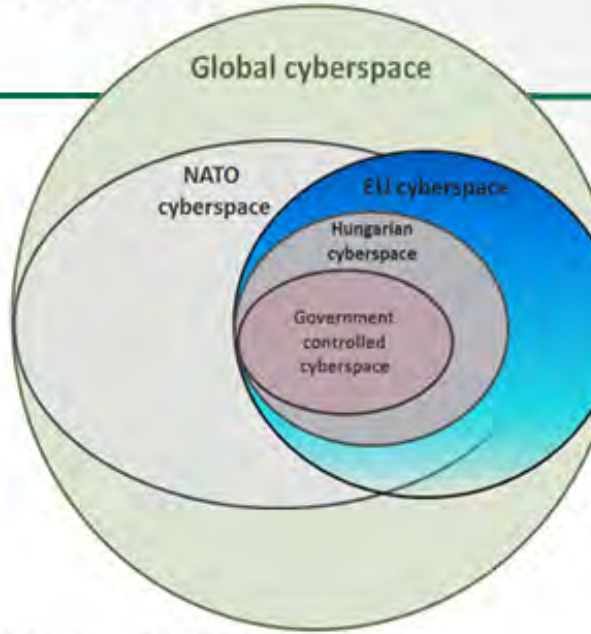
NEMZETI
KIBERVÉDELMI INTÉZET

Az NKI bemutatása

Tikos Anita
Nemzeti Kibervédelmi Intézet

NEMZETI KIBERVÉDELMI INTÉZET

EGY KIS TÖRTÉNELEM



- 2013. Nemzeti Kiberbiztonsági Stratégiája
- 2013. július 1.:
  hatályba lép az Információbiztonsági törvény (Ibtv.)

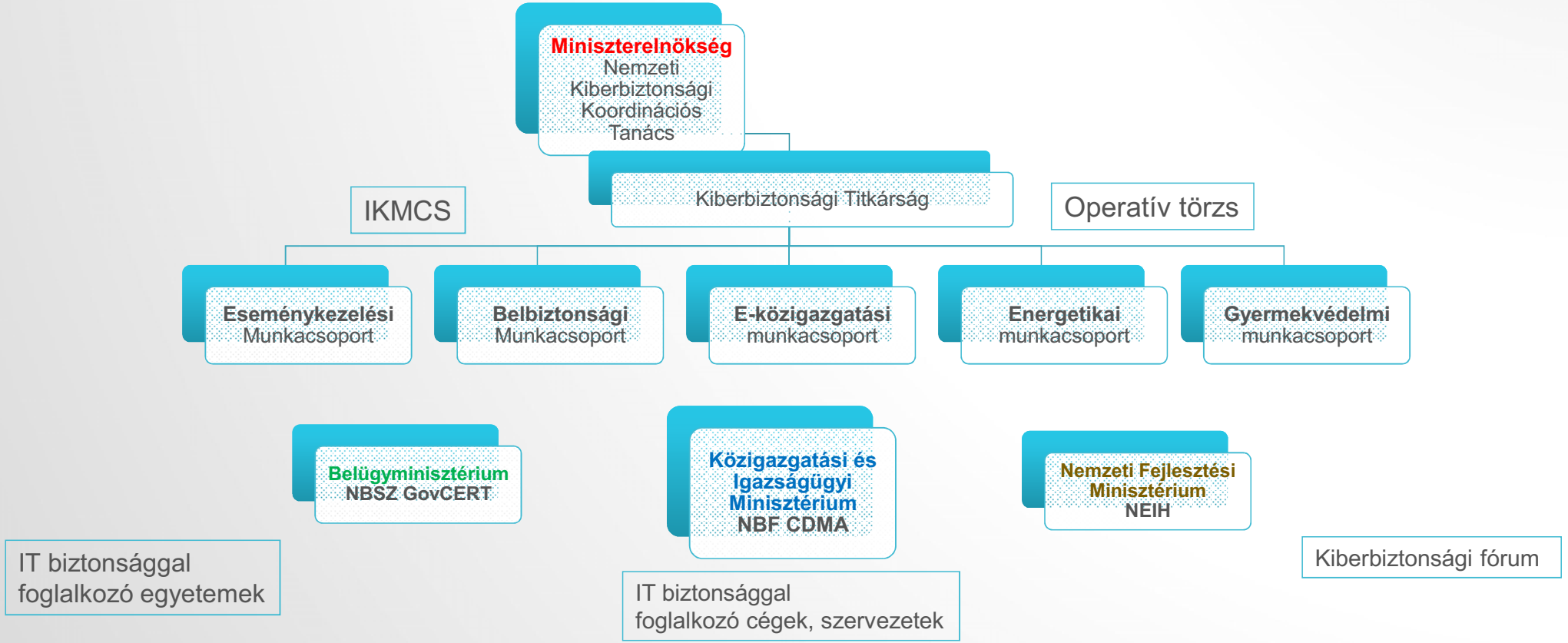
Heterogén szervezetrendszer:

