# Nederlandse Cybersecuritystrategie 2022-2028

Ambities en acties voor een digitaal veilige samenleving

*Foto omslag: We zijn meer online dan ooit. In 2021 telde Nederland maar liefst 17,01 miljoen mobiele connecties. 95,7% daarvan is een smartphone en door ruim 90% wordt deze ook gebruikt voor internettoegang. Ruim 15 miljoen mensen hebben een of meerdere accounts op sociale media.*

De Nederlandse Cybersecuritystrategie (NLCS) is tot stand gekomen met een brede betrokkenheid van publieke, private en maatschappelijke organisaties, onder coördinatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het Cybersecurity Beeld Nederland 2022 (CSBN) vormt het uitgangspunt voor de pijlers en doelstellingen van de NLCS.



# Voorwoord

Internet heeft ons leven ingrijpend veranderd. We leven en werken online, in veel opzichten maakt dat ons leven gemakkelijker en de economische voordelen zijn evident. Burgers en bedrijven moeten ten volle kunnen profiteren van de digitale samenleving en economie; veiligheid is hiervoor essentieel.

Maar de veiligheid in de digitale wereld blijft nog ver achter bij die in de fysieke wereld. Wie een auto koopt, weet dat die aan allerlei veiligheids- en kwaliteitseisen voldoet. En de koper weet precies wat van hem of haar verwacht wordt om die auto veilig te kunnen en mogen besturen; een rijbewijs, geen alcohol, jaarlijkse APK-keuringen.

In de digitale wereld is dat heel anders. Bij het ontwerp van veel digitale systemen was en is veiligheid nog níet het uitgangspunt. Decennialang heeft de verantwoordelijkheid voor die veiligheid gelegen bij de eindgebruikers als burgers en kleinere ondernemingen en organisaties. Maar veel van die eindgebruikers zijn in de praktijk helemaal niet in staat om aan die verantwoordelijkheid invulling te geven. Ze weten bijvoorbeeld niet hoe ze een wifi-router moeten updaten en worstelen met de beveiliging van systemen, privacy-vereisten, et cetera.

Intussen groeien de risico's. Als hoogontwikkelde samenleving wordt Nederland in hoog tempo afhankelijker van digitale systemen. Maar zelfs in meer volwassen organisaties, techbedrijven en overheidsinstanties staat of valt de veiligheid van die systemen bij het gedrag van individuen. Alles ligt plat als een werknemer een phishing mail opent of niet de juiste beveiliging installeert.

Het kabinet meent dat de eenzijdige nadruk op de verantwoordelijkheid van het individu een doodlopende weg is en kiest voor een andere route naar een veilig digitaal ecosysteem. Mede namens het kabinet presenteer ik daarom een nieuwe cybersecuritystrategie. Die kent de volgende speerpunten:

1. **Beter zicht op de dreiging.** Het kabinet investeert in mensen en systemen die scherper zicht geven op de herkomst van dreigingen en tegen wie ze gericht zijn.

2. **Meer cybersecurityspecialisten.** We nemen verschillende acties om meer ICT-specialisten op de arbeidsmarkt te krijgen.

3. **Overheid en sectoren nemen verantwoordelijkheid.** De verantwoordelijkheid voor veiligheid wordt deels verplaatst van eindgebruikers naar de overheid en specifieke sectoren. De meest volwassen en bepalende organisaties dragen de zwaarste verantwoordelijkheden. Voor de gehele overheid zelf zullen stevige wettelijke eisen voor veiligheid en toezicht op naleving erop worden ingericht.

4. **Beter toezicht en de noodzakelijke wet- en regelgeving.** Herschikking van verantwoordelijkheden vergt uitbreiding van wettelijke regels en toezicht. Veiligheid moet het fundament worden waarop nieuwe systemen worden ontworpen. Er komen nieuwe regels waar (rijks)overheden, vitale aanbieders, en leveranciers van digitale producten en diensten aan moeten voldoen.

5. **Heldere informatie via een nationale cyberautoriteit.** Er komt een centrale cyberautoriteit in Nederland: het nationale Cyber Security Incident Response Team. Deze nieuwe organisatie zal in samenwerking met publieke en private partners, vitale en niet-vitale organisaties, overheden en burgers voorzien van informatie over (dreigende) cyberincidenten om hen in staat te stellen zich te beveiligen.

Deze strategie beschrijft de ambities van het kabinet voor de komende zes jaar. In de eerste fase investeren we fors in de AIVD en de MIVD, in het NCSC en de versterking van het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden waarmee organisaties van beveiligingsadvies worden voorzien, en in de versterking van digitale weerbaarheid van specifieke sectoren.

Tot slot. Dit is een gezamenlijke verantwoordelijkheid van alle partijen in het cyberveld, waarbij doelgerichte publiek-private samenwerking essentieel is. Ik ben dan ook alle publieke en private partijen en de wetenschap, en in het bijzonder de leden van de Cyber Security Raad, zeer erkentelijk die aan de totstandkoming van deze strategie hebben bijgedragen. Hou dat vast in de uitvoering!

Dilan Yeşilgőz-Zegerius, minister van Justitie en Veiligheid



# Inhoud

*Toenemende digitalisering biedt het onderwijs veel kansen, bijvoorbeeld door het aanbieden van online colleges en voor het ontsluiten van kennis. Tegelijkertijd brengt deze grotere afhankelijkheid van technologie risico's met zich mee. Verschillende universiteiten zijn de laatste jaren doelwit van ransomware geweest.*

# Inleiding en context

Met de Nederlandse cybersecuritystrategie streeft het kabinet naar een digitaal veilig Nederland. Hierdoor zijn we als Nederland in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en tegelijkertijd onze veiligheid en publieke waarden te beschermen. Nederland is een van de meest gedigitaliseerde landen ter wereld. We werken digitaal, we winkelen digitaal en we ontmoeten elkaar steeds vaker digitaal. Digitale systemen vormen inmiddels het 'zenuwstelsel' van onze maatschappij. Dat biedt onze maatschappij veel kansen, maar het brengt ook risico's met zich mee.

De recente geschiedenis laat zien dat cyberincidenten, zoals ransomware-aanvallen, aan de orde van de dag zijn. Dat heeft ertoe geleid dat cybersecurity in belangrijke mate vanuit het perspectief van de dreiging en dus in termen van risico's wordt beleefd: welke hackers moeten worden gestopt? Welke kwetsbaarheden moeten worden gepatcht? Hoe kan informatie over cyberdreigingen sneller en beter worden gedeeld? Hoe kan georganiseerde cybercriminaliteit, zoals ransomware effectief worden aangepakt? Hoe worden (potentiele) slachtoffers tijdig genotificeerd, indien hierover informatie beschikbaar is? Vele en relevante uitdagingen die overwonnen moeten worden en deel uitmaken van deze strategie.

We mogen echter niet vergeten dat het einddoel is om onze publieke waarden te borgen. We willen een open, vrij, stabiel en veilige digitale wereld realiseren waarin burgers en bedrijven op een vergelijkbare veilige manier als in de fysieke wereld kunnen participeren. Cybersecurity is een investering in onze toekomst en moet niet worden beschouwd als een kostenpost. Om dit te kunnen bereiken, is het cruciaal dat we ons ervan bewust zijn dat elk onderdeel van het digitale ecosysteem, of het nu specifieke technologie, een organisatie, een informatiesysteem, een digitaal product of een persoon betreft, deel uitmaakt van een wereldwijd verknoopt netwerk. De cybersecurity van al die losse onderdelen dragen bij aan de digitale weerbaarheid van het totale systeem.

Dit is de grote uitdaging voor de komende jaren. Het digitale ecosysteem is inmiddels zo verknoopt en complex, dat het voor individuele organisaties en personen ingewikkeld zo niet onmogelijk is om het geheel te doorgronden, terwijl juist dit ecosysteem ons moderne leven, en onze economie en samenleving als geheel mogelijk maakt. Criminelen maar ook kwaadwillende staten misbruiken deze complexiteit door zich ongezien op te houden en via digitale kwetsbaarheden onze publieke waarden aan te tasten.

Vanuit deze context constateert het kabinet dat het toegenomen belang en complexiteit van het digitale ecosysteem niet langer in verhouding staan tot de autonome wijze waarop het cyberlandschap zich afgelopen jaren heeft ontwikkeld. Het is daarom nodig het ecosysteem aan te passen aan de veranderende omstandigheden. In het huidige systeem kan één phishing email of een verloren wachtwoord grote impact hebben omdat een deel van de verantwoordelijkheid voor het managen en beheersen van de

risico's voor het totale ecosysteem waaronder vitale sectoren en processen, bij de minst volwassen digitale deelnemers ligt: individuen, kleine bedrijven, en lokale overheden. Vele meer volwassen organisaties, techbedrijven en overheidsinstanties werken aan een veiliger en meer stabiel internet, maar gaan er tegelijkertijd impliciet van uit dat individuen in staat zijn te bepalen welke beveiliging ze moeten installeren en hoe een passwordmanager te gebruiken. Natuurlijk is en blijft eigen cyberhygiëne van eenieder een wezenlijk punt, maar vanuit systemisch oogpunt ontoereikend om onze belangen digitaal weerbaar te houden. Als kabinet hebben we daar een taak, namelijk ervoor zorgen dat het ecosysteem bijdraagt en dienend is aan onze publieke waarden en de randvoorwaarden van cybersecurity daarin dekt.

Veel (digitale) systemen, diensten en processen zijn niet ontworpen met cybersecurity en risicomanagement als fundament (security-by-design en security-by-default) met als gevolg dat de eindgebruikers verantwoordelijk zijn om ons systeem digitaal veilig te houden. In andere sectoren is het ecosysteem in de loop der jaren uitgewerkt in een uitgebalanceerde samenstelling van instrumenten, zoals wettelijke veiligheidseisen, certificeringen, keurmerken en verplichte opleidingen. Op den duur zal ook voor de cyberveiligheid van digitale producten en diensten dergelijke structuren worden opgezet.

Het kabinet zet daarom in op het versterken en transformeren van het digitale ecosysteem waarbij één organisatie of één individu niet langer de zwakste schakel kan zijn. Dat betekent dat een herschikking van de verantwoordelijken van alle spelers in het ecosysteem noodzakelijk is waarbij de juiste rechten en plichten bij de juiste partijen terecht komen. Het herschikken van verantwoordelijkheden in de digitale ruimte vergt de inzet van een uitgebalanceerd samenspel aan instrumenten: van intensievere publiek-private samenwerking tot nieuwe wetgeving, met als doel een ecosysteem te creëren waarbij burgers en (kleine) bedrijven in beginsel veilige producten en diensten kunnen afnemen.

In het kader de Europese digitaal eengemaakte markt, het streven naar een gelijk speelveld en veilige (Internet of Things) producten en diensten zet het kabinet daarbij zo veel mogelijk in op het ontwikkelen van Europese wet- en regelgeving. In Europees verband zijn inmiddels diverse wettelijke maatregelen en initiatieven gerealiseerd om dit te bewerkstelligen.

We zullen uiteindelijk moeten komen tot een situatie waarbij elke partij die deel uitmaakt van het digitale ecosysteem inzicht heeft in zijn bijdrage aan de veiligheid en stabiliteit van het totaal. Dit vergt een systeemtransformatie. Geen enkele partij kan dat alleen, ook de overheid niet. Het is een gezamenlijke inspanning waarbij alle deelnemers aan de transformatie bijdragen. Dat is niet vrijblijvend. Cybersecurity zal immers altijd een gedeelde verantwoordelijkheid blijven tussen degene die de (digitale) infrastructuur bouwen, degenen die deze beheren en degenen die deze gebruiken. Dit vergt samenwerking, maar ook stevige coördinatie, zodat dat de inspanningen in samenhang verlopen en uiteindelijk meer zijn dan de som der delen.

Het kabinet beschrijft in de Nederlandse cybersecuritystrategie de visie op een digitaal veilig Nederland waarin burgers en bedrijven ten volle kunnen profiteren van deelname aan de digitale samenleving, vrij van zorgen over cyberrisico's. Dit is de stip op de horizon. Op sommige thema's zal de realisatie van deze visie meerdere kabinetsperioden in beslag nemen of zelfs een permanent streven blijven. Met de strategische doelen en het actieplan beschrijft het kabinet op welke manier het de komende jaren zal bijdragen aan het realiseren van de visie. Fasering, prioritering en keuzes maken zijn daarbij nodig want het realiseren van een digitaal veilig Nederland zal jaren in beslag nemen. Niet alle ambities zullen op korte of middellange termijn kunnen worden gerealiseerd. Daar waar het realiseren van de ambities extra middelen behoeft, kiest het kabinet er in deze fase voor om structureel te investeren in de AIVD en de MIVD met als doel beter zicht en grip te krijgen op de dreiging. Daarnaast worden er ook middelen beschikbaar gesteld om het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden te versterken, onder andere door de doorontwikkeling van het NCSC richting een nationale CSIRT en door het centraliseren van overheidsschakelorganisaties waar dit kan en dit het publieke belang dient. Tenslotte worden er middelen beschikbaar gesteld voor departementen met grote sectorale uitdagingen zodat zij de digitale weerbaarheid van deze sectoren gericht kunnen versterken. In het algemeen geldt dat er voor het uitvoeren van de acties zoals verwoord in het actieplan voldoende dekking is. Wanneer er echter sprake zal zijn van vervolgstappen of aanvullende (wetgevings)trajecten als gevolg van de acties, zal additionele dekking gevonden moeten worden. In de bijlagen staat een uitgebreidere toelichting op de financiële onderbouwing van deze strategie.

De strategie zal tevens duidelijk maken wat concreet van de overheid kan worden verwacht en waarvoor ze ook aanspreekbaar is.

