# 5. Kibervédelem és biztonság

*Kovács Zoltán*

A kibervédelemmel foglalkozó szervezetek fontos feladatot látnak el a kibertérben vagy az annak segítségével elkövetett bűncselekmények elleni küzdelemben is. Egyrészt azért, mert azon támadók között, akik ellen küzdenek, megtalálható – a kevés tudással rendelkező személyektől a kiberbűnözőkön át egészen az államilag támogatott hackercsoportokig – a kibertérben illegális tevékenységet folytatók teljes palettája. A kibervédelmi szervek által végzett tevékenység azonban jelentősen akadályozza, adott esetben meg is akadályozza az említett támadókat céljaik elérésében. Másrészt pedig azért, mert ezek a szervezetek az általuk elérhető információk megosztásával és kapcsolatrendszerük segítségével hathatósan tudják támogatni akár a nyomozásokat, akár a szükséges intézkedések (például egy külföldi, káros tevékenységet folytató szerver lekapcsoltatása) végrehajtását.

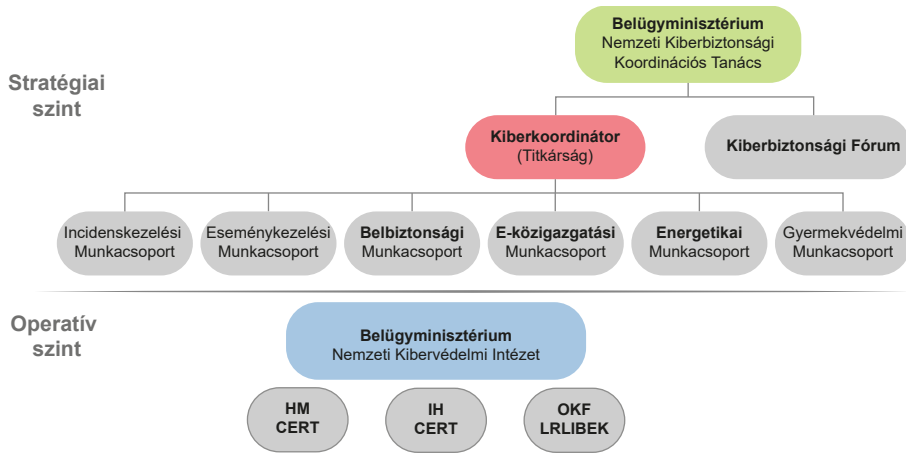
## 5.1. A hazai kibervédelemi szervezetek

Az elmúlt években kialakult a hazai kiberbiztonságért felelős szervezeti rendszer, amely alapvetően két szintre bontható: stratégiaira és operatívra. A stratégiai szinten a Kiberbiztonsági Fórum, a kiberkoordinátor, valamint az általa vezetett munkacsoportok találhatók, míg az operatív szintet – több esetben hatósági funkciókkal is kiegészülve – a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézet (NKI), az Országos Katasztrófavédelmi Főigazgatóság szervezetében található Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK), a Honvédelmi Minisztérium és az Információs Hivatal saját hálózatbiztonsági vészhelyzeteket elhárító csoportjai (*Computer Emergency Response Team,* a továbbiakban: CERT[1]) alkotják. Ezt mutatja be az 1. ábra.

Ezt a struktúrát egészítik ki azok a szintén operatív tevékenységet ellátó szervezetek (NISZ Zrt. kibervédelmi szervezeti egysége, Hun-CERT, KIFÜ CSIRT), amelyek vagy speciális kibervédelmi részfeladatokat látnak el az állami, önkormányzati rendszerekben, vagy nem az állami, önkormányzati rendszerek területén fejtik ki kibervédelmi tevékenységüket. Ezen szervezetekről a későbbiekben még esik szó.

---

[1] Az Amerikai Egyesült Államokban működő US-CERT feloldásaként a United States Computer Emergency Readiness Teamet használják.




1. ábra

*A hazai kibervédelmi struktúra 2015. július 16. után*

*Forrás:* saját szerkesztés TIKOS 2017 alapján

### 5.1.1. A hazai kibervédelem stratégiai szintje

A hazai kibervédelmi struktúra szervezeti, funkcionális és hatásmechanizmusait a 2. ábrán láthatjuk.


2. ábra

*A magyarországi kibervédelmi struktúra szervezeti, funkcionális és hatásmechanizmusai*

*Forrás:* saját szerkesztés RAJNAI 2016 alapján

*5.1.1.1. Nemzeti Kiberbiztonsági Koordinációs Tanács*

A Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) feladatait a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet[2] határozza meg. E szerint a Tanács feladata, hogy elősegítse a kormányzati tevékenységek koordinációját a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott cselekvési területeken, valamint azokon figyelemmel kísérje az egyes feladatok végrehajtását. Ennek érdekében a meghatározott cselekvési területekhez társított kormányzati intézkedések alapján a Tanácsnak a kiberbiztonsági munkacsoportok, valamint a kiberkoordinátor irányításával és a Fórum javaslatainak figyelembevételével el kell készítenie és évente felül kell vizsgálnia az úgynevezett Nemzeti Kiberbiztonsági Akciótervet.

*5.1.1.2. A kiberkoordinátor*

A kiberkoordinátor feladatait szintén a 484/2013. (XII. 17.) Korm. rendelet tartalmazza. E szerint a kiberkoordinátor látja el

- a Kiberbiztonsági Fórum munkájának szakmai koordinálását;
- az állami szerveknek a kiberbiztonsági munkacsoportok munkájában való részvételre történő felkérését, ahol a delegált közszolgálati tisztviselő tagok mellett ő maga is részt vesz azok munkájában;
- a Tanács, a Fórum és a kiberbiztonsági munkacsoportok működtetésével kapcsolatos adminisztratív teendők irányítását;
- a kiberbiztonsági munkacsoportok és a kiberkoordinátor irányításával a Nemzeti Kiberbiztonsági Akcióterv elkészítését;
- a Tanács üléseinek összehívását;
- a Tanács elnökének irányításával a Tanáccsal kapcsolatos kommunikációs feladatok ellátását és felügyeletét.

A kiberkoordinátor szakértői támogatását az e-közigazgatásért felelős miniszter által vezetett minisztériumban működő titkárság látja el.

*5.1.1.3. Kiberbiztonsági Fórum*

A Kiberbiztonsági Fórum (a továbbiakban: Fórum) a stratégiából adódóan fontos szerepet tölt be a hazai kibervédelmi szervezetrendszerben. Fő feladata a Tanács munkájának segítése, elsősorban a nem kormányzati szervezetek (*non-governmental organization,* a továbbiakban: NGO) és más szakmai tömörülések, mint például a Szövetség a Digitális Gazdaságért Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (a továbbiakban: IVSZ), Neumann János Számítógép-tudományi Társaság (a továbbiakban: NJSZT) és egyéb

[2] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről.

mértékadó szolgáltatók (például a Magyar Telekom Csoport) alkotják. A Fórum elsősorban a jogszabályalkotás szakmai támogatását biztosítja, de képes elősegíteni, motiválni a Tanács által igényelt szolgáltatások megvalósulását is.

*5.1.1.4. Kiberbiztonsági munkacsoportok*

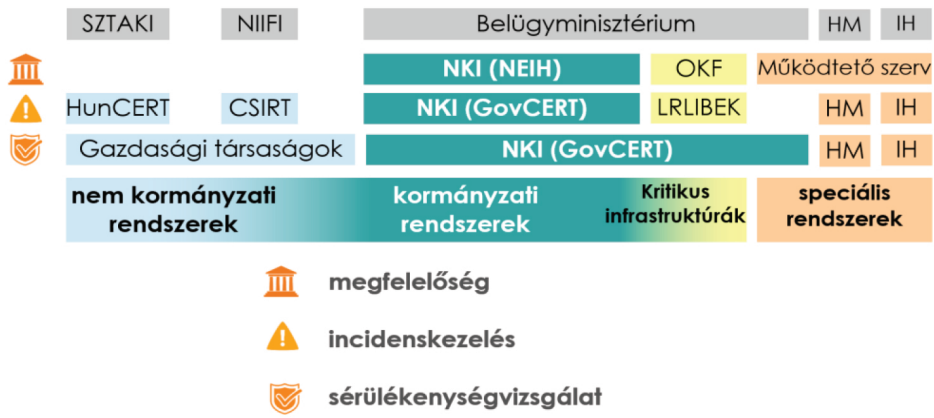
A 484/2013. (XII. 17.) Korm. rendeletben meghatározottak szerint ágazati és funkcionális kiberbiztonsági munkacsoportok segítik a Tanács koordinációs tevékenységét és döntéseinek végrehajtását. A jogszabály az alábbi olyan szakterületeket nevesíti, amelyeken kiberbiztonsági munkacsoportoknak kell működniük:

a) eseménykezelés,
b) belbiztonság,
c) e-közigazgatás,
d) energetika,
e) gyermekvédelem.

A Tanács felkérésére a fentieken kívül további munkacsoportok is létrehozhatók. Az 1. ábrán látható Incidenskezelési Munkacsoportot a 484/2013. (XII. 17.) Korm. rendelet nem nevesíti. Rajnai Zoltán kiberkoordinátorrá történő kinevezése után 2016-ban összesen hat munkacsoport alakult meg (vagy újjá). Ezek a Belbiztonsági Munkacsoport, az E-közigazgatási Munkacsoport, az Energiabiztonsági Munkacsoport, a Gyermekvédelmi Munkacsoport, az Egészségügyi Munkacsoport, valamint a Pénzügyi Munkacsoport (RAJNAI 2016). Jelenleg a 484/2013. (XII. 17.) Korm. rendeletben nevesített területekből a belbiztonsági és a gyermekvédelmi munkacsoportok működnek aktívan, ám a Belbiztonsági Munkacsoport ellátja az e-közigazgatási területen jelentkező feladatokat is. A Gyermekvédelmi Munkacsoport a Nemzetközi Gyermekmentő Szolgálat bázisán alakult meg, ez jelenleg a legintenzívebben működő munkacsoport. Tevékenységei között szerepel a szülőfelügyeleti programok támogatása, a gyermekbűnözés elleni fellépés elősegítése, de a munkacsoport aktívan részt vesz a digitális gyermekvédelmi stratégia megvalósításában is. A fent említettek mellett a bankbiztonsági, az egészségügyi munkacsoportokat sikerült aktívvá tenni. Ennek mozgatórugója elsősorban az volt, hogy ezt a két szektort érintették talán a legérzékenyebben az elmúlt időszak kibertámadásai (ilyen volt az egészségügyi szektort 2017-ben jelentősen érintő *WannaCry* zsarolóvírusos támadás (PALMER 2017) vagy a bankszektort megrázó, a SWIFT-rendszer sérülékenységét kihasználó támadássorozat (ANANTHALAKSHMI–BERGIN 2018; PAUL 2016). A Bankbiztonsági Munkacsoport a Bankszövetség információbiztonsági munkacsoportjának bázisán jött létre, fő feladata a bankszektor biztonságának erősítése, az állampolgárok e-banki tevékenysége biztonságának szavatolása. A 484/2013. (XII. 17.) Korm. rendeletben nevesített területek közül az energetika és az eseménykezelési szakterületen 2018. első félévének végéig még nem sikerült aktívan működő munkacsoportot kialakítani. Az e szektorokban felmerülő eseménykezelési problémákat, feladatokat az operatív szinten működő szervezetek kezelik.

### 5.1.2. A hazai kibervédelem operatív szintje

A hazai kibervédelem operatív szintjét mutatja be az alábbi 3. ábra. Az ábra jól szemlélteti, hogy megfelelőség, incidenskezelés és sérülékenységvizsgálat tekintetében mely szervezetnek milyen hatáskörrel milyen feladatai vannak, kiegészítve a civil szervezetek által működtetett CERT-ek feladataival.




3. ábra

*Kibervédelmi feladatok a hazai struktúra operatív szintjén*

*Forrás:* Bencsik 2017

#### *5.1.2.1. Nemzeti Kibervédelmi Intézet*

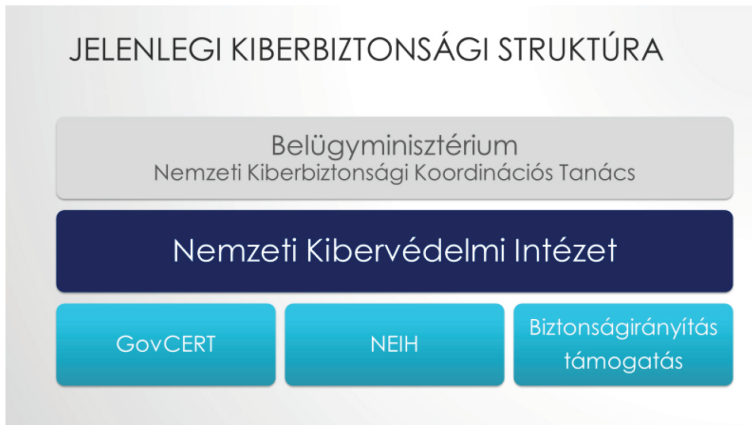
Az operatív szervezetek közül kiemelést érdemel a központi, vezető szerepet játszó Nemzeti Kibervédelmi Intézet. Az NKI 2015. október 1-jén alakult meg a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) bázisán, egységes szakmai keretbe foglalva a már ekkor az NBSZ alatt működő GovCERT-et, a 2015. január elsejétől már a Belügyminisztérium (a továbbiakban: BM) szervezeti keretében működő Nemzeti Elektronikus Információbiztonsági Hatóságot és az ezt megelőzően a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) alatt tevékenykedő és szakhatósági, valamint sérülékenységvizsgálati feladatokat ellátó E-biztonsági Intelligencia Központot (NBF-CDMA).[3] Így egy egységes, koordináltabb, hatékonyabb feladat-végrehajtást és információáramlást lehetővé tevő kibervédelmi szervezetet sikerült létrehozni. Az NKI szervezetén belül három szakmai terület került kialakításra:

- a Kormányzati Eseménykezelő Központ (GovCERT-Hungary, a továbbiakban: GovCERT), amely a kibertérből érkező támadásokkal és fenyegetettségekkel foglalkozó incidenskezelési szakterület;
- a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH), amely a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület;

[3] CDMA: Cyber Defence Management Authority.

- a Biztonságirányítási és Sérülékenységvizsgálati Osztály, amely az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó szervezetek esetében a kibervédelmi képességek fejlesztését és üzemeltetését támogatja, valamint ellátja az EMIR- és a FAIR-rendszerek elektronikus információbiztonsági feladatait is.[4]

Az NKI felépítését mutatja a 4. ábra. Az NKI szervezeti egységeinek fő feladatai viszont az 5. ábrán láthatók.




4. ábra

*Az NKI szervezeti egységei*

*Forrás:* Bencsik 2017

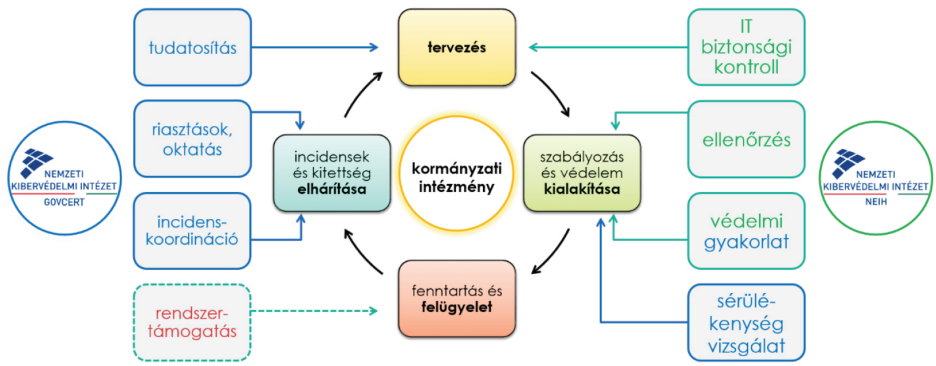

5. ábra

*Az NKI szervezeti egységei és fő feladataik*

*Forrás:* Tikos 2017

[4] Nemzetbiztonsági Szakszolgálat. Elérhető: http://nbsz.hu/?mid=42 (A letöltés dátuma: 2018. 06. 03.)

Az NKI így az egyes elektronikus információs rendszerek minden életciklusában rendelkezik valamilyen ellátandó információbiztonsági feladattal. Az egyes életciklusokban jelentkező feladatokat mutatja be a következő ábra.




6. ábra

*A GovCERT- és NEIH-feladatok az elektronikus információs rendszerek életciklusában*

*Forrás:* Bencsik 2017

Az NKI egyik kiemelendő feladata a nemzetközi kiberbiztonsági szervezetekkel való kapcsolattartás, az ezekkel való információmegosztás, az innen érkező információk eljuttatása az érintett hazai szervezetek számára, valamint a hazai szervezetek képviselete. Ennek érdekében az NKI (adott esetben a GovCERT) számos nemzetközi kiberbiztonsági tömörülésnek a tagja. Az NKI legfontosabb nemzetközi partnerei:

- ENISA: European Network and Information Security Agency,[5]
- FIRST: Forum of Incident Response and Security Teams,[6]
- TI: Trusted Introducer,[7]
- IWWN: International Watch and Warning Network,
- CECSP: Central European Cyber Security Platform (a visegrádi négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform).

Az NKI fent említett három szervezeti egységének a fő feladatai és hatáskörei az alábbiak.

### *5.1.2.2. Kormányzati Eseménykezelő Központ (GovCERT)*

Az Ibtv. alapján 2013. július elsején létrejött a Kormányzati Eseménykezelő Központ (GovCERT-Hungary), amely a magyar kormányzat információmegosztó és incidenskezelő

[5] ENISA European Network and Information Security Agency. Elérhető: www.enisa.europa.eu (A letöltés dátuma: 2018. 06. 03.)

[6] FIRST Forum of Incident Response and Security Teams. Elérhető: www.first.org (A letöltés dátuma: 2018. 06. 03.)

[7] TI Trusted Introducer. Elérhető: www.trusted-introducer.org (A letöltés dátuma: 2018. 06. 03.)

szervezete. Alapvető rendeltetése az Ibtv. hatálya alá tartozó szervezetek informatikai biztonsági támogatása, amely két részből, megelőzési és reaktív tevékenységekből tevődik össze. Egyrészt megelőző jelleggel végzi a szoftversérülékenységek és információbiztonsági fenyegetések összegyűjtését, kezelését, valamint az információk megosztását, az érintettek tájékoztatását. Másrészt reaktív tevékenységként az Ibtv. hatálya alá tartozó szervezeteknél az elektronikus információbiztonsági incidensek kivizsgálásában, azok kezelésének koordinációjában működik közre.[8] A kormányzati eseménykezelő központ feladat- és hatáskörét a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet határozza meg. Eszerint a GovCERT főbb feladatai a következők:

1. a biztonsági események és fenyegetések kezelésével támogatja az állami és önkormányzati szerveket, ami kapcsán
   a) értesíti az érintetteket,
   b) az érintettek számára szakmai támogatás nyújt,
   c) a biztonsági eseményekről a megtett intézkedéseket és azok eredményét tartalmazó nyilvántartást vezet;
2. együttműködik
   a) az alábbi hatóságokkal:
      - a szintén az NKI keretein belül működő NEIH-hel,
      - a polgári hírszerzési szervezetrendszeren belül működő hatósággal,
      - a honvédelmi ágazaton belül működő hatósággal,
      - a hivatásos katasztrófavédelem szervezetrendszerén belül működő hatósággal;
   b) az alábbi eseménykezelő központokkal:
      - a kijelölt létfontosságú rendszerelem elektronikus információs rendszereit érintő eseményeket kezelő központtal,
      - a honvédelmi célú, elektronikus információs rendszereket érintő eseményeket kezelő központtal,
      - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő eseményeket kezelő központtal,
   c) a rendvédelmi szervekkel és a Katonai Nemzetbiztonsági Szolgálattal (a továbbiakban: KNBSZ),
   d) a Nemzeti Média- és Hírközlési Hatósággal (a továbbiakban: NMHH) és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,
   e) az elektronikus hírközlési szolgáltatókkal,

[8] Nemzeti Kibervédelmi Intézet – Kormányzati Eseménykezelő Központ. Elérhető: www.cert-hungary.hu/node/1 (A letöltés dátuma: 2018. 06. 03.)

   f) a központosított informatikai és elektronikus hírközlési szolgáltatóval [a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet alapján ez a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság, a továbbiakban: NISZ Zrt.],
   g) az elektronikus kereskedelmi szolgáltatókkal és a közvetítő szolgáltatókkal,
   h) az elektronikus információs rendszerek biztonságáért felelős személyekkel,
   i) a magyar és a nemzetközi hálózatbiztonsági szervekkel,
   j) az iparági szereplőkkel;
3. kivizsgálhatja a biztonsági eseményre vagy fenyegetésre utaló tevékenységeket;
4. figyelmeztetést ad ki konkrét biztonsági események kapcsán
   a) a NISZ Zrt.,
   b) a felhasználók,
   c) az eseménykezelő központok,
   d) a hatóságok felé;
5. sérülékenységekkel és fenyegető kockázatokkal, valamint a javasolt biztonsági intézkedésekkel összefüggésben tájékoztatást nyújt
   a) az elektronikus információs rendszerek biztonságáért felelős személyeknek,
   b) a hatóságoknak,
   c) az eseménykezelő központoknak,
   d) valamint az érdeklődőknek a saját honlapján keresztül;
6. elemzéseket, jelentéseket készít
   a) a magyar és nemzetközi információbiztonsági irányokról,
   b) a Tanács részére negyedévente,
   c) az irányító miniszter részére évente;
7. nem kötelező érvényű állásfoglalásokat, ajánlásokat ad ki;
8. mint országon belüli koordinációs szervezet kapcsolatot tart, információt cserél, tájékoztatást kérhet, valamint végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, együttműködve
   a) az Európai Hálózat- és Információbiztonsági Ügynökséggel (European Union Agency for Network and Information Security, a továbbiakban: ENISA)
   b) a számítógép-biztonsági eseményekre reagáló csoportok (Computer Security and Incident Response Team, a továbbiakban: CSIRT) hálózatával,
   c) más országok CERT-jeivel,
   d) a magyar és nemzetközi kritikus információs infrastruktúra védelmi szervezeteivel,
   e) a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló Lrtv. szerint kijelölt, alapvető szolgáltatásokat nyújtó szereplőkkel,
   f) az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény szerinti bejelentésköteles szolgáltatást nyújtókkal;
9. tájékoztatási, tudatosítási, szakértői-oktatói tevékenységet folytat (például szakmai anyagokat, útmutatókat készít, kiberbiztonsági konferenciákat, gyakorlatokat szervez, kiberbiztonsági témában megjelenik a médiában);
10. részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályozások előkészítésében.

Kiemelendő, hogy a GovCERT a kibertérben elkövetett bűncselekmények kapcsán hathatós segítséget tud nyújtani a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek. Fontos szerepe van ugyanis a határon átnyúló kibertérben vagy annak segítségével elkövetett bűncselekmények, káros tevékenységek esetében az információk megosztásában. Egyrészt a hazai nyomozások során feltárt információkat továbbítani tudja az illetékes ország(ok) CERT-je(i) felé, például kérve intézkedésüket egy káros tevékenységet folytató szerver lekapcsoltatásához, másrészt a külföldi CERT-ek hasonló jellegű megkereséseit továbbítani tudja a hazai bűnüldöző szervek irányába.

*5.1.2.3. Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)*

Alapvető rendeltetése az Ibtv. és más vonatkozó, az elektronikus információbiztonsággal kapcsolatos előírásokat tartalmazó jogszabályokban foglalt előírásoknak, követelményeknek való megfelelőség ellenőrzése az érintett szervezeteknél, de kiemelt szerepe van abban is, hogy e követelmények a központi költségvetésből és/vagy európai uniós forrásból megvalósuló infokommunikációs fejlesztések során elektronikus információs rendszerek teljes életciklusa alatt konzekvensen, teljes mértékben megvalósításra kerüljenek. A NEIH feladat- és hatáskörét az Ibtv. és az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet határozza meg. Eszerint a NEIH főbb feladatai a következők:

1. az elektronikus információs rendszerek osztályba sorolása és a szervezetek biztonsági szintje kapcsán
   a) a bejelentett biztonsági osztályba sorolások nyilvántartása,
   b) az érintett szervezet által hozott döntés felülvizsgálata,
   c) hatósági eljárás keretében a jogszabályban meghatározott követelmények teljesülésének ellenőrzése,
   d) a biztonsági hiányosságok elhárításának elrendelése,
   e) utóellenőrzése,
   f) kockázatelemzés elvégzése;
2. elektronikus információs rendszer külföldön történő üzemeltetése esetén
   a) az Európai Gazdasági Térség (a továbbiakban: EGT) tagállamaiban történő üzemeltetésének engedélyezése,
   b) az EGT tagállamain kívül történő üzemeltetés ellenőrzése;
3. biztonsági eseményekkel kapcsolatos
   a) bejelentések fogadása,
   b) a kivizsgálásukra irányuló hatósági eljárás megindítása;
4. az európai uniós vagy központi költségvetési támogatásból információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülésének ellenőrzése;
5. éves ellenőrzési terv készítése;
6. nyilvántartások vezetése
   a) a szervezetek elektronikus információs rendszereiről (megnevezés, biztonsági osztályba sorolás, a szükséges védelmi intézkedések adatai stb.)
   b) a GovCERT-től kapott biztonsági eseményekkel kapcsolatos értesítésekről (amelyeket a honlapján közzé is tesz);

7. javaslattétel ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére;
8. együttműködés és kapcsolattartás
   a) az Elektronikus Ügyintézési Felügyelettel[9] (a továbbiakban: Felügyelet),
   b) a nemzetbiztonsági szolgálatokkal,
   c) az alábbi eseménykezelő központokkal:
      - a GovCERT-tel,
      - a kijelölt létfontosságú rendszerelem elektronikus információs rendszereit érintő eseményeket kezelő központtal,
      - a honvédelmi célú, elektronikus információs rendszereket érintő eseményeket kezelő központtal,
      - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő eseményeket kezelő központtal,
      - a magyar és a nemzetközi hálózatbiztonsági szervekkel;
   d) a hálózati és információs rendszerek biztonságáért felelős nemzetközi szervezetekkel,
   e) az érintett EGT-tagállamok hatóságaival,
   f) a Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH);
9. az Európai Bizottság részére tájékoztatás adása és adatok szolgáltatása (például az alapvető szolgáltatásokról, az azokat nyújtó szereplőkről, az információbiztonságra vonatkozó szabályokról).

*5.1.2.4. Biztonságirányítási és Sérülékenységvizsgálati Osztály*

A biztonságirányítás területén az NKI a biztonsági felügyeletére bízott, kiemelt kormányzati rendszerek esetében információbiztonsági irányítási rendszert (IBIR) működtet, emellett pedig egyrészt szakmai támogatást nyújt a NEIH, másrészt az állami és önkormányzati szervek számára. Sérülékenységvizsgálat kapcsán az NKI-nak több feladata is van. Az Ibtv. és a 185/2015. (VII. 13.) Korm. rendelet értelmében kizárólag a GovCERT jogosult a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek, a zárt célú elektronikus információs rendszerek, valamint az állami és önkormányzati szervek létfontosságú rendszerelemeinek elektronikus információs rendszerei esetében sérülékenységvizsgálatot végezni. Az ebbe a körbe nem tartozó állami és önkormányzati rendszerek esetében az Ibtv. és a 185/2015. (VII. 13.) Korm. rendelet alapján megfelelő engedélyekkel rendelkező, az Alkotmányvédelmi Hivatal (a továbbiakban: AH) nyilvántartásában szereplő, a szakmai és biztonsági elvárásoknak megfelelő gazdálkodó szervezet végezhet sérülékenységvizsgálatot. Az AH a nyilvántartásába történő felvétel során a szakmai kompetenciák ellenőrzése érdekében kikéri a GovCERT állásfoglalását is. A vizsgálatok célja az adott elektronikus információs rendszer gyenge pontjainak feltárása, valamint javaslatok megfogalmazása azok javítására, kiküszöbölésére. Az IBIR és a sérülékenységvizsgálat is – megelőző intézkedésként – hathatósan elősegíti az elektronikus információbiztonsági incidensek megelőzését, bekövetkeztük megakadályozását.

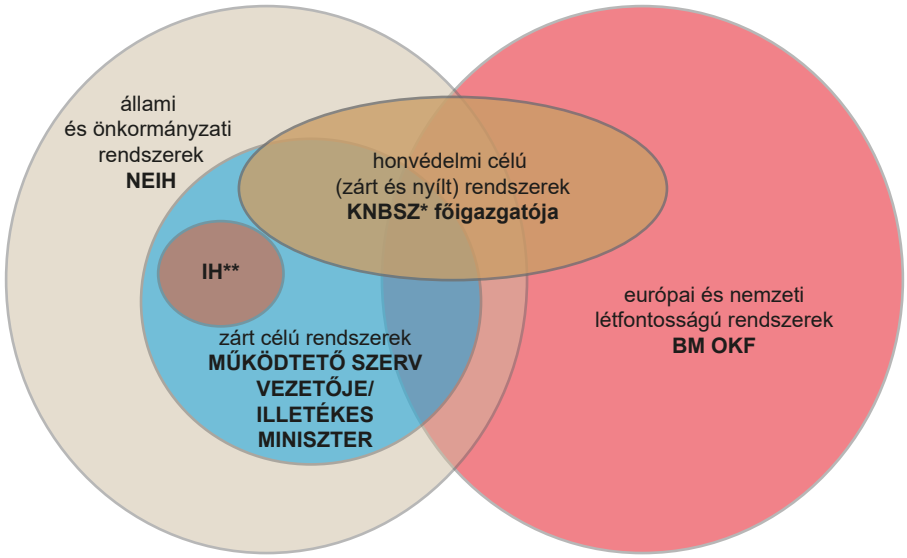
[9] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.

*5.1.2.5. OKF Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ*

A BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: OKF) szervezetén belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (a továbbiakban: LRLIBEK) látja el – az Ibtv. hatálya alá eső szervezetek által üzemeltetett létfontosságú rendszerek és létesítmények kivételével – a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységeket. Az LRLIBEK feladat- és hatáskörét az Ibtv., a 185/2015. (VII. 13.) Korm. rendelet, valamint az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet határozza meg. Ezek alapján az LRLIBEK főbb feladatai:

1. eseménykezelés [a 185/2015. (VII. 13.) Korm. rendelet szerint];
2. biztonsági események kapcsán
   a) nyilvántartás vezetése,
   b) az érintettek haladéktalan értesítése,
   c) szakmai támogatás nyújtása,
   d) együttműködés a hatósággal, az érintett szervezetekkel,
   e) a kezelésükre irányuló tájékoztató tartása;
3. folyamatosan elérhető, 24 órás ügyelet működtetése;
4. sérülékenységekről és fenyegető kockázatokról tájékoztatás nyújtása;
5. a magyar kibertér rendszeres biztonsági helyzetértékelésének elvégzése;
6. hazai és nemzetközi információbiztonsági és kibervédelmi gyakorlatok tervezése, szervezése, gyakorlatokon történő részétel;
7. szakértői-oktatói, tudatosító tevékenység végzése;
8. információtechnológiai, hálózatbiztonsági és biztonságiesemény-kezelési együttműködési fórum működtetése.

2017 végén megjelent a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelvet (a továbbiakban: NIS-irányelv) a hazai jogrendbe átültető, a bejelentésköteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelet, amely kibővítette a BM Országos Katasztrófavédelmi Főigazgatóság feladat- és hatáskörét. A NIS-irányelv az alapvető (az energia, a pénzügyi, az egészségügyi, a vízügyi és a közlekedési ágazatokban kijelölt kritikus) infrastruktúrák és bejelentésköteles szolgáltatást (online piacterek és keresőprogramok, felhőalapú számítástechnikai szolgáltatások) nyújtók esetében kívánja az általuk nyújtott szolgáltatások folyamatossága és az általuk kezelt adatok és információk védelme tekintetében emelni az információbiztonság szintjét. Az ehhez szükséges eseménykezelő központi és hatósági feladatokat utalta a 410/2017. (XII. 15.) Korm. rendelet az OKF feladat- és hatáskörébe. Az elektronikus információs rendszerek hatósági felügyeletének feladat- és hatáskörmegosztását a 7. ábra szemlélteti.




7. ábra

*Az elektronikus információs rendszerek hatósági felügyelete*

Megjegyzés:

* KNBSZ = Katonai Nemzetbiztonsági Szolgálat

**IH = Információs Hivatal, polgári hírszerző tevékenységet vezető nemzetbiztonsági szolgálat főigazgatója

*Forrás:* Országos Katasztrófavédelmi Főigazgatóság Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ alapján saját szerkesztés

### *5.1.2.6. A HM CERT és az IH CERT*

A Honvédelmi Minisztérium (a továbbiakban: HM) a KNBSZ keretein belül működteti saját, honvédelmi célú zárt és nyílt rendszerei kibervédelmét biztosító és mind az incidenskezelési feladatokat, mind pedig a hatósági funkciókat ellátó szervezetét, amely az 1. ábrán HM CERT néven szerepel. Ez a szervezet a szakfeladat szerint elkülönülő – a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – eseménykezelő központokkal együtt látja el a biztonsági események és fenyegetések kezelését. A HM a honvédelmi szervezetek 2016. évi fő célkitűzéseinek és fő feladatainak, valamint a 2017–2018. évi tevékenysége fő irányainak meghatározásáról szóló 3/2016. (I. 22.) HM utasításban Military Computer Emergency Response Team, MilCERT megnevezéssel azonosította a szervezetet. Az Információs Hivatal (a továbbiakban: IH) szintén önálló, a szervezet keretein belül működő szervezetet működtet a saját zárt és nyílt célú elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére. Az IH CERT az eseménykezelő központot a 185/2015. (VII. 13.) Korm. rendelet alapján IntCERT megnevezéssel azonosítja.

### 5.1.3. A hazai kibervédelem rendvédelmi szervezete – Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) Kiberbűnözés Elleni Főosztály

A rendőrség az Alaptörvényben, a Rendőrségről szóló 1994. évi XXXIV. törvényben, valamint ez utóbbi felhatalmazása alapján más jogszabályban meghatározott bűnmegelőzési, bűnüldözési feladatkörében általános bűnügyi nyomozó hatósági jogkört gyakorol, végzi a bűncselekmények megelőzését, megakadályozását és felderítését, valamint a bűncselekményből származó vagyon visszaszerzését. A rendőrség fellép a kiberbűnözés valamennyi szegmense, így különösen a számítógépes rendszerek elleni támadások, a rosszindulatú számítógépes szoftverek, az adathalászat, az internetes csalások, az elektronikus banki csalások, a bankkártyabűnözés, valamint a gyermekek online szexuális kizsákmányolása ellen. A rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet, valamint az egyéb hatásköri és illetékességi szabályok alapján a rendőrség valamennyi területi és helyi bűnügyi szerve tevékenyen részt vesz a kiberbűnözés elleni harcban, így mind a megyei rendőrfőkapitányságok, mind a helyi rendőrkapitányságok folytatnak kiberbűnözéshez köthető büntetőeljárásokat. 2008. január elsején jött létre a Budapesti Rendőr-főkapitányság (a továbbiakban: BRFK) Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztálya, amelynek többek között a bankkártyához köthető kiemelt jelentőségű visszaélések is a feladatkörébe kerültek. Szintén a BRFK-n került megalakításra a Bűnügyi Főosztály Gyermek- és Ifjúságvédelmi Osztálya, amely egyéb, fiatalkorúakkal kapcsolatos nyomozások mellett végzi a főváros területén a gyermekek online szexuális kizsákmányolásával kapcsolatos ügyek felderítését és nyomozását. A kiberbűnözés elleni fellépés prioritására tekintettel 2017. január elsején került felállításra a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya, a legnagyobb létszámú, kifejezetten kiberbűnözés elleni küzdelemre szakosodott rendvédelmi egység Magyarországon. A főosztály jelentős mértékű létszámbővítése és technikai fejlesztése jelenleg is folyamatban van. A KR NNI titkos információgyűjtést, titkos adatszerzést és nyomozási feladatokat ellátó, országos illetékességű szervezeti egység. A 25/2013. (VI. 24.) BM rendelet 2. mellékletének értelmében a főosztály kizárólagos hatáskörébe tartozik a Büntető Törvénykönyvről szóló 2012. évi C. törvény 375. §-ba ütköző, különösen jelentős kárt okozó, információs rendszer felhasználásával elkövetett csalás, ha annak elkövetője bűnszervezet vezetője vagy tagja, a 423. §-ba ütköző, közérdekű üzem ellen elkövetett információs rendszer vagy adat megsértése, valamint a 424. §-ba ütköző, közérdekű üzem ellen elkövetett információs rendszer védelmét biztosító technikai intézkedés kijátszása. A 2. mellékletben felsorolt bűncselekményeken kívül a KR NNI akkor rendelkezik hatáskörrel, ha a nyomozás alapjául szolgáló bűncselekménynek az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről szóló 2006. évi CI. törvény 3. cikk (2) bekezdésében meghatározottak alapján nemzetközi jellege van. Tekintettel a fentiekre, a főosztály bűnügyi nyomozó tevékenysége kiterjed a számítástechnikai eszközökkel, különösen az internet felhasználásával elkövetett kiemelt súlyú, speciális számítástechnikai ismereteket igénylő, gyakran nemzetközi vonatkozású bűncselekmények nyomozására és vizsgálatára (például információs rendszer elleni támadás, információs rendszer felhasználásával elkövetett csalás, gyermekek online szexuális kizsákmányolása, tiltott online szerencsejáték szervezése, személyes adattal való

visszaélés). A kiberbűnözés tágabb fogalmába tartozó készpénz-helyettesítő fizetési eszközökkel kapcsolatos szervezett és nemzetközi jellegű bűncselekmények nyomozása a szintén a KR NNI szervezetén belül működő Felderítő Főosztály Pénz- és Bankkártya Hamisítás Elleni Osztály hatáskörébe tartozik. A folyamatban lévő kiberbűncselekményekkel kapcsolatos nyomozások operatív támogatása mellett a Kiberbűnözés Elleni Főosztály egyéb feladatai:

1. bűnügyi hírszerző tevékenység folytatása a kiberbűnözéssel összefüggő legújabb jelenségekkel kapcsolatban (például: Bitcoin és egyéb elektronikus fizetőeszközök, darknet-jelenség, hackertevékenység, illegális online piacok, új típusú piramisjáték és csalás jellegű tevékenységek stb.);
2. forenzikus tevékenység végzése a KR NNI saját, valamint a területi és helyi rendőri szervek kiemelt jelentőségű ügyeiben (például a lefoglalt számítástechnikai adathordozók, így asztali számítógépek, laptopok, szerverek, pendrive-ok, külső merevlemezek, SD-kártyák, valamint mobiltelefonok és tabletek adatainak lementése, elemzése és értékelése);
3. közreműködés helyszíni intézkedésekben, házkutatásokon és lefoglalásokon;
4. együttműködik és kapcsolatot tart
   a) a helyi és területi rendvédelmi szervekkel,
   b) ügyészségekkel,
   c) az Alkotmányvédelmi Hivatallal,
   d) a Terrorelhárítási Központtal,
   e) a TIBEK-kel,
   f) a Nemzeti Kibervédelmi Intézettel,
   g) az Országos Katasztrófavédelmi Főigazgatósággal,
   h) a legjelentősebb hazai hírközlési szolgáltatókkal,
   i) a Nemzetközi Gyermekmentő Szolgálat Magyar Egyesülettel,
   j) a Nemzeti Média- és Hírközlési Hatósággal,
   k) a Nemzeti Infokommunikációs Szolgáltató Zrt.-vel,
   l) a Magyar Bankszövetséggel;
5. az ORFK és az NMHH, illetve az ORFK és a NISZ Zrt. között megkötött együttműködési megállapodások alapján a két magyar Internet Hotline-ra (internethotline.hu, biztonsagosinternet.hu) érkező állampolgári bejelentésekkel kapcsolatos elsődleges feladatok ellátása (bejelentés értékelése, nyomozás elrendelése, hatáskör és illetékesség megállapítása, adott esetben a nyomozás lefolytatása);
6. oktatási tevékenység végzése:
   a) az NKE Rendészettudományi Kar nappali és levelező tagozatos képzésén,
   b) a Magyar Igazságügyi Akadémia ügyészi és bírói továbbképzésein,
   c) regionális rendőri, ügyészi és bírói továbbképzéseken,
   d) a kormányzati szervek és a velük együttműködő civil szervezetek által szervezett képzéseken, továbbképzéseken és konferenciákon.

### 5.1.4. A NISZ Zrt. kibervédelmi szervezete

A hazai állami, önkormányzati szektor kibervédelmére is erős befolyást gyakorol az a központosított informatikai és elektronikus hírközlési szolgáltató/szolgáltatások kialakítása érdekében zajló folyamat, amelyet azért indítottak el, hogy a korábbi széttagolt, drágán fenntartható, heterogén eszközrendszerű, sőt sok esetben elavult állami, önkormányzati infokommunikációs rendszert konszolidálja, és egységes, megfelelő szolgáltatási és biztonsági szintű szolgáltatást nyújtson minden érintettnek. A feladatra a NISZ Zrt.-t jelölte ki a kormány. A NISZ Zrt. működését meghatározó legfontosabb jogszabályok a már említett és hivatkozott 309/2011. (XII. 23.) Korm. rendelet mellett a kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet, az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) Korm. rendelet, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet, valamint a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet. A NISZ Zrt. működését meghatározó szabályozók mellett a téma szempontjából fontos megemlíteni az információbiztonság feladatait rögzítő, a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendeletet is. Az említett jogszabályok természetesen elsősorban a NISZ Zrt. által ellátandó feladatokról szólnak, ezáltal közvetetten az érintett szervezetek infokommunikációs rendszereinek konszolidálását irányozzák elő, e rendszerek egy részének, vagy adott esetben egészének központi szolgáltató által történő biztosításával – és adott esetben kiváltásával. Ez azonban az ezekben a rendszerekben tárolt, kezelt elektronikus információk biztonságát is érinti, hiszen az adott elektronikus információs rendszer azon részének, amelyet a NISZ Zrt. biztosít, neki kell megteremtenie az Ibtv. és a 41/2015. (VII. 15.) BM rendelet által előírt biztonsági kontrollok rá eső részét. Azaz akárcsak az elektronikus információs rendszer elemeinek tervezése, üzemeltetése, úgy a biztonság megteremtésének feladata, felelőssége is megoszlik a szolgáltató és a felhasználó között. A 186/2015. (VII. 13.) Korm. rendeletben foglaltak szerint a központi szolgáltató főbb kiberbiztonsági feladatai a következők:

1. informatikai biztonsági irányítási rendszer kialakítása és működtetése;
2. szolgáltatásokról, azok kritikusságáról, a szolgáltatásokban részt vevőkről (felhasználó, üzemeltető, fejlesztő stb.), a távoli hozzáférésekről, az igénybe vett egyéb külső szolgáltatásokról nyilvántartás vezetése;
3. kockázatértékelés végzése és ennek megfelelően a szükséges védelmi elemek kialakítása;
4. a szükséges és megfelelő azonosítási, hozzáférés-kezelési és jogosultságkiosztási feladatok biztosítása;
5. a szolgáltatások biztonsági állapotának folyamatos ellenőrzése, a biztonsági események azonosítása, a biztonsági információk gyűjtésének, elemzésének elvégzése;

6. a szolgáltatások biztonsági állapota megfelelőségének folyamatosan biztosítása, intézkedés a biztonsági események megelőzésére, a bekövetkezett biztonsági események által okozott kár csökkentésére;
7. biztonsági események kezelése során az illetékes eseménykezelő központok számára tájékoztatás nyújtása, a biztonsági események azonosításához, elemzéséhez és kezeléséhez szükséges bizonyítékok, adatszolgáltatás biztosítása, vizsgálatok elvégzése, valamint az elrendelt biztonságnövelő intézkedések végrehajtása.

A releváns jogszabályokban megfogalmazottak teljesítése érdekében a NISZ Zrt.-n belül kialakításra került az Elektronikus Információbiztonsági Igazgatóság. A fentiek mellett az igazgatóság látja el a jogosult szervezetek, így a rendvédelmi szervek számára a különböző nyílt és titkos információgyűjtés keretében kért, a NISZ Zrt. által üzemeltetett rendszerekből kinyerhető adatok tekintetében az adatszolgáltatási tevékenységet is.

### 5.1.5. Hun-CERT

A Hun-CERT egy, a Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézetében (MTA SZTAKI) működő, az Internet Szolgáltatók Tanácsának (ISZT) támogatásával létrejött munkacsoport, amely éppen ezért a hazai internetszolgáltatók, különösképpen a Magyar Internet Szolgáltatók Tanácsának (ISZT) tagjai szolgálatában fejti ki tevékenységét. Mindezek mellett a Hun-CERT az egész hazai internetes közösség számára is szolgáltat a hálózati biztonságról szóló nyilvános információkat. A Hun-CERT fő célkitűzése, hogy segítse a magyar internetes társadalmat, ezen belül különösen a magyar internetszolgáltatókat abban, hogy megfelelő eljárásokat alkalmazzanak a kiberbiztonsági incidensek kockázatainak kezelésére és az ilyen incidensek előfordulásakor az azokra adandó válaszokra.

Főbb feladatai eszerint:

1. incidensek felderítése,
2. incidensek elemzése,
3. incidensek kezelése,
4. biztonsági tudatosság növelése.

Ennek megfelelően a Hun-CERT segítséget nyújt az ISZT tagszervezeteinél előforduló hálózati incidensek felderítésénél, elemzésénél és kezelésénél, valamint elsősorban az ISZT-tagok nagyszámú, nem hivatásszerűen számítástechnikával foglalkozó dolgozói számára szolgáltat olyan, a biztonsági tudatosság növeléséhez szükséges információkat, amelyek képessé teszik őket az internet használatával együtt járó kockázatok minél teljesebb megértésére és a sikeres védekezésre. A Hun-CERT kapcsolatot tart fenn más CSIRT-egységekkel Magyarországon belül és kívül.

### 5.1.6. KIFÜ CSIRT

Az Innovációs és Technológiai Minisztérium irányítása alatt működő Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) az a Kormányzati Informatikai Fejlesztési Ügynökségről szóló 268/2010. (XII. 3.) Korm. rendeletben meghatározottak alapján végzi tevékenységét, amelynek két fő eleme van:

1. az uniós és hazai forrásból megvalósuló informatikai projektek vezetési, minőségbiztosítási feladatainak ellátása az előkészítéstől kezdve a megvalósításon keresztül egészen azok lezárásáig,
2. a hazai közoktatási, felsőoktatási, kutatási intézmények, közgyűjtemények számára informatikai infrastruktúra fejlesztése és üzemeltetése, valamint arra épülő szolgáltatások nyújtása.

Ez utóbbi tevékenységén belül a magyar köznevelés, felsőoktatás, kutatás és közgyűjtemények szolgáltatójaként a KIFÜ egy IT-biztonsági és incidenskezelő csoportot, CSIRT-et működtet. A KIFÜ CSIRT alapfeladata minden olyan kiberbiztonsági incidens kezelését és koordinációját segíteni, amelyben legalább egy KIFÜ által kiszolgált intézmény érintett. Ezek mellett tudatosító tevékenysége keretében a kiberbiztonsággal, az incidensek megelőzésével és elhárításával kapcsolatos rendszeres és eseti tájékoztatókat juttat el minden KIFÜ által kiszolgált intézmény számára. A KIFÜ a partnerei számára a CSIRT-szolgáltatást alapszolgáltatásként biztosítja.[10] A 3. számú ábrán a szervezet még a korábbi nevén, NIIFI (Nemzeti Információs Infrastruktúrafejlesztési Intézet) CSIRT-ként szerepel.

### 5.1.7. Tervezett kiberbiztonsági fejlesztések Magyarországon

2018-ban intenzív munka kezdődött a hazai kibervédelem továbbfejlesztése érdekében.

Megindult a nemzeti kibervédelmi stratégiája átalakítása, amely a tervek szerint a 2013-ban elfogadotthoz képest jelentősen ki fog bővülni. Várhatóan egy, a korábbinál részletesebb, a stratégiai célokat, az érintett területeket és az elérendő célokat pontosabban meghatározó stratégia kialakítása történik meg.

Változások várhatók az operatív szintű szervezetek feladatrendszerében és ezáltal azok felépítésében is. A 2018. év végi tervek szerint az NKI feladat- és hatásköre jelentősen kibővül, így többek között beolvad majd a Nemzeti Biztonsági Felügyelet szervezete és tevékenysége, valamint ide kerül a NIS-irányelv által Magyarországra rótt feladatok ellátása is, amely jelenleg az OKF feladat- és hatáskörébe tartozik. Ennek megfelelően várhatóan az NKI jelentősen kibővített feladat- és hatáskörrel, átalakított szervezeti struktúrával és felbővített létszámmal, talán egy új név alatt fogja folytatni tevékenységét, míg az LRLIBEK jelenlegi formájában várhatóan megszűnik.[11]

---

[10] KIFÜ. Elérhető: http://kifu.gov.hu (A letöltés dátuma: 2018. 06. 03.)

[11] T/2930. számú törvényjavaslat egyes belügyi tárgyú és más kapcsolódó törvények módosításáról http://www.parlament.hu/irom41/02930/02930.pdf (letöltés: 2018.12.09.)

Jelenleg az említett változásokról szóló jogszabálytervezetek kialakítása még folyamatban van, azok elfogadása még nem történt meg. A magyar kibervédelmi struktúra és feladatrendszer átalakulását ezek véglegesítése és közzététele után lehet és kell újra áttekinteni.

## 5.2. A fontosabb nemzetközi kibervédelemi szervezetek, együttműködések

### 5.2.1. ENISA (European Union Agency for Network and Information Security)

Az ENISA,[12] azaz az Európai Hálózat- és Információbiztonsági Ügynökség, a tagállamok és intézmények érdekében tevékenykedő, azokkal együttműködő szakértői központ, amely meghatározó szerepet tölt be az európai információbiztonság területén. Egyik legfontosabb feladata ezen a területen az ismeretek és a bevált gyakorlatok terjesztése, valamint az információcsere biztosítása. Az ENISA mint az EU által felállított, európai ügynökségként dolgozó szakértői testület specifikus technikai és tudományos feladatokat is ellát, valamint segíti az Európai Bizottság hálózat- és információbiztonsághoz kapcsolódó jogszabály-előkészítő és -fejlesztő munkáját. Az ENISA székhelye Görögországban, ezen belül Kréta legnagyobb városában, Irákliónban található, de Athénban is működtet egy irodát. Az ügynökség szorosan együttműködik a tagállamokkal és a magánszektorral, akik számára kiberbiztonsági kérdésekben tanácsokat és megoldásokat nyújt. Ennek keretében páneurópai kiberbiztonsági gyakorlatokat szervez, hozzájárul a nemzeti kiberbiztonsági stratégiák fejlesztéséhez, elősegíti a CSIRT-ek együttműködését és ilyen kapacitások kiépítését, valamint tanulmányokat készít és ad ki többek között a felhőalapú rendszerek biztonságos adaptálásáról és alkalmazásáról, az adatvédelmi kérdésekről és technológiákról, az e-igazolványokról és a bizalmi szolgáltatásokról, valamint a számítógépes fenyegetések aktuális helyzetéről. A hatáskörébe tartozó kérdésekben az ENISA támogatja az Európai Unió kiberbiztonsági politikájának és jogi eszközeinek kidolgozását és azok végrehajtását.

### 5.2.2. FIRST (Forum of Incident Response and Security Teams)

A FIRST a kiberbiztonsági eseménykezelés elismerten vezető szervezete a világon, amelynek tagjai a kormányzati, kereskedelmi és oktatási szervezetek eseménykezelő csapataiból tevődnek össze. Jelenleg Afrikából, Amerikából, Ázsiából, Európából és Óceániából több mint 400 szervezet tagja a FIRST-nek. A FIRST elsődleges célja az incidensek megelőzésében való együttműködés és koordináció elősegítése, az incidensekre való gyors reagálás ösztönzése, valamint a tagok és a nagyközönség közötti információcsere elősegítése. A FIRST azon kívül, hogy globális bizalmi hálózatot hozott létre és tart fenn

[12] European Union Agency for Network and Information Security (eredeti nevén European Network and Information Security Agency), Európai Hálózat- és Információbiztonsági Ügynökség.

a kiberbiztonsági incidensekre reagáló közösségben, egyéb hozzáadott értékű szolgáltatásokat is kínál. Ezek közül néhány:

1. a tagok számára hozzáférést biztosít a legfrissebb bevált gyakorlatokat leíró dokumentumokhoz;
2. lehetőséget biztosít a biztonsági szakértők számára technikai beszélgetésekre, vitákra;
3. gyakorlati oktatásokat szervez, tart;
4. éves konferenciát rendez a kiberbiztonsági eseménykezelés témakörében;
5. kiadványokat készít és webes szolgáltatásokat nyújt;
6. speciális érdeklődési körök mentén úgynevezett különleges érdekcsoportokat (*Special Interest Groups,* a továbbiakban: SIG) működtet.[13]

A különleges érdekcsoportokat azért hozták létre, hogy a FIRST-tagok közös érdeklődésre számot tartó témákról beszélhessenek. A SIG-ek a FIRST-tagokból és meghívott felekből állnak, akik rendszeresen találkoznak annak érdekében, hogy feltárják a speciális technológiai vagy az érdeklődési területükön felmerülő egyéb jellegű vizsgálandó kérdéseket, megosszák egymással tapasztalataikat, együttműködjenek a kihívások közös kezelésében.

A FIRST jelenleg az alábbi kategóriákban a következő SIG-eket működteti:

1. Munkacsoportok:
   a) egyetemi környezet biztonsági kérdései,
   b) Big Data,
   c) kiberbiztonsági fenyegetések figyelése és jelzése,
   d) etika,
   e) a kiberbiztonsági gyakorlatok támadó csapatainak (Red Team) kérdései,
   f) sérülékenységek jelentése és adatcseréje,
   g) információmegosztás;
2. szabványosítási csoportok:
   a) közös sérülékenységpontozási rendszer (*Common Vulnerability Scoring System,* CVSS) kialakítása,
   b) információmegosztási szabályok kidolgozása,
   c) érzékeny információk megosztásánál használt jelzések (*Traffic Light Protocol,* TLP) egységesítése,
   d) passzív DNS-csere;
3. vitafórumok:
   a) internetinfrastruktúra-szállítói,
   b) malware-elemzési,
   c) mérőszámokkal kapcsolatos,
   d) ipari vezérlőrendszerekkel foglalkozó (*Industrial Control Systems,* ICS);
4. konferenciákon tartandó találkozók előkészítését végzők.[14]

[13] FIRST Forum of Incident Response and Security Teams. Elérhető: www.first.org (A letöltés dátuma: 2018. 06. 03.)

[14] FIRST Special Interest Groups (SIGs). Elérhető: www.first.org/global/sigs (A letöltés dátuma: 2018. 06. 03.)

### 5.2.3. TI (Trusted Introducer)

A Trusted Introducer szolgáltatást 2000-ben az európai CERT-közösség hozta létre a közös igények kielégítésére és egy olyan szolgáltatási infrastruktúra kiépítésére, amely létfontosságú támogatást nyújt az összes kiberbiztonsági eseménykezelő csoport számára. A TI legfontosabb szolgáltatásai, hogy megbízható gerincinfrastruktúrát biztosítson az eseménykezelő szervezetek számára, valamint listázza az ismert incidenskezelő csapatokat, akkreditálja őket a kiírt feltételek szerint, valamint igazolja az általuk bemutatott és visszaellenőrzött érettségi szintjüket. A szolgáltatásai egy részét a nyilvánosság számára is hozzáférhetővé teszi annak érdekében, hogy tovább javítsák és megkönnyítsék az érintett felhasználók és szervezetek közötti együttműködés kialakulását. Így a TI honlapján elérhető egy lista az összes felsorolt, akkreditált és tanúsított incidenskezelő csapat adatairól és egyéb hasznos információkról.[15]

### 5.2.4. IWWN (International Watch and Warning Network)

Az IWWN-t 2004-ben hozták létre a számítógépes fenyegetések, támadások és sebezhetőségek kezelésére irányuló nemzetközi együttműködés előmozdítása érdekében. Az IWWN a globális kiberbiztonsági tudatosító és eseménykezelő képességek kiépítése érdekében a részt vevő országok számára információcserét biztosít.[16] Az IWWN világméretű hálózat, amely a szabályzás és az operatív végrehajtás területén fejt ki tevékenységet, és jelenleg tizenöt ország kormányzati képviselőit tömöríti. Az IWWN feladatai között az alábbiak találhatók:

1. a kiberbiztonsági eseménykezelő csapatok elérhetőségi adatainak folyamatos karbantartása a nemzeti képviselők közreműködésével;
2. a fenyegetések és válságok idején koordinátori tevékenység végzése;
3. gyakorlatok szervezése;
4. az együttműködések előmozdítása;
5. az információmegosztás ösztönzése.

### 5.2.5. EC3 (European Cybercrime Centre)

Az EC3, avagy magyar nevén a Számítástechnikai Bűnözés Elleni Európai Központ az EU számítástechnikai bűnözéssel szembeni kollektív fellépéseként jött létre annak érdekében, hogy megerősítse az EU-ban a számítógépes bűnözésre adott bűnüldözési válaszokat, és ezáltal segítse az európai polgárokat, vállalkozásokat és kormányokat az online bűnözés elleni védelemben. Ennek indoka az volt, hogy nincs még egy olyan bűncselekménytípus, amely annyira független lenne az országhatároktól, mint a bűnözés e fajtája. Az EC3-at 2013 januárjában az Europol keretein belül azzal a céllal hozták létre, hogy az EU számítástechnikai

---

15 TI Trusted Introducer. Elérhető: www.trusted-introducer.org (A letöltés dátuma: 2018. 06. 03.)

16 IT Law Wiki – International Watch and Warning Network. Elérhető: http://itlaw.wikia.com/wiki/International_Watch_and_Warning_Network (A letöltés dátuma: 2018. 06. 03.)

bűnözés elleni küzdelmének központi szervezeteként működjön. Feladata az EU tagállamainak és intézményeinek támogatása a kibertérben vagy annak segítségével elkövetett bűncselekmények nyomozásához szükséges operatív és elemzői kapacitás kiépítésében, valamint a nemzetközi partnerekkel való együttműködés az európai kiberbűnözés felszámolása érdekében. Tevékenységeinek köre magában foglalja a rosszindulatú szoftverek, rendszerfeltörések, adathalászat, rendszerekbe történő illetéktelen behatolások, manipuláció, személyazonosság-lopások és fizetőeszközökkel összefüggő csalások, valamint a gyermekek elcsábítása és online szexuális kizsákmányolása elleni küzdelmet is.[17] Az EC3 minden évben közzéteszi az interneten a szervezett bűnözéssel kapcsolatos fenyegetésértékelést (*Internet Organised Crime Threat Assessment,* a továbbiakban: IOCTA), amely stratégiai jelentés a legfontosabb eredményekről és a számítógépes bűnözésben felmerülő veszélyekről és fejleményekről. Az IOCTA bemutatja, hogy az internetes bűnözés menynyire széles és változatos, valamint azt is, hogy az EC3 milyen szerepet játszik az ezek elleni európai fellépésben. Az EC3 működése a számítógépes bűnözés elleni küzdelemben három alappilléren nyugszik:

1. Stratégiai tevékenység: Az EC3-nak két stratégiai csapata létezik. Az egyik a megelőzési és tudatosítási tevékenységeket koordináló, valamint a partneri együttműködésért felelős tájékoztató és támogató csapat. A másik pedig a stratégiai elemzésekért, a jogszabályalkotásért és a standardizált képzések kidolgozásáért felelős stratégiai és fejlesztő csapat.
2. Műveleti tevékenység (azaz a műveleti szinten az EC3 az alábbi kiberbűncselekményekre összpontosít):
   a) kibertéren alapuló high-tech bűnözés,
   b) gyermekek online, szexuális kizsákmányolása,
   c) fizetési csalás.
3. Forenzikus tevékenység: Az EC3-nak két forenzikus tevékenységet végző csoportja van: a digitális és a dokumentum-szakértőket magában foglaló, amelyek mindegyike operatív tevékenységek támogatására, kutatásra és fejlesztésre összpontosít.

A három kiemelt kiberbűncselekmény-fajta fajta kapcsán az EC3

1. a bűnügyi és hírszerzési információk központi elosztójaként működik;
2. operatív elemzésekkel, koordinációs tevékenységgel és jelentős szakértelem biztosításával támogatja a tagállamokat műveleti és nyomozati munkájuk során;
3. különböző stratégiai elemzéseket biztosít, amelyek segítik a taktikai és a stratégiai szintű, informált döntéshozatalt a kiberbűnözés elleni küzdelemben és megelőzésben;
4. átfogó tájékoztatási funkciót biztosít a bűnüldöző hatóságok számára, amelyek a számítógépes bűnözést a magánszektorral, az egyetemekkel és más nem bűnüldöző szervekkel együttműködve kezelik;
5. támogatja a képzést és a kapacitásépítést, különösen a tagállamok illetékes hatóságai számára;

[17] Az Europol profilja az Európai Bűnüldözési Hatóság. Elérhető: www.europol.europa.eu/publications-documents/europol-profile (A letöltés dátuma: 2018. 06. 03.)

6. magasan specializált technikai és digitális igazságügyi támogatási képességeket biztosít a műveleti és nyomozati munkához;
7. az EU bűnüldözési közösségét képviseli a közös érdekű területeken (kutatás-fejlesztési követelmények, internetes irányítási és szabályzófejlesztés).

A fenti tevékenységeket támogatja az úgynevezett Cyber Intelligence Team (CIT), akik az állami, magán- és nyílt forrásokból összegyűjtik és feldolgozzák a számítógépes bűnözéssel kapcsolatos információkat, és azonosítják a felmerülő fenyegetéseket és támadási mintákat. Az EC3 mellett dolgozik a kiberbűnözéssel foglalkozó közös munkacsoport (Joint Cybercrime Action Taskforce, a továbbiakban: J-CAT), amely azokkal a legfontosabb, nemzetközi kibertérben vagy annak segítségével elkövetett bűnügyekkel foglalkozik, amelyek hatással vannak az EU tagállamaira és állampolgáraira.[18]

### 5.2.6. CECSP (Central European Cyber Security Platform)

A CECSP a V4-országok (Csehország, Lengyelország, Magyarország, Szlovákia) és Ausztria együttműködési platformja a kiberbiztonság területén. A platform Ausztria és Csehország kezdeményezésére jött létre 2013 májusában, célkitűzésként pedig a kiberbiztonsági információk egymás közötti megosztását, a bevált gyakorlatok és különleges eljárásmódok cseréjét, a kibervédelmi kapacitás és képesség bővítését, közös képzések, oktatások és gyakorlatok megszervezését és megtartását, valamint koordinált kiberbiztonsági kutatási és fejlesztési programok elindítását fogalmazták meg. Hosszú távú célként egy nemzeteken átívelő, regionális kibervédelmi tudatosság és kockázatkezelés kialakítását tűzték ki.[19]

### 5.2.7. ENCS (European Network for Cyber Security)

Az ENCS egy 2012-ben alapított, nonprofit tagszervezet, amely a biztonságos európai létfontosságú energiahálózatok és infrastruktúrák kialakításának támogatása érdekében jött létre. Ennek megfelelően az ENCS megteremti a lehetőséget arra, hogy a létfontosságú infrastruktúrák tulajdonosai, üzemeltetői, valamint a biztonsági szakemberek között kialakulhasson a megfelelő kapcsolat. Az ENCS olyan kutatókkal és tesztelő szakemberekkel rendelkezik, akik képesek az ENCS-tagokat és partnereiket segíteni az alkalmazott kutatásban, a technikai biztonsági követelmények, rendszerelemek és tesztelési eljárások meghatározásában, valamint az oktatási és képzési programokban.[20]

---

[18] Europol: European Cybercrime Centre; EC3. Elérhető: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (A letöltés dátuma: 2018. 06. 03.)

[19] Central European Cyber Security Platform held its third meeting in Vienna (2014). Elérhető: http://2010-2014.kormany.hu/en/ministry-of-public-administration-and-justice/news/central-european-cyber-security-platform-held-its-third-meeting-in-vienna (A letöltés dátuma: 2018. 06. 03.)

[20] European Network for Cyber Security. Elérhető: https://encs.eu (A letöltés dátuma: 2018. 06. 03.)

### 5.2.8. ECSO (European Cyber Security Organisation)

Az ECSO egy teljesen önfinanszírozású, nonprofit szervezet, amely a belga jog szerint 2016 júniusában jött létre. Az ECSO képviseli az ipari szereplőket az Európai Bizottságnál a kiberbiztonság szerződéses formában, a köz- és a magánszféra közötti partnerség (*Contractual Public Private Parntership,* cPPP) keretében történő kialakítása érdekében. Az ECSO tagjai között nagyvállalatok, kis- és középvállalatok (kkv), induló vállalkozások, kutatóközpontok, egyetemek, végfelhasználók, üzemeltetők, egyesületek mellett az európai tagállamok helyi, regionális és nemzeti közigazgatásának képviselői, valamint az Európai Gazdasági Térség (EGT) és az Európai Szabadkereskedelmi Társulás (EFTA) és a H2020 társult országok képviselői is megtalálhatók. Az ECSO fő célja az európai kiberbiztonsági fejlesztések, kezdeményezések vagy projektek támogatása, ösztönzése, különösen az alábbiak:

1. az európai digitális egységes piac növekedésének előmozdítása és védelme a számítógépes fenyegetések ellen;
2. az európai kiberbiztonsági piac fejlesztése, valamint a kiberbiztonsági és az infokommunikációs ágazat versenyképességének növelése;
3. a kiberbiztonsági megoldások kidolgozása és kialakítása a megbízható ellátási lánc azon kritikus összetevőihez, ahol Európa vezető szerepet tölt be.

Az ECSO különösen az alábbi területeken fejt ki aktivitást:

1. infokommunikációs infrastruktúrák (felhőalapú rendszerek, mobilhálózatok, hálózati megoldások stb.),
2. intelligens hálózatok (energiaszektor),
3. közlekedés (beleértve az autóipari és az elektromos járműveket),
4. okosépületek és okosvárosok,
5. ipari vezérlőrendszerek (ipar 4.0),
6. közigazgatás és nyitott kormányzás,
7. egészségügy,
8. pénzügy és biztosítás.

Az ECSO a kitűzött célok elérése érdekében jelenleg az alábbi munkacsoportokat működteti:

1. WG1: szabványosítás, tanúsítás, osztályozás és ellátásilánc-menedzsment;
2. WG2: piaci bevezetés, beruházások és nemzetközi együttműködés;
3. WG3: ágazati igények;
4. WG4: kkv-k támogatása, koordináció az országokkal (különösen Kelet- és Közép-Európa országaival) és régiókkal;
5. WG5: oktatás, biztonságtudatosság, képzés, kibergyakorlatok;
6. WG6: stratégiai kutatási és innovációs menetrend.[21]

[21] European Network for Cyber Security. Elérhető: https://encs.eu (A letöltés dátuma: 2018. 06. 03.)

### 5.2.9. Tervezett kiberbiztonsági fejlesztések az EU-ban

A fenti, már létező szervezetek mellett az EU komoly lépéseket tervez a kiberbiztonság megerősítése érdekében. A 2017-ben közzétett elképzelések szerint ennek fontosabb elemei a következők:

1. *Egy erős Európai Uniós Kiberbiztonsági Ügynökség létrehozása:* a már működő ENISA továbbfejlesztésével létrejövő szervezet feladata lesz a tagállamok segítése a kibertámadások megelőzésében, a bekövetkezett incidensekre történő reagálásban, évente páneurópai kiberbiztonsági gyakorlatok szervezése, a fenyegetettséggel összefüggő információk és tudás megosztása. A hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló, az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.)[22] végrehajtásának elősegítése, valamint az infokommunikációs termékek és szolgáltatások kiberbiztonságának garantálása érdekében uniós tanúsítási keretrendszer kialakításának és végrehajtásának elősegítése.
2. *Európai Kiberbiztonsági Kutatási és Kompetenciaközpont kialakítása:* a tervezett központ, együttműködve a tagállamokkal, segítséget nyújt a fejlett kibervédelmi eszközök és technológiák kifejlesztéséhez és alkalmazásához. Működésével kiegészíti az erre a területre irányuló uniós és nemzeti szintű kapacitásépítési erőfeszítéseket.
3. *Európa és a tagállamok gyors kibervédelmi reagálási képességének növelése:* a célkitűzés a nagyszabású kibertámadások miatti egységes operatív fellépés érdekében egy uniós kiberbiztonsági válságreagálási keretrendszer létrehozása, amelyhez a tagállamok és az uniós intézmények közreműködése elengedhetetlen. A keretrendszert a kiberbiztonsági és egyéb válságkezelési gyakorlatok során tervezik rendszeresen tesztelni és az eredmények alapján finomhangolni.
4. *Kiberbiztonsági Vészhelyzet-elhárítási Alap létrehozása:* az unió tervezi egy új Kiberbiztonsági Vészhelyzet-elhárítási Alap létrehozását azon tagállamok számára, amelyek az uniós jog által előírt összes kiberbiztonsági intézkedést felelős módon megvalósították. Az alap vészhelyzeti támogatást nyújt a tagállamok megsegítésére.
5. *A kibervédelmi kapacitások megerősítése:* a kibervédelem terén jelentkező készséghiány kezelésére az EU 2018-ban kibervédelmi képzési és oktatási platformot hoz létre, valamint elmélyíti a NATO-val való együttműködést, többek között párhuzamos és összehangolt gyakorlatok megtartásával.
6. *A nemzetközi együttműködés fokozása:* a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretrendszerének végrehajtásával, a kibertérben kialakuló konfliktusok megelőzését és a stabilitást szolgáló stratégiai keretrendszer kialakításával, valamint új, harmadik országoknak a kiberfenyegetések elleni küzdelemhez segítséget nyújtó kapacitások kiépítésével kívánja az EU megerősíteni a kibertámadásokra való reagálási képességeket.
7. *Hatékony büntetőjogi válaszintézkedések kialakítása:* a kibertérben vagy annak segítségével elkövetett bűncselekményektől való hatékony visszatartás érdekében

[22] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

> az EU egy új, a csalással és a készpénz-helyettesítő fizetési eszközök hamisításával szembeni küzdelemről szóló irányelv kialakítását tervezi. Ebben az információs rendszerekkel kapcsolatos bűncselekmények körét kiterjesztenék minden fizetési tranzakcióra, beleértve a virtuális fizetőeszközökkel végrehajtott tranzakciókat is, így erősítve meg a bűnüldöző hatóságokat, kiterjesztve azok lehetőségeit. A tervek szerint a jogszabály a szankciók mértékére vonatkozó közös szabályokat is bevezetne, valamint tisztázná a tagállami illetékességet a csalással és a készpénz-helyettesítő fizetési eszközök hamisításával elkövetett bűncselekmények tekintetében.

A számítástechnikai eszközök felhasználásával elkövetett bűncselekményekre vonatkozó nyomozások és büntetőeljárások, így a felderítésre, nyomon követhetőségre és büntetőeljárás alá vonásra vonatkozó bűnüldözési válaszlépések hatékonyságának növelése céljából az Európai Bizottság javaslatokat fog előterjeszteni az elektronikus bizonyítékokhoz való határon átnyúló hozzáférés megkönnyítéséről, valamint a titkosítás bűnügyi nyomozásokban betöltött szerepéről.[23]

[23] Az unió helyzetéről szóló beszéd: *Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet* (2017). Elérhető: http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (A letöltés dátuma: 2018. 06. 03.)