- hatósági feladatok: Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)
- szakhatóság: Nemzeti Biztonsági Felügyelet CDMA
- Informatikai biztonsági eseménykezelés : NBSZ GovCERT
- Kiberbiztonsági Koordinációs Tanács

Nehézkes együttműködés, forráshiány, infóhiány…

NEMZETI KIBERVÉDELMI INTÉZET

KIBERBIZTONSÁGI STRUKTÚRA 2015. JÚLIUS 16. ELŐTT



NEMZETI KIBERVÉDELMI INTÉZET

JELENLEGI KIBERBIZTONSÁGI STRUKTÚRA

Belügyminisztérium
Nemzeti Kiberbiztonsági Koordinációs Tanács

Nemzeti Kibervédelmi Intézet

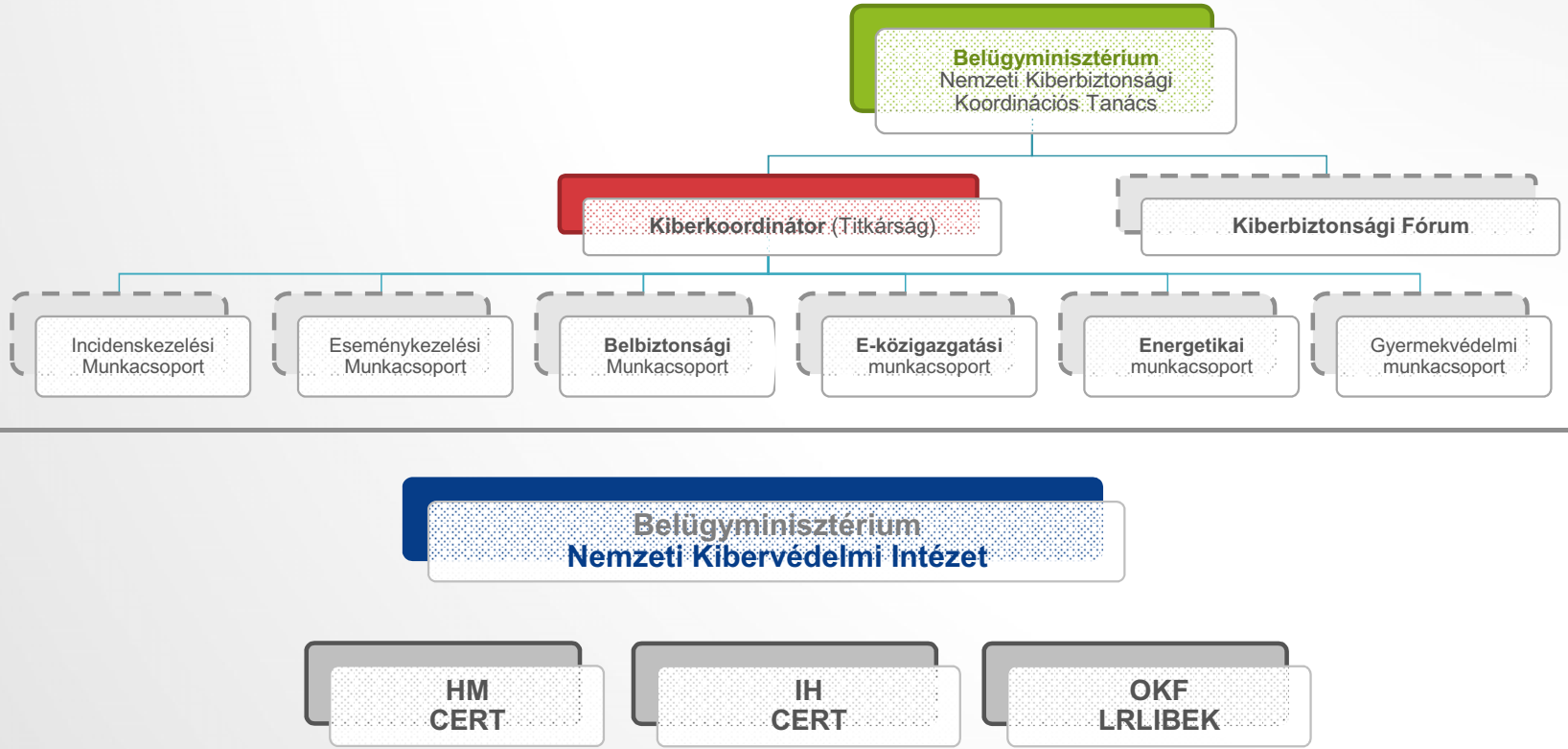
GovCERT

NEIH

Biztonságirányítás támogatás

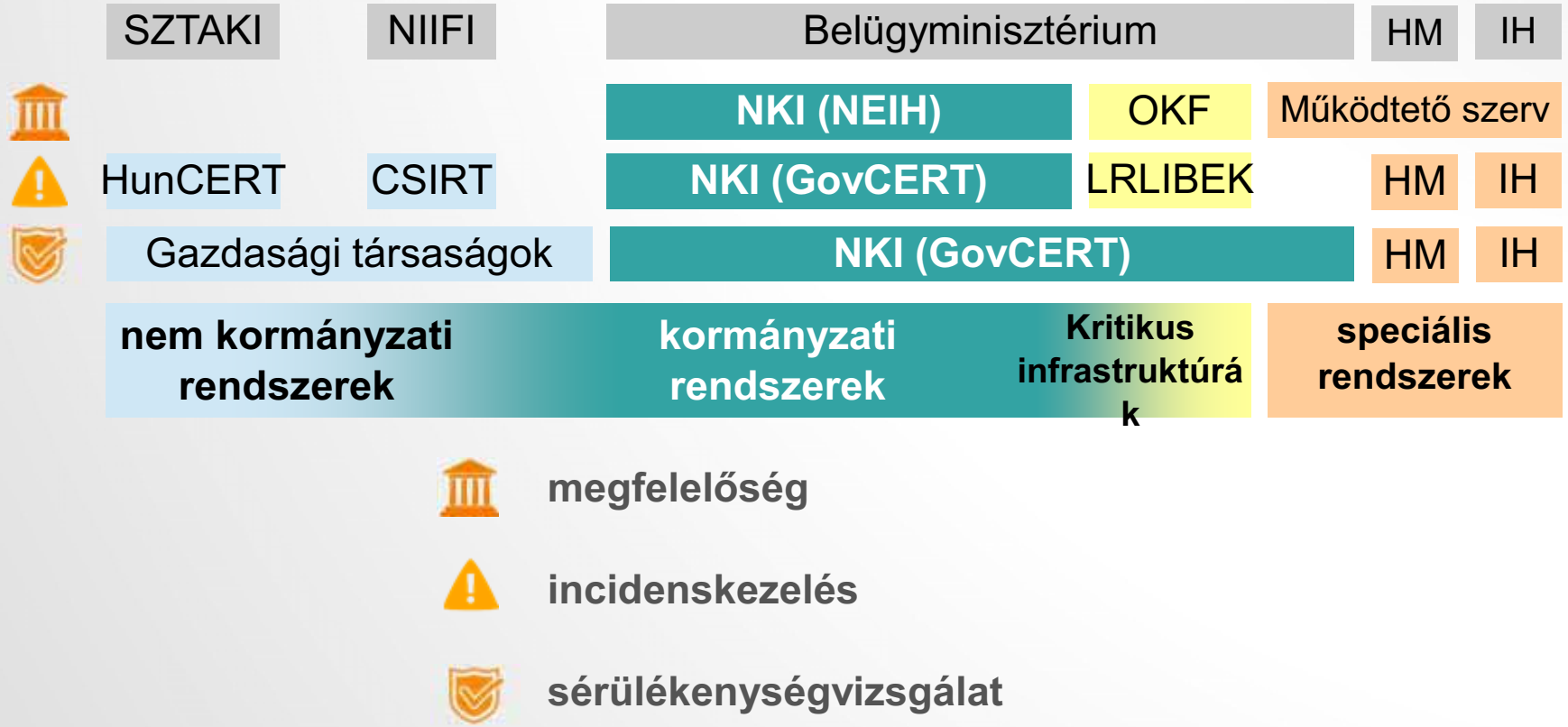
NEMZETI KIBERVÉDELMI INTÉZET

ÚJ STRUKTÚRA 2015 JÚLIUS 16. UTÁN



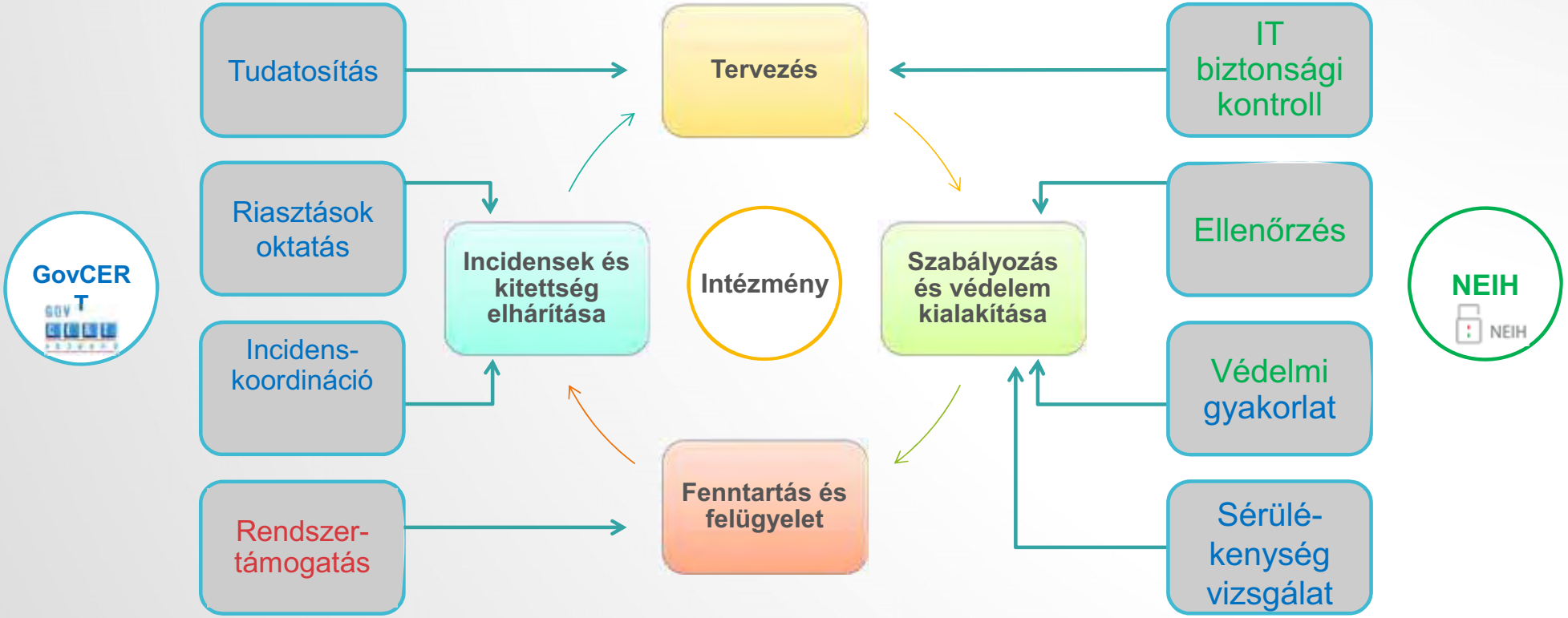
NEMZETI KIBERVÉDELMI INTÉZET

ÚJ SZERVEZETI MODELL (2015)



NEMZETI KIBERVÉDELMI INTÉZET

KORMÁNYZATI IT BIZTONSÁGI ÉLETCIKLUS



NEMZETI KIBERVÉDELMI INTÉZET

SZERVEZETI FELÉPÍTÉS

GovCERT Incidenskezelő Osztály	- Biztonsági események kezelése - Fenyegetésmenedzsment - Ügyeleti szolgálat - Elemzés/értékelés - Kibervédelmi gyakorlat - Képzés, tudatosítás
Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)	- Ügyfelek és rendszerek nyilvántartása - Biztonsági osztályba és szintbe sorolás ellenőrzése - Követelmények teljesülésének ellenőrzése - Javaslat információbiztonsági felügyelő kirendelésére
Biztonságirányítási és Sérülékenységvizsgálati Osztály	- Sérülékenységvizsgálat - EMIR/FAIR rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása -IT biztonsági tanácsadás

