1139/2013. (III. 21.) Korm. határozat

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1. A Kormány elfogadja az 1. mellékletben foglalt Magyarország Nemzeti Kiberbiztonsági Stratégiáját.

2. A Kormány felhívja a Miniszterelnökséget vezető államtitkárt, hogy tegye meg a Nemzeti Kiberbiztonsági Koordinációs Tanács kialakításához szükséges intézkedéseket.

Felelős: Miniszterelnökséget vezető államtitkár a feladat- és hatáskörrel rendelkező miniszterek bevonásával

Határidő: 2013. június 30.

3. A Kormány felhívja a Miniszterelnökséget vezető államtitkárt a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott feladatok ellátását szolgáló munka- és intézkedési terv elkészítésére.

Felelős: Miniszterelnökséget vezető államtitkár a feladat- és hatáskörrel rendelkező miniszterek bevonásával

Határidő: 2013. június 30.

4. Ez a határozat a közzétételét követő napon lép hatályba.

1. melléklet az 1139/2013. (III. 21.) Korm. határozathoz

Magyarország Nemzeti Kiberbiztonsági Stratégiája

1. Jelen stratégia célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. A stratégia célja a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme a XXI. század meghatározóvá vált új közege, a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben. Célja továbbá a nemzetgazdaság és társadalom szabad tevékenységének védelme és biztonságának garantálása, az új technológiai innovációk biztonságos adaptálása a gazdaság növekedésének biztosítása érdekében, valamint nemzetközi együttműködések kialakítása ezen a téren a magyar nemzeti érdekek szerint. Jelen stratégia jelzi, hogy Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté kívánja alakítani. A megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése.

2. Jelen stratégia Magyarország Alaptörvényében megfogalmazott alapértékek – szabadság, biztonság, jogállamiság, nemzetközi és európai együttműködés – leképezése egy külön

biztonság-, és gazdaságpolitikai területre, az Alaptörvény 38. cikkéből levezetett, a nemzeti vagyon részét képező nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának dokumentuma. A stratégia összhangban az 1035/2012. (II. 21.) Korm. határozattal elfogadott Magyarország Nemzeti Biztonsági Stratégiájával, abból kiindulva kifejti annak a kiberbiztonságról szóló 31. pontjában meghatározott törekvéseket és megfogalmazott kormányzati felelősséget. Gyökereiben a 2001-ben elfogadott Budapesti Konvencióig nyúlik vissza („Convention on Cybercrime"), mely nemzetközi egyezmény napjainkban is referenciaként használt, nemzetközileg elfogadott alapelveket fogalmaz meg. A stratégia egyben igazodik az Európai Parlament által 2012. november 22-én elfogadott, „A kiberbiztonságról és védelemről szóló", 2012/2096(INI) számú határozatában a tagállamok felé megfogalmazott ajánlásokhoz, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményhez. A stratégia illeszkedik továbbá a NATO 2010 novemberében elfogadott Stratégiai Koncepciójához, a Szövetség 2011 júniusában elfogadott Kibervédelmi Politikájához és ennek végrehajtási tervéhez, valamint a 2010. november 19–20-ai lisszaboni és a 2012. május 20–21-ei chicagói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elvekhez és célokhoz.

I. Magyarország kiberbiztonsági környezete

3. A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.

4. A kibertérben megjelenő, különböző forrásból származó fenyegetések megnövekedett száma és ezek nagyságrendekkel megnövekedett következményei jelzik, hogy az elmúlt évtizedben nagy gyorsasággal nőtt azon állami és nem állami felhasználók száma és hatékonysága, akik a kiberteret kritikus adatok, információk illegális megszerzésére, valamint a kommunikációs és informatikai rendszerekben történő károkozásra használják. Elektronikus információs rendszereinkre, illetve azokon keresztül létfontosságú rendszereink és létesítményeink működésére jelent fenyegetést a hadviselés új formája, az információs hadviselés, ami által a modern hadviselés egyik legfontosabb színtere a kibertér lett. A külső károkozások mellett további kockázatot jelent, hogy a kibertér alkotóelemeiként szolgáló informatikai és hírközlési rendszerek üzembiztonsági szabályozása sem kellően rendezett. A dinamikusan megjelenő új technológiák, mint például az informatikai felhő vagy a mobilinternet, újabb biztonsági kockázatok folyamatos kialakulásához vezetnek. Jelen stratégia egyik fő célja annak a döntéshozó politikai és szakmai figyelemnek és képességnek a kiépítése, mely rugalmasan reagálva lehetővé teszi a belátható jövőben a technológiai fejlődésből fakadó új kiberbiztonsági problémák kezelését.

5. A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a

kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

II. Magyarország kiberbiztonsági értékrendje, jövőképe, céljai

6. Magyarország szuverenitásának védelme a magyar kibertérben is nemzeti érdek; a magyar 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.

7. Magyarország a globális kibertér minden Magyarországgal hasonló értékrendet valló állami és nem állami szereplőjével kölcsönös bizalmon alapuló együttműködés kialakítását és fenntartását célozza meg, továbbá szövetségi és nemzetközi kapcsolati rendszerén, különösen az EU és a NATO, továbbá az Európai Biztonsági és Együttműködési Szervezet (EBESZ), az ENSZ, az Európa Tanács és más nemzetközi szervezeti tagságán keresztül törekszik a globális kibertér szabad és biztonságos használatának szavatolására. Magyarország tudatában van annak, hogy a kibertérben megjelenő fenyegetések és támadások elérhetnek egy olyan szintet, ami szövetségesi együttműködést tehet szükségessé, ezért kiemelten fontosnak tartja, hogy a kiberbiztonság kérdése bekerült a NATO Alapító Okmányának 5. cikkelye alá tartozó kollektív védelem körébe. E szövetségesi nemzetközi együttműködésben Magyarország saját biztonsága miatt is érdekelt. Magyarország különös figyelemmel tekint a közép- és kelet európai régióra, melynek kiberbiztonságát regionális együttműködések keretében tovább erősíthetőnek látja.

8. Magyarország a jelen és a jövő kihívásaihoz igazodva követelményként rögzíti, hogy a magyar kibertér nyújtson biztonságos és megbízható környezetet:

a) az egyének és közösségek számára a szabad, félelemmentes, a személyes adatok védelmét garantáló kommunikáción keresztül a társadalmi fejlődéshez és integrációhoz,

b) a gazdasági szereplők számára a hatékony, innovatív üzleti megoldások kialakításához,

c) a jövő generációi számára az értékelven alapuló tanuláshoz és az egészséges lelki fejlődést eredményező, sérülésmentes tapasztalatszerzéshez,

d) az elektronikus közigazgatás számára, hozzájárulva az állami szolgáltatások innovatív és előremutató fejlesztéséhez.

9. Magyarország a szabad és biztonságos kibertér használat érdekében a nemzetbiztonság, a hatékony válságkezelés és a felhasználó-védelem szempontjainak összehangolásával megvalósítandó célként rögzíti, hogy:

a) rendelkezzen hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességekkel a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen,

b) nemzeti adatvagyona megfelelő szintű védelemben részesüljön, létfontosságú rendszereinek és létesítményeinek kibertérhez kapcsolódó működése üzembiztos legyen,

valamint rendelkezésre álljon kompromittálás esetén a megfelelően gyors, hatékony és a veszteséget minimalizáló, különleges jogrend idején is alkalmazható helyreállítási képesség,

c) a magyar kibertér biztonságos működéséhez szükséges informatikai, hírközlési termékek és szolgáltatások színvonala elérje a legjobb nemzetközi gyakorlatokét, kiemelt hangsúlyt fektetve a hazai és nemzetközi biztonsági tanúsítási szabványoknak való megfelelésre,

d) a kiberbiztonsági oktatás, képzés, valamint a kutatás és fejlesztés színvonala megfeleljen a legjobb nemzetközi gyakorlatoknak, hozzájárulva egy világszínvonalú hazai tudásbázis kialakításához,

e) a gyermekek és a jövő nemzedékek számára a biztonságos kibertér kialakítása megfeleljen a legjobb nemzetközi gyakorlatoknak.