## Samenwerking in het cybersecuritydomein

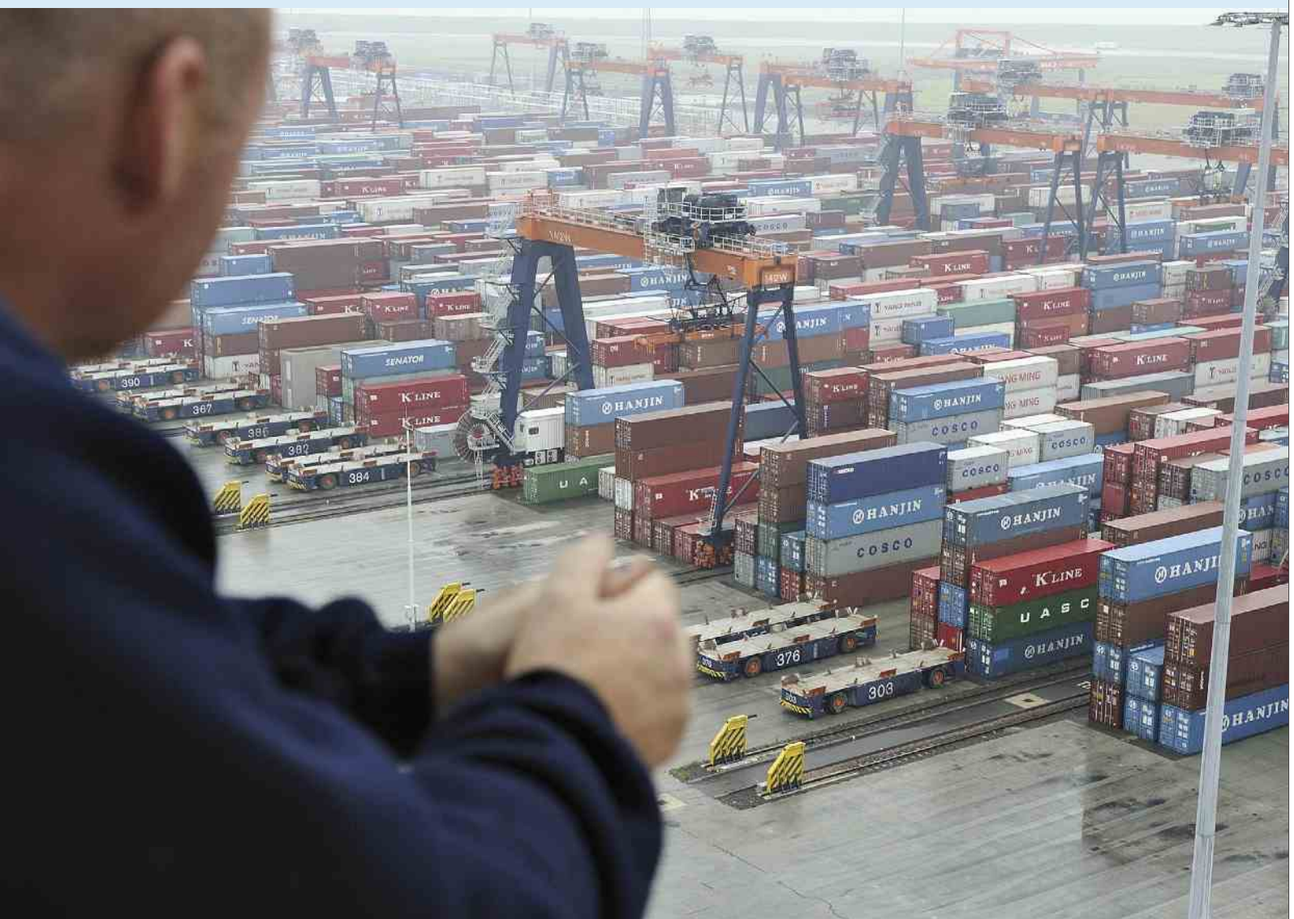
De strategie is tot stand gekomen met een brede betrokkenheid van vele publieke, private en maatschappelijke organisaties en bouwt voort op eerdere kabinetsbrede cybersecuritystrategieën uit 2011, 2013 en 2018. Voor de totstandkoming en implementatie van de strategie werken alle ministeries samen, ook met publieke en private partners. De minister van Justitie en Veiligheid is coördinerend bewindspersoon voor cybersecurity, en verantwoordelijk voor de aanpak van cybercrime, en voert regie op de uitvoering van deze strategie en de monitoring daarvan. Echter, voor het behalen van de cybersecuritydoelen houdt iedere partij zijn eigen taken en verantwoordelijkheden Tot slot is er een nauwe samenhang met de inzet van het kabinet op digitalisering, onder regie van de staatssecretaris voor Koninkrijksrelaties en Digitalisering, zoals uiteengezet in de hoofdlijnenbrief digitalisering van 8 maart 2022.[1]

**Cybersecurity:** het geheel aan maatregelen om relevante digitale risico's tot een aanvaardbaar niveau te reduceren. Dit omvat ook het omgaan met risico's op schade of uitval van digitale systemen en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en - wanneer cyberincidenten zich hebben voorgedaan - deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risico-afweging.[2]

**Digitale weerbaarheid:** het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging. Die kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen.[3]

**Cybercriminaliteitsbestrijding:** bestrijding van criminaliteit waarbij een computersysteem wordt aangevallen of misbruikt voor criminele activiteiten. Cybercrimebestrijding is een integraal onderdeel van de cybersecurity aanpak.

*De Rotterdamse haven heeft een van de meest geavanceerde ICT-systemen van Nederland. Het bevat een specifieke infrastructuur om terminals, depots en distributiecentra met elkaar te verbinden. Zo is op elk moment duidelijk waar een container zich bevindt. Dat zorgt ook voor een grote afhankelijkheid. In 2019 werd dat duidelijk toen een hack van de systemen van Maersk het containervervoer volledig lamlegde.*




# 1. Maatschappelijke opgave cybersecurity

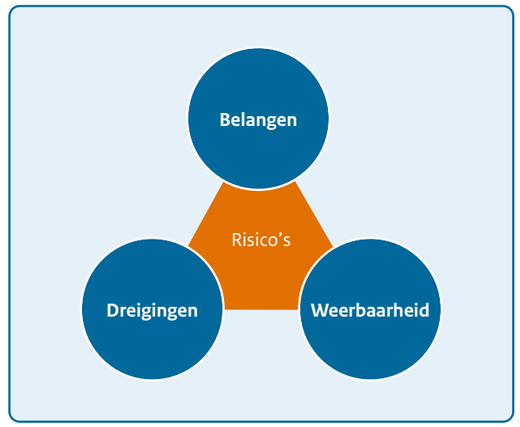
Dit hoofdstuk geeft een overzicht van de huidige en toekomstige uitdagingen op het gebied van cybersecurity, die het uitgangspunt zijn voor de pijlers en doelstellingen van de Nederlandse cybersecuritystrategie. Om te komen tot een breed gedragen strategie zijn in verschillende stappen partijen betrokken die binnen en buiten de overheid een belangrijke rol spelen op het gebied van cybersecurity.

## Digitale risico's onverminderd groot

Binnen het brede domein van digitalisering staat het realiseren van een veilige, inclusieve en kansrijke digitale samenleving voor alle Nederlanders centraal. Door technologische ontwikkelingen en vergaande digitalisering van de maatschappij neemt het belang van digitale processen toe. Om een succesvolle digitalisering te realiseren is cybersecurity een essentiële randvoorwaarde.[4] Digitale processen vormen het 'zenuwstelsel' van de maatschappij en economie, omdat ze onmisbaar zijn voor het ongestoord functioneren daarvan. Digitale veiligheid is dan ook onlosmakelijk verbonden met de nationale veiligheidsbelangen. De zes nationale veiligheidsbelangen zijn: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en internationale rechtsorde.[5]

Het raken van vitale processen, zoals de elektriciteits- of drinkwatervoorziening, de scheepvaartafwikkeling of het betalingsverkeer, kan de samenleving kort of langdurig tot stilstand brengen.

Figuur 1: Digitale risico's worden bepaald door de samenhang tussen belangen, de dreiging daartegen en de weerbaarheid.




De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien. De dreiging kan onder andere voortkomen uit cyberaanvallen of uitval van digitale processen. Uitval kan het gevolg zijn van natuurlijke of technische oorzaken, of van menselijke fouten. Statelijke actoren en cybercriminelen vormen de voornaamste dreiging in relatie tot moedwillig handelen, waarbij ze niet altijd goed van elkaar te onderscheiden zijn vanwege onderlinge relaties. Statelijke actoren kunnen cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen op gewenste doelwitten uit te voeren.[6]

Cyberaanvallen door statelijke actoren zijn niet meer zeldzaam.

Statelijke actoren kunnen hiervoor onder meer de volgende digitale middelen inzetten: beïnvloeding en inmenging (inclusief het verspreiden van desinformatie); spionage, waaronder economische of politieke spionage; voorbereidingshandelingen voor en daadwerkelijke verstoring en sabotage. Volgens de AIVD blijft de dreiging van offensieve cyberprogramma's tegen Nederland en de Nederlandse belangen onverminderd hoog en zal deze in de toekomst alleen maar toenemen.[7] Ook cybercriminelen zijn onverminderd in staat om omvangrijke schade toe te brengen aan digitale processen. Zij handelen vanuit financieel motief en hebben niet de intentie om de maatschappij te ontwrichten. Desondanks kunnen hun aanvallen zoveel impact veroorzaken dat ze nationale veiligheidsbelangen raken. De dreiging die uitgaat van hacktivisten is relatief klein, maar kan Nederlandse belangen wel indirect raken.

De afgelopen jaren is geconstateerd dat de digitale weerbaarheid van Nederland onvoldoende is.[8] Ondanks de inspanningen om de weerbaarheid te verhogen, is sprake van een scheefgroei tussen de toenemende dreiging en de ontwikkeling van de weerbaarheid. Volledige weerbaarheid tegen digitale dreigingen is onmogelijk, maar verhoging van de weerbaarheid tegen uitval en misbruik is wel het belangrijkste instrument om digitale risico's te beheersen. De digitale weerbaarheid is nog niet overal op orde doordat basismaatregelen niet voldoende doorgevoerd worden. Er zijn grote verschillen in weerbaarheid tussen en binnen sectoren en ketens.

## Complicaties risicobeheersing gevaar voor samenleving

In het CSBN2022 zijn in samenwerking met partners strategische thema's geïdentificeerd die nu en de komende jaren relevant zijn voor de digitale veiligheid van Nederland:

***Risico's vormen de keerzijde van een gedigitaliseerde samenleving.*** De Nederlandse samenleving is in hoge mate gedigitaliseerd. Dat heeft een keerzijde: de afhankelijkheid van digitale processen heeft ons ook kwetsbaar gemaakt voor uitval en voor de activiteiten van kwaadwillenden. Keteneffecten kunnen sectoren of zelfs de gehele maatschappij raken. Daarbij kan de verstoring van digitale processen fysieke consequenties hebben.

***Digitale ruimte is speelveld voor regionale en mondiale dominantie.*** Digitale veiligheid is nauw verbonden met geopolitiek. Staten gebruiken de digitale ruimte structureel én intensief voor de behartiging van hun geopolitieke belangen. Cyberaanvallen, bijvoorbeeld voor het vergaren van politieke en economische inlichtingen, zijn daartoe een belangrijk instrument: ze zijn relatief goedkoop en schaalbaar en ze hebben een hoge, vaak langdurige opbrengst. Ook het ultieme geopolitieke conflict, oorlog, gaat gepaard met cyberaanvallen. Daarnaast is attributie een lastige kwestie. Individuele burgers, organisaties, sectoren en landen kunnen weinig invloed uitoefenen op die geopolitieke wedijver, terwijl die wel bijdraagt aan de verhoging van risico's.

***Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet.*** Zware, georganiseerde cybercriminaliteit is zeer schaalbaar geworden en heeft daardoor in de afgelopen jaren qua slachtoffers, schade en criminele opbrengsten een industriële omvang aangenomen. Ransomware is daarbij een gamechanger gebleken. Zware cybercriminelen en hun dienstverleners zijn primair financieel gemotiveerd en gaan voor maximale opbrengsten, waarbij ze dankbaar gebruik maken van de mogelijkheden die de digitale ruimte biedt. Gezien de aard en groeiende omvang van de cybercriminele dreiging is het schaalbaar maken én houden van de weerbaarheidsketen een fundamentele uitdaging voor de komende jaren.

***Marktdynamiek compliceert beheersing digitale risico's.*** Op digitale markten komen vraag en aanbod naar digitale diensten, (componenten van) hardware, software en netwerken samen. Deze markten hebben enkele unieke kenmerken. Bijvoorbeeld de (semi)monopolistische status van bepaalde leveranciers, de hoge mate van onderlinge verweving en de focus op het vergaren van zoveel mogelijk data. Ook zijn in deze markten prikkels voor digitale veiligheid niet (altijd) doorslaggevend. Die kenmerken compliceren de beheersing van risico's voor individuele burgers, organisaties, sectoren en landen.

***Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen.*** Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal staat nog in de kinderschoenen. Digitale risico's hebben nog geen structurele plaats in het bredere risicomanagement binnen en tussen de drie eerdergenoemde niveaus. Risicomanagement is nog niet vanzelfsprekend, terwijl een risicogebaseerde manier van werken instrumenteel is voor het bepalen en op het gewenste niveau brengen van de weerbaarheid. Uiteraard hebben talrijke organisaties hun risicomanagement op orde. Toch schort het binnen organisaties vaak aan inbedding in het primaire proces.[9]

Aanvullend is een overkoepelend thema geïdentificeerd dat de andere thema's raakt: ***beperkingen in digitale autonomie beperken ook digitale weerbaarheid.***[10] Voor Europese landen en Nederland gelden beperkingen in digitale autonomie. Die autonomie omvat het vermogen en de middelen die Nederland heeft om zelfstandig beslissingen te kunnen nemen over (verdere) digitalisering én de gewenste mate van digitale weerbaarheid. De autonomie staat onder druk door diverse oorzaken, die samenhangen met de hierboven genoemde strategische thema's. Die oorzaken verminderen de beïnvloedings- en keuzemogelijkheden voor en controle over de digitale weerbaarheid van Nederland. Hoewel uiteenlopend van aard, illustreren de thema's ieder op zich en in samenhang complicaties voor strategische risicobeheersing.

