés és az ezen alapuló innováció fokozására, folyamatos fejlesztésére. A bizalmi alapú információmegosztást alapértelmezetté, általánossá kell tenni, mivel minden szereplő célja az egyenszilárdságú védelem megteremtése.

Ennek érdekében gyakorlati ajánlásokat és ellenőrzési irányelveket kell megfogalmazni a releváns hazai és európai jogszabályokhoz kapcsolódóan, ki kell alakítani a kiberfenyegetésekkel, az eseményekkel és egyéb releváns információkkal kapcsolatos megosztás szabályait, szervezeti és technikai feltételeit, valamint a szereplőket folyamatos tapasztalatcserére kell bátorítani a megosztási lehetőségek biztosításával, és ezen tevékenységhez be kell vonni a releváns piaci és tudományos szférát is.

Ezen túl erősíteni, lehetőleg automatizálni kell a megbízható, biztonságos információátadási megoldásokat a védelmi és biztonsági szervezetek felé, az összetett fenyegetettségek időben történő észlelése és kezelése érdekében. Ez a cél elérhető többek között a kibertámadások észlelését és megelőzését elősegítő mesterséges intelligencia megoldások fejlesztésének célzott ösztönzésével is.

Be kell vonni a releváns magyar kis- és középvállalkozásokat, a tudományos közösségeket és az állam különböző szereplőit a különböző hazai, uniós és egyéb projektekbe, illetve érdekeltté kell tenni a szereplőket a kutatási tevékenység fokozásában is. Intézkedéseket szükséges hozni a kis- és középvállalkozások ellátási láncaiban felmerülő kihívások kezeléséhez. Szintén javasolt olyan szolgáltatások létrehozása, mint a honlapok konfigurációja és naplózás lehetővé tétele, az ilyen képességekkel nem rendelkező mikro- és kisvállalkozások számára.

Magyarország ösztönzi és támogatja a kibertér biztonságát növelő tudományos tevékenységeket, kutatásokat és azok eredményeinek hasznosítására irányuló induló vállalkozásokat. Ennek keretében kiemelt támogatást nyújt a mesterséges intelligenciával, az IoT-vel, az 5G technológiákkal és a dezinformáció elleni védekezéssel kapcsolatos kiberbiztonsági kutatások és fejlesztések részére.

8.3. Tudatosítás és a kibertudatosság megteremtése

Magyarországnak széles körű, nagy hatású, koordinált, általános és speciális célú kiberbiztonsági tudatosító tevékenységet kell végeznie annak érdekében, hogy a szereplők és végső soron az állampolgárok kiberhigiénés és dezinformációval kapcsolatos ellenálló képessége még dinamikusabban fejlődjön, és így a kiberbiztonsági események többsége megelőzhetővé váljon. Mindezek megvalósításához a trendek folyamatos megfigyelése, valamint a hazai és nemzetközi együttműködési csatornák segítségül hívása szükséges. Minden szereplőnek törekednie kell arra, hogy az általa akár ügyfélként, akár egyéb módon elért állampolgárok biztonságtudatosságát a lehető legmagasabb szintre emelje.

A megfelelő biztonsági szint elérése, fenntartása és fejlesztése érdekében Magyarország elkötelezett abban, hogy a hazai elektronikus információs rendszerek biztonságos használatához és üzemeltetéséhez kapcsolódóan megfelelő oktatási és képzési hátteret biztosítson, és ahhoz a társadalom legszélesebb rétege – így az olyan speciális célcsoportok, mint a gyermekek, idősek, fogyatékkal élők, mikro- és kisvállalkozások vagy a civil szervezetek – is hozzáférhessenek. Magyarország külön figyelmet fordít a kritikus szervezetek és infrastruktúrák, valamint a Kiberbiztonsági tv. szerinti alapvető és fontos szervezetek tudatosítási folyamatára, valamint kiváló hazai szakemberek Európai Kiberbiztonsági Készség Keretrendszerrel (ECSF) összhangban történő képzésére és itthon tartására.

A kiberhigiénés képességek hátterének biztosításában különleges felelőssége van a kiberbiztonsági szervezetrendszer operatív elemeinek, valamint az oktatási és tudományos szférának, amelyek szellemi hátteret és folyamatos képzési lehetőséget biztosítanak mindenki, de kiemelten a polgárok, az érdekelt felek és a szervezetek számára a kiberhigiénés képességek fejlesztéséhez, valamint folyamatosan, a trendeknek megfelelő figyelemfelhívó kampányokkal segítik a megfelelően magas szintű tájékoztatást.

A fentiek eléréséhez a kiberbiztonsági szempontok általános érvényre juttatására, kibervédelmi eszközök és szoftverek üzemeltetését célzó képzések megjelenítésére van szükség a köznevelésben és a felsőoktatásban. Az informatikához kapcsolódó képzésekben meg kell jeleníteni a kiberbiztonság olyan elemeit, mint a biztonságfejlesztés („security-by-design”) és a biztonságos programozás. Ennek nemcsak a kiberbiztonság általános erősítése, hanem a szakemberek toborzása szempontjából is kiemelkedő jelentősége van. A meglévők erősítése mellett olyan további tudásközpontokat, tudástranszfer bázisokat kell létrehozni, ahol az ország legkiválóbb szakemberei hatékonyan tudnak dolgozni a fenti cél elérése érdekében.

