Contextschets
Nederlandse Cybersecurity Strategie 2027

- Pijler I
- Pijler II
- Pijler III
- Pijler IV

Wat zijn voor de rijksoverheid relevante feiten en ontwikkelingen bij het denken over de NLCS tot 2027?

Pijler I

Digitale weerbaarheid van burgers en de cybersecurity-arbeidsmarkt

Burgers zijn beperkt digitaal weerbaar

- Burgers zijn zich beperkt bewust van cybersecurityrisico's en digitale dreigingen.
- Burgers hebben onvoldoende kennis en vaardigheden om zich te weren tegen digitale dreigingen.
- Er zijn grote verschillen in de digitale kennis en vaardigheden van burgers, zowel tussen als binnen groepen.
- Burgers weten veelal niet welke informatie en hulp zij van de overheid en andere partijen kunnen krijgen.

Het onderwijs heeft onvoldoende aandacht voor cybersecurity vaardigheden

- Digitale vaardigheden zijn geen stuctureel onderdeel van het onderwijscurriculum, van basisschool tot (vervolg)studie.

Het tekort aan (technische) cybersecuritykennis en -experts groeit

- De vraag naar (technische) cybersecurity experts door organisaties en overheden neemt toe en is groter dan het aanbod.
- Cybersecurity-opleidingen sluiten slecht aan op vervolgopleidingen en de arbeidsmarkt.
- Cybersecuritykennis is vaak te duur en lastig te vinden voor (een deel) van de bedrijven, met name het mkb.

Pijler II

Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Organisaties zijn beperkt digitaal weerbaar

- Organisaties hebben vaak onvoldoende (basis)veiligheidsmaatregelen, risicomanagement of respons- en testcapaciteit.
- Het bewustzijn van organisaties over het risico en de impact van cyberincidenten groeit gestaag maar is nog onvoldoende.
- Organisaties wegen cybersecurity (naast politieke en economische factoren) te weinig mee in belangenafwegingen.
- Organisaties hebben vaak te weinig kennis, vaardigheden en geld om cybersecuritymaatregelen te nemen, vooral in het mkb.
- De digitale weerbaarheid van sectoren en partijen binnen sectoren verschilt sterk.
- De herziening van de NIB-richtlijn leidt tot uitbreiding van zorg- en meldplicht van meer sectoren in Nederland.
- Politici en beleidsmakers verantwoordelijk voor cybersecurity missen soms kennis en ervaring.

Organisaties hebben beperkt zicht op de risico's van en schade door uitval van digitale systemen

- Data over aantallen en schade door storingen of menselijke fouten ontbreken.
- Door toenemende complexiteit van digitale ketens hebben organisaties beperkt zicht op cybersecurityrisico's.
- Door digitalisering en keteneffecten is het onderscheid tussen (niet-)vitale sectoren steeds minder relevant.

Organisaties werken niet effectief samen aan de digitale weerbaarheid van Nederland

- Het aantal organisaties gericht op het vergroten van digitale weerbaarheid neemt toe, één regievoerende partij ontbreekt.
- Door versnippering van kennis en gebrek aan samenwerking, slagen organisaties niet (altijd) tijdig te handelen.
- Wettelijke regels of het gebrek eraan, zorgen er soms voor dat organisaties informatie niet kunnen delen.
- Door de economische waarde van dreigingsinformatie willen organisaties deze soms niet (gratis) delen.

Taken en verantwoordelijkheden rond cybersecurity zijn niet helder en stevig belegd

- Verantwoordelijkheden van publieke en private organisaties zijn niet helder afgebakend en hun belangen soms tegenstrijdig.
- Organisaties weten veelal niet welke informatie en hulp zij van de overheid en andere partijen kunnen krijgen.
- De uitgaven van de rijksoverheid aan cybersecurity blijven achter bij adviezen van experts, zoals de Cyber Security Raad.

in opdracht van: Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Over deze kaart

gemaakt door: De ArgumentenFabriek De Informatiekaart

Contextschets
Nederlandse Cybersecurity Strategie 2027

Pijler I
Pijler II
Pijler III
Pijler IV

Wat zijn voor de rijksoverheid relevante feiten en ontwikkelingen bij het denken over de NLCS tot 2027?

Pijler III

Veilige en innovatieve digitale producten en diensten

Burgers en organisaties zijn voor cybersecurity steeds afhankelijker van enkele (producten en diensten van) anderen
- Burgers en organisaties gebruiken steeds vaker dezelfde digitale diensten en producten, zoals Citrix of Log4J.
- Burgers en organisaties zijn steeds afhankelijker van enkele (buitenlandse) leveranciers.

Fabrikanten dragen beperkt verantwoordelijkheid voor cybersecurity
- Digitale consumentenproducten zijn vaak slecht beveiligd, zoals Internet of Things -toepassingen.
- Fabrikanten zijn niet aansprakelijk voor de schade die (onveilige) digitale producten veroorzaken.
- Er bestaan nog geen breed gedragen keurmerken voor fabrikanten, zoals voor Internet of Things -producten.
- Organisaties hebben vaak onvoldoende onderhandelingsmacht om veiligheidseisen te stellen aan digitale producten.

Cybersecuritykennis en -innovatie blijft onderbenut en lekt weg naar het buitenland
- Nederlandse wetenschappers doen excellent onderzoek, publieke en private partijen benutten dit beperkt.
- Cybersecurity-experts vertrekken naar het buitenland door vaak hogere onderzoeksbudgetten en salarissen.
- De overheid heeft zeer beperkt (financieel) beleid dat partijen aanzet tot het ontwikkelen van cybersecurityoplossingen.
- Innovaties uit de wetenschap vinden moeilijk een weg naar de markt, zoals door veeleisende overheidsregels.
- Buitenlandse partijen nemen bedrijven over met relevante kennis voor de cybersecurity van Nederland, zoals start-ups.

Pijler IV

Pijler IV: Aanpak van cyberaanvallen van staten en cybercriminelen

Het aantal digitale aanvallen neemt toe
- Het aantal (on)gerichte digitale aanvallen neemt toe en heeft steeds vaker wereldwijd impact.
- Digitale aanvallen op buitenlandse doelwitten hebben steeds vaker neveneffecten in Nederland.
- Kwaadwillenden voeren steeds vaker digitale aanvallen uit via derde partijen (zonder dat deze partijen dit weten).
- Door technologische ontwikkelingen zoals kwantumtechnologie en artificiële intelligentie ontstaan nieuwe dreigingen.

Staten voeren een steeds openlijker offensief cyberbeleid
- Steeds meer staten hebben offensieve cyberprogramma's, gericht tegen Nederland.
- Steeds meer staten zetten digitale middelen in voor eigen politieke en economische doeleinden in Nederland.
- Nederland werkt steeds meer samen met de EU en NAVO voor (militaire) belangenbehartiging in het digitale domein.

Internationale normontwikkeling rond cybersecurity is uitdagend
- De invloedsfeer van geografisch afgebakende staten sluit niet goed aan bij de digitale vraagstukken.
- Het opstellen, adopteren en implementeren van internationale normen voor staatsaansprakelijkheid gaat langzaam.
- Nederland levert een internationaal gewaardeerde bijdrage aan cyberdiplomatie, zoals rond mensenrechten.

Cybercriminelen voeren steeds meer en steeds makkelijker digitale aanvallen uit
- Burgers en organisaties zijn steeds vaker slachtoffer van cybercrime, zoals van ransomware.
- Cybercriminelen voeren steeds gemakkelijker grootschalige (en geavanceerde) aanvallen uit, zoals via cybercrime-as-a-service.
- Ook minder capabele actoren kunnen digitale aanvallen uitvoeren, zoals jongeren.
- Cybercriminelen handelen steeds vaker als proxy voor een staat, in opdracht, met steun of gedoogd.
- Kwaadwillenden wereldwijd misbruiken Nederlandse infrastructuur voor digitale aanvallen.

Het aanpakken van cybercriminaliteit is moeilijk
- Opsporingsdiensten hebben vaak onvoldoende mensen en kennis om cybercriminaliteit effectief te bestrijden.
- Burgers en organisaties hebben beperkte kennis over wat de politie kan en mag om cybercrimineel gedrag op te sporen.
- Internationale samenwerking rond opsporing, vervolging en bestrijding van grensoverschreidende cybercriminaliteit is beperkt.
- Internationale attributie- en responsregimes zijn relatief nieuw en nog onvoldoende ontwikkeld en geïmplementeerd.

in opdracht van: Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Justitie en Veiligheid

Over deze kaart

gemaakt door: De ArgumentenFabriek De Informatiekaart

Nederlandse Cybersecuritystrategie
Doelenkaart Pijler I

Pijler I
Pijler II
Pijler III
Pijler IV

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.

in opdracht van: Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

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.

gemaakt door: De ArgumentenFabriek De Informatiekaart

Nederlandse Cybersecuritystrategie
Doelenkaart Pijler II

Pijler I
Pijler II
Pijler III
Pijler IV

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 veiligheidscertificaten 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.

in opdracht van: Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

gemaakt door: De ArgumentenFabriek De Informatiekaart

Nederlandse Cybersecuritystrategie
Doelenkaart Pijler III

Pijler I
Pijler II
Pijler III
Pijler IV

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 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.

in opdracht van: Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

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.

gemaakt door: De ArgumentenFabriek De Informatiekaart

Nederlandse Cybersecuritystrategie
Doelenkaart Pijler IV

Pijler I
Pijler II
Pijler III
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 rbeidsmarkt 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.

in opdracht van: Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

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 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.

gemaakt door: De ArgumentenFabriek De Informatiekaart