## Noodzaak tot een integrale aanpak digitale weerbaarheid

In de afgelopen jaren hebben verschillende gezaghebbende organisaties adviezen aan de overheid en het kabinet verstrekt op het gebied van cybersecurity en het verhogen van de digitale weerbaarheid. Deze zijn, in aanvulling op de hiervoor genoemde strategische thema's, meegenomen in de totstandkoming van deze strategie. Aanvullend hieraan is een brede groep belanghebbenden middels een enquête en in werksessies[11] gevraagd om (aanvullende) uitdagingen te identificeren.[12] Dit heeft geleid tot de volgende belangrijke additionele inzichten die meegenomen zijn in deze strategie:

- Er is sprake van een groeiende cyberweerbaarheidskloof tussen organisaties. Er zijn organisaties die hun cybersecurity goed op orde hebben, maar er zijn ook organisaties die hun cybersecurity nog niet voldoende op orde hebben;
- naar verwachting blijft de vraag naar cybersecurity-expertise toenemen waarbij het aanbod van gekwalificeerd personeel achterblijft;
- er is geconstateerd dat verantwoordelijkheden in het Nederlandse cybersecuritystelsel op dit moment niet eenduidig zijn belegd of duidelijk zijn gedefinieerd, wat effectieve samenwerking belemmert;
- de afgelopen jaren is ervaren gebleken dat informatie-uitwisseling gefragmenteerd is, waardoor dreigingsinformatie niet altijd alle organisaties tijdig heeft bereikt en in staat heeft gesteld om maatregelen te treffen;
- organisaties hebben beperkt zicht op de risico's van en schade door uitval van digitale systemen en data over de omvang van schade door storingen of

menselijke fouten ontbreekt;
- de gewoonte om van incidenten te leren in de digitale ruimte is in ontwikkeling;
- wetenschappelijke cybersecurity kennis en innovatie vinden nog te weinig hun weg naar de markt;
- internationale normontwikkeling rond cybersecurity is uitdagend en het opstellen, adopteren en implementeren van internationale normen voor staatsaansprakelijkheid gaat langzaam;
- het bewustzijn van burgers en kleine organisaties van de noodzaak om zich te weren tegen digitale dreigingen is nog te beperkt.

Om deze uitdagingen het hoofd te bieden is een integrale aanpak op het gebied van cybersecurity noodzakelijk.

### Terugblik versterking digitale weerbaarheid onder NCSA

- In 2018 is de Wet beveiliging netwerk- en informatiesystemen (Wbni) in werking getreden. Hiermee is onder meer geregeld dat aanbieders van essentiële diensten en digitale dienstverleners een plicht hebben om passende en evenredige technische en organisatorische maatregelen op het gebied van cybersecurity te nemen.
- Eveneens is in 2018 het Digital Trust Center opgericht zodat ook niet-vitale bedrijven een aanspreekpunt hebben op het gebied van cybersecurity. Het Digital Trust Center geeft informatie en advies en stimuleert de oprichting van cybersecurity samenwerkingsverbanden.
- Met het wetsvoorstel 'bevorderen digitale weerbaarheid bedrijven' en de oprichting van de informatiedienst is het Digital Trust Center gestart met het ontvangen en delen van informatie over digitale dreigingen en risico's met bedrijven.
- Met de Strategische I-agenda Rijksdienst 2019-2021, is ingezet op versterking van de rijksbrede informatiebeveiligingskolom.
- Door het opbouwen en versterken van een Landelijk Dekkend Stelsel (LDS) van cybersecurity-samenwerkingsverbanden kan informatie steeds breder, efficiënter en effectiever worden gedeeld tussen schakelorganisaties ten behoeve van de informatievoorziening richting hun doelgroepen.
- In 2020 is de Cyber Intel/Info Cel (CIIC) ingesteld, waarbinnen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), het Nationaal Cyber Security Centrum (NCSC), het Openbaar Ministerie (OM) en de Nationale Politie dreigingsinformatie bijeenbrengen en medewerkers van deze organisaties deze informatie gezamenlijk beoordelen. Zo kan sneller een beeld worden gevormd van nieuwe dreigingen en kunnen organisaties sneller van handelingsperspectief worden voorzien.
- Daarnaast is het Nationaal Detectie Netwerk de afgelopen jaren uitgebreid, waardoor stappen zijn gezet in detectie en monitoring van dreigingen binnen de Rijksoverheid en vitale infrastructuur.
- In 2021 is het nieuwe dcypher formeel gelanceerd. Dcypher is de plek waar publieke, private en kennispartijen, middelen en expertise bij elkaar komen om effectief in te zetten op cybersecurity onderwijs, onderzoek, innovatie en concrete toepassingen.

*Het einde van de OV-chipkaart is nabij. Binnenkort is inchecken met een betaalplas of smartphone mogelijk in het openbaar vervoer. Dit moet zorgen voor meer reis- en betalingsgemak. Een dergelijke verandering is een behoorlijke operatie. Ruim 60.000 poortjes en kaartlezers moeten worden omgebouwd.*




# 2. Visie: Digitale veiligheid voor iedereen een vanzelfsprekendheid

De visie die onderliggend is aan de strategie beschrijft hoe een digitaal veilig Nederland er in de toekomst uit zou moeten zien. Dit is de stip op de horizon.

## Visie

De samenleving is in de toekomst volledig gedigitaliseerd: onze manier van leven is grotendeels verknoopt met de digitale ruimte. De risico's van misbruik, zoals door statelijke of criminele actoren, of uitval van processen, vormen de keerzijde van deze gedigitaliseerde samenleving. Digitale weerbaarheid, inclusief de bestrijding van cybercrime, is een essentiële randvoorwaarde voor het functioneren van de samenleving en de economie. Het is niet alleen een kostenpost maar een rendabele investering: digitale weerbaarheid biedt concurrentievoordelen en versterkt onder meer het vestigingsklimaat, innovatie en de werkgelegenheid.

Met de voorliggende strategie werkt het kabinet aan een toekomst waarin de schreefgroei tussen digitale dreiging en digitale weerbaarheid zo klein mogelijk is en blijft. In de toekomstvisie is digitale beveiliging op een niveau dat past bij de dreiging en bij het belang van de continuïteit, integriteit en betrouwbaarheid van digitale systemen en processen. Daarnaast worden cyberdreigingen gesignaleerd en aangepakt. Tenslotte is de samenleving veerkrachtig: er is voldoende redundantie en herstelvermogen om de gevolgen van cyberdreigingen, zoals uitval, op te vangen.

### Onderliggende strategische keuzes

1. **Ten aanzien van het Landelijk Dekkend Stelsel:**
   a. Er komt één nationale CSIRT waar het NCSC, DTC en CSIRT-DSP samen in gaan. Dit is de centrale cyberautoriteit van Nederland.[13]
   b. De overheid pakt de regie. Dat betekent centraal waar kan, decentraal/sectoraal waar dat moet.
   c. Meer regie op ontwikkeling van het Landelijk Dekkend Stelsel (LDS) op basis van toegevoegde waarde en beoogde effect.
   d. De overheid werkt samen en treedt daadkrachtig op. Actuele kennis en informatie over cyberdreigingen, -incidenten, -trends, en –kwetsbaarheden moeten zo snel mogelijk beschikbaar zijn voor partners in het LDS zodat zij tot handeling kunnen overgaan. De overheid heeft hierbij het voortouw.
   e. Informatiedeling met handelingsperspectief als uitgangspunt. Differentiatie in advies, informatie, en informatiedeling afgestemd op volwassenheidsniveau en in begrijpelijke taal.
   f. Groot helpt klein: LDS-partners dragen de verantwoordelijkheid informatie te brengen en halen informatie op, en dragen op deze manier bij aan het versterken van de weerbaarheid binnen hun respectievelijke ketens en sectoren.
   g. Binnen het LDS zijn er heldere aanspreekpunten en wordt voor leemtes op basis van bovenstaande punten met private partijen naar een oplossing gezocht.

2. **Iedereen in Nederland moet gewaarschuwd kunnen worden die (mogelijk) slachtoffer of doelwit is van een cyberaanval.**

3. **Ten aanzien van wet- en regelgeving:**
   a. Europese wet- en regelgeving waar kan, aanvullende nationale wet- en regelgeving waar dat moet.
   b. Nieuwe wetgeving vormt het kader waarbinnen het stelsel effectief en in samenhang kan opereren.
   c. Marktfalen op het gebied van veiligheid via regelgeving reguleren.
   d. Cybersecuritymaatregelen en -eisen zijn proportioneel, en worden gedifferentieerd naar het belang dat organisaties vertegenwoordigen en hun mate van volwassenheid. Het MKB wordt zoveel mogelijk ontzorgd.
   e. Voor de gehele overheid zelf zullen stevige wettelijke eisen voor veiligheid en toezicht op naleving erop worden ingericht.

4. **Ten aanzien van samenwerking:**
   a. Publiek-privaat waar kan, publiek waar dat moet.
   b. Vrijblijvendheid voorbij. Samenwerking is vrijwillig, maar niet vrijblijvend.
   c. Groot helpt klein - de sterkste/meest volwassen organisaties helpen de minder sterke/volwassen organisaties (publiek-publiek, publiek-privaat & privaat-privaat).

5. **Ten aanzien van kennis en innovatie:**
   a. Het kabinet stimuleert via het samenwerkingsplatform dcypher, via thematische routekaarten en communities, gesprekken tussen kennisinstellingen en bedrijfsleven met betrekking tot de high-end kennisontwikkeling die nodig is om innovatieve kennis en productontwikkeling tot stand te brengen. Dcypher kan een faciliterende en aanjagende rol spelen in het zoeken naar financiering voor de genoemde high-end kennis- en productontwikkeling.

6. **Ten aanzien van tegengaan digitale dreigingen van statelijke actoren en criminelen:**
   a. De onderliggende strategische keuze ten aanzien van cybercrimebestrijding bestaat uit twee onderdelen: inzet op opsporen, vervolgen, en verstoren van cybercriminelen, en inzet op preventie van cybercrime[14]

7. **Digitale risico's voor burgers** worden zoveel mogelijk verkleind door verantwoordelijkheden voor de veiligheid van digitale producten en diensten grotendeels bij burgers en MKB weg te nemen en neer te leggen bij de overheid, producenten en dienstverleners. Op die manier worden burgers en MKB ontzorgd.

8. **De overheid stuurt** op de verdeling van schaarse van cybersecurity- en ICT-expertise bij (grootschalige) crises aan de hand van objectieve criteria, als onderdeel van het landelijk crisisplan digitaal.



## De publieke waarden centraal

In de digitale ruimte dienen publieke waarden en grondrechten te allen tijde gewaarborgd te worden. Hierbij hoort verantwoord datagebruik en digitaal gedrag door overheidsinstanties. Bij het inzetten van bevoegdheden omwille van de (nationale) digitale veiligheid dient altijd een zorgvuldige afweging gemaakt te worden tussen collectieve veiligheid, en individuele grondrechten en publieke waarden. Wettelijke vereisten als proportionaliteit en subsidiariteit zijn hierin leidend om publieke waarden als privacy, veiligheid en non-discriminatie te garanderen.

## De rol en verantwoordelijkheid van de Rijksoverheid

De burger moet zich net zo veilig kunnen begeven in de digitale ruimte als in de fysieke ruimte. Digitale risico's voor burgers worden zoveel mogelijk verkleind door verantwoordelijkheden voor de veiligheid van digitale producten en diensten grotendeels bij burgers weg te nemen en te beleggen bij leveranciers en producten.

Daarnaast moeten burgers kunnen rekenen op betrouwbare dienstverlening van bedrijven en overheden in de digitale ruimte. De Rijksoverheid is verantwoordelijk voor het creëren van een systeem waarbinnen organisaties de juiste maatregelen kunnen nemen om hun digitale weerbaarheid te vergroten en daarmee hun continuïteit en betrouwbaarheid te borgen. Dit doet de Rijksoverheid door het verhogen van de bewustwording, voorlichting en het geven van eenduidige en consistente adviezen over risicobeheersing, het nemen van weerbaarheidsmaatregelen, het voorbereiden op incidenten en waar nodig het verlenen van bijstand. De mate van bijstand vanuit de overheid wordt bepaald door het risico dat organisaties lopen, het volwassenheidsniveau en de impact van bijstand. Deze afweging is inzichtelijk en transparant.

Daarnaast stimuleert en faciliteert de Rijksoverheid dat bedrijven en andere organisaties dit ook doen voor hun eigen doelgroepen, waaronder consumenten. Samenwerkingsverbanden, organisaties en overheden wisselen binnen het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden informatie uit om ieder voor zijn eigen doelgroep dienstverlening op maat te kunnen leveren. Om versnippering en tijdverlies te voorkomen is er één nationale CSIRT, hierdoor stroomt daar waar mogelijk informatie direct naar de organisaties die kwetsbaar zijn of bedreigd worden. Operationele expertise wordt binnen de Rijksoverheid samengebracht en zoveel mogelijk gezamenlijk ingezet. In de toekomst werken cybersecurity experts van de overheid, bedrijfsleven en ICT- en cybersecuritydienstverleners samen, ook deels op één fysieke locatie, om informatie, kennis en expertise te bundelen om digitale weerbaarheid en gezamenlijk

handelingsperspectief en respons op (dreigende) cyberincidenten te borgen.

De Rijksoverheid zorgt tenslotte voor het kader waarbinnen het stelsel effectief en in samenhang kan functioneren. De overheid zal daartoe een uitgebalanceerd samenspel van instrumenten inzetten, bijvoorbeeld wet- en regelgeving (nationaal en in EU verband), financiële ondersteuning of financiële prikkels (belastingkorting, subsidie), opleiding en training (skills), de overheid als launching customer voor secure-by-design innovaties en meer.

## Digitaal weerbare bedrijven, overheden en organisaties

In de visie van het kabinet worden bedrijven, overheden en maatschappelijke organisaties in staat gesteld om in principe zelfstandig, in samenspel met elkaar en met behulp van ICT- of cybersecuritydienstverleners te bepalen welke risico's zij lopen in de digitale ruimte en welke maatregelen er nodig zijn om deze risico's voldoende te beheersen. Digitale risicobeheersing is gemeengoed geworden en wordt van alle organisaties verwacht: door hun klanten en afnemers maar bijvoorbeeld ook door verzekeraars of aandeelhouders.

Vanwege het belang van de vitale infrastructuur voor het functioneren van onze maatschappij kennen deze organisaties een hoog niveau van weerbaarheid. De overheid stelt mede gelet op Europese wet- en regelgeving extra eisen aan organisaties. Dat betekent dat er soms maatregelen verplicht gesteld worden die risico's voor de nationale veiligheid beperken, ook als zij niet direct bijdragen aan het commerciële belang van een organisatie of bedrijf.

## Digitaal veilige en innovatieve economie

Afnemers en consumenten kunnen er gedurende de vastgestelde levenscyclus van alle digitale producten en diensten op vertrouwen dat deze adequaat beveiligd zijn en blijven. Organisaties maken afspraken met leveranciers over weerbaarheidsmaatregelen. Fabrikanten en leveranciers hebben een zorgplicht op het gebied van digitale veiligheidsmaatregelen, onder andere voortvloeiend uit Europese wet- en regelgeving, gedurende de hele levenscyclus van producten en diensten. Afnemers of klanten hebben daarnaast de mogelijkheid om inzicht te krijgen in de cyberweerbaarheid van bedrijven waar zij producten of diensten afnemen, bijvoorbeeld door certificering of rapportages.