III. A célok eléréséhez szükséges feladatok

10. Magyarország kiberbiztonsági helyzete alapvetően szilárd. A kibertér sajátos szerkezetéből eredően azonban számos olyan biztonsági kockázattal és fenyegetéssel kell számolni, amelyek nemzeti szempontból stratégiai kihívást jelentenek. A kiberbiztonság megfelelő szinten tartásához és folyamatos fejlesztéséhez, a kitűzött célok eléréséhez rendelkezésre álló eszközök és a feladatellátással érintett területek a következők:

a) Kormányzati koordináció. A kibertér szabad és biztonságos használatában gyakorlatilag minden kormányzati szervnek elsődlegesen saját felelőssége van. Azonban e terület összetettsége következtében ezen felelősségek csak világos és hatékony kormányzati koordináció keretein belül tudják a szabad és biztonságos kibertérre irányuló kormányzati célt megvalósítani. Ezért kiemelt figyelmet kell fordítani a Miniszterelnökség keretében megvalósuló összkormányzati koordináció erősítésére, amely alapfeltétele a kormányzati és ágazati erőforrások koordinált és koncentrált alkalmazásának.

b) Együttműködés. Kiberbiztonsági érdekeink és céljaink eléréséhez szükséges az együttműködés javítása és a hatékony információcsere. Ennek érdekében olyan operatív együttműködési fórumok működtetése szükséges, amely a civil, a gazdasági és a tudományos területek képviselőinek részvételét biztosítja a kormányzati döntés-előkészítési folyamat során és lehetőséget nyújt arra, hogy ezen fórumok tagjai ajánlásokat és véleményt fogalmazzanak meg a kiberbiztonsági tevékenység fejlesztésére, folyamatos újítására.

c) Szakosított intézmények. A kiberbiztonsággal összefüggő feladatok ellátását a specifikus szakértelemmel és hatáskörrel rendelkező szervezetekhez szükséges telepíteni, amely szervezetek nem csak egymással, hanem az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködnek. A feladatellátás érinti a nemzetbiztonsági, honvédelmi, bűnüldözési, katasztrófavédelmi és létfontosságú intézmények és létesítmények védelmével kapcsolatos feladatokat ellátó szervezeteket, valamint az elektronikus információbiztonság területén hatósági jogosítványokkal rendelkező intézményeket. A kiberbiztonsági eseményekkel kapcsolatos feladatok ellátását az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által akkreditált tagszervezetként működő kormányzati eseménykezelő központ, valamint az egyes szakágazatok területén működtetett ágazati eseménykezelő központok végzik.

d) Szabályozás. A többlépcsős jogalkotási tevékenység mellett szükséges a civil, a gazdasági és a tudományos terület szereplőivel együttműködési megállapodásokat kötni, amelyek megfelelő alapot és szabályozást biztosítanak a közös felelősségvállaláson alapuló kiberbiztonság hatékony működtetéséhez.

e) Nemzetközi együttműködések. Magyarország tovább kívánja erősíteni aktív szerepét az EU és a NATO keretein belül folyó kibervédelmi kezdeményezésekben és együttműködésben, valamint az ENSZ és az EBESZ kiberbiztonsági együttműködéseiben. Folytatni és erősíteni kívánja együttműködését az EU és a NATO kibervédelmi gyakorlataiban és tervezésében, továbbá fenntartja élenjáró szerepét az operatív kormányzati együttműködések kialakításában és működtetésében ezen szervezetekben, valamint a közép- és dél-kelet európai régióban. Magyarország különös gondot fordít azon tevékenységek megvalósítására, melyeket egyrészt az Európai Unió Digitális menetrendje határoz meg a tagállamok számára, másrészt a NATO Kibervédelmi Politikája és végrehajtási terve ír elő a szövetségesek részére. Az atlanti együttműködést a kiberbiztonság terén kiemelten fontosnak tartja. Magyarország fenntartja aktív szerepét a nemzeti/kormányzati és ágazati incidenskezelő központok európai, atlanti és globális szervezeteiben, az Európai Hálózati és Információ Biztonsági Ügynökségben, valamint az Európai Elektronikus Hírközlési Hatóságok Testületében.

