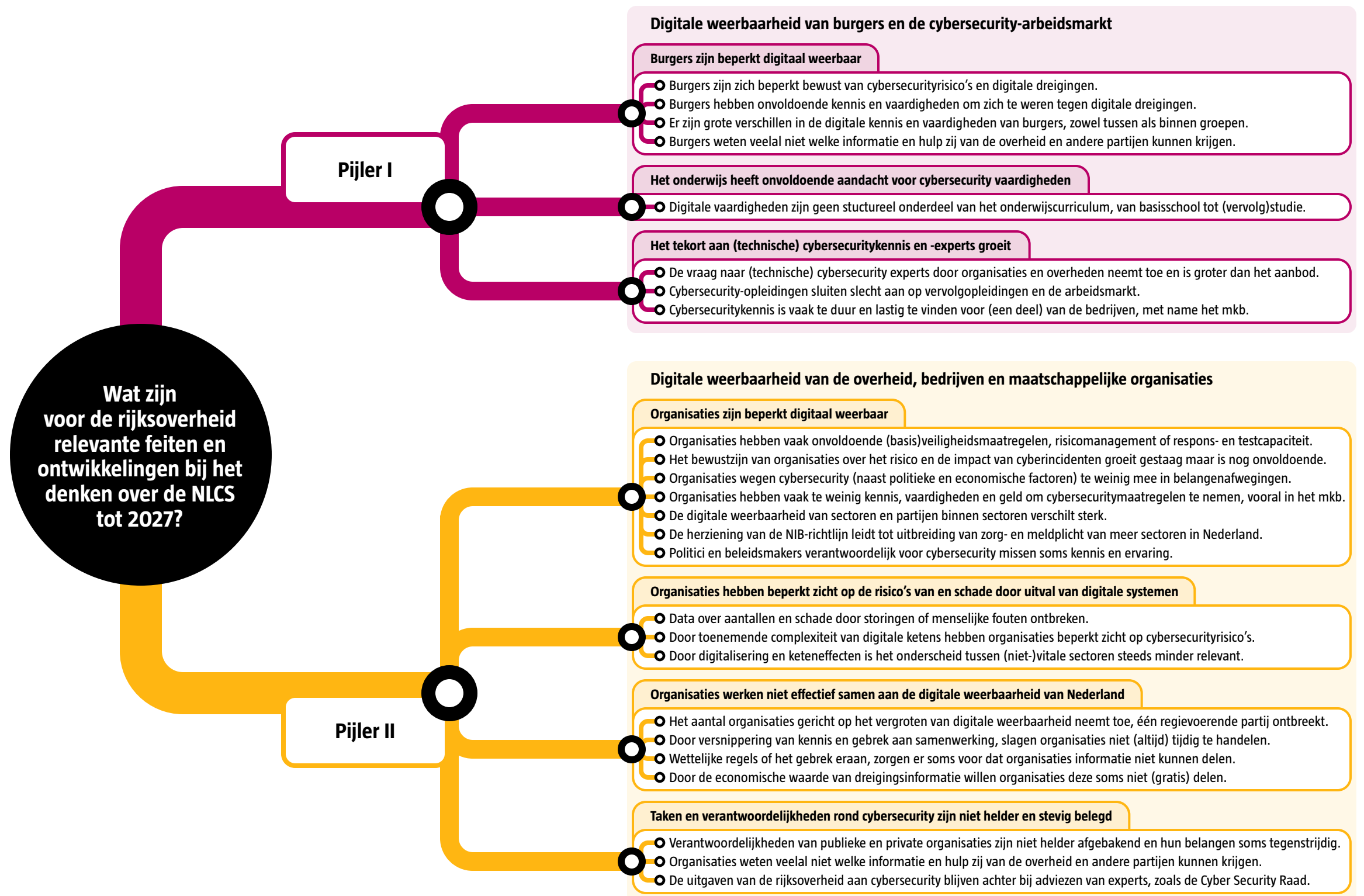
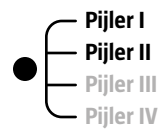


Contextschets

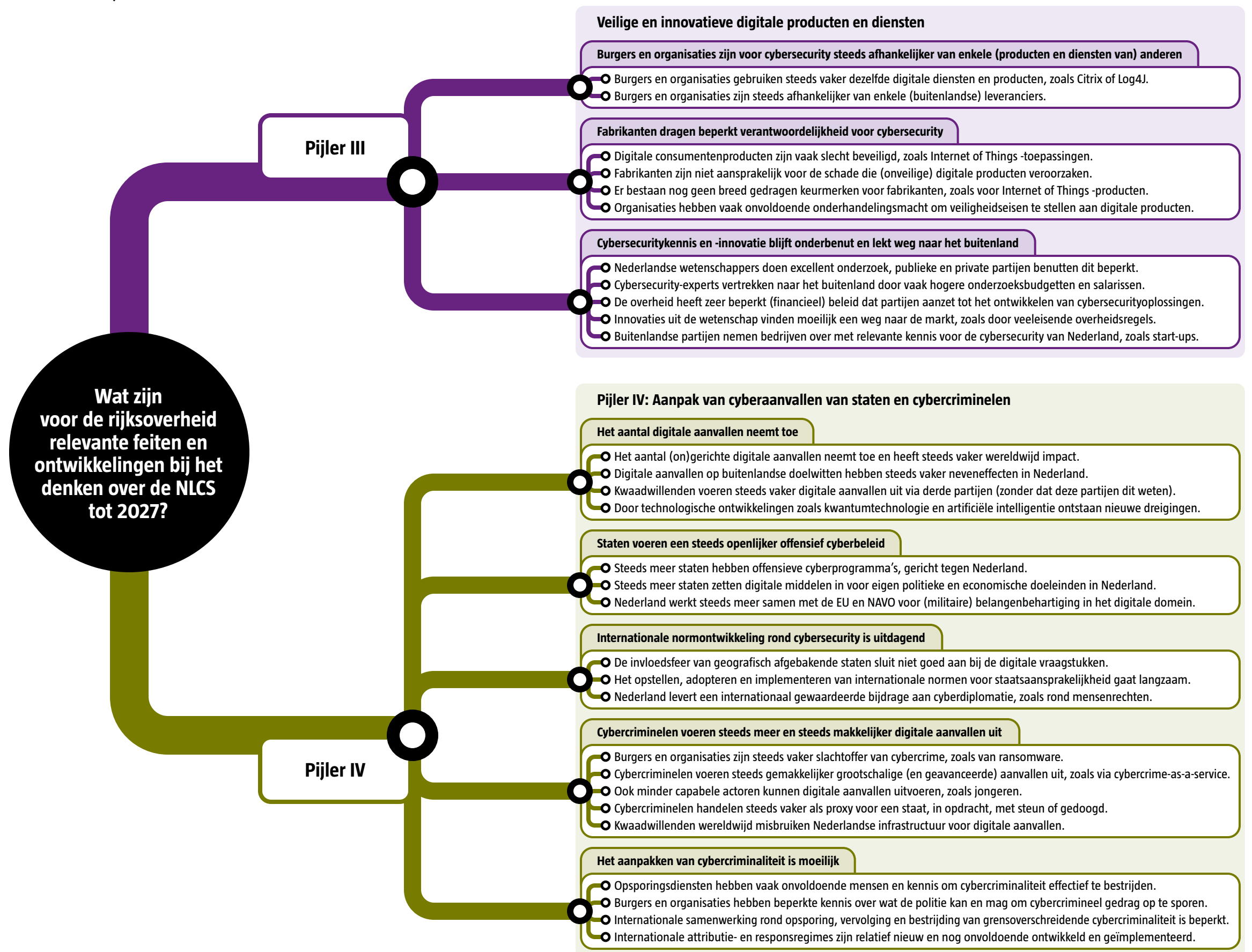
Nederlandse Cybersecurity Strategie 2027



Contextschets

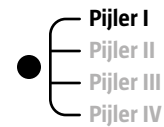
Nederlandse Cybersecurity Strategie 2027

Pijler I
Pijler II
Pijler III
Pijler IV



Nederlandse Cybersecuritystrategie

Doelenkaart Pijler I



Wat zijn voor de Rijksoverheid doelen voor het vergroten van de cybersecurity in Nederland tot aan 2027?

Pijler I

Pijler I: Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hiermee om te gaan

- De overheid heeft een actueel en omvattend beeld van cyberincidenten, -dreigingen, en -risico's.
- De overheid en bedrijven wisselen effectief en efficiënt dreigingsinformatie en handelingsperspectief uit, passend bij de kennis en kunde van de ontvanger.
- Het Landelijk Dekkend Stelsel van cybersecuritysamenwerkingsverbanden is goed gecoördineerd, zoals door heldere aanspreekpunten.
- Overheidsorganisaties, zoals CSIRTs en toezichthouders, delen informatie (inter)nationaal effectief.

Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee

- Organisaties weten wat de cybersecuritybasismaatregelen zijn en passen deze toe.
- Overheidsorganisaties en NIB2-organisaties voldoen aan hoge veiligheidseisen op basis van (nieuwe) wet- en regelgeving.
- Organisaties zijn zich op alle niveaus (ook bestuurlijk) bewust van het belang van cybersecurity.
- Organisaties richten hun risicomanagement ook op cybersecurityrisico's en maken dit vaker inzichtelijk.
- Toezicht op de digitale weerbaarheid van organisaties is afgestemd op risico's voor henzelf, hun sector en hun belang voor anderen.

Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en -crises

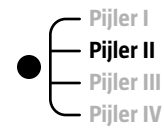
- Organisaties zijn in staat snel te reageren op en te herstellen na een cyberincident en oefenen hiermee.
- De overheid biedt samenhangende cybersecuritydienstverlening met een herkenbaar aanspreekpunt voor organisaties.
- De overheid, bedrijven en wetenschap werken intensief samen om cybersecurity-expertise effectief in te zetten.
- Organisaties werken goed samen in geval van (landelijke) cybersecuritycrises, passend bij (boven)regionale en (inter)nationale crisismechanismen.
- Organisaties evalueren cyberincidenten, leren hiervan en delen deze lessen onderling.

Over deze kaart

Op deze kaart staan de hoofd- en subdoelen van pijler II van de Nederlandse Cybersecurity Strategie (NLCS) van de rijksoverheid. De Argumentenfabriek maakte deze kaart op basis van een aantal denksessies met belanghebbenden van binnen en buiten de rijksoverheid. In de strategie geven de Nationaal Coördinator Terrorismebestrijding en Veiligheid en betrokken departementen verdere context en onderbouwing van deze doelen. Hierin staan ook de afkortingen en definities van de op deze kaart gebruikte begrippen en een toelichting op de totstandkoming van deze Doelenkaart en de bredere strategie.

Nederlandse Cybersecuritystrategie

Doelenkaart Pijler II



Wat zijn voor de Rijksoverheid doelen voor het vergroten van de cybersecurity in Nederland tot aan 2027?

Pijler II

Pijler II: Veilige en innovatieve digitale producten en diensten

Digitale producten en diensten zijn veiliger

- Er is een Europese wettelijke zorgplicht voor cybersecurity voor fabrikanten en leveranciers van digitale producten en diensten, gedurende hun hele levenscyclus.
- Er is een meer samenhangend stelsel van EU-regelgeving voor cybersecurity van digitale producten en diensten.
- Er zijn Europese veiligheids certificaten voor verschillende categorieën digitale producten en diensten.
- Organisaties hebben contractuele afspraken met afnemers over het garanderen van cybersecurity.
- De overheid heeft (inkoop)beleid gericht op veiligheid van digitale producten en diensten en kent de eisen hiervoor.

Nederland heeft een sterke cybersecuritykennis- en innovatieketen

- Nederlandse (en Europese) cybersecuritybedrijven leveren kwalitatief hoogwaardige producten en diensten van belang voor onze digitale veiligheid en economie.
- De overheid, bedrijven en kennisinstellingen werken intensief samen aan kennis en innovatie rond digitale veiligheid.
- Nederland is aangesloten bij Europese initiatieven en fondsen om kennisontwikkeling en innovatie in cybersecurity in Nederland te stimuleren.

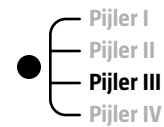
Over deze kaart

Op deze kaart staan de hoofd- en subdoelen van pijler III van de Nederlandse Cybersecurity Strategie (NLCS) van de rijksoverheid. De Argumentenfabriek maakte deze kaart op basis van een aantal denksessies met belanghebbenden van binnen en buiten de rijksoverheid. In de strategie geven de Nationaal Coördinator Terrorismebestrijding en Veiligheid en betrokken departementen verdere context en onderbouwing van deze doelen. Hierin staan ook de afkortingen en definities van de op deze kaart gebruikte begrippen en een toelichting op de totstandkoming van deze Doelenkaart en de bredere strategie.



Nederlandse Cybersecuritystrategie

Doelenkaart Pijler III



Wat zijn voor de Rijksoverheid doelen voor het vergroten van de cybersecurity in Nederland tot aan 2027?

Pijler III

Pijler III: Digitale dreigingen van staten en criminelen

Nederland heeft zicht op digitale dreigingen van staten en criminelen

- De overheid heeft de capaciteiten om informatie en inlichtingen over cybersecuritydreigingen van staten en criminelen te analyseren en te delen.
- De overheid heeft effectieve inlichtingen- en informatie-uitwisseling over digitale dreigingen met internationale partners.

Nederland heeft grip op digitale dreigingen van staten en criminelen

- De overheid heeft een effectief, internationaal afgestemd attributie- en responskader met heldere bevoegdheden en verantwoordelijkheden.
- De overheid beschikt over offensieve en defensieve cybercapaciteiten die effectief zijn in vredes- en oorlogstijd.
- De overheid zet instrumenten tegen cybersecuritydreigingen van staten en criminelen (inter)nationaal goed gecoördineerd in.
- De overheid beschikt over (niet-)strafrechtelijke interventies tegen cybercriminelen en hun dienstverleners, zoals tegen en ransomware.

Staten hoden zich aan het normatief kader voor verantwoord statelijk gedrag in de digitale ruimte

- Staten hebben een gedeeld begrip van het belang van gedragsnormen en het internationaal recht in de digitale ruimte en passen dit toe.
- Nederland maakt deel uit van een brede coalitie die naleving van internationale gedragsnormen en het internationaal recht in de digitale ruimte bevordert.
- Het multistakeholder-model blijft het leidende principe voor het beheer van het internet wereldwijd.

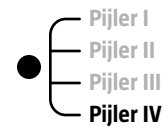
Over deze kaart

Op deze kaart staan de hoofd- en subdoelen van pijler IV van de Nederlandse Cybersecurity Strategie (NLCS) van de rijksoverheid. De Argumentenfabriek maakte deze kaart op basis van een aantal denksessies met belanghebbenden van binnen en buiten de rijksoverheid. In de strategie geven de Nationaal Coördinator Terrorismebestrijding en Veiligheid en betrokken departementen verdere context en onderbouwing van deze doelen. Hierin staan ook de afkortingen en definities van de op deze kaart gebruikte begrippen en een toelichting op de totstandkoming van deze Doelenkaart en de bredere strategie.



Nederlandse Cybersecuritystrategie

Doelenkaart Pijler IV



Wat zijn voor de Rijksoverheid doelen voor het vergroten van de cybersecurity in Nederland tot aan 2027?

Pijler IV

Pijler IV: Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Burgers zijn goed beschermd tegen digitale risico's

- Burgers zijn zich bewust digitale risico's, dreigingen en maatregelen, en weten waar ze hulp kunnen krijgen.
- Burgers passen basale cybersecuritymaatregelen toe bij het gebruik van digitale producten en diensten.
- Burgers kunnen op meerdere plekken laagdrempelig cybersecurity-informatie en -advies inwinnen, passend bij hun kennis en kunde.

Burgers reageren snel en adequaat op cyberincidenten

- Burgers krijgen snel adequate informatie over (acute) cyberincidenten en hoe hierop te reageren.
- Burgers kunnen eenvoudig melding of aangifte doen van cyberincidenten.

Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid

- Digitale vaardigheden gericht op veiligheid zijn onderdeel van het landelijk curriculum in het primair en voortgezet onderwijs.
- Docenten in het primair en voortgezet onderwijs kunnen (met hulp van anderen) goed onderwijs bieden in digitale vaardigheden gericht op veiligheid.

De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts

- Er is zicht op de tekorten op de cybersecurity-arbeidsmarkt en hoe deze het hoofd te bieden.
- Organisaties bieden bij- en omscholingsprogramma's voor cybersecurity-expertise aan.
- Er zijn meer mbo-, hbo- en wo-cybersecurityopleidingsplekken die aansluiten op de arbeidsmarkt, mede door een bijdrage van bedrijven en kennisinstellingen.

Over deze kaart

Op deze kaart staan de hoofd- en subdoelen van pijler I van de Nederlandse Cybersecurity Strategie (NLCS) van de rijksoverheid. De Argumentenfabriek maakte deze kaart op basis van een aantal denksessies met belanghebbenden van binnen en buiten de rijksoverheid. In de strategie geven de Nationaal Coördinator Terrorisbestrijding en Veiligheid en betrokken departementen verdere context en onderbouwing van deze doelen. Hierin staan ook de afkortingen en definities van de op deze kaart gebruikte begrippen en een toelichting op de totstandkoming van deze Doelenkaart en de bredere strategie.