A kiberbiztonsági tudatosság újabb szintje az állami „hibavadász” („bug bounty”) program, amelynek keretei meghatározásra kerültek a Kiberbiztonsági tv.-ben. Ennek során lehetőség nyílik az elektronikus információs rendszerekben meglévő hibáknak, sérülékenységeknek a társadalomra nem veszélyes formában és mértékben történő felkutatására és az illetékesek felé történő jelzésére. A Kiberbiztonsági tv. megalkotta a sérülékenységek összehangolt nyilvánosságra hozatalának jogszabályi kereteit, s ehhez kapcsolódóan meg kell teremteni a végrehajtás szervezeti és technikai feltételeit. Ezzel párhuzamosan biztosítani kell a technikai fejlesztések kapcsán azt, hogy az ezektől elvárható kiberbiztonsági szintet biztosító, korszerű védelmi megoldások már a tervezés legkorábbi szakaszában, kötelező jelleggel beépítésre kerüljenek.

Az egyes állami és piaci szereplők kiberbiztonsági elemző képességének nyilvántartásával, illetve általában az állami és piaci szereplők kiberbiztonságot érintő együttműködésének fokozása révén lehetőség nyílna a szinergiák kihasználására és egy súlyos kiberbiztonsági incidens bekövetkezése esetén lehetőség lenne az erőforrások megfelelő szintű koordinálására. Ezen képességeket operatív szinten folyamatosan mérni kell, amelyekhez megfelelő standardok és mérési követelmények adaptációja vagy kidolgozása szükséges.

Magyarország célul tűzi ki, hogy a 2026. év végére az alap- és középfokú oktatási intézményekben érzékenyítő programok induljanak, és a 2027. év végére legalább a középfokú végzettségűek megkapják a kibertér biztonságos használatához szükséges ismeretanyagot, valamint a felsőoktatás releváns képzésein nagyobb hangsúlyt kapjon a biztonságtudatossági szemlélet kialakítása. Az iskolarendszerből kikerült felnőttek, különösen az időskorúak és a hátrányos helyzetű társadalmi csoportok részére speciális képzéseket kell indítani.

8.4. Kiberbiztonsági tanúsítás ösztönzése

A digitalizációs transzformáció eredményeként az állampolgárok, vállalkozások és államigazgatási intézmények által egyre szélesebb körben használt infokommunikációs termékek és szolgáltatások kiberbiztonsági kockázatot hordoznak. Az infokommunikációs termékek és szolgáltatások tekintetében a nemzeti tanúsító hatóságoknak az IKT termékek és szolgáltatások minél szélesebb körére nemzeti kiberbiztonsági tanúsítási rendszert kell kidolgozniuk, amelyek az egyes termék- és szolgáltatástípusok tekintetében biztonsági garanciát jelentenek. A kiberbiztonsági követelményeket a termék gyártójának vagy a szolgáltatás nyújtójának kell teljesítenie. A követelményeknek való megfelelést, a megvalósított védelmi kontrollok vizsgálatát elsődlegesen külső harmadik fél (megfelelőségértékelő szervezet) által elvégzendő független értékeléssel kell biztosítani.

Az infokommunikációs termékek és szolgáltatások európai és nemzeti kiberbiztonsági tanúsítási rendszerek alapján végzett tanúsítása pozitív hatást gyakorol a piacra, mivel az ahhoz történő alkalmazkodás növeli a hazai infokommunikációs szektor teljesítményét és versenyképességét, továbbá a harmadik országból származó eszközök is ellenőrizhetővé válnak. Az állami szabályozás ösztönzően kell, hogy fellépjen a piacon elérhető digitális eszközök közötti szelekció érdekében, előnyben részesítve olyan eszközöket, amelyek kiberbiztonsági tanúsítvánnyal rendelkeznek (pl. közbeszerzés során). Azon ágazatok, szervezetek esetén, amelyek a társadalom és a magyar gazdaság működése szempontjából alapvető igényeket elégítenek ki, Magyarország kötelezővé teszi tanúsított infokommunikációs termékek és szolgáltatások használatát. A tanúsítványok kötelezővé tétele emeli az érintett termékek, illetve szolgáltatások minőségét és megbízhatóságát, nemzetközi szinten is versenyképesebbé, versenyállóbbá téve a magyar gyártású termékeket.

8.5. Piaci szereplők

A fenti célok hatékony elérése és a kiszámítható környezet megteremtése érdekében szükséges a piaci szereplők és a kiberbiztonsági szervezetrendszer viszonyrendszerének tisztázása, együttműködésük fokozása.

A mai infrastrukturális környezetben valamennyi szereplő számára számos előnyt nyújthatnak a felhőalapú szolgáltatások. Igénybevételük azonban csak úgy képzelhető el, ha a használatból fakadó előny jelentős, és a használatuk nem csökkenti, hanem számottevően és a felhasználó számára is nyomon követhető módon növeli a kiberbiztonságot.