NEMZETI KIBERVÉDELMI INTÉZET

NEMZETKÖZI SZEREPVÁLLALÁS

- **szervezeti tagságok:**
  - FIRST — globális
  - Trusted Introducer — európai súlypontú
  - CECSP — V4 és Ausztria
  - IWWN — globális
- **munkacsoport tagságok**
  - Berni klub – elektronikus támadások (EA)
  - ENISA szakértői munkacsoportok
  - Európai Bizottsági munkacsoportok (EFMS, EP3R)
  - NIS munkacsoportok (Együttműködési Csoport, CSIRT hálózat stb.)

NEMZETI KIBERVÉDELMI INTÉZET

NEMZETKÖZI SZEREPVÁLLALÁS 2016

- **kibervédelmi gyakorlatok**
  - Cyber Storm V.
  - CMX
  - Locked Shields
  - Cyber Europe 2016
- **együttműködések**
  - Európai Hálózat- és Információbiztonsági Irányelv (NIS)
  - Smart Project

NEMZETI
KIBERVÉDELMI INTÉZET

Az EU-s információbiztonsági szabályozás

NEMZETI KIBERVÉDELMI INTÉZET

NIS IRÁNYELV: ELŐZMÉNYEK

- 2013. február 7: Az **Európai Unió Kiberbiztonsági Stratégiája**: Nyílt, megbízható és biztonságos kibertér" című közlemény **hálózat- és információbiztonságnak** az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló **irányelv javaslatát**
- Cél: EU-s szinten közös minimum szabályok és képességek
- Intézmények és követelmények definiálása
- Tagállamok által kialakított struktúra fenntartása
- Biztonságos, hatékony együttműködés EU-s szinten (CSIRT és hatóság esetében egyaránt)

NEMZETI KIBERVÉDELMI INTÉZET

NIS IRÁNYELV

- új EU-szintű kiberbiztonsági szabályozás
  - az EU **2016/1148** irányelve (2016. július 19.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedések
  - **Cél:** EU-s szinten közös minimum szabályok és képességek
  - Tagállamok által kialakított **struktúra fenntartása**
- a piaci és kormányzati szereplők széles körét érinti
- IT-biztonsági követelményeket, incidens bejelentési eljárásokat ír elő
  - **alapvető szolgáltatást nyújtó szereplők**nek és
  - **digitális szolgáltatók**nak

