Netwerk- en InformatieBeveiligingrichtlijn (NIB)

Ir. Eric Luiijf

Agenda

- Relatie tussen verschillende programma's en wetten
- Doelstelling NIB
- NIB Richtlijn
- NIB in de EU en waar staat Nederland
- Fricties in NL- en EU-brede aanpak

Context: Bescherming Vitale Infrastructuur

Nederland BZK actieplan
tegen terrorisme

- 2003:
  12 vitale sectoren; 35 producten

  2005: prioritaire
  vitale infrastructuren

EU Home Affairs – **antiterrorisme**

- 2008/114/EC "EPCIP"
  Identificatie van CI & betere beveiliging
- Eisen aan lidstaten: identificeer CI
  => ECI & OPS
- EU-brede CI: power, transport, …

Context: Bescherming Vitale Infrastructuur

…

EU landen onderkennen vitale infrastructuur

- AT: 13, BE: 4, CR: 11, CZ: 9 , DK: 10, EE: 9, FI: ~, FR: 12: GE: 9, PO: 10, SK: 9, SL: 8, SP: 12, SE: 11, UK: 9
- zie: CI sectors op www.cipedia.eu

2014/15: Herijking Vitale Infrastructuur

Context: Bescherming Vitale Infrastructuur

Categorie A: minstens een van

> 50 miljard schade

> 10.000 doden, zwaargewonden

> 1 miljoen zwaar getroffenen

plus cascade-uitval > 2 infrastructuren

Categorie B: minstens een van

> 5 miljard schade

> 1.000 doden / zwaargewonden

> 100.000 zwaar getroffenen

- Afwijkend van alle andere EU landen

- Tijdsduur?

Wet gegevensverwerking en meldplicht cyber security (Wgmc)

- 27/7/2017 "tussenwet" Vitale Infrastructuuraanbieders en Rijksoverheid
- Wettelijke taken NCSC: bijstand, informatie delen, technische analyse
- Meldplicht *deel van* vitale infra per 1/1/2018
  - drinkwater
  - elektriciteits- en gastransport en –distributie
  - nucleair
  - financieel onder toezicht DNB
  - telecom > 1 miljoen klanten / internetknooppunt > 8 Tb/s
  - havenbedrijf Rotterdam, Schiphol (luchthaven, KMar, LVNL, operators > 25% vliegverkeer)
  - keren en –beheren (Rijkswaterstaat)

NIB richtlijn & doelstelling

- Wetgeving door economische 'pillar' van de EU
- Doel: **hoog gemeenschappelijk niveau aan NIB in de EU**
  teneinde de werking van de interne markt te verbeteren door
  - betere nationale capaciteiten (NCSS, bevoegde autoriteit(en))
  - verbeterde samenwerking (EU beleidsgroep, samenwerkend netwerk CSIRTs)
  - risicomanagement- en rapportageverplichtingen AEDs (OES) en DSPs
  - focus op uitval IT/OT en de businesscontinuïteit van de dienstverlening

- (EU) 2016/1148: deze richtlijn ***staat geheel los van EPCIP !***

NIB richtlijn (2)

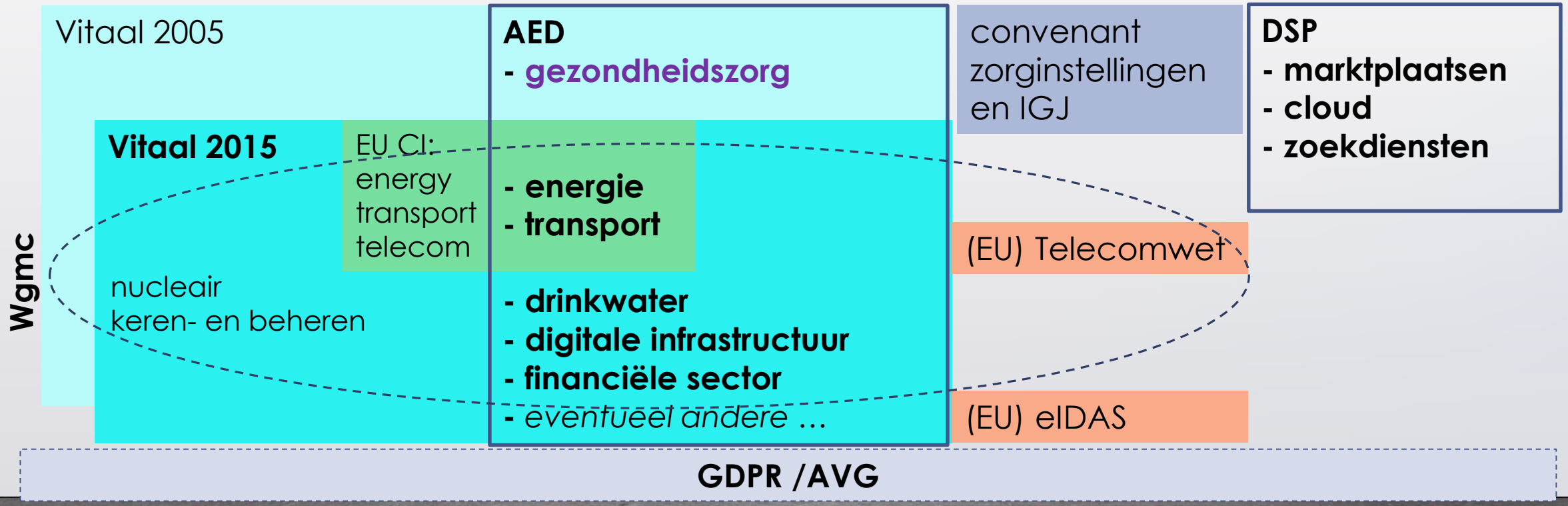
- AED
  - essentiële dienst voor vitale activiteiten van de samenleving en economie: energie, vervoer, bankwezen, **gezondheidszorg**, drinkwater, **digitale infrastructuur** (IXen, DNS, TLD registraties)
  - controleerbare beveiliging
- DSPs (> 10 M€/jaar, > 50 mdw's)
  - online markplaatsen, zoekmachines, cloud computerdiensten
  - minimale eisen: beveiliging, BCM, incident handling, standaarden
- CA meldplichtdrempel
  - op basis van: aantal getroffenen, gebiedsgrootte, uitvalduur
  - voor DSP ook: omvang impact samenleving en omvang verstoring van de werking

NIB richtlijn (3)

- 8/2016: NIB richtlijn in werking
- 9/5/2018: deadline voor transponering in nationale wet- en regelgeving
  - 15 van de 28 landen hebben de wetgeving nog niet klaar
- 9/11/2018: deadline voor identificatie AEDs/DSPs
  - NL denkt aan ~ 60 AEDs en 100 – 200 DSPs
    IGJ: gezondheidszorg voldoet niet aan ***vitaal-B criteria***; dus geen AEDs?
    - uitval ICT ziekenhuizen, ICT-verstoring apotheekdistributie, 50.000 pacemakers … ?
  - VK: 47 energy, 268 health en 80 transport AEDs,
    129 cloud operators, 3 marktplaatsen + Amazon & eBay
    gedetailleerde criteria per sector

Meer meldplichten per sector

NCSC, bevoegde autoriteit, AP

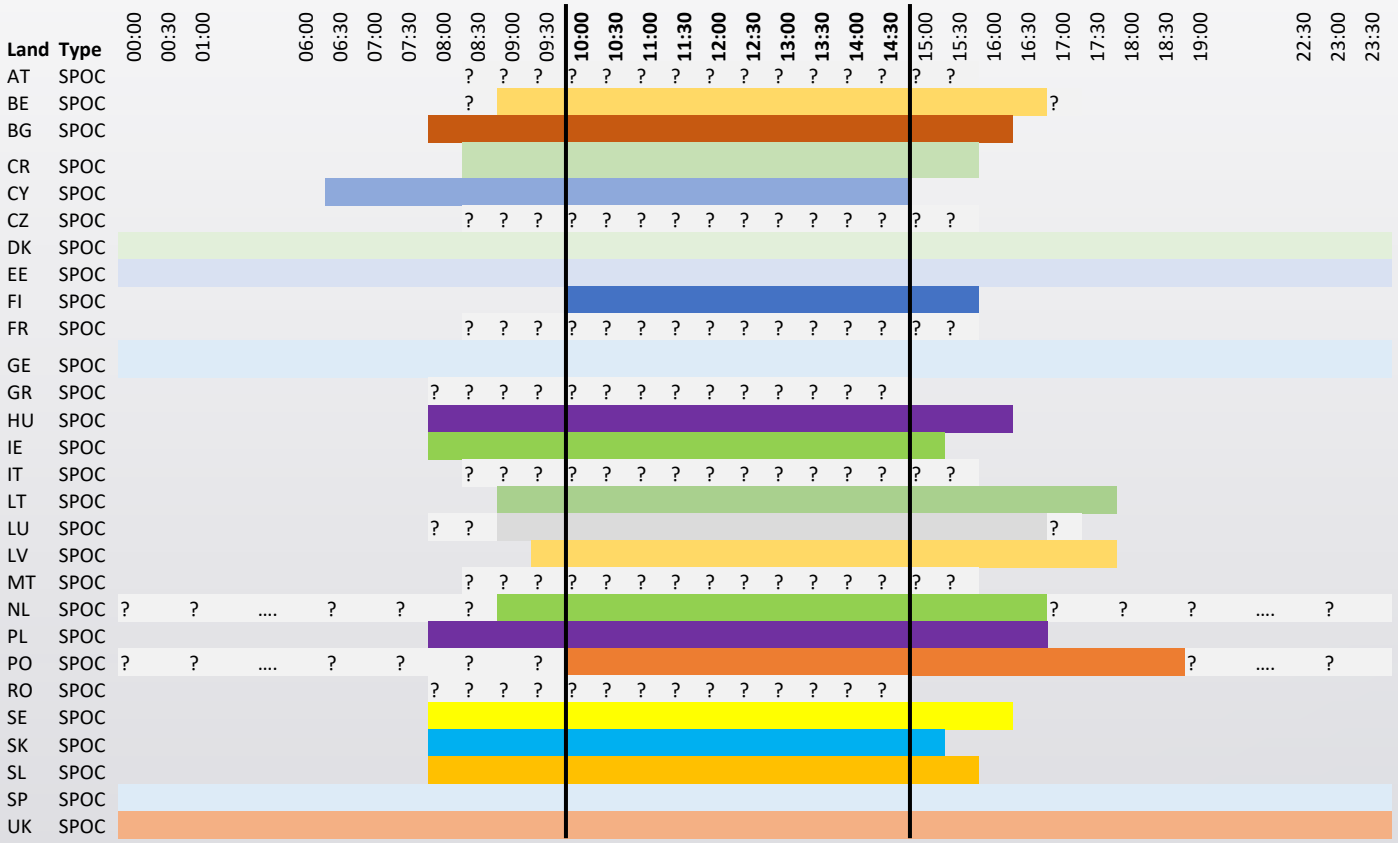


Wie zijn onze bevoegde autoriteiten (CA) ?

- Minister EZK
  (Agentschap Telecom)
- DNB
- Minister I&W
- Minister Medische zorg
- energie en digitale infrastructuur
  DSPs
- bankwezen
  infrastructuur financiële markt
- transport
  drinkwater
- gezondheidszorg

Nationale centraal contactpunten (bron: ENISA site)

- 21/28 niet open op nationale feestdagen, weekeinden … alleen tussen 10 en 15 uur *(en niet tijdens de lunch)*



5/28 zijn 24/7 bereikbaar

2/28 lezen soms e-mail

Incidenten **onverwijld** melden

- CA AEDs
  - één autoriteit per land (NCSC) (9)
  - ministeries (6)
  - toezichthouders (6)
  - veiligheidsdiensten (4)
  - nog onbekend (3)

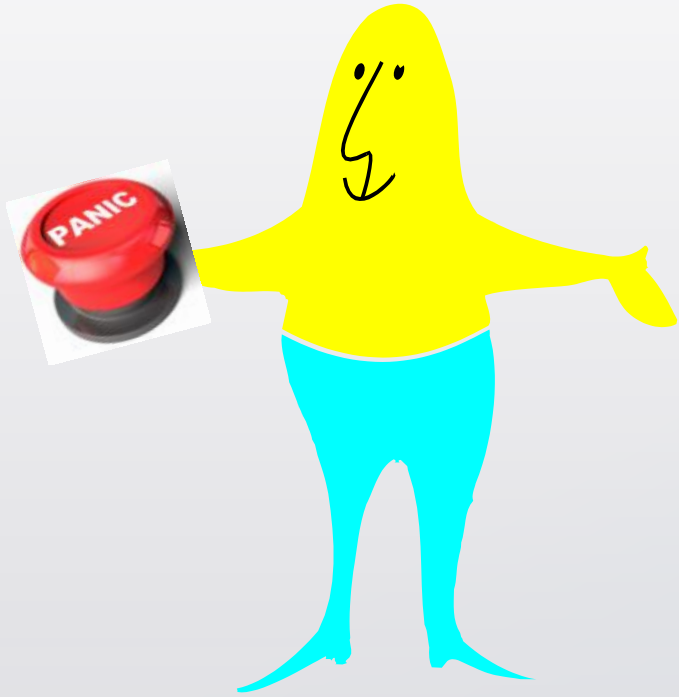
- Opvallend
  - Noord-Ierland anders dan VK … Brexit voorbereiding?
  - ES splitst AED in publiek (24/7) – privaat (werkuren)

NIB fricties

- In Nederland complexe meldplichten
  - van alleen eigen toezichthouder tot toezichthouder + NCSC + AP
- Niet geharmoniseerd over de grens heen, bijv. gezondheidszorg
- Bereikbaarheid van NPoCs en CAs toont geen internationale urgentie/paraatheid

- Buiten scope: EU 910/2014 eIDAS (DigiD, eID e.d.)
  2002/21/EG essentiële telecomdiensten
- Belangrijke gaten in aanpak, bijv. sectorbrede databases nummerportabiliteit, energiecontracten, …

Bedankt voor uw aandacht



luiijfconsultancy@ziggo.nl