Meg kell ismerni azokat a technológiai megoldásokat, amelyek biztosítják, hogy a magyar adatok feletti felügyelet a felhő technológiák alkalmazása mellett sem csökken, és a magyar adatok magyar célok érdekében hasznosulnak. Meg kell vizsgálni, hogy a technikai és a szabályozási eszközök egymást kiegészítő alkalmazásával kezelhetők-e a legújabb technológiákkal együtt járó kockázatok, és ennek tükrében informált döntéseket hozni az egyes területeken a legalkalmasabb eszközökről. A vizsgálatot a ma és a holnap fenyegetéseinek és kockázatainak figyelembevételével kell elvégezni.

A saját szuverenitásunk attól is függ, hogy más országok nálunk eredményesebben tudják-e saját szolgálatukba állítani a legmodernebb technológiát és infrastruktúrát. Ezért körültekintően kell meghozni azokat a döntéseket, amelyek mellékhatásaként valamely modern technológia legversenyképesebb fajtájáról lemondunk. A megfelelő technológiai beruházások nélkül csökkenhet a képességünk arra, hogy a kihívó országokkal szemben érvényesítsük egyéb területeken megszerzett komparatív előnyeinket konfliktushelyzetekben.

A felhőszolgáltatások egyre elterjedtebbek, és az innovációk, újdonságok, illetve a legújabb biztonsági technológiák egyre inkább ezekben az alkalmazásokban jelennek meg. Így a publikus felhőszolgáltatások igénybevételének támogatása érdekében célszerű egy minősítési rendszert (mellette referencia architektúrák, fejlesztési, implementációs és üzemeltetési jó gyakorlatok) létrehozni – az EUCS (EU Cloud Service Scheme) figyelembevétele mellett –, amely lehetővé teszi a felhasználók eligazodását a napjainkra több száz, ezer elemi szolgáltatásból álló felhőszolgáltatások (IaaS, PaaS, SaaS) között, illetve mindezt beépíteni a hazai közbeszerzési gyakorlatba olyan módon, hogy a minősített felhőszolgáltatások kategóriába kerüljenek. A felhő szolgáltatókkal és szoftver gyártókkal történő kiberbiztonsági együttműködés kialakítása jelentős tudástranszfert tesz lehetővé, ami akár a hazai felsőoktatásban, akár a közigazgatási IT üzemeltetésben naprakész, magas szintű ismereteket eredményezhet.

Jelenleg a magyar szoftverexport fejlesztés finanszírozása és támogatása gyerekcipőben jár. A hazai IKT termékeket és szolgáltatásokat nyújtó szereplők nagy része kis- és középvállalkozás, ennek ellenére a szegmensre hiányoznak azok az állami ösztönzők és a pénzügyi termékek, amelyek igénybevétele lehetővé tenné a hazai „szoftver innovációt”, azaz a hazai digitális – kifejezetten nem hardver, hanem szoftver termékek fejlesztését. Célként kell kitűznie az érintett szektoroknak és vállalatoknak azt, hogy a vállalkozások és fejlesztések finanszírozására és támogatására megfelelő eszközök álljanak rendelkezésre. A pénzügyi szektor együttműködésén túl a szabályozási környezetet is átalakítani szükséges. Különösen fontos ez az átfogó cél hazánk versenyképességének fokozása szempontjából, mivel hozzáadott érték tekintetében jelenleg az egyik legdinamikusabban fejlődő stratégiai irány az IKT termékeket és szolgáltatásokat nyújtó szereplők köre, és azon belül az exportképes szoftverfejlesztési

tevékenység. Ezen kívül célként megfogalmazható, hogy a 2025. január 1-jén hatályba lépett hazai szabályozói környezet folyamatosan aktualizálásra, konszolidálásra és harmonizálásra kerüljön, lekövetve a digitális technológiákban történő robbanásszerű fejlődést.

A piaci szereplők hatékony elérése és a felhőalapú szolgáltatások igénybevétele (valamint pl. a hozzájárulás alapú adatszolgáltatások biztosítása) a DÁP tv. és az NDÁP céljai között is szerepel, többek között ezért kiemelten fontos, hogy a szabályozást úgy kell kialakítani, hogy a piaci szereplők és így Magyarország kiberbiztonsága is egységesen egyre szilárdabbá váljon és a harmadik fél általi adatkezelés olyan garanciális elemeket tartalmazzon, amely az ország infrastrukturális és technológiai integritását és szuverenitását nem veszélyezteti. A harmadik fél általi adatkezelés elvárásrendszerének pontosítása, egységesítése, illetve bizonyos informatikai képességek és funkcionalitások külső szolgáltató által történő ellátására vonatkozó szabályozások egységesítése, konszolidálása szintén hozzájárulna a legújabb technológiák elterjedéséhez, s így a magasabb szintű kiberbiztonság eléréséhez.

Olyan szabályozási, infrastrukturális és oktatási környezetet szükséges létrehozni, amely arra ösztönzi a nemzetközi szervezeteket, hogy a kiberbiztonsággal kapcsolatos operatív tevékenységüket érdemes legyen Magyarországra telepíteni, így kétirányú tudástranszfer indulhat meg az oktatási szféra és a privát szféra között.

A piaci szférát is ösztönözni és támogatni szükséges a saját kiberbiztonsági ellenálló képességének növelésére. Ennek érdekében támogatási mechanizmusokat kell kialakítani, amelyek révén a szereplők hozzáférhetnek kiberbiztonsági fejlesztési forrásokhoz és célzott támogatási pályázatokhoz. Emellett oktatási és tudatosságnövelő programok – például ingyenes vagy kedvezményes tréningek, edukációs konferenciák – is segítsék a vállalkozásokat a digitális fenyegetések felismerésében és kezelésében.

9. Ágazati célok és prioritások

9.1. Közigazgatási ágazat

A közigazgatás kibervédelme súlyponti kérdés, egyrészt az állampolgári bizalom fenntartása oldaláról, másrészt a nemzetbiztonsági szempontból kritikus állami adatvagyon megóvása szempontjából. A költséghatékony és korszerű közigazgatás jelentősen átalakul és az ügyek intézése helyett a proaktív, automatizált szolgáltatások nyújtására helyeződik a fókusz, amelyek széles körű igénybevételének alapfeltétele a digitális állami szolgáltatásokkal szembeni állampolgári bizalom fenntartása és további erősítése. Ehhez kapcsolódó elvárás a kibervédelmi tevékenységek tekintetében, hogy az alapszolgáltatásokhoz kapcsolódóan ne történhessen olyan incidens, amely miatt az állampolgárokban megrendülhet a digitális szolgáltatásokba vetett bizalom. Az állami adatvagyon megóvása és a digitális szolgáltatások működésének szavatolása alapvető fontosságú, amelynek érdekében a kibervédelmi ágazat folyamatos erősítése szükséges, különös tekintettel a fenyegetettségek jelentős mértékben növekvő globális trendjére.

A fentiek alapján rögzíthető, hogy a digitális állampolgárság létrehozása keretében a digitális térben történő ügyintézés és a szolgáltatások nyújtása felhasználóbarát alapokra helyeződik. Az egységes alapokon működő, széles körű digitális szolgáltatások – különösen azonosítás és aláírás, biztonságos elektronikus kommunikáció és dokumentumkezelés, a szolgáltatásokhoz kapcsolódó online fizetési rendszer – biztonságos igénybevétele és további fejlődésének lehetősége az ágazati célok és prioritások támogatásával kerül kialakításra. Kiemelt

jelentőséggel bír az állami adatvagyon védelme, amely a technológiai színvonalemelés és az állami szervek fokozottabb együttműködése érdekében továbbfejlesztésre kerül, biztosítva ezzel a mobiltelefon és egyéb hordozható, digitális adatkapcsolat létesítésére alkalmas eszközök elsődleges és biztonságos használatát a digitális ügyintézésben.

A közigazgatási ágazat kibervédelmének optimális kialakításához ágazati CSIRT/SOC elemek közül kiemelkedő fontosságú a nemzeti kiberbiztonsági incidenskezelő központ és a honvédelmi kiberbiztonsági incidenskezelő központ, illetve SOC bővítése és folyamatos fejlesztése, annak érdekében, hogy a gyakorlatban is tapasztalható jelentős mértékű és fokozódó fenyegetettségekhez igazadó mértékű védelmi képességet elérje hazánk. Mindemellett kiemelt jelentőségű, hogy a közigazgatási CSIRT/SOC rendszerek a hazánkban elérhető honvédelmi, katonai és szakszolgálati célú kibervédelmi rendszerektől is kapjanak folyamatosan információkat a fenyegetettségekről, tekintettel arra, hogy az esetleges támadások elsődleges célpontjai a társadalom működésének alapjait biztosító közigazgatási rendszerek.

9.2. Honvédelmi ágazat

A nemzeti kiberbiztonsági ellenálló képesség erősítése és fenntartása érdekében a honvédelmi ágazat célja az alábbi területek kiemelt támogatása.

Magyarország a nemzeti gazdaság és ipar fejlődését és ezáltal az ország védelmét elősegítő beruházásként tekint a honvédelemhez kapcsolódó gazdasági társaságok kiberbiztonságának folyamatos magas szinten tartására. Ezért támogatja ezen szereplők esetében is a biztonságot megerősítő kiberképességek fejlesztését, lehetővé teszi azok állami eszközökkel történő felügyeletét, ellenőrzését.

A honvédelmi ágazati jelentős infrastruktúrák és szervezetek ellenálló képességének fokozása és valamennyi kritikus szervezet és infrastruktúra egységes elvek mentén történő védelme érdekében erősítjük a kibervédelemmel foglalkozó gazdasági, valamint állami szereplők közötti együttműködést, tapasztalatcserét.

Az ágazatok közötti kommunikációnak kiemelt jelentősége van az együttműködés erősítése területén. Az ágazaton belüli kommunikáció hatékonyságának növelésén keresztül hatással lehetünk az ágazatok közötti, különösen a kríziskommunikáció eredményességére is. Ez kiemelten fontos válsághelyzetekben, azok kezelése során.

Az ország biztonsága szempontjából nélkülözhetetlen a személyi állomány kiberbiztonsági kultúrájának erősítése, folyamatos fejlesztése. Az új technológiák és eljárások megismerését ösztönző honvédelmi kibergyakorlatok lehetővé teszik a személyi állomány számára, hogy felkészültségük korszerű maradjon. Az állomány folyamatos oktatása, tudatosítása és a megszerzett ismeretek készség szinten történő alkalmazása biztosítja a humánerőforrás képességének fejlődését. A gyakorlatokon történő folyamatos és magas szintű részvétel a konstruktív tudásmegosztás, a nemzetközi együttműködés hatékonyságának növelése, a kapcsolatok erősítése szempontjából is kiemelt jelentőségű, ezért ennek folyamatos fenntartására van szükség.

A kognitív térben végrehajtott műveletek hatássokszorozó képességének kihasználása céljából ezen képességek fejlesztése prioritást élvez. A kiberműveleti képesség, mind a saját haderő tagjai ellenálló képességének fokozásával, mind az ilyen jellegű támadásokkal szembeni

védekező képesség fenntartásával hozzájárul a szembenálló fél kognitív hadviselés hatásainak csökkentéséhez.

9.3. IKT és digitális infrastruktúra ágazat

A digitális infrastruktúra tekinthető a kibertér „vérkeringését" biztosító hálózatnak, az IKT termékek és szolgáltatások pedig rendkívül fontos alkotóelemnek, amely szerkezetét tekintve heterogén felépítésű, nagyszámú szolgáltató van jelen a piacon és egymással konkuráló szolgáltatásokat, megoldásokat nyújtanak. A piaci szektor esetében a versenysemlegesség alapelveinek betartása mellett törekedni kell a technológiai standardok megerősítésére, a katasztrófatűrő képesség és a reziliencia fejlesztésére. Az állami szektor esetében megvalósítandó feladat az infrastruktúra elemek konszolidációja, egységesítése, amelynek eredményeként kialakuló homogén(ebb) állami digitális infrastruktúra elősegíti az optimális kibervédelmi megoldások kiépítését. Tekintettel arra, hogy az egyes rendszerek zártsága, szeparáltsága folyamatosan csökken az IoT technológiák, az okos megoldások (pl. közmű szektor okosmérés) és a magas szolgáltató képességű integrációk miatt, ezért a proaktív és öntanuló kibervédelmi megoldások széles körű alkalmazásának kialakítása elkerülhetetlen.

Megfelelően erős biztonsági követelményeket, szabályokat és kereteket kell alkotni a nyílt internet nyilvános alkotóelemei általános rendelkezésre állásának, sértetlenségének és bizalmasságának fenntartására vonatkozóan.

Az IKT- és digitális infrastruktúra szolgáltatóknak kiemelt jelentősége van abban, hogy ezen szolgáltatást biztonságosan és folyamatosan üzemeltessék.

A stratégiai időszakban célkitűzés a kiberbiztonsági kötelezettségek hatálya alá tartozó szervezetek egészére kiterjedő szabályozás kialakítása, amely az EIR-ek és IKT termékek és szolgáltatások, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával, üzemeltetésével és selejtezésével kapcsolatosan közreműködő ellátási lánc kockázatainak és esetlegesen bekövetkező biztonsági eseményei elemzésére és kezelésére vonatkozóan előírja a tervezési dokumentumrendszer (stratégia; szabályzat; eljárásrend; folyamat; terv stb.) készítését és aktuálisan tartását. Ennek alapjait a Kiberbiztonsági tv. és végrehajtási rendeletei megteremtették.

Tekintettel a digitális infrastruktúra szolgáltatásokban érintett szereplők jelentős számára, fontos, hogy az érintett szervezetek az IKT-termékek és szolgáltatások kapcsán megosszák a biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket az ágazati incidenskezelési szervezet útján és így járuljanak hozzá a sérülékenységek összehangolt közzétételéhez, valamint az önkéntes kiberbiztonsági információmegosztáshoz.

9.4. Egészségügy

Az egészségügyben, mint kiemelten kritikus ágazatban egyre inkább előtérbe kerülnek a digitális technológiák. Ez a digitalizáció előnyösen hat az egészségügyi ágazatra, ugyanakkor fokozott kiberfenyegetést is jelent. Éppen ezért az egészségügyi informatikai infrastruktúra minden résztvevőjére nézve kiemelten fontos az információbiztonság, az e-egészségügyi (e-health) ökoszisztéma fenntarthatóságához szükséges bizalom megerősítése. Ennek érdekében kiemelten fontos az információbiztonsági és kibervédelmi szabályoknak történő megfelelés és működtetés.

Az egészségügyben alkalmazott mesterséges intelligencia alapú döntéstámogatás, az egészségügyi ágazat kutatási fejlesztési területének mesterséges intelligencia fejlődése, az ágazatban zajló adatvezérelt fejlődés komoly biztonsági kihívások elé állítja az ágazatot. A jelenleg szigetszerűen működő egészségügyi alkalmazások egységesítése, mesterséges intelligenciával történő támogatása az adatok védelmében is fontos szerepet fog játszani.

Az Internet of Things (IoT), illetve az Internet of Medical Things (IoMT) vagyis a dolgok, illetve orvosi dolgok internete, az egészségügy területén számos előnyt hoz, ugyanakkor komoly adatvédelmi kihívásokat is felvet. Az IoT szenzorok folyamatosan adatokat gyűjtenek a környezetükről és a betegekről. Az eszközök által generált adatokat megfelelően szükséges védeni. Az adatok titkosítása, hitelesítése és biztonságos tárolása elengedhetetlenül fontos.

9.5. Agrár ágazat

A mezőgazdasági adatok jellege nagyon specifikus, kiterjed a termőföldre, agronómiára, az állatállományra, takarmányozásra, időjárási adatokra, a technológiára, a pénzügyi adatokra és a szabályozást érintő megfelelőségi adatokra is. Az adatok egy része személyes adatnak tekinthető, hiszen például a termőföldre vonatkozó adatok GPS koordinátái megadják a pontos földrajzi helyet, amihez személyes tulajdon kapcsolható, így érzékeny adatoknak minősülnek. Az adatok a döntések támogatása mellett leírják, és adott körülmények között meghatározzák a termőföld, az üzem piaci értékét, előre jelzik az előállított termékek mennyiségét, minőségét, ütemezését, valamint az input anyagok felhasználását és a szükséges beruházásokat is. Mivel a mezőgazdasági adatok mind a gazdálkodói, mind a teljes értéklánc szempontjából gazdasági jelentőségűek, ezért elengedhetetlen kiberbiztonsági biztosítékok beépítése.

A kiberbiztonság tekintetében az ágazatban négy szint azonosítható.

a) A fizikai adatgyűjtő és műveletvégző szint, itt találhatóak mindazok a szenzorok és munkavégző gépek, amelyekkel egyrészt megtörténik a termelés körülményeiről az adatgyűjtés, másrészt elvégzésre kerülnek a termelés egyes folyamatai. Ebben a rétegben keletkezik az adatok legnagyobb része.

b) A felhasználói réteg – e rétegben azon számítógépek jelennek meg, amelyek az üzem tulajdonában vannak, és amelyekre befutnak a szenzoros adatgyűjtés eredményei, illetve amelyeken megtörténik a döntéstámogatás, illetve a munkavégző gépek vezérlése.

c) A hálózati réteg – ezen réteg elemei kötik össze a fizikai és műveletvégző réteget egymással és a felhasználói réteg számítógépeivel, valamint a felhő réteggel – ide tartozik minden kábeles és rádiójeles technológia, ami gépek között adatátvitelt végez.

d) A felhő réteg – ide futnak be a hálózaton keresztül mindazon adatok, amelyek az üzem gazdálkodásával kapcsolatosak – így mondható, hogy az üzem tulajdonában levő dolgok nemcsak a fizikai és a felhasználói, hanem a felhő rétegben is jelen vannak.

Az előzetes elemzések alapján mind a négy szinten komoly kockázatokat jelent az adatok jelenlegi felhasználása.

A kockázatok közül prioritásként kezeljük az adat- és felhőszolgáltatási kockázatokat, mert ezen folyamat végén előálló döntési és vezérlési utasításokban keletkező hiba a termelők sokaságánál okozhat egyszerre komoly meghibásodást és leállást.

Az ide tartozó szolgáltatók zöme külföldi, gyakran nem EU-s tulajdonban van, erőfölényből fakadó kockázatok szinte a teljes agrárdigitalizációs szférában jelentkeznek, mivel egyrészt a szereplők jelentős része külföldi, másrészt olyan globális nagyvállalatokról van szó, amelyek technológiai fejlesztéseiket monopolizálva jelentős erőfölényre tesznek szert, nem csupán a termelővel szemben, de akár a hazai kormányzatra is komoly nyomást képesek gyakorolni.

A digitalizáció szintjének növekedésével a helyzet teljes egészében megváltozhat, ezért már most érdemes kiemelt védelemben részesíteni a hazai mezőgazdaság azon legnagyobb kockázati értékkel bíró és legszélesebb elterjedtségnek örvendő szegmenseit (meteorológiai szolgáltatások, navigációs szolgáltatások, gépoptimalizálási szolgáltatások, farmmenedzsment-rendszerek), amelyek akár már a közeljövőben egy ilyen típusú támadás célpontjává válhatnak, súlyos károkat okozva úgy a szolgáltatások nyújtóinak, mint igénybe vevőinek.

9.6. Világűr ágazat

A dinamikusan fejlődő technológiák között fontos megemlíteni a kiberbiztonság űrrendszereket érintő vonatkozásait. Az űrrendszerek kritikus szerepet játszanak az államok védelmét és biztonságát garantáló műveletekben, a szuverén állami politika megannyi dimenziójában, valamint az állampolgároknak és a gazdaság szereplőinek nyújtott kulcsfontosságú szolgáltatások biztosításában. Hosszú ideig az űr esetében a legelterjedtebb kiberbiztonsági kockázatokat a „zavarás" és „maszkolás" jellegű tevékenységekben kellett keresni, melyek a „rendszerek rendszere megközelítés" mentén első körben a földi kiszolgáló infrastruktúrák ellenálló képességét teszik próbára. Azonban napjainkban már az űrtevékenységek teljes beszállítói, szolgáltatásnyújtási és szolgáltatásfelhasználói értéklánca ki van téve a kiberműveleti támadó tevékenységek teljes spektrumának, ezért a védelem átfogó megközelítést igényel. Az esetleg kompromittáló tevékenységek mentén olyan láncreakció idézhető elő, amelyben sérülhet a kritikus adatok pontossága, bizalmassága, integritása vagy rendelkezésre állása, illetve a műhold üzemeltetés biztonsága vagy szolgáltatásnyújtó képessége.

Az űrszektorhoz köthető kibervédelmi aspektusoknak meg kell akadályozniuk az űrtevékenységekkel kapcsolatos érték láncok felderítését, támadóképességek kifejlesztését, a rendszerekhez való hozzáférését, a támadó tevékenység végrehajtását, hosszú idejű fenntartását, a védelmi rendszerek elkerülését és az alrendszerek közötti rosszindulatú átjárást annak érdekében, hogy az ellátási láncok biztonságát biztosítani tudjuk. Az Európai Bizottság által egy uniós űrjogszabály-javaslat kidolgozása folyamatban van, amely többek között a NIS 2 irányelvre is épít. A több pilléres javaslat egyik meghatározó ága az ellenálló képesség növelése, amelynek egyik jelentős eleme a kibervédelmi kérdések kezelése.

9.7. Energetika, víziközművek és hulladékgazdálkodás

A digitális megoldások működésének nélkülözhetetlen feltétele a villamos energia biztosítása. Megfelelő ellátás nélkül a digitális és távközlési szolgáltatások rövid időn belül megszűnnek. Az ágazatra jellemző a növekvő hálózati ellátásbiztonság, ennek részeként a kiberbiztonság mind nagyobb mértékben szükséges fejlesztése. Az iparágban kihívást jelent a változásra körültekintőbb módon reagáló ellátásbiztonság és a gyorsan változó igényekkel fellépő kiberbiztonság eltérő reakcióideje. Az infóbiztonság hatékony működésének feltétele a mind nagyobb mértékű felkészült szakember-ellátottság; jelenleg azonban ennek inkább érzékelhető hiánya mutatkozik. A hazai nagyfeszültségű hálózat a nemzetközi, európai hálózat része, ahol kedvező helyzetet jelent, hogy számosságában jól kezelhető mennyiségű ponton szükséges a

védekezés megvalósítása, azonban a kiberbiztonsági feladatokat az országos kiterjedésen túl régiós, valamint nemzetközi összefüggésben is értelmezni kell. A közép- és kisfeszültségű hálózat számos végpontból áll, működtetése, védelme jelentősebb erőfeszítést igényel, azonban a bekövetkező események korlátozott kiterjedésűek lehetnek. A megújuló energiatermelők által jelentett kihívások kezelésére egyre több digitális eszköz kerül a hálózatra beépítésre, jellemzően a nyilvános mobil hálózaton elérhető módon. Jelentős kiberbiztonsági kockázatot hordoz a különböző digitális eszközök (például napelem-inverterek, felhőszolgáltatások) beépítése a hálózati működésbe, amelyek kezeléséről, a kockázatok csökkentéséről felügyeleti rendszerekkel, azonnali beavatkozást lehetővé tevő központok (SOC) alapításával és működtetésével célszerű gondoskodni. A megújuló energiatermelők között sérülékenység szempontjából különös figyelmet érdemel a hazai háztartási méretű kiserőművek (HMKE) állománya. Az 50 kVA teljesítményt meg nem haladó eszközök számossága a 2025. évben elérte a 300.000-t, és a beépített összteljesítménye meghaladta a 2,5 GW-ot, ugyanakkor ezen eszközök a kibervédelmi képességeiknek szintje alacsony egyéni teljesítményük, és a velük szemben támasztott csatlakozási követelmények okán jellemzően alacsony. Az elosztottság rendkívüli magas mértékének fényében nagyszámú és/vagy területileg célzott kibertámadás komoly kihívást jelenthet az érintett kisfeszültségű hálózati elemekre nézve.

A víziközművek területén jelenleg mind az ivóvíz ellátás, mind a szennyvízelvezetés és víztisztítás területén a digitalizáció szintje alacsonynak mondható. Ugyanakkor a korábbi irányítástechnikai rendszerek fejlesztése miatt ezen a területen is egyre több távmenedzselésű, digitális rendszerből lekérdezhető, és irányítható elem jelenik meg. Ezek egységes kiberbiztonsági ellenálló képességéről a kialakítást megelőző tervezési folyamat során szükséges gondoskodni.

A hulladékgazdálkodási értéklánc elemeit figyelembe véve, kiberbiztonsági szempontok a hulladékégető létesítmények kapcsán jelentkezhetnek kiemelt jelentőséggel, tekintettel arra, hogy a rendszerszerű működésben kialakuló zavar következtében gyors reagálást igényel a hulladékok megfelelő elhelyezése és a kieső hulladékhasznosításból származó energia pótlása. Fontos megjegyezni, hogy hazai szinten jelenleg egy létesítmény tekinthető jelentős szereplőnek a települési hulladék energetikai hasznosítása terén. A hulladékgyűjtés és szállítás, valamint a hulladékkezelés egyéb szereplői kevésbé érintettek a kibervédelem területén, esetükben az alkalmazott logisztikai megoldások védelmét szükséges megfelelően biztosítani.
A hulladékgazdálkodás értéklánc mentén kibervédelmi stratégiai szempontok jelentkeznek az alábbiak szerint:

a) A hulladékkezelési folyamatok digitalizációja és automatizációja növeli a hatékonyságot, egyben kiszolgáltatottabbá teszi a rendszert a kiberfenyegetésekkel szemben.

b) A hulladékgazdálkodási adatok védelme kiemelt jelentőséggel bír, mivel érzékeny információkat tartalmaznak a hulladéktermelőkről, a hulladék mennyiségéről, összetételéről, kezeléséről.

c) A hulladékgazdálkodási infrastruktúra védelme magában kell, hogy foglalja a hulladékgyűjtő, -szállító, -feldolgozó és -tároló eszközöket és létesítményeket, amelyek potenciális célpontjai lehetnek a kibertámadásoknak.

d) A hulladékgazdálkodási szereplők és a kiberbiztonsági hatóságok közötti együttműködés és koordináció erősítése azért fontos, mert az elősegíti a kibervédelmi tudatosság növelését, a

kockázatok felmérését és kezelését, valamint a kiberbiztonsági incidensek megelőzését és kezelését.

10. Zárás

10.1. Finanszírozás

A kiberbiztonsági rendszeren belül a kiberbiztonságért felelős szervezetek mindegyikének, ideértve adott esetben a piaci szereplőket is, elegendő forrást kell biztosítani a kiberbiztonsági rendszer elvein alapuló feladatok és tevékenységek teljesítéséhez. A pénzügyi források biztosítása során nemcsak az állami költségvetésből származó forrásokra kell támaszkodni, hanem az európai uniós alapok operatív programjaiból származó forrásokra is, valamint megfelelően, hatékonyan és célorientáltan kihasználni az állami és magánszféra együttműködésén alapuló finanszírozási formákat is.

Az államnak, valamint szervezeteinek és intézményeinek alapvető érdeke, hogy minden szinten elegendő forrást biztosítsanak a kiberbiztonságra, a megfelelő képzettséggel, tapasztalattal rendelkező kiberbiztonsági szakemberek anyagi elismerésére, megtartására, hogy a jelen stratégiában meghatározott stratégiai kiberbiztonsági célkitűzések teljesülhessenek, ezáltal az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk védelmének biztosítása és így a kibertér védelme megvalósuljon.

A finanszírozáshoz kapcsolódó stratégiai célkitűzés, hogy a döntéshozók makró szinten megkapják a megfelelő tájékoztatásokat a fenyegetettségekről és a kockázatokhoz kapcsolódó gazdasági-társadalmi hatásokról, amelyek ismerete elősegítheti a védelmi és biztonsági intézkedések implementációs költségeinek eredményes allokálását.

A pénzügyi források biztosítása során mindenekelőtt az e célra felhasználható európai uniós forrásokra, illetve az állami és magánszféra együttműködésén alapuló finanszírozási formákra szükséges támaszkodni.

Emellett a stratégiai célkitűzések megvalósításában és a végrehajtásban érintett költségvetési szerveknek és háttérintézményeiknek a Stratégiában meghatározott szerepükből adódó feladataik finanszírozását a rendelkezésükre álló forrásokból szükséges biztosítani.

10.2. Végrehajtás

A kiberstratégia hatékony végrehajtásához egy kooperatív elvek mentén megfogalmazott intézkedési terv elkészítése és végrehajtása szükséges, amelynek segítségével a stratégiában megfogalmazott célkitűzések és szakpolitikai intézkedések maradéktalanul és hatékonyan teljesülhetnek, segítve a beazonosított kitettségek és kockázatok minimalizálását, különös tekintettel a szakemberhiányra, az együttműködés elmélyítésére, az ellenálló képesség célrendszerének érvényesülésére, az adatbiztonság növelésére, a kiberbiztonsági oktatásban részt vevők körének kiszélesítésére és a tananyagok folyamatos felülvizsgálatára. A magyar kibertér biztonságáért felelős intézményrendszer folyamatosan figyelemmel kíséri a digitális környezetben jelentkező kihívások dinamikus változását, és szükség szerint a stratégia felülvizsgálatával reagál az új feladatokra.