NEMZETI KIBERVÉDELMI INTÉZET

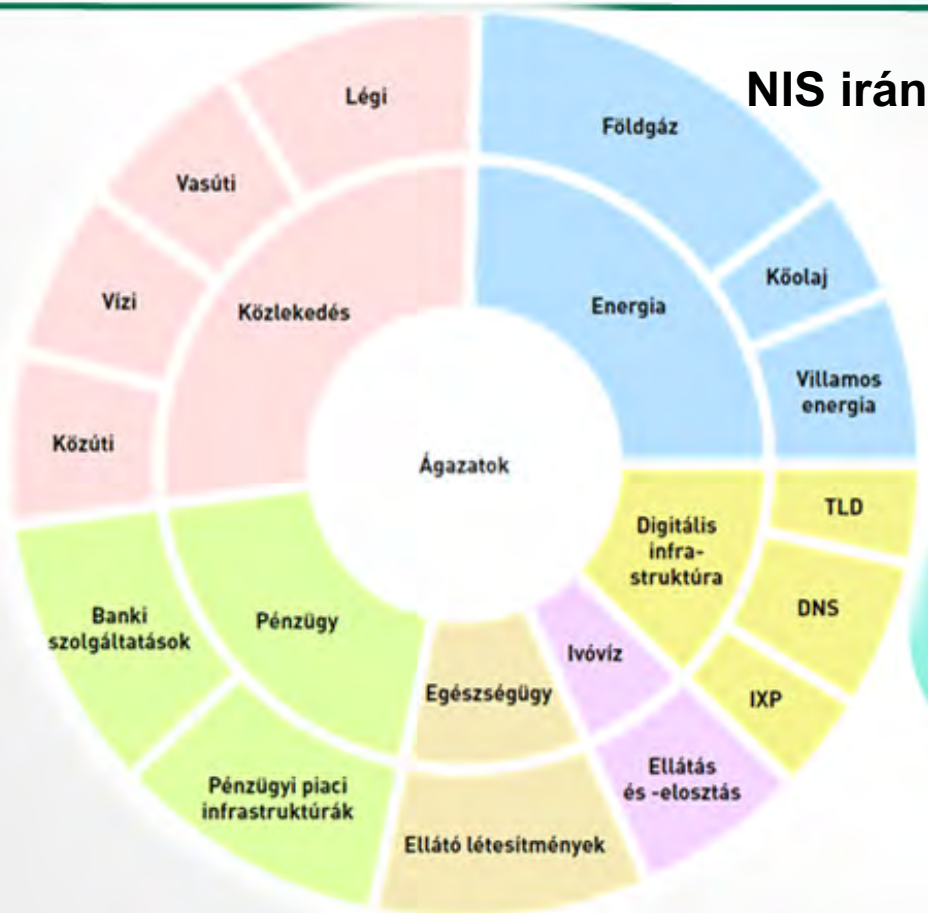
HATÁLY JOGSZABÁLYOK

Ibtv.

állami és önkormányzati szervek

+

NIS irányelv



Digitális szolgáltatók

NEMZETI KIBERVÉDELMI INTÉZET

ALAPVETŐ SZOLGÁLTATÓK

- **alapvető szolgáltatásokat nyújtó szereplő(6 szektor)**
  - **közjogi vagy magánjogi szervezet**, amely
    - kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt
    - a szolgáltatása IT rendszerektől függ
    - a szolgáltatását érintő biztonsági esemény jelentős zavart okozna a szolgáltatásban

- **feladatai**
  - megfelelő és arányos műszaki és szervezési intézkedéseket tesz
    - IT rendszerei biztonságát fenyegető kockázatok kezelésére, és
    - IT rendszereit érintő biztonsági események megelőzésére, hatásainak csökkentésére
  - bejelenti a szolgáltatásaira jelentős hatást gyakorló biztonsági eseményeket

NEMZETI KIBERVÉDELMI INTÉZET

DIGITÁLIS SZOLGÁLTATÓK

- **digitális szolgáltató**
  - minden digitális szolgáltatást nyújtó jogi személy

- **feladatai**
  - az alábbi szolgáltatások EU-n belül nyújtása során általa használt IT rendszerek biztonságát fenyegető kockázatok kezelése érdekében megfelelő és arányos műszaki és szervezési intézkedéseket tesz:
    - online piactér
    - online keresőprogram
    - felhőalapú számítástechnikai szolgáltatás
  - bejelenti a szolgáltatásaira jelentős hatást gyakorló biztonsági eseményeket

NEMZETI KIBERVÉDELMI INTÉZET

ALANYI HATÁLY: KIVÉTELEK

- **nem vonatkozik**
  - mikro- és kisvállalatok;
  - más EU-szintű IT-biztonságot érintő ágazati szabályozás hatálya alá (is) esők (pl. kritikus infrastruktúra)
  - a nemzeti ágazati kijelölési kritériumokat nem teljesítő alapvető szolgáltatók
  - gyártók, fejlesztők

- **vonatkozik**
  - EU-n kívüli székhelyű, de az **EU területén szolgáltatást nyújtók** (pl. Google)
  - (közvetve, az érintetteknek IT szolgáltatást nyújtó harmadik felek)

NEMZETI KIBERVÉDELMI INTÉZET

TAGÁLLAMOK FELADATAI

- kapcsolattartási pontok kijelölése (SPoC)
- részvétel az EU-szintű
  - stratégiai együttműködési csoportban és
  - CSIRT-hálózatban
- jogszabályalkotás illetve -harmonizáció
  - stratégia elfogadása
  - jogszabályok elfogadása
    - ágazati kijelölés kritériumai
    - IT-biztonsági követelmények
    - incidens-bejelentési követelmények
- statisztikai adatszolgáltatás időszakosan

NEMZETI KIBERVÉDELMI INTÉZET

TAGÁLLAMOK FELADATAI

Más szabályozások is fogalmaznak meg biztonsági követelményeket, incidens bejelentési kötelezettséget:

- eIDAS
- CI
- Adatvédelmi rendelet
- elektronikus hírközlés keretszabályozás

\+

NIS irányelv

ENISA 2012

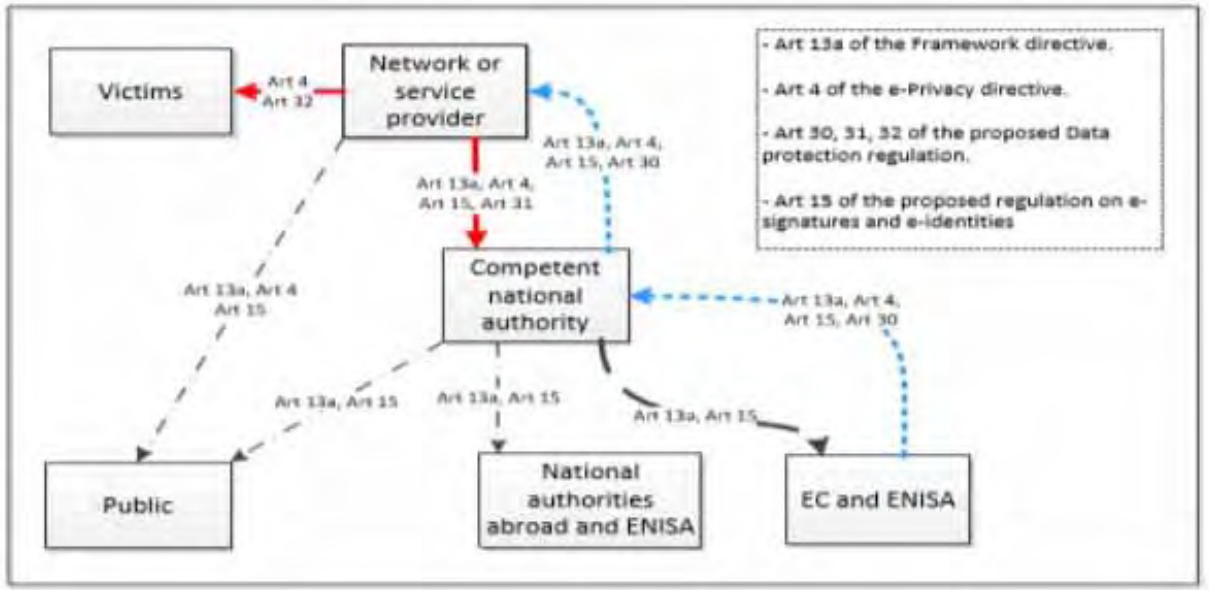
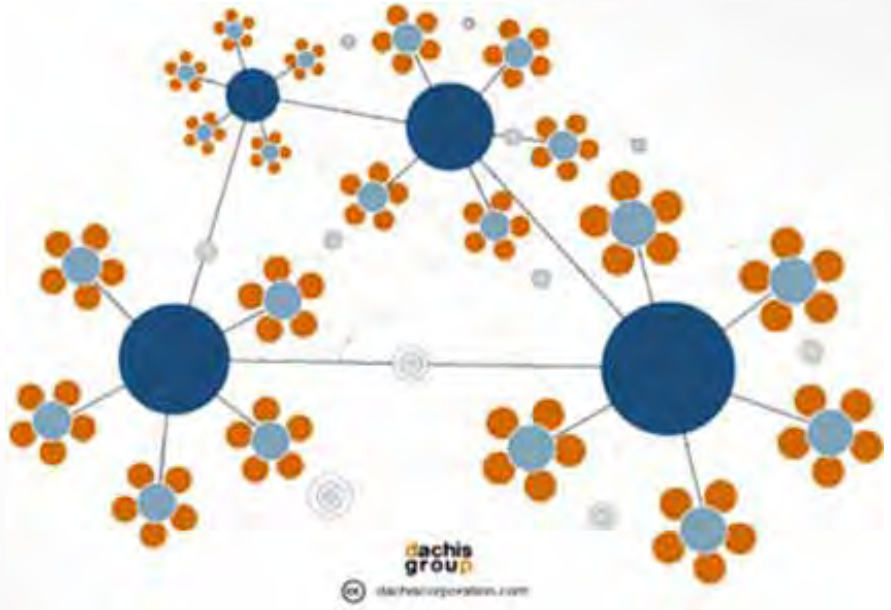


Figure 2: Commonalities and differences between the security articles

NEMZETI KIBERVÉDELMI INTÉZET

ÁGAZATI MODELLEK

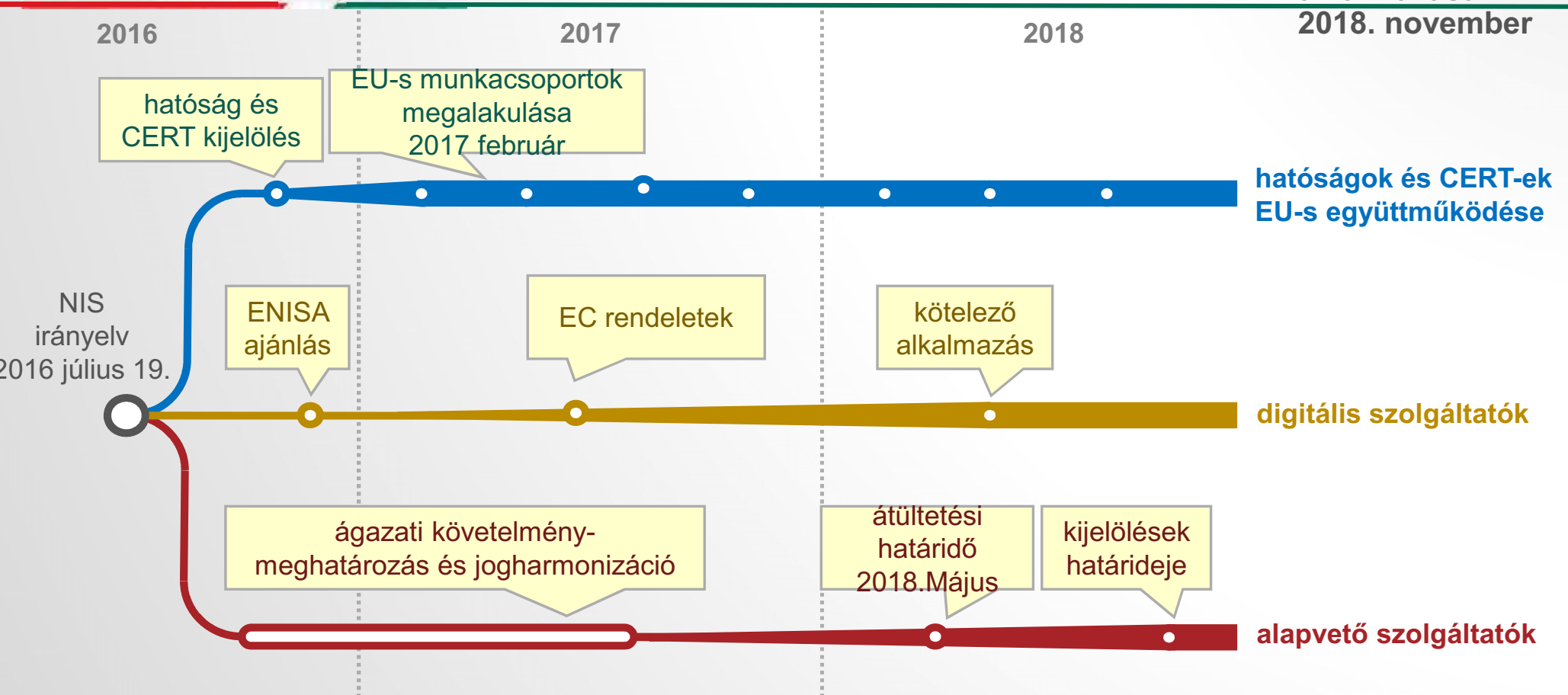
- **decentralizált**
  - az ágazati szereplők önszerveződően hoznak létre CERT-et
- **részben centralizált**
  - a meglévő ágazati szabályozó szerv vállalja fel a CERT szerepét
- **centralizált**
  - az ágazati szereplők a GovCERT szolgáltatásait közvetlenül veszik igénybe



- itthon várhatóan hibrid, azaz ágazatonként eltérő modell alakul ki

NEMZETI KIBERVÉDELMI INTÉZET

MENETREND



NEMZETI
KIBERVÉDELMI INTÉZET

?

cert@govcert.hu
info@neih.gov.hu