f) Tudatosság. Magyarország fenntartja élen járó szerepét a kiberbiztonsággal összefüggő hazai és nemzetközi szakmai fórumok szervezésében. Szakosított intézményein, a civil, a gazdasági és a tudományos terület szereplőivel kialakított együttműködéseken keresztül támogatja a kibertér biztonságos használatát célzó és figyelemfelhívó tevékenységeket, valamint a kiberbiztonsági gyakorlati tudást elősegítő kezdeményezéseket, különös figyelmet fordítva az egyéni felhasználók, valamint a kis- és középvállalkozások tudatosítására.

g) Oktatás, kutatás-fejlesztés. Magyarország kiemelt figyelmet fordít arra, hogy az általános, a közép- és felsőoktatásban, a kormányzati tisztviselők képzésében és a szakmai továbbképzéseken a kiberbiztonság szakterülete integrálódjon az informatikai oktatásba. Magyarország stratégiai együttműködés kialakítására törekszik azon egyetemi és tudományos kutatóhelyekkel, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását.

h) Gyermekvédelem. Magyarország a kiberbiztonság lényegi elemének tekinti a gyermekek egészséges fejlődését lehetővé tevő környezet kialakítását és fenntartását, melyet minden érintett területen prioritásként kezel, megvalósítva egyben a Gyermekbarát Internet Európai Stratégiájának célkitűzéseit. Kifejezett hangsúlyt fektet a gyermekeknek és fiataloknak szóló minőségi online tartalmak előállításának ösztönzésére, a tudatosságnövelő és felkészítő intézkedések támogatására, a gyermekek zaklatása és kizsákmányolása elleni küzdelemre, s a biztonságos online környezet megteremtésére. A gyermekvédelem területén kiemelt partnerének tekinti az online gyermekvédelem terén eredményeket elért magyar civil szervezeteket.

i) Gazdasági szereplők motivációja. Az informatikai és hírközlési közbeszerzések kiberbiztonsági követelményeinek meghatározása során Magyarország abban érdekelt, hogy azok a lehető legmagasabb szintű kiberbiztonsági védelem kialakítására ösztönözzék a közbeszerzéseken résztvevő informatikai és hírközlési eszközgyártókat és szolgáltatókat, kiemelt hangsúlyt fektetve a nemzetközi biztonsági tanúsítási szabványoknak való megfelelésre. Magyarország törekszik egyben arra, hogy a gazdasági élet szereplőivel

közösen dolgozzon ki olyan ösztönző intézkedéseket a gazdaság szereplői számára, amelyek a kiberbiztonság fokozását célozzák.

IV. A Nemzeti Kiberbiztonsági Stratégia végrehajtásához rendelkezésre álló, illetve megerősítendő kormányzati eszközök

11. Magyarország a stratégia céljainak eléréséhez mind a kompetenciák, mind a potenciális erőforrások terén a szükséges eszközök jelentős részével már rendelkezik, ezek között szerepel:

a) a magyar kibertér biztonságáért felelős kormányzati szervezetek számbavétele és koordinációja, a hatékony együttműködés kialakítása;

b) a magyar kibertér biztonságáért felelős civil, gazdasági és tudományos szervezetek számbavétele és intézményes keretek között folyó együttműködés kialakítása;

c) a létfontosságú információs infrastruktúrák és vagyonelemek, illetve a nemzeti adatvagyon számbavétele és védelmének biztosítása;

d) a szakosított kormányzati intézmények működtetése;

e) a szabályozási környezet biztosítása;

f) a nemzetközi és regionális együttműködésekben történő részvétel, politikai, operatív és szabályozási szinten egyaránt;

g) a támogatási keretrendszer kialakítása a kutatás és fejlesztés, valamint az oktatás és tudatosítás terén;

h) gazdasági motivációs rendszerek megteremtése;

i) a kiberbiztonsági szempontok érvényesítése az állami műszaki fejlesztési feladatok, valamint a kormányzati információs rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatok ellátása során.

12. A rendelkezésre álló eszközök megerősítéséhez, hatékonyabb felhasználásához és nemzeti biztonsági szempontok szerinti eredményesebb gyakorlatba ültetéséhez szükséges egy koherens, kormányon belüli és nem-kormányzati együttműködési rendszer kialakítása és működtetése.