Bij de ontwikkeling en toepassing van nieuwe technologieën is *security by design* en *security by default* altijd het uitgangspunt. Tevens worden bij de inkoop en aanbesteding van digitale producten en diensten structureel de risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren beoordeeld.

Nederland heeft voldoende expertise op het gebied van digitale veiligheid, zowel aan de weerbaarheidszijde als op het gebied van cybercrimebestrijding. Enerzijds door een groeiend aanbod van experts op de arbeidsmarkt en anderzijds door het gericht stimuleren van innovatie.

## Tegengaan van cyberdreigingen

De overheid heeft samen met het bedrijfsleven zicht op de digitale dreiging vanuit binnen- en buitenland, en heeft haar detectie op orde. Nederland is bovenal in staat digitale aanvallen van statelijke en niet-statelijke actoren te beperken, door de inzet van brede attributie- en responsmechanismes, bij voorkeur in samenwerking en coalities met EU- en NAVO-partners en andere gelijkgezinde landen. De overheid intervenieert op onderkende aanvallen om de schade voor Nederland zo beperkt mogelijk te houden, aantasting te repareren en kwetsbaarheden te herstellen.

Cybercriminaliteit zal minder lonen. Politie en OM bestrijden cybercriminele netwerken en hun criminele dienstverleners met een brede, schaalbare en innovatieve aanpak die leidt tot een grote pakkans en het effectief verstoren van criminele activiteiten, het voorkomen van strafbaar gedrag en het wegnemen van criminele winsten. Naast opsporing en strafrechtelijke vervolging beschikt Nederland ook over interventiemogelijkheden om cybercriminelen en criminele dienstverleners te bestrijden, zoals mogelijkheden tot verstoren, slachtoffernotificatie en/of schadebeperking. Hierbij worden slachtoffers en/of doelwitten waar mogelijk tijdig genotificeerd.
De overheid bestrijdt deze dreiging niet alleen, maar doet dat in een netwerk van publieke en private (cybersecurity)organisaties waar informatie verzameld, geanalyseerd en met afnemers gedeeld wordt. Ook het leveren van hulp en bijstand aan organisaties gebeurt gezamenlijk.
Cybersecuritydienstverleners zijn beschikbaar om hun diensten te verlenen en werken samen met de overheid aan de digitale weerbaarheid van organisaties binnen en buiten Nederland.

## Internationale samenwerking

Cyberincidenten stoppen niet bij landgrenzen. Daarom benut de overheid actief de kansen die samenwerking binnen en buiten de Europese Unie biedt. Nederland heeft het voortouw in de samenwerking tussen EU-lidstaten en draagt op deze manier bij aan een digitaal veilige en, waar nodig, een autonome Unie. Hiermee worden digitale risico's van grensoverschrijdende aard aangepakt en wordt een gecoördineerde reactie gegeven op grootschalige cyberincidenten en -crises binnen en buiten de EU. Er wordt met cyberdiplomatieke middelen – waaronder capaciteitsopbouw – continu gewerkt aan versterking en verbreding van de landencoalitie die verantwoordelijk statelijk gedrag in de digitale ruimte aanjaagt.

# 3. Doelen

Om de visie te realiseren zijn doelen geformuleerd langs vier pijlers. Deze doelen bieden een antwoord op de huidige en toekomstige uitdagingen zoals in hoofdstuk twee weergegeven.

## Pijler I

### Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Deze pijler ziet toe op de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties. Hierbij gaat het om het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

Doelen

- Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan.
- Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee.
- Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises.

## Pijler II

### Veilige en innovatieve digitale producten en diensten

Deze pijler focust op de aanbieders en afnemers van digitale producten en diensten en de versterking van cybersecurity kennisontwikkeling en innovatie. Het toewerken naar een veilige en innovatieve digitale economie draagt bij aan de digitale veiligheid en het verdienvermogen van Nederland.

Doelen

- Digitale producten en diensten zijn veiliger.
- Nederland heeft een sterke cybersecuritykennis- en innovatieketen.

## Pijler III

### Tegengaan van digitale dreigingen van staten en criminelen

Deze pijler richt zich op de nationale en internationale aanpak van kwaadwillende actoren waar een cyberdreiging vanuit gaat. Het vergroten van het zicht op de digitale dreiging om op basis hiervan te handelen. De overheid heeft een speciale verantwoordelijkheid en beschikt over het instrumentarium om de digitale dreiging te adresseren.

Doelen

- Nederland heeft zicht op digitale dreigingen van staten en criminelen.
- Nederland heeft grip op digitale dreigingen van staten en criminelen.
- Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte.

## Pijler IV

### Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Deze pijler richt zich op de mens achter de techniek en de digitale weerbaarheid van burgers. Voor de samenleving als geheel is een belangrijke rol weggelegd om digitale vaardigheden te ontwikkelen, van basiskennis en -vaardigheden tot aan hoogwaardige kennis en specialistische cybersecurityvaardigheden.

Doelen

- Burgers zijn goed beschermd tegen digitale risico's.
- Burgers reageren snel en adequaat op cyberincidenten.
- Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid.
- De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts.

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

Voor het veilig en ongestoord functioneren van onze maatschappij is digitale veiligheid voor alle bedrijven, maatschappelijke organisaties en overheidsinstellingen cruciaal. Denk aan het continue beschikbaar houden van vitale infrastructuur in Nederland, en de vertrouwelijkheid en integriteit van processen. Cybersecurity maakt het mogelijk om informatie- en communicatietechnologie succesvol in te zetten, en de vruchten van innovatie en automatisering te plukken. Het op orde hebben van cybersecurity beschermt onder andere de bedrijfswinst, het concurrentievermogen, (waardevol) intellectueel eigendom en gevoelige klantdata van organisaties. Cyberincidenten bij bedrijven en overheden kunnen leiden tot een afname van het consumentenvertrouwen of het vertrouwen van burgers in de overheid.

Het Nederlandse cybersecuritystelsel dat onder andere gericht is op het ondersteunen van organisaties bij hun digitale weerbaarheid, heeft zich de afgelopen jaren autonoom ontwikkeld tot een stelsel met een grote verscheidenheid aan samenwerkingsverbanden in sectoren, ketens en regio's. Met als positief effect dat cybersecurity kennis breed verspreid wordt en er sectorale expertise is opgebouwd. Tegelijkertijd constateren we dat dit ook leidt tot versnippering en fragmentatie van activiteiten en verantwoordelijkheden.[15] Gevolg hiervan is dat informatie over kwetsbaarheden of risico's niet altijd of niet tijdig de relevante organisaties bereikt. Hierdoor zijn deze organisaties niet altijd in staat
om maatregelen te treffen en wordt expertise niet optimaal benut. Ook hebben juridische en organisatorische belemmeringen effectieve informatie-uitwisseling bemoeilijkt. Daarnaast is het voor organisaties binnen en buiten de overheid niet altijd duidelijk welke ondersteuning beschikbaar is en waar ze terecht kunnen met kwesties rondom digitale veiligheid.

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

Om ervoor te zorgen dat organisaties goed inzicht hebben en goed weten om te gaan met de dreiging en risico's is het van belang dat daar goede informatie over beschikbaar is. Organisaties mogen van de overheid verwachten dat deze actuele kennis en informatie over cyberdreigingen, -incidenten, -trends, en -kwetsbaarheden beschikbaar stelt zodat zij tot handeling kunnen overgaan.

Verdergaande samenwerking tussen overheidsorganisaties om te komen tot een zo actueel mogelijk situationeel beeld van cyberrisico's is van groot belang. Een dergelijk beeld is van belang voor het nemen van preventieve maatregelen en het organiseren van adequate incidentrespons, tot aan het effectief verstoren, opsporen en vervolgen.[16] Om zoveel mogelijk organisaties te bereiken met informatie (zoals analyses, fenomeenanalyses en handelingsperspectieven) over dreigende cyberincidenten en een adequate reactie te organiseren, zet de overheid in op intensieve publiek-private informatie-uitwisseling die zoveel mogelijk aansluit bij de behoefte van de doelgroep. Daarbij heeft de overheid aandacht voor doelgroepen waarin organisaties, zoals midden- en kleinbedrijven, verenigingen en stichtingen beperkte capaciteit (tijd, kennis, middelen, netwerk) hebben om deze informatie op een juiste manier toe te passen.

Binnen het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden kan algemene informatie over digitale veiligheid en specifieke dreigings- en risico-informatie worden gedeeld.[17] De overheid voert regie op de doorontwikkeling van dit stelsel. Het NCSC zal zich doorontwikkelen tot het nationaal Cyber Security Incident Response Team (CSIRT). Het Nationaal Cyber Security Centrum, het Digital Trust Center en het Cyber Security Incident Response Team voor digitale dienstverleners zullen worden samengevoegd tot één organisatie. Daarnaast wordt er meer samenhang gecreëerd tussen bestaande schakelorganisaties door integratie, waar nuttig, te stimuleren. Voor alle bestaande sectorale CERT's en CSIRT's wordt daarom door de Rijksoverheid verkend in hoeverre meer samenwerking, samenhang of samenvoeging met het NCSC toegevoegde waarde heeft. Nieuwe CSIRT's ontstaan in principe alleen daar waar dit toegevoegde waarde heeft.[18]

Het bereik van het stelsel wordt uitgebreid tot in de haarvaten van de samenleving om het actueel situationeel beeld en dreigingsinformatie en slachtofferinformatie waarover de overheid, bedrijven en maatschappelijke organisaties beschikken, zo veel als mogelijk te ontsluiten. In het bijzonder wordt het stelsel door de overheid verder doorontwikkeld en uitgebreid ten behoeve van alle overheidslagen, zoals gemeenten, provincies, waterschappen, uitvoeringsorganisaties en veiligheidsregio's.

### Doorontwikkeling van het Landelijk Dekkend Stelsel

Het doel van het LDS is om (publieke en private) organisaties in staat te stellen hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen door informatie over cybersecurity breed, efficiënt en effectief met elkaar te delen. Het is essentieel dat deze informatie-uitwisseling via schakelorganisaties leidt tot handelingsperspectief waarmee organisaties hun weerbaarheid kunnen verbeteren. Tot de functionaliteiten behoren informatiedeling, het faciliteren en aanjagen van samenwerkingen, algemene doelgroepanalyse en situationele analyse.

CSIRT's en toezichthouders zullen nationaal, maar ook Europees en internationaal intensiever samenwerken met partners. CSIRT's kunnen op Europees niveau baat hebben bij samenwerking op het gebied van technisch onderzoek naar cybersecurity-incidenten, ontwikkeling van technische oplossingen en respons op grootschalige cyberincidenten. Toezichthouders werken nationaal meer samen om te komen tot een effectieve inzet van schaarse capaciteit. In Europees verband wordt gestreefd naar intensievere samenwerking en informatie-uitwisseling en waar mogelijk bijstand in grensoverschrijdende zaken.

***Dit leidt tot de volgende subdoelen:***

- 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 cybersecurity-samenwerkingsverbanden is goed gecoördineerd, zoals door heldere aanspreekpunten.
- Overheidsorganisaties, zoals CSIRT's 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 binnen de keten mee

### Alle organisaties

Voor de digitale veiligheid van Nederland is inzet van alle bedrijven en organisaties noodzakelijk, niet alleen vanwege de continuïteit van de eigen dienstverlening maar ook vanwege de mogelijk bredere negatieve effecten voor afnemers, toeleveranciers of afhankelijke derden. De Rijksoverheid stimuleert organisaties een basisniveau van maatregelen te implementeren om zo bij te dragen aan de digitale weerbaarheid van organisaties. De overheid werkt ook aan veiligere ICT-producten en -diensten op Europees niveau om organisaties te stimuleren en faciliteren om hun eigen verantwoordelijkheid te kunnen nemen. Om organisaties, in het bijzonder het midden- en kleinbedrijf, te ondersteunen in het waarborgen van dit basisniveau is een belangrijke rol weggelegd voor de overheid om (in begrijpelijke taal) informatie en handelingsperspectief over digitale dreigingen en risico's te ontsluiten onder meer via het Landelijk Dekkend Stelsel. Ook is hierin een rol weggelegd voor brancheorganisaties en grotere of meer cybersecurityvolwassen organisaties om hier een bijdrage te leveren gelet op eventuele risico's voortkomend uit keten- en/of sectorale afhankelijkheden.

### Cybersecurityeisen voor een grotere groep bedrijven (NIB2)

Cyberincidenten stoppen niet bij landgrenzen. Ook de EU houdt zich daarom bezig met het versterken van de digitale veiligheid en weerbaarheid binnen de Unie. Als gevolg van de herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB2) krijgen veel meer sectoren en organisaties binnen de EU, te maken met wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen. Dit zijn bedrijven maar ook overheden. Dit betreft reeds gereguleerde sectoren onder NIB1 zoals energie, vervoer, drinkwater en digitale infrastructuur. Met NIB2 komen hier sectoren bij, zoals afvalwater, Rijksoverheid, ruimtevaart, levensmiddelen, vervaardiging en post- en koeriersdiensten. Medeoverheden, zoals provincies en gemeenten kunnen onder de NIB2 worden aangewezen op basis van een risicoanalyse. Deze organisaties dienen in het kader van een zorgplicht te voldoen aan een hoog niveau van cybersecurity. Incidenten met een bepaalde impact zullen ook tijdig gemeld moeten worden, zodat de impact zo beperkt mogelijk kan blijven. De taken van organisaties zoals het NCSC en de sectorale toezichthouders zullen als gevolg van de implementatie van deze richtlijn flink worden uitgebreid. In de herziening van de Netwerk- en Informatiebeveiligingsrichtlijn (NIB2) worden meer en andere organisaties aangemerkt dan nu onder de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) aangewezen zijn. Bij de herziening van het vitaal stelsel zal de samenhang met de nationale terminologie, de NIB2-terminologie en de terminologie uit de richtlijn voor weerbaarheid van kritieke entiteiten (CER) worden uitgewerkt. Voor deze strategie worden organisaties die onder de NIB2- en de CER-richtlijn vallen veelal als onderdeel van de vitale infrastructuur beschouwd.[19]



### Vitale infrastructuur en de overheid

Van organisaties binnen de vitale infrastructuur en de overheid wordt een hoog niveau van digitale weerbaarheid verwacht en dit wordt ook opgelegd. De overheid acht een risico-gebaseerde benadering van belang waarbij bedrijven en organisaties maatregelen nemen die proportioneel zijn aan het risico van de organisatie. Dat start met inzicht in zijn te beschermen belangen, kwetsbaarheden, dreigingen en risico's. Het inrichten van gedegen risicomanagement is fundamenteel. Daarbij hoort ook dat door een directeur of aan de bestuurstafel bewuste keuzes hierover worden gemaakt. Hierbij wordt verwacht dat ook rekening gehouden wordt met risico's voortkomend uit (inter)sectorale afhankelijkheden en het belang en de veiligheid voor anderen, bijvoorbeeld toeleveranciers in de keten. Vanwege het cruciaal belang van operationele technologie voor de continuïteit van de (vitale) infrastructuur is hiervoor extra aandacht noodzakelijk.[20] Hierin worden van organisaties concrete stappen verwacht om de digitale weerbaarheid van deze technologie te verhogen. Vitale infrastructuur organisaties worden ondersteund door het NCSC en de verantwoordelijke vakdepartementen om hun digitale weerbaarheid te versterken.

De overheid zorgt dat haar eigen systemen digitaal veilig zijn, dat overheidsdienstverlening voldoende beschermd is tegen cyberincidenten en dat (sensitieve) gegevens van burgers veilig zijn. Voor de gehele overheid zal hiertoe stevige wet- en regelgeving, en toezicht op naleving daarvan worden ingericht. Ten behoeve van de eigen beveiliging bevordert de Rijksoverheid de eigen digitale autonomie op het terrein van bijzondere producten en diensten.[21] De Rijksoverheid heeft bovendien continue aandacht voor de (keten)kwetsbaarheden van eigen digitale systemen en processen. Ook van medeoverheden, zoals gemeenten, provincies, waterschappen en veiligheidsregio's, wordt verwacht dat zij voldoende weerbaar zijn en hierin werken Rijksoverheidsorganisaties en medeoverheden nauw samen.

Ook geldt voor sommige sectoren aanvullende wet- en regelgeving die sectorspecifieke cybersecurityeisen opleggen van minimaal gelijkwaardig niveau als de eisen voortkomend uit de NIB2.[22] De vakdepartementen zijn verantwoordelijk voor het opstellen van deze sectorspecifieke wet- en regelgeving. Het ministerie van Justitie en Veiligheid zorgt dat Europese en nationale wetgeving op het gebied van cybersecurity in samenhang gerealiseerd en geïmplementeerd worden.

### Inzicht, toezicht en handhaving

Het inzichtelijk maken van en verantwoorden over cybersecurity door organisaties zou meer gemeengoed moeten worden. Belanghebbenden zoals afnemers, aandeelhouders en verzekeraars zouden daarom gemakkelijker inzicht moeten krijgen in het cybersecurityniveau van de organisatie. Daarnaast stelt deze transparantie belanghebbenden in staat om een gedegen risico afweging ten aanzien van de geleverde dienst of product te maken. Het inzichtelijk maken hiervan maakt organisaties daarmee economisch aantrekkelijker. Dit kan bijvoorbeeld worden bewerkstelligd door het opnemen van cybersecurity in rapportages die organisaties opstellen en overeenkomsten die organisaties afsluiten.[23]

Gereguleerde organisaties zijn op dit moment al verplicht om zich te verantwoorden over cybersecurity aan toezichthouders op basis van wettelijke verplichtingen zoals de toekomstige NIB2 en/of sectorale wetgeving. Toezichthouders beschikken over verschillende instrumenten om onder toezicht staande organisaties te stimuleren hun weerbaarheid te verhogen en te borgen. Zij kunnen inschatten welke maatregelen proportioneel zijn en passen bij het risico dat een organisatie loopt. Toezichthouders hebben daarnaast goed overzicht van de daadwerkelijke weerbaarheid van organisaties en sectoren. Tegelijk zullen toezichthouders worden geconfronteerd met nieuwe (technologische) ontwikkelingen die zich in een sector of markt voordoen, waardoor er ook nieuwe cybersecurityvraagstukken zullen ontstaan.

***Dit leidt tot de volgende subdoelen:***

- 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 digitale risico's en maken dit vaker inzichtelijk.
- Toezicht op de digitale weerbaarheid van organisaties is meer afgestemd op risico's voor zichzelf, hun sector en hun belang voor anderen.

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

Voor een effectieve voorbereiding op digitale incidenten dienen organisaties incident-, continuïteit- en herstelplannen te ontwikkelen, passend bij het (risico)profiel van de organisatie. Deze plannen moeten regelmatig geoefend worden, binnen de eigen organisatie en met partners in de sector en keten zodat werknemers weten hoe te handelen ten tijden van incidenten. Hierbij is ook aandacht nodig voor effecten die kunnen optreden in de fysieke wereld.

Mocht een incident toch plaatsvinden dan is het voor organisaties van belang dat zij hulp hebben georganiseerd. Daarnaast heeft het NCSC een wettelijke bijstandsrol, waarbij de primaire focus ligt op nationale veiligheid en het voorkomen van maatschappelijke ontwrichting. Het NCSC is verantwoordelijk voor de operationele coördinatie en regie in tijden van landelijke crises. Ook zorgt de overheid voor samenhangende publieke- en private cybersecuritydienstverlening bij incidenten, bijvoorbeeld samen met (vertrouwde) cybersecuritybedrijven.[24] Zo stimuleert de Rijksoverheid ook dat organisaties meer en beter samenwerken om cybercapaciteiten bij crises zo effectief en efficiënt mogelijk in te zetten.

Voor een respons bij een landelijke cybercrisis is een efficiënte samenwerking tussen overheidsorganisaties, het bedrijfsleven, de wetenschap en maatschappelijke organisaties van groot belang — ook over lokale, regionale en nationale grenzen heen. De overheid stimuleert dat bij overstijgende cyberincidenten en -crises volwaardig geïntegreerd wordt gehandeld op basis van een overkoepelend landelijk kader in de vorm van het Landelijk Crisisplan Digitaal.

We moeten ten slotte lessen blijven trekken uit incidenten- en crises. Daartoe zullen organisaties onderling actiever ervaringen en geleerde lessen moeten delen, waarbij vertrouwen voorop staat. Overheidsorganisaties delen gerichter informatie om zo beter inzicht te krijgen in de mate van weerbaarheid van organisaties, sectoren en ketens, waar mogelijk in samenwerking met bijvoorbeeld het bedrijfsleven of brancheorganisaties. De overheid benut dit inzicht om te sturen daar waar de weerbaarheid achterblijft bij de dreiging. Om dit mogelijk te maken is aandacht voor de meetbaarheid van weerbaarheid, meer inzicht in de kosten en baten van cybersecurityincidenten- en maatregelen onontbeerlijk.

***Dit leidt tot de volgende subdoelen:***

- 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.



## Acties met prioriteit pijler I

Onderstaande acties geven de prioriteiten voor de lopende kabinetsperiode weer waarmee het kabinet invulling geeft aan de doelstellingen uit deze pijler. Een uitgebreid overzicht van acties wordt weergegeven in de bijlage. Dat actieplan wordt jaarlijks geactualiseerd en geeft inzicht in de onderliggende acties, verwachte doorlooptijd en verantwoordelijken.

**A. Versnippering binnen het stelsel tegengaan**

- Het tijdig ontvangen van informatie over dreigingen en kwetsbaarheden op een manier die past bij het volwassenheidsniveau van de organisatie is een van de belangrijkste elementen voor een digitaal weerbaar Nederland. Om dit te realiseren moet de beschikbare capaciteit en expertise zo effectief mogelijk ingezet worden. Versnippering binnen het cybersecurity informatiedelingsstelsel moet zoveel mogelijk worden tegengegaan. Het NCSC, DTC en CSIRT-DSP worden daarom samengevoegd tot één nationale cybersecurity autoriteit. Deze nieuwe organisatie zal in samenwerking met publiek en private parners, vitale en niet-vitale organisaties, overheden en burgers voorzien van beveiligingsinformatie en handelingsperspectief, passend bij hun volwassenheidsniveau.
- Van de overige schakelorganisaties binnen het cybersecurity informatiedelingsstelsel wordt beoordeeld welke van hun taken (beveiligingsinformatie verspreiden; bijstand verlenen; oefeningen organiseren etc.) centraal (bij de nationale cybersecurity autoriteit) of sectoraal belegd moeten worden.
- Cybersecurity is een dreiging die publiek-privaat aangepakt moet worden. Een belangrijk element hierin is gezamenlijk verzamelen en duiden van dreigingsinformatie. Daarom start het kabinet met uitwerken van publiek-privaat platform voor informatie-en kennisdeling.

**B. Vrijblijvendheid voorbij**

- Met de implementatie van de NIB2 richtlijn worden ruim 5000 bedrijven in Nederland verplicht om cybersecurity incidenten te melden en specifieke maatregelen te nemen om hun digitale weerbaarheid te verhogen. Er wordt toezicht gehouden op de naleving van deze plichten. Deze plichten gelden nu nog maar voor slechts 200 organisaties in Nederland, deze uitbreiding zorgt dus voor een verhoging van de digitale weerbaarheid van aangewezen organisaties.
- Het kabinet neemt daarnaast verschillende maatregelen om de digitale weerbaarheid van specifieke sectoren te verhogen. Zo komen er extra normen voor de zorg- en onderwijssectoren. Het kabinet stelt verschillende tools beschikbaar om organisaties te helpen om hier aan te voldoen. Gemeenten en provincies krijgen te maken met aangescherpte beveiligingseisen. Om hen hierbij te helpen worden vanuit het ministerie van BZK meerdere ondersteuningsprogramma's worden aangeboden. Tenslotte is het kabinet van mening dat niet alleen de digitale weerbaarheid van IT-systemen aandacht moet krijgen maar ook de weerbaarheid van OT (operationele technologie). Dit zijn complexe digitale systemen die onze sluizen aansturen of de productie in fabrieken reguleren, de impact van uitval is hoog. Het kabinet zet daarom in op het vergroten van kennis en bewustzijn van de risico's bij organisaties die gebruik maken van deze systemen.

>>

**C. Voorbereid zijn op digitale incidenten en crises**

- Eind 2022 presenteert het kabinet het Landelijk Crisis Plan digitaal. In dit plan wordt uiteengezet hoe publieke en private organisaties in Nederland zich moeten voorbereiden op en handelen tijdens cybersecurity incidenten of crises.
- Het kabinet stelt op basis van de Rijksbrede risicoanalyse en de Rijksbrede veiligheidsstrategie een interdepartementale oefenagenda op. Hierin wordt ook de planning van internationale en nationale cyber- en hybride oefeningen meegenomen.



# Pijler II: Veilige en innovatieve digitale producten en diensten

Voor de veiligheid van onze gedigitaliseerde samenleving is het belangrijk dat we digitale producten en diensten tot onze beschikking hebben die gedurende hun gehele levenscyclus goed beveiligd zijn. Momenteel komt dit in de markt moeilijk tot stand. Afnemers zien het verschil niet tussen veilige en onveilige producten of diensten. Het is mede daardoor voor leveranciers en fabrikanten minder aantrekkelijk om voldoende te investeren in de digitale beveiliging van de producten en diensten die zij aanbieden. Daarnaast worden steeds meer producten en diensten gedigitaliseerd, van slimme televisies tot verbonden auto's en medische apparatuur. Er worden dagelijks kwetsbaarheden gevonden in software en er zijn nog te veel apparaten en diensten voor consumenten en organisaties op de markt, die eenvoudig kunnen worden misbruikt voor criminele acties, spionage of grootschalige aanvallen.

De marktdynamiek in een internationale competitieve markt waarbij er onvoldoende prikkels voor leveranciers bestaan om digitale producten gedurende de hele levenscyclus veiliger te maken, noopt tot wettelijke maatregelen, veelal op Europees niveau. Deze wettelijke maatregelen maken leveranciers meer verantwoordelijk voor de veiligheid van hun product en dienst en bieden afnemers houvast om eventuele schade als gevolg van cybersecurityincidenten te verhalen.[26] De overheid is een belangrijke afnemer en inkoper van digitale producten en diensten, en zal deze positie inzetten om de ontwikkeling van veilige producten en diensten te stimuleren.

Het is van belang om in te spelen op toekomstige kansen en dreigingen. Snelle ontwikkelingen in het digitale en technologische domein, zoals bij kwantumtechnologie of artificiële intelligentie (AI), vereisen structurele inzet op ontwikkeling en toepassing van kennis en innovatie ten behoeve van de ontwikkeling van cybersecurityproducten en -diensten. Om de Nederlandse concurrentiepositie op de Europese en internationale markt te verbeteren en om de ongewenste afhankelijkheid van buitenlandse partijen te minimaliseren moet samenwerking binnen de Nederlandse innovatieketen zoveel mogelijk worden gestimuleerd.

**Terugblik Roadmap Digitaal Veilige Hard- en Software**

De beveiliging van digitale producten en diensten is een complex en mondiaal vraagstuk waarvoor een mix aan maatregelen bestaat. Onder de NCSA werden de maatregelen op dit terrein beschreven in de Roadmap Digitaal Veilige Hard- en Software.[25] Zo zijn de afgelopen jaren Europese wettelijke markttoegangseisen voor draadloos verbonden apparaten gerealiseerd, is er een Europees stelsel ontwikkeld voor cybersecuritycertificering van ICT-producten, -diensten en -processen en is het Nederlandse stelsel ingericht met toezicht.[27] Ook hebben Europese consumenten recht gekregen op updates bij digitale producten, digitale inhoud en diensten en zijn Europese cybersecurityeisen gesteld aan medische apparatuur.[28] Daarnaast zijn op mondiaal niveau cybersecurity-eisen gerealiseerd voor met het internet verbonden auto's en andere voertuigen.[29]

## Digitale producten en diensten zijn veiliger

Ondanks de inzet op de beveiliging van digitale producten en diensten bestaat er nog geen sluitend systeem van (Europese) wet- en regelgeving met bijbehorende standaarden voor de cybersecurity van digitale producten, processen en diensten gericht op de verantwoordelijkheid van fabrikanten en leveranciers. Europese wet- en regelgeving creëert een gelijk speelveld en verbetert het concurrentievermogen van Nederlandse aanbieders. Doordat Europese kaders tot stand komen op basis van Europese publieke normen en waarden dragen zij ook bij aan de versterking van de digitale autonomie van Europa op mondiaal niveau, in zowel een geopolitieke context als ten opzichte van *techreuzen*. In de komende periode maakt Nederland zich in de Europese Unie sterk voor een samenhangend systeem van Europese wet- en regelgeving met bijbehorende standaarden. Hierbij gaat het om een samenspel van sectorale maatregelen, zoals bij medische apparatuur en apparatuur gebruikt voor energielevering, en meer horizontale maatregelen.[30] De Europese en nationale inzet zorgt ervoor dat afnemers kunnen vertrouwen op aantoonbaar veiligere producten en diensten. Duidelijkheid over de verantwoordelijkheid voor digitale beveiliging en de eisen waaraan deze moet voldoen, zorgt er bovendien voor dat eventuele schade gemakkelijker kan worden verhaald via het reguliere aansprakelijkheidsrecht.

Binnen Nederland zijn cybersecurity-inkoopeisen ontwikkeld voor alle overheidsorganisaties. Deze stevigere overheidsinzet via inkoop en aanbestedingen zorgt er ook voor dat de overheid haar rol als marktspeler meer inzet om de ontwikkeling van veilige ICT-producten en -diensten te stimuleren. De overheid heeft daarnaast beleid dat voorschrijft dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van (digitale) producten en diensten.

***Dit leidt tot de volgende subdoelen:***

- 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.
- Europese veiligheidseisen en -standaarden worden ook in landen buiten de EU gebruikt.
- Organisaties hebben contractuele afspraken met afnemers over 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

Om nu en in de toekomst maatregelen te kunnen nemen tegen digitale dreigingen moet de ontwikkeling en toepassing van Nederlandse kennis en kunde op het gebied van cybersecurity continu worden versterkt. Een hoogwaardige en autonome Nederlandse kennispositie en innovatieketen op het gebied van cybersecurity vermindert ongewenste afhankelijkheid van bedrijven, mensen en oplossingen uit het buitenland en biedt economische kansen voor het Nederlandse bedrijfsleven. Intensieve samenwerking tussen overheid, bedrijfsleven en kennisinstellingen is hiervoor essentieel.

Verschillende onderdelen van de keten - zoals fundamenteel en toegepast onderzoek, het bedrijfsleven en overheden – moeten elkaar beter gaan vinden en samenwerken aan concrete meerjarige projecten. Door een gezond innovatie-ecosysteem te creëren zorgen we ervoor dat waardevolle cybersecuritykennis niet weglekt naar buitenlandse partijen, maar wordt omgezet naar concrete producten en diensten.



Alleen dan kan Nederland op een veilige wijze de economische en maatschappelijke kansen van digitalisering verzilveren.

Een goede innovatiebasis zorgt ervoor dat Nederland minder afhankelijk wordt van cybersecurity expertise en oplossingen uit andere landen. Dit is van belang om de nationale veiligheid en onze meest gevoelige informatie te beschermen, vandaag en in de toekomst. Hiervoor is het onder meer van belang dat Nederland beschikt over hoogwaardige beveiligingsproducten waaronder cryptografische producten en diensten. Nederland is een van de weinige landen waar cryptografische producten en diensten worden ontwikkeld en vervaardigd omdat deze zeldzame kennis en expertise in Nederland beschikbaar is. Het is essentieel om deze expertise te behouden en door te ontwikkelen zodat Nederland haar gevoelige informatie goed kan beschermen.

### Dcypher

Het samenwerkingsplatform dcypher is de plek waar publieke, private en kennispartijen, middelen en expertise bij elkaar komen om effectief in te zetten op cybersecurity onderwijs, onderzoek, innovatie en concrete toepassingen. De missie van dcypher is om bij te dragen aan een veiliger, slimmer, digitaal autonoom en economisch sterker Nederland. De partners van dcypher moeten de ontwikkeling en toepassing van kennis in Nederland op het gebied van cybersecurity gaan verdiepen en verbreden. Het platform beoogd kennisontwikkeling in het cybersecuritydomein te stimuleren, een significante impuls te geven aan het cybersecurity bedrijfsleven en de overheid te ondersteunen in haar rol als launching customer.

Voor een gezond cybersecurity innovatie-ecosysteem wordt ingezet op het centrale publiek-private samenwerkingsplatform dcypher. Met dcypher is de afgelopen jaren de basis gelegd voor inhoudelijke agendering en programmering van meerjarige onderzoeks- en innovatietrajecten op het gebied van digitale veiligheid samen met overheidspartijen, bedrijven en kennisinstellingen. Deze aanpak richt zich op de hele keten, dus van fundamenteel onderzoek, via toegepast onderzoek naar de introductie van innovatieve cybersecurityproducten en -diensten. Dit zal leiden tot meer kennis en innovatie met een blijvende impact op het cybersecurity-ecosysteem, om een koploperpositie te verwerven binnen Europa. Het is van belang om daarbij de verbinding tussen nationale en Europese initiatieven en de daarbij behorende instrumenten en EU-middelen goed te verankeren. Dit zal gebeuren via het Nationaal Coördinatie Centrum (NCC) als schakelpunt tussen het nationale cybersecuritynetwerk en het Europese Cybersecurity Competence Centre (ECCC) en bijbehorend netwerk.

***Dit leidt tot de volgende subdoelen:***

- 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.

## Acties met prioriteit pijler II

Onderstaande acties geven de prioriteiten voor de lopende kabinetsperiode weer waarmee het kabinet invulling geeft aan de doelstellingen uit deze pijler. Een uitgebreid overzicht van acties wordt weergegeven in de bijlage. Dat actieplan wordt jaarlijks geactualiseerd en geeft inzicht in de onderliggende acties, verwachte doorlooptijd en verantwoordelijken.

**A. Veiligheid verplicht bij de ontwikkeling van digitale producten**

- Een van de belangrijkste stappen richting digitaal weerbare burgers en organisaties zijn veilige digitale producten. Een uitgangspunt bij het ontwikkelen van digitale producten zou veiligheid moeten zijn. Het kabinet borgt dit hoofdzakelijk via de '*Cyber Resilience Act*'. Nederland maakt zich tijdens de onderhandelingen voor deze verordening hard voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, diensten en processen, die gedurende de hele levenscyclus geldt, inclusief bijbehorende standaarden en toezicht.
- Het kabinet draagt daarnaast in samenwerking met private partijen bij aan de ontwikkeling en adoptie van Europese cybersecurity certificeringschema's voor ICT-producten, diensten en processen zoals voor clouddiensten, 5G technologie en Common Criteria. EZK stimuleert de bewustwording en implementatie van certificeringsschema's onder de Cyber Security Act. Door het gebruik van certificering te stimuleren en faciliteren worden consumenten en organisaties in staat gesteld om veilige keuzes te maken.

**B. De overheid stimuleert de ontwikkeling van veilige digitale producten via inkoop**

- De overheid moet de eigen cybersecurity op orde hebben en kan als grote afnemer van ICT-producten via het stellen van inkoopeisen de markt beïnvloeden. Het inkoopbeleid van de overheid draagt op die manier bij aan innovatie en de ontwikkeling van veilige producten en diensten.
- Er worden bijvoorbeeld Algemene Beveiligingseisen opgesteld voor de Rijksoverheid (ABRO) opgesteld waaraan bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten vervullen aan moeten voldoen.
- De tool inkoopeisen cybersecurity overheid (ICO) wordt doorontwikkeld, verbreed en geïmplementeerd. Inclusief verdere ontwikkeling van overheidsbrede eisensets. Deze tool wordt ook beschikbaar gesteld voor bedrijven zodat zij ook de inkoopeisen kunnen toepassen.
- De productontwikkeling voor high assurance producten wordt gestimuleerd middels versterkt en eensgezind opdrachtgeverschap vanuit de Rijksoverheid, zodat Nederland de beschikking houdt over betrouwbare cryptografische oplossingen.



**C. Sterke cybersecurity kennis- en innovatieketen**

- De ontwikkeling binnen het cryptografische domein wordt voortgezet door implementatie van de Nationale Crypto Strategie.
- Uit de raakvlakken in kennis- en innovatiebehoeften tussen de overheid en het bedrijfsleven komen nieuwe projecten en werkprogramma's voort. Het publiek-private samenwerkingsplatform dcypher faciliteert de verbinding tussen overheid, bedrijven en kennisinstellingen en draagt zorg voor de agendering en programmering van cybersecurity kennis- en innovatie projecten en werkprogramma's. Dcypher kan een faciliterende en aanjagende rol spelen in het zoeken naar financiering voor de genoemde high-end kennis- en productontwikkeling.

# Pijler III: Tegengaan van digitale dreigingen van staten en criminelen

De digitale ruimte is in toenemende mate een plaats waar spanningen tot uitdrukking komen: statelijke en niet-statelijke actoren voeren steeds vaker kwaadaardige digitale campagnes uit, vaak onderdeel van een hybride campagne, om zo uiteenlopende doeleinden te bereiken. De capaciteiten van criminele groeperingen doen in sommige gevallen niet meer onder voor die van staten. En het komt voor dat staten de samenwerking met criminele groepen juist opzoeken, of die groepen bewust niet hinderen. Dit raakt Nederland op vele manieren: diefstal ondermijnt ons verdienvermogen, sabotage is een directe bedreiging van onze nationale veiligheid en digitale dreigingen zetten onze democratie en rechtstaat onder druk. De koppeling tussen cyberaanvallen en de geopolitieke dynamiek kan in potentie de bondgenootschappelijke cohesie binnen de NAVO en de EU onder druk zetten.

Cybersecurity, en daarmee ook de bestrijding van cybercrime, moet dan ook als vast onderdeel van het nationale en internationale veiligheids- en cybersecuritybeleid gezien worden. Die vaststelling brengt het besef met zich mee dat we dit als Rijksoverheid en als Nederland niet alleen kunnen oplossen. Om gelijke tred te houden met de vele kwaadwillende actoren en de stijgende kwetsbaarheid van de digitale ruimte, moeten wij beter zicht krijgen op wat op ons afkomt. Hoe cruciaal zicht op de dreiging ook is, met zicht alleen wordt Nederland niet direct veiliger. Wel is het een essentiële stap voor effectief (schaalbaar) handelen.[31]

## Nederland heeft zicht op digitale dreigingen van staten en criminelen

Het gaat niet alleen om de betere waarneming van feitelijke handelingen van statelijke en niet-statelijke actoren in de digitale ruimte. Ook het politieke, diplomatieke, militaire en economische gedrag van derde landen geeft inzicht in hun opvattingen en intenties aangaande het gebruik van de digitale ruimte als middel om geopolitieke invloed te krijgen. De inzet van diplomatieke middelen is dan ook essentieel voor een beter zicht – bijvoorbeeld via gerichte diplomatieke rapportages, consultaties en coalitievorming met gelijkgezinden en dialogen met niet-gelijkgezinde partijen.

Een groot deel van deze opgave ligt binnen de unieke verantwoordelijkheid van de overheid met onder andere de politie, het OM en de Algemene- en Militaire Inlichtingen-en Veiligheidsdienst (inlichtingen- en veiligheidsdiensten) in samenwerking met partijen, zoals het NCSC en het DTC.[32] Daarmee heeft Nederland de mogelijkheden om de snelgroeiende dreiging en een deel van de actoren in het zicht te krijgen en te houden. Daarnaast zullen we nog vaker, inniger en actiever samenwerken met onder andere EU-partners en NAVO-bondgenoten zodat we eerder dreigingen en kwaadwillende actoren in het zicht kunnen krijgen. Om gedeeld begrip van de dreiging te bevorderen zal de overheid vaker proactief (cyber)inlichtingen delen en zo anderen in staat te stellen hun weerbaarheid te verhogen of op te treden tegen cybercriminelen.



De overheid moet ook intensiveren in de samenwerking met andere partijen en meer verbanden aangaan om de informatie die buiten de Rijksoverheid ligt, binnen te krijgen. Te denken is aan bedrijven, kennisorganisaties en internationale organisaties. Op basis van de eigen en andermans informatie is de overheid in staat een beter beeld te schetsen van de cyberdreiging gericht tegen Nederlandse belangen en die van onze partners.

***Dit leidt tot de volgende subdoelen:***

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

## Nederland heeft grip op cybersecurity-dreigingen van staten en criminelen

De overheid zet de komende jaren in op versterkte informatie-uitwisseling en verhoging van weerbaarheid wat bijdraagt aan het beperken van digitale dreigingen.[33] Daarnaast zal de overheid, binnen de juridische kaders, nog meer dan nu de mogelijkheden benutten om een kwaadwillende actoren en hun facilitators (digitaal) op te sporen, aan te pakken, te verstoren en te vervolgen. Dit kan de overheid bewerkstelligen met de inzet van onder andere de AIVD, de MIVD, de politie en het Openbaar Ministerie, Defensie, en Buitenlandse Zaken.[34] Het is hierbij van belang de (wettelijke) kaders in acht te nemen.

De politie en het OM gebruiken een brede, schaalbare en effectieve bestrijdingsstrategie voor de aanpak van cybercriminaliteit, waarmee zowel de plegers als dienstverleners van cybercriminaliteit worden aangepakt. Naast strafrechtelijke interventies zetten politie en OM ook in op alternatieve interventies. Met de brede bestrijding worden criminele activiteiten en netwerken verstoord, wordt strafbaar gedrag voorkomen, worden criminele winsten afgepakt en wordt opgetreden tegen strafbare gedragingen.

In verschillende internationale gremia, waaronder de EU, de Raad van Europa en de VN, draagt Nederland actief bij aan de (door-)ontwikkeling van juridische instrumenten die ten doel hebben de internationale samenwerking tegen cybercriminaliteit te versterken, met een sterke borging van mensenrechten en vrijheden. Statelijke cyberoperaties zullen effectiever door de AIVD en de MIVD verstoord worden. Defensie zal de capaciteiten die zij beschikbaar heeft voor haar grondwettelijke taken vaker structureel in het nationale domein inzetten en klaar moeten staan wanneer zij bevraagd wordt: niet alleen als laatste redmiddel, maar ook als digitale vuist.[35]

Gelet op de geopolitieke dimensie van digitale dreigingen is onze inzet in de digitale ruimte integraal onderdeel van ons bredere buitenlandbeleid. Het ministerie van Buitenlandse Zaken zal samen met (inter)nationale partners effectiever diplomatieke middelen inzetten in reactie op cyberaanvallen en -incidenten. Het in ontwikkeling zijnde Rijksbreed Responskader Statelijke Dreigingen zal waar mogelijk ook in de digitale ruimte toepassing vinden. Hiervoor zal gebruik worden gemaakt van het interdepartementale responskader voor cyberincidenten, onder coördinatie van het ministerie Buitenlandse Zaken. Dit kader wordt sinds 2018 met succes toegepast en zal de komende jaren verder worden ontwikkeld.

Waar de juridische kaders de operationele slagkracht te veel beperken om het doel te bereiken, zal verruiming van de kaders overwogen worden, uitgaande van onze publieke  waarden en rekening houdend met het normatief kader voor verantwoordelijk statelijk gedrag, inclusief grondrechten en het internationaal recht (onder andere mensenrechten en het humanitair oorlogsrecht).

***Dit leidt tot de volgende subdoelen:***

- 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 digitale dreigingen van staten en criminelen (inter)nationaal goed gecoördineerd in.
- De overheid beschikt over (niet-)strafrechtelijke interventies tegen cybercriminelen en hun dienstverleners, zoals tegen ransomware.

## Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte

Gegeven de geopolitieke spanningen zullen cyberdreigingen en -aanvallen de komende periode alleen maar toenemen. De beste manier om de bron van die dreiging in de kiem te smoren bestaat eruit om de geopolitieke arena meer naar onze hand te zetten door het bevorderen van de internationale rechtsorde in de digitale ruimte.

Nederland zal aan de basis staan van stevige coalities die verantwoordelijk statelijk gedrag in de digitale ruimte bepleiten en zal bijdragen aan de verdere uitwerking van een uniform en breed gedragen normatief kader in de digitale ruimte om geopolitieke spanningen te verminderen. Dit doen we door democratische en rechtsstatelijke normen en waarden uit te dragen, inclusief mensenrechten, onder andere via cyberdiplomatie. De Rijksoverheid leeft dit normatief kader zelf na en draagt het actief uit. Onze waarden en normen en onze visie voor een vrij, open en veilig internet vormen hiervoor de basis.

### Normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte

Om de dreiging van destabiliserende cyberaanvallen het hoofd te bieden is het noodzakelijk om internationale afspraken te maken. In VN-verband is sinds 1998 onderhandeld over de spelregels die gelden in de digitale ruimte.[36] Dit is inmiddels uitgegroeid tot meerdere overleg- en onderhandelingsmechanismes gericht op de digitale ruimte, waaraan Nederland actief bijdraagt of heeft bijgedragen: de Group of Governmental Experts (GGE), de Open Ended Working Group (OEWG), en het Program of Action (PoA).

De behoefte aan stabiliteit heeft geleid tot de vaststelling van een normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte, dat de VN-lidstaten in 2021 met consensus hebben herbevestigd.[37] Dit kader draagt bij aan stabiliteit, want zo kunnen landen die in overtreding zijn worden aangesproken op hun gedrag. Het uitgangspunt is dat bestaand internationaal recht van toepassing is in cyberspace.

Dit betekent dat onder andere dat het interstatelijke geweldverbod en het internationaalrechtelijke non-interventiebeginsel ook op de digitale ruimte van toepassing zijn, en dat een (onmiddellijk dreigende) cyberaanval onder bepaalde omstandigheden kan worden beschouwd als een gewapende aanval waartegen een staat het recht op individuele en collectieve zelfverdediging kan inroepen. Ook is erkend dat mensenrechten zowel online als offline gelden en dat staten zich moeten houden aan hun mensenrechtelijke verplichtingen in de digitale ruimte, evenals aan het humanitair oorlogsrecht. Complementair daaraan zijn er elf niet-bindende gedragsnormen overeengekomen. Deze bieden beneden de grens van gewapend conflict afspraken, waarborgen en beschermingen.



Het kabinet steunt het zogenoemde multi-stakeholdermodel voor het beheer van het internet. In dit model bestaat een open samenwerking tussen de belanghebbende overheden, maatschappelijke organisaties, bedrijven, wetenschap en de technische internetgemeenschap binnen organisaties als de *Internet Corporation for Assigned Names and Numbers* (ICANN), de *Internet Engineering Task Force* (IETF) en het *Institute of Electrical and Electronics Engineers* (IEEE). Zij moeten het voortouw hebben bij aanpassingen van de standaarden, protocollen en procedures voor de kernfunctionaliteit van het internet, zonder ongepaste inmenging van statelijke of private actoren. Nederland zet zich in om te voorkomen dat nationale en regionale wet- en regelgeving barrières opwerpt die uiteindelijk leiden tot versplintering van het internet.

***Dit leidt tot de volgende subdoelen:***

- 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.

### Acties met prioriteit pijler III

Onderstaande acties geven de prioriteiten voor de lopende kabinetsperiode weer waarmee het kabinet invulling geeft aan de doelstellingen uit deze pijler. Een uitgebreid overzicht van acties wordt weergegeven in de bijlage. Dat actieplan wordt jaarlijks geactualiseerd en geeft inzicht in de onderliggende acties, verwachte doorlooptijd en verantwoordelijkheden.

**A. Vergroten van het zicht op de dreiging**

- De dreiging kennen en begrijpen is de eerste stap richting een digitaal weerbaar Nederland. Het kabinet investeert daarom fors in de onderzoekscapaciteit van de I&V-diensten ten behoeve van inlichtingenmatig-diepteonderzoek. Hierdoor ontstaat breder zicht in huidige en voorstelbare digitale dreiging. Daarmee worden unieke inlichtingen vertaald naar specifiek handelingsperspectief zodat afnemers zich beter kunnen weren.

**B. Versterken onderzoeks-en opsporingscapaciteit cyber criminelen**

- Naast zicht op de dreiging is de mogelijkheid om daders te onderzoeken en op te sporen van groot belang, dit gaat verder dan alleen strafrechtelijke interventies. Politie en OM zetten daarom met publieke en private partners in op het ontwikkelen van niet-strafrechtelijke interventies te bestrijding van cybercrime, waaronder ransomware.
- Het OM breidt de komende jaren haar kennis en kunde uit op dit onderwerp en onderzoekt de mogelijkheid om middels een *'fasttrack'* zaken versneld af te doen.
- De politie maakt vanaf 2023 voor meer cybercrime fenomenen het mogelijk om online melding of aangifte te doen.
- De politie start daarnaast met het opstellen van een veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit. Hierin worden

de belangrijkste criminele fenomenen, werkwijzen en het risico hiervan, voor de samenleving geschetst. De beelden geven richting aan de keuze van de politie en het OM voor wat betreft de fenomenen waarop wordt ingezet en de onderzoeken die worden geprioriteerd.

**C. Uitbreiden diplomatieke respons en defensieve cybercapaciteit**

- Het kabinet investeert in het cyberdiplomatennetwerk en taken worden uitgebreid ten behoeve van een versterkte informatiepositie over digitale dreigingen en ontwikkelingen. Daarnaast zet het kabinet zich in coalitieverband in voor naleving van internationale gedragsnormen en toepassing van het internationaal recht in het digitale domein, alsook voor een open, vrij en veilig internet door middel van een versterkte inzet op internet governance waarin deelname van de Nederlandse multistakeholdergemeenschap bevorderd wordt middels een open, vrij en veilig internet.
- Samen met internationale partners worden nieuwe en effectievere opties voor diplomatieke respons op cyberdreigingen ontwikkeld. Bestaande kaders en instrumenten zoals het interdepartementale cyber responskader, de EU Cyber Diplomacy Toolbox en de NATO Guide worden doorontwikkeld. Daarnaast bouwt het kabinet verder aan het Rijksbreed Responskader voor Statelijke Dreigingen, waarin alle mogelijke responsopties binnen de Rijksoverheid met een escalatieladder en afwegingskader bij elkaar worden gebracht.
- Defensie investeert in zijn gehele keten van cybercapaciteiten en het vergroten van de personele gereedheid via opleiding, training en oefening. Defensie breidt bijstandsconstructies uit om andere organisaties te kunnen helpen bij grootschalige incidenten. Onder andere via het Nationale Respons Netwerk (NRN).



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

Het ongestoord functioneren van de samenleving is in toenemende mate afhankelijk van het veilig gebruik van digitale middelen. In pijler 2 wordt de Europese aanpak beschreven om de veiligheid van digitale producten en diensten te borgen. Daarnaast is de digitale weerbaarheid van burgers zelf een belangrijke randvoorwaarde.[38] Voor veel Nederlanders is het echter nog een te grote opgave om voldoende digitaal veilig te zijn en te blijven. De meest kwetsbare groepen lopen daarbij de grootste risico's.[39] Cybercriminelen maken veel slachtoffers.[40] Digitale veiligheid kan goed helpen om slachtofferschap van cybercriminaliteit te verminderen.[41]

Door de digitalisering van onze maatschappij komen kinderen op steeds jongere leeftijd in aanraking met digitale producten en diensten. Het is van belang dat zij over de digitale vaardigheden beschikken om adequaat om te gaan met cyberrisico's en het in de praktijk brengen van maatregelen voor digitale veiligheid. Daar is nog onvoldoende structurele aandacht voor in het basis- en voortgezet onderwijs, terwijl het juist van belang is om hen de vaardigheden mee te geven voor hun veiligheid in deze digitale wereld.

Om onze samenleving duurzaam weerbaar te maken en te houden wijst de Cybersecurity Raad op het zorgdragen voor voldoende gekwalificeerde vakmensen.[42] In het algemeen is er sprake van een tekort aan expertise in de cybersecuritymarkt.[43] Voor de digitale veiligheid en weerbaarheid van organisaties zijn onder andere specialisten op MBO-, HBO- en WO-niveau nodig die digitale systemen en processen veilig kunnen maken en houden.

## Burgers zijn goed beschermd tegen digitale risico's

Het is van groot belang dat burgers zoveel mogelijk in staat worden gesteld om zelfredzaam te zijn en beschikken over de nodige basiskennis en -vaardigheden om effectieve maatregelen te kunnen nemen tegen cyberdreigingen en risico's, en dat zij deze maatregelen ook daadwerkelijk toepassen. Om dit te bereiken blijft inzet nodig om burgers ICT-vaardiger te maken en via bewustwordingscampagnes alert te maken op de maatregelen die zij zelf kunnen nemen om digitaal veiliger te zijn. Zo wordt onze samenleving digitaal veerkrachtiger.

Het doel is dat burgers basis cybersecuritymaatregelen toepassen, zoals het gebruik van sterke wachtwoorden, multi-factor authenticatie, het maken van back-ups, het uitvoeren van updates en het adequaat reageren op phishingaanvallen. Daarbij is het ook van belang dat zij beschikken over de kennis en instrumenten om maatregelen toe te passen. Daarom is het van belang dat burgers op vertrouwde en bekende plekken laagdrempelige toegang hebben tot informatie- en adviesverstrekking op maat voor het vergroten van digitale veiligheidsvaardigheden.

***Dit leidt tot de volgende subdoelen:***

- Burgers zijn zich bewust van 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

Het is van belang dat burgers in staat gesteld worden om snel en effectief te reageren op digitale dreigingen, aanvallen en verstoringen. Dat kan door vroegtijdig geïnformeerd te worden over voor hen relevante actuele dreigingen en met name over wat zij zelf kunnen doen om hiervoor veilig te blijven. De komende jaren wordt ingezet op het sneller en kwalitatief beter informeren van burgers. Het is belangrijk dat het duidelijk is waar burgers deze informatie kunnen vinden en dat zij ook geïnformeerd worden over hun handelingsperspectief. Burgers moeten daarnaast in de toekomst laagdrempelig en eenvoudig melding of aangifte kunnen doen van cyberincidenten, zoals phishing.

***Dit leidt tot de volgende subdoelen:***

- 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

Het is belangrijk dat kinderen vroeg leren om te gaan met de digitale wereld en het herkennen van de daarbij behorende risico's. Het is van belang dat leerlingen veilig onlinegedrag aanleren. Digitale vaardigheden, waaronder bewustwording van cyberrisico's en veiligheid, zijn op dit moment geen onderdeel van het landelijk curriculum voor basis- en voortgezet onderwijs. Om leerlingen digitaal vaardig te maken, moeten ook docenten hier vaardig in zijn en hier goed les in kunnen geven. Het is belangrijk dat scholen hierin passende ondersteuning kunnen krijgen.

***Dit leidt tot de volgende subdoelen:***

- 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

Om de toenemende vraag naar cybersecurityexpertise het hoofd te bieden moet worden ingezet op voldoende specialisten op de arbeidsmarkt. Publiek-private samenwerking is hiervoor essentieel. Om te zorgen voor een beter aanbod moet helder zijn waar het tekort precies zit en welk aanbod er nodig is om dit op te lossen. Welke mechanismen zijn er bijvoorbeeld om cybersecurityexpertise op de arbeidsmarkt te bevorderen en effectief in te zetten? Er kan bijvoorbeeld worden aangesloten bij het aanvalsplan voor de techniek, gericht op onder andere de digitale transitie.[44]

***Dit leidt tot de volgende subdoelen:***

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



## Acties met prioriteit pijler IV

Onderstaande acties geven de prioriteiten voor de lopende kabinetsperiode weer waarmee het kabinet invulling geeft aan de doelstellingen uit deze pijler. Een uitgebreid overzicht van acties wordt weergegeven in de bijlage. Dat actieplan wordt jaarlijks geactualiseerd en geeft inzicht in de onderliggende acties, verwachte doorlooptijd en verantwoordelijken.

**A. Bewustzijn van cyberrisico's onder burgers vergroten**

- De risico's van digitale kwetsbaarheden en dreiging moeten zoveel als mogelijk worden gedragen door de ontwikkelaars en aanbieders van digitale-producten en –diensten. Er zal echter bijna altijd een restrisico blijven waardoor de burger of MKB ook zelf maatregelen moet nemen. Om deze maatregelen te kunnen nemen moeten burgers en MKB zich allereerst bewust zijn van de risico's en de te nemen maatregelen. Een belangrijk instrument dat het kabinet hiertoe inzet zijn verschillende doelgroep specifieke voorlichtingscampagneprogramma cyberveiligheid gericht op de cybersecurity basismaatregelen.
- Het kabinet versterkt daarnaast de Informatiepunten Digitale Overheid. Deze worden gefaciliteerd om hulpvragen van burgers op het terrein van cyberveiligheid te beantwoorden en waar nodig door te verwijzen naar steunpunten, informatieloketten en lokale ondersteuningsinitiatieven van private partners.

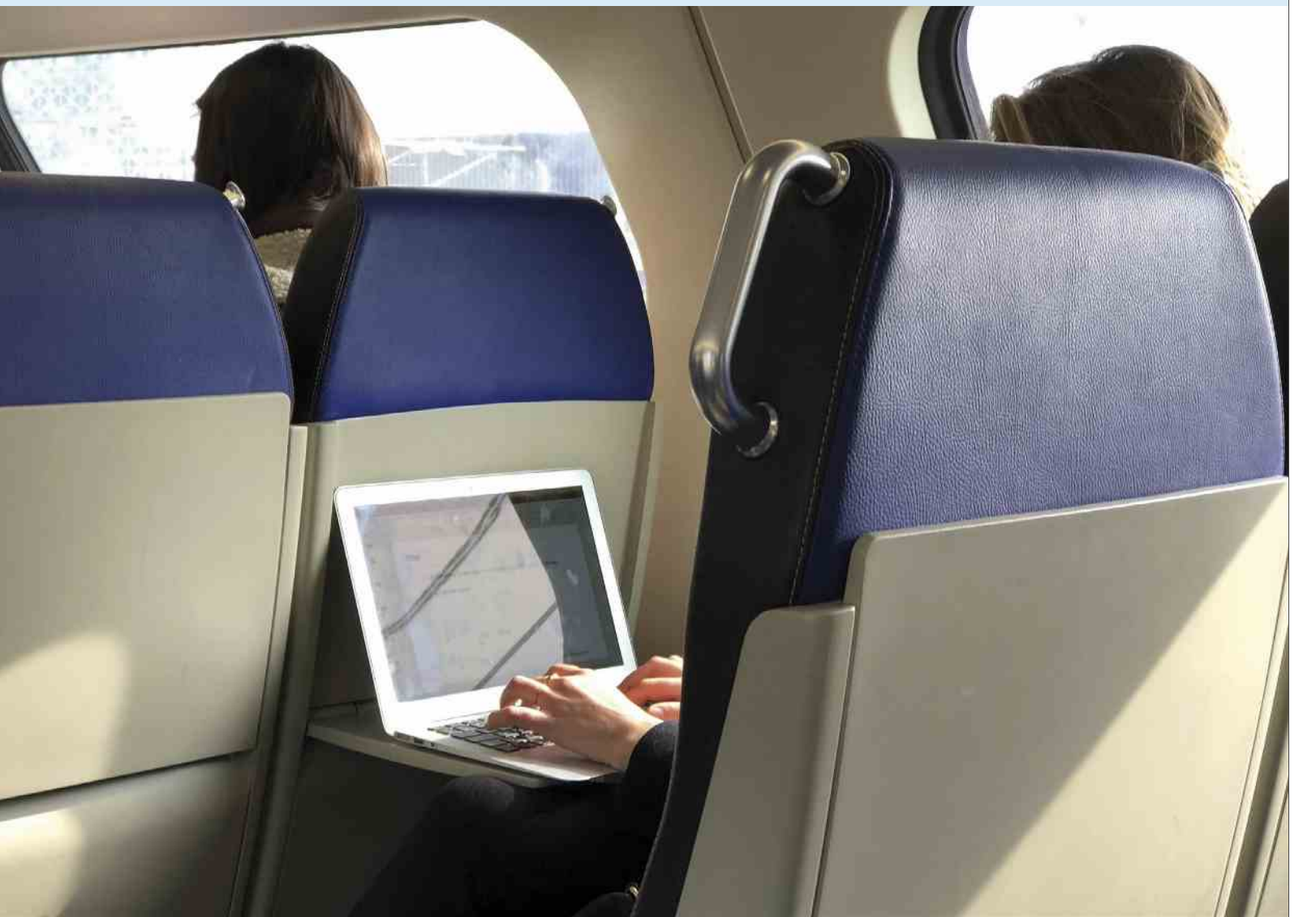
**B. Digitale weerbaarheid wordt onderdeel van het curriculum**

- Kinderen moeten vanaf jonge leeftijd veilig leren omgaan met digitale producten en diensten. Stichting Leerplan Ontwikkeling (SLO) heeft de opdracht gekregen om samen met het onderwijsveld concrete kerndoelen voor zowel het PO als het VO voor de basisvaardigheden te ontwikkelen waar digitale veiligheid deel van uit moet maken. De aangescherpte kerndoelen voor het PO & VO in een wetsvoorstel aan de Tweede Kamer voorgelegd.
- Het 'masterplan basisvaardigheden' wordt opgezet dat er voor moet zorgen dat de leraar goed toegerust is om het beste onderwijs te geven in taal, rekenen/wiskunde, burgerschap en digitale geletterdheid.

**C. Aandacht voor cybersecurity op de arbeidsmarkt**

- Het kabinet werkt samen met onderwijsinstellingen aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Daartoe werken zij samen met het bedrijfsleven en andere relevante partijen. Hierbij worden onder andere knelpunten en beperkingen in die samenwerking voortvloeiend uit regelgeving geïnventariseerd en bezien welke oplossingen daarvoor nodig zijn.
- Het kabinet investeert in hbo-opleidingen in de bètatechniek, waar cyber security opleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere uitval en switch, (3) hogere zijinstroom, (4) inductie/warme overgang van opleiding naar arbeidsmarkt.

*Werk is al lang niet meer verbonden met kantoor. Met behulp van laptops, hotspots en wifi in de trein is het mogelijk om vanaf elke locatie mails te versturen of vergaderingen bij te wonen. Wat betekent dit voor de bescherming van data en gegevens?*



# 4. Governance, evaluatie en monitoring

## Governance, regie en samenwerking

Digitale veiligheid is ‘chefsache’. Leiderschap, regie en eigenaarschap zijn daarbij cruciaal. Binnen het kabinet werken de betrokken ministers nauw met elkaar samen onder verantwoordelijkheid van de minister van Justitie en Veiligheid als coördinerend bewindspersoon voor cybersecurity. Cybersecurity is een vast thema in de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV), waar integraal gestuurd wordt op de uitvoering van deze strategie en het bijbehorende actieplan.

Stevige regie draagt bij aan het synchroniseren en verbinden van nationale initiatieven en investeringen. Een belangrijk uitgangspunt is dat regievoering vanuit de minister van Justitie en Veiligheid vooral faciliterend, ondersteunend en stimulerend dient te zijn en gericht op effectiviteit, samenhang en slagkracht van het kabinetsbeleid op het terrein van cybersecurity.

De NLCS kan alleen succesvol ten uitvoer worden gebracht in nauwe samenwerking tussen (vertegenwoordigers uit) het bedrijfsleven, de wetenschap en decentrale, regionale en nationale overheden en uitvoeringsorganisaties. Begin 2023 wordt een integraal sturingsmodel ingericht. Daarbij zal worden aangesloten bij de bestaande (inter)bestuurlijke structuren en gebruik worden gemaakt van de positieve ervaringen die afgelopen jaren op het gebied van publiek-private samenwerking zijn opgedaan. In dit model wordt op deelonderwerpen de gezamenlijke inzet van publieke en private partijen gericht en geïntensiveerd met het oog op het behalen van de doelstellingen. Bijvoorbeeld rondom de doelstellingen gericht op versterking van de arbeidsmarkt, het intensiveren van innovatie of het efficiënter en effectiever inrichten van het cybersecuritystelsel.

De Cyber Security Raad (CSR) heeft als taak het kabinet te adviseren over de uitvoering en uitwerking van de Nederlandse Cybersecuritystrategie. De CSR wordt gevraagd om periodiek te adviseren over de ontwikkelingen die meegewogen moeten worden in de herijking van het actieplan.

De NLCS is een duidelijk kader aan de hand waarvan bewaakt wordt dat het cybersecuritybeleid zich op alle niveaus samenhangend en gestructureerd ontwikkelt. Vakdepartementen vertalen dit generieke kader naar sectorspecifieke kaders en regelgeving voor de organisaties en processen waar zij een systeemverantwoordelijkheid voor dragen. Bij het opstellen van aanvullend beleid of wetgeving op het gebied van cybersecurity hanteert het kabinet de volgende leidende principes.

**Leidende principes vanuit de Rijksoverheid voor cybersecuritybeleid en wetgeving:**

- Digitale veiligheid is integraal onderdeel van de digitaliseringsopgave van Nederland.
- Digitale veiligheid, weerbaarheid en veerkracht dienen gemeengoed te zijn. Cyberrisico's zijn integraal onderdeel van een bredere risicobeoordeling. In lijn daarmee nemen organisaties maatregelen die proportioneel, realistisch en, waar nodig, sectorspecifiek zijn.
- Organisaties, overheden en bedrijven hebben ieder een eigen verantwoordelijkheid om hun digitale weerbaarheid op orde te brengen en up-to-date te houden; de overheid informeert, stimuleert, faciliteert, verleent bijstand op basis van risicobeoordeling en stelt (juridische) kaders en intervenieert waar nodig, daarbij rekening houdend met het volwassenheidsniveau van organisaties en het belang dat organisaties vertegenwoordigen.
- Het is voor organisaties en burgers duidelijk waar en wanneer zij terecht kunnen voor informatie, kennis en bijstand.
- De Rijksoverheid en medeoverheden geven het goede voorbeeld, en hebben een weerbaarheidsniveau dat past bij de risico's. Dat is nodig om onze publieke belangen te beschermen.
- Effectieve en efficiënte inzet van capaciteit binnen de overheid door zaken doeltreffend te organiseren, tijdig te handelen en zoveel mogelijk samen te werken. De Nederlandse Cybersecuritystrategie is het generieke kader dat versnippering van de inzet op digitale veiligheid tegengaat, dit is de basis. Hier bovenop is er ruimte voor specifieke invulling onder andere door sectorale beleidskaders, strategieën, agenda's, routekaarten op deelonderwerpen of aanvullende normenkaders.
- Publiek-private samenwerking is en blijft het fundament - de krachten bundelen. Publiek-private samenwerking is erop gericht om concrete en meetbare resultaten te behalen.
- Digitale veiligheid is grensoverschrijdend en daarom is internationale samenwerking in EU- en NAVO-verband en daarbuiten essentieel. Nederland neemt hierbij een voortrekkersrol. Waar mogelijk wordt gezocht naar oplossingen in internationaal en Europees verband om de cybersecurity en digitale autonomie te versterken.



## Evaluatie en monitoring

De digitale veiligheid van Nederland is onlosmakelijk verbonden met technologische en maatschappelijke ontwikkelingen. Cybersecuritymaatregelen die vandaag effectief zijn, kunnen morgen alweer achterhaald zijn. Voor deze strategie en het bijbehorende actieplan is daarom gekozen voor een adaptieve benadering. Om in te kunnen spelen op trends, actuele dreigingen en risico's, moeten de maatregelen die volgen uit de Nederlandse Cybersecuritystrategie in de loop van de tijd kunnen worden uitgewerkt, aangepast of versterkt.

Daarbij is het van belang om te onderzoeken wat wel en niet werkt, zodat de overheid en andere partners zo effectief mogelijke (beleids)interventies kunnen doen en investeringen zoveel mogelijk resultaat opleveren voor de samenleving. Het is echter niet eenvoudig om het effect van cybersecuritybeleid te meten, zoals onder andere is beschreven door de Cyber Security Raad.[45] Allereerst bestaat deze strategie uit verschillende doelen die erop gericht zijn Nederland in staat te stellen de economische en maatschappelijke kansen van digitalisering te verzilveren en tegelijkertijd onze veiligheid te beschermen. Het succesvol realiseren van de doelstellingen van deze strategie is daarmee een optelsom van allerlei verschillende factoren. Ten tweede zijn veiligheidsinterventies gericht op het voorkomen van incidenten. Het is per definitie ingewikkeld om te meten hoeveel en wat voor incidenten er voorkomen zijn. Ten derde is cybersecurity ook afhankelijk van externe factoren. Het is de vraag in hoeverre de verbetering van cybersecurity is toe te schrijven aan het cybersecuritybeleid zelf. De evaluatieaanpak van deze strategie moet hier dus rekening mee houden.

Het is echter van belang om te blijven werken aan het verbeteren van ons inzicht in de effecten van cybersecuritybeleid, om ook in de toekomst een effectieve cybersecurityaanpak te hebben. Hiervoor is er een monitoring- en evaluatieprogrammering opgesteld bij de Nederlandse Cybersecuritystrategie, waarbij is uitgegaan van wat er wel mogelijk is.

## Aanpak

De Nederlandse Cybersecuritystrategie (NLCS) is de vierde Nederlandse integrale cybersecuritystrategie. Voor het opstellen van deze monitoring- en evaluatieprogrammering is gebruik gemaakt van de methodiek van de Strategische Evaluatie Agenda (SEA).[46] Het doel van deze methode is om op een gestructureerde manier monitoring- en evaluatieactiviteiten te plannen, zodat op de juiste momenten relevante inzichten voor leren en verantwoorden worden verkregen.

## Evaluatieprogramma

### Ex-ante fase

Onder het vorige kabinet is er voor het eerst een evaluatie uitgevoerd van de Nederlandse Cybersecurity Agenda (NCSA).[47] Naar aanleiding van de ervaringen met de NCSA is er bij het opstellen van deze strategie voor gekozen om een striktere scheiding tussen strategie en actieplan aan te brengen. De strategie kan meer toekomstgericht en duurzaam zijn, met daarbij een adaptief actieplan om bij veranderingen in de belangen, de dreiging, de weerbaarheid of andere politiek-bestuurlijke behoeften te kunnen bijsturen of intensiveren. Daarnaast kunnen acties die afgerond zijn weer leiden tot vervolgacties, bijvoorbeeld als er een verkenning of onderzoek wordt gedaan.

Andere aandachtspunten die uit deze evaluatie meegenomen (of meegenomen worden in het opstellen van de actieplannen) zijn het expliciet beleggen van eigenaarschap en verantwoordelijkheden en beoogde acties en effecten concreter te beschrijven. Ten slotte is het van belang om meer aandacht te schenken aan de meetbaarheid van de beoogde resultaten en effecten van de strategie en (tussentijdse) evaluatie.

In de evaluatie van de NCSA wordt een methodiek voorgesteld om te komen tot een logische opbouw van een strategie. Deze is gevolgd door hoofddoel-

stellingen te formuleren die een gewenste situatie of een te realiseren effect in de toekomst beschrijven. Onder de hoofddoelstellingen vallen subdoelstellingen die bijdragen aan de realisatie ervan. De doelen worden uitgewerkt in een actieplan, waarin de maatregelen worden beschreven die vanuit de overheid worden genomen om het bereiken van deze doelen dichterbij te brengen. De activiteiten of maatregelen zