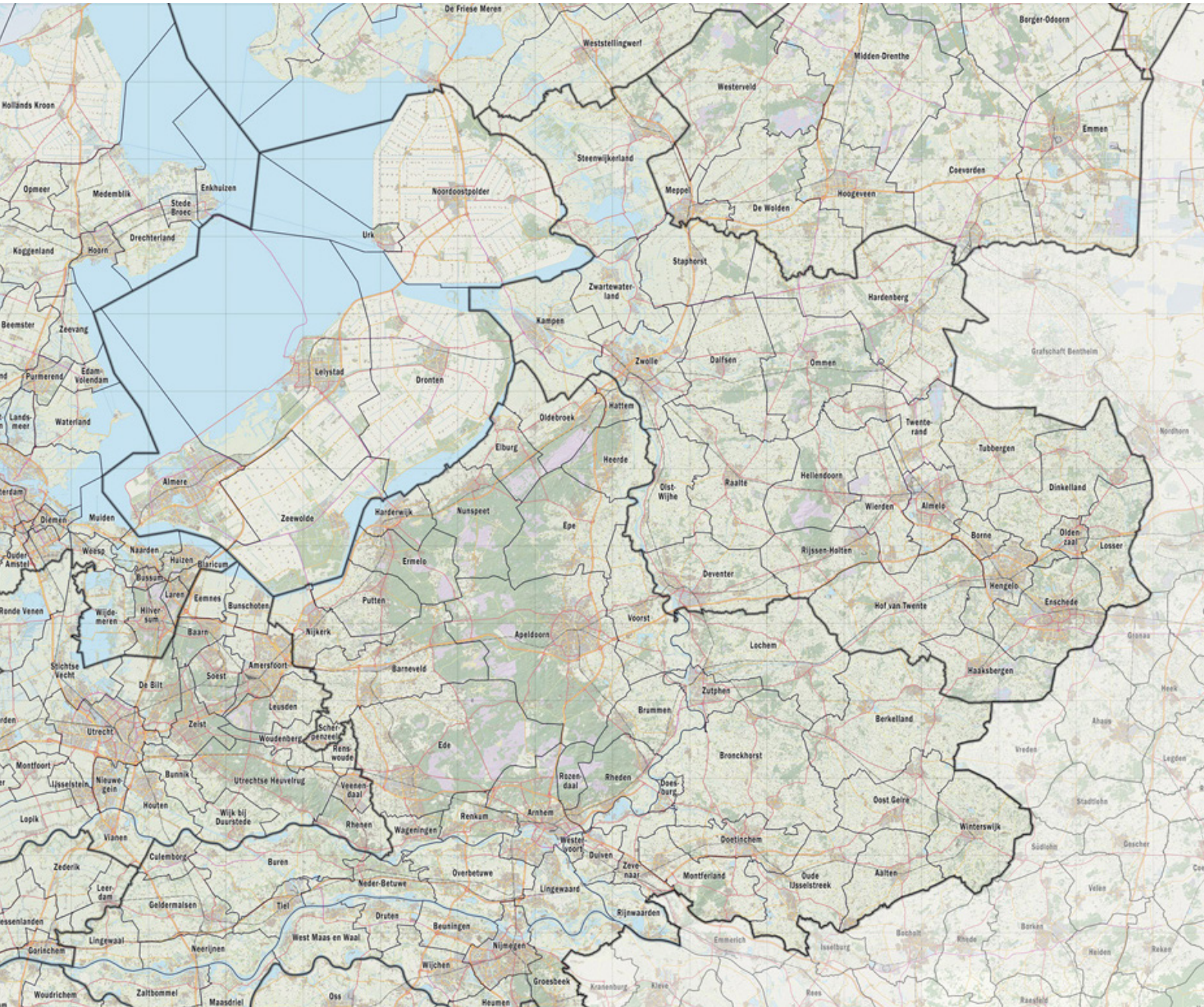
Instituut
Fysieke
Veiligheid

Bestuurlijke Netwerkkaarten Crisisbeheersing

Netwerkkaart 21b
Cybersecurity



21b Cybersecurity

Voor telecommunicatie (en providers), zie *Bestuurlijke Netwerkkaart telecommunicatie*
Voor media/omroepen, *zie Bestuurlijke Netwerkkaart media*

versie 2019

Crisistypen	• inbreuk internetveiligheid (cybersecurity)
Bevoegd gezag	• minister van JenV (computercriminaliteit, persoonlijke levenssfeer en cybersecurity) • minister EZK, minister IenW (toezicht op cybersecurity van aanbieders van essentiële diensten en digitale dienstverleners)
Soorten maatregelen	• eigen maatregelen door aanbieders van essentiële diensten en digitale dienstverleners • handhaving jegens digitale dienstverleners en aanbieders van essentiële diensten • waarschuwingen en advisering bij een dreiging of daadwerkelijke inbreuk op internetveiligheid (cybersecurity)

Algemeen

- Bedrijven en instellingen zijn zelf verantwoordelijk voor de continuïteit van hun diensten: zij treffen maatregelen om een verstoring zo spoedig mogelijk op te heffen.

Eigen maatregelen

- Grote digitale dienstverleners (online marktplaatsen, clouddiensten, zoekmachines) en zogeheten aanbieders van essentiële diensten zijn verplicht digitale verstoringen zo snel mogelijk te verhelpen en de gevolgen zoveel mogelijk te beperken.
- Aanbieders van essentiële diensten zijn onder meer:
  - de landelijke en regionale elektriciteits- en gasnetbeheerders;
  - de NAM en de Stichting Centraal Orgaan Voorraadvorming Aardolieproducten (COVA);
  - de Rotterdamse Haven en de luchthaven Schiphol;
  - drinkwaterbedrijven;
  - beheerders van digitale infrastructuur, zoals grote internetknooppunten en Stichting Internet Domein Registratie (SIDN), als beheerder van toplevel-domeinnaam .nl en DNS-dienstverlener.
- Noot: de financiële kerninfrastructuur is al op basis van andere regelgeving verantwoordelijk voor de continuïteit van hun diensten (inclusief cyberveiligheid). Zie verder *Bestuurlijke Netwerkkaart Financieel verkeer,* met name onder *Continuïteit betalings- en effectenverkeer* en *Cybersecurity*.

Toezicht

- Het toezicht is sectoraal belegd:
  - het Agentschap Telecom (namens minister EZK) voor de grote digitale dienstverleners en beheerders van digitale infrastructuur en de energiesector (landelijke en regionale elektriciteits- en gasnetbeheerders, de NAM en de COVA);
  - de Inspectie Leefomgeving en Transport (de minister IenW) voor de drinkwaterbedrijven, Schiphol en de Rotterdamse haven;
- De toezichthouder kan aanwijzingen geven en spoedbestuursdwang toepassen.

Overheidsinterventie in de ICT-sector

- Een interventie jegens de ICT-sector als zodanig is voorbehouden aan de minister van EZK en kan (ook) plaatsvinden op basis van de Telecommunicatiewet. Het aanbieden van internettoegang valt onder 'het aanbieden van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten' in de zin van de Telecommunicatiewet (zie verder *Bestuurlijke Netwerkkaart Telecommunicatie*).

Cybercrime

- De aanpak van cybercrime valt onder de reguliere opsporingsverantwoordelijkheid van politie en OM. Cybercrime kan leiden tot een digitale verstoring.

Computercrisisteams

- De operationele respons op beveiligingsincidenten en verstoringen met computers of netwerken vindt in veel organisaties plaats in zogeheten CERTs/CSIRTs (*Computer Emergency Response Teams*/*Computer Security and Incident Response Teams)*, gespecialiseerde computercrisisteams van ICT-professionals. Er zijn CERTs voor grote bedrijven en instellingen, maar ook voor sectoren, zoals de voor de zorgsector (Zorg-CERT). CSIRTs zijn de computercrisisteams met een wettelijke basis.

Nationaal Cyber Security Centrum

- Het Nationaal Cyber Security Centrum (NCSC) valt onder het ministerie van JenV.
- De CSIRTs voor de aanbieders van essentiële diensten en voor de rijksoverheid vallen onder het NCSC. De CSIRT DSP (de digitale dienstverleners) valt onder het ministerie van EZK.
- Bij een dreiging of daadwerkelijke inbreuk doet het NCSC waarschuwingen uitgaan en kan het overheden en bedrijfsleven bijstaan en adviseren over te treffen maatregelen.
- Afhankelijk van de dreiging of het incident nemen ICT-experts van vitale aanbieders / sectoren deel in de *ICT Response Board* (IRB) dat door het NCSC wordt gefaciliteerd. De IRB is een publiek-privaat samenwerkingsverband, dat bij elkaar komt wanneer een grote ICT-crisis dreigt of zich voordoet in meerdere sectoren. De IRB zal indien nodig ook direct waarschuwingen doen uitgaan en adviseert binnen de nationale crisisbesluitvormingstructuur de rijksoverheid en (zie verder *Bestuurlijke Netwerkaart Rampenbestrijding algemeen en handhaving openbare orde*).
- Het NCSC onderhoudt contacten met buitenlandse CSIRTs/CERTs en met het Europese ENISA (zie hierna).

Militaire steunverlening cybersecurity

- Militaire steunverlening: op verzoek van de minister van JenV kan Defensie de CSIRT-functie ondersteunen van de NCSC (voor de rijksoverheid en de aanbieders van essentiële diensten). In andere gevallen kan de desbetreffende minister, commissaris van de Koning, dijkgraaf of burgemeester om militaire steun verzoeken.
- In geval van cybercrime kan Justitie en Veiligheid/Openbaar Ministerie ook militaire (politie)bijstand aanvragen ten behoeve van de opsporing.
- Zie verder *Bestuurlijke Netwerkkaart Defensie*.

Afstemming met veiligheidsregio's

- Samenwerking tussen aanbieders van vitale diensten (vitale sectoren) en veiligheidsregio's is in enkele gevallen vastgelegd in convenanten. *Zie desbetreffende bestuurlijke netwerkkaarten.* De convenanten hebben niet specifiek betrekking op cyberincidenten.
- Op basis van die convenanten kan een liaison van een vitale aanbieder desgevraagd zitting nemen in het regionaal beleidsteam. Dit kan ook anders zijn georganiseerd door een liaison van de veiligheidsregio in het crisisteam van de aanbieder(s).
- In geval van grote cyberverstoringen zal de aanpak van de verstoring op nationaal

niveau plaatsvinden, in de nationale crisisstructuur. Het NCC informeert de veiligheidsregio's. Zie verder deel *Nationale afstemming* in *Bestuurlijke Netwerkkaart Rampenbestrijding algemeen en handhaving openbare orde*.

Burgemeester en voorzitter veiligheidsregio

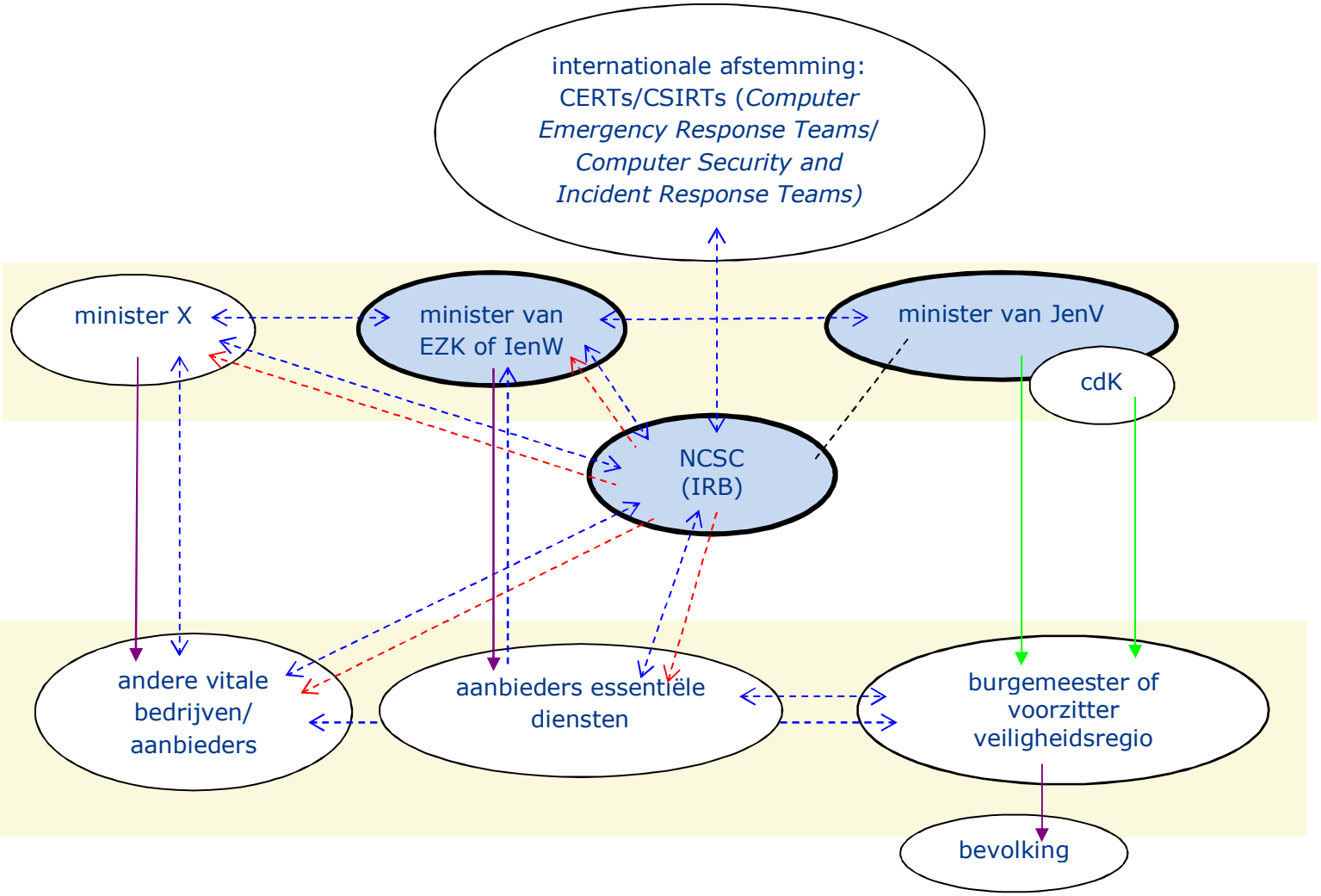
- De burgemeester of voorzitter veiligheidsregio heeft geen invloed op het functioneren van de sector zelf (de continuïteit van de verlening van vitale diensten of de aanpak van een cyberincident als zodanig).
- De burgemeester of voorzitter veiligheidsregio is verantwoordelijk voor aanpak van de effecten voor de openbare orde en de openbare veiligheid.

Europese Unie

- Het Europees Agentschap voor netwerk- en informatiebeveiliging/*European Network and Information Security Agency* (ENISA) vervult evenwel op dit moment geen rol in de responsfase. Bijstand door ENISA geschiedt op vrijwillige basis en heeft betrekking op preventie en preparatie.

functionele ketens vitaal **algemene keten**

cybersecurity



- Informatie en afstemming
- Bijstand
- Maatregelen jegens bevolking/bedrijven
- Bestuurlijk toezicht, tevens onderlinge informatie
- Interne lijn

NB 1. Het Nationaal Cyber Security Centrum (NCSC) informeert en adviseert overheden en (vitaal) bedrijfsleven en onderhoudt contacten met buitenlandse zusterorganisaties. Het merendeel van deze contacten is niet expliciet in dit schema weergegeven.

NB 2: Het Agentschap Telecom oefent het toezicht uit namens de minister EZK; ILT oefent het toezicht uit namens de minister van IenW.

NB 3: De digitale dienstverleners zijn voor de overzichtelijkheid niet opgenomen in dit schema. Hun informatielijnen mbt cybersecurity lopen direct naar EZK en niet naar NCSC.

NB 4: De AP (Autoriteit persoonsgegevens) vervult geen rol in de responsfase

Colofon

Titel:	Bestuurlijke Netwerkkaarten Crisisbeheersing
Datum:	April 2019
Status:	Definitief
Versie:	Achtste druk
Auteurs:	Merijn ten Dam & Ernst Brainich
Projectleider:	Oscar Koebrugge
Omslag:	Rob Kruitwagen
Copyright	IFV en provincie Noord-Holland
Eindverantwoordelijk:	IFV, afd. Onderzoek en kennisdocumenten

Instituut Fysieke Veiligheid
Postbus 7010
6801 HA Arnhem
T 026 355 24 00
www.ifv.nl

Instituut Fysieke Veiligheid

Het Instituut Fysieke Veiligheid (IFV) draagt bij aan een veilige samenleving door het versterken van de veiligheidsregio's en hun partners bij het professionaliseren van hun taken. Wij ontwikkelen en delen relevante kennis, wij hebben expertise voor het verwerven en beheren van gemeenschappelijk materieel en wij adviseren de betrokken besturen.

Ons motto hierbij is: signaleren en verbinden.

IFV Instituut Fysieke Veiligheid

Instituut Fysieke Veiligheid
Postbus 7010
6801 HA Arnhem
026 355 24 00
www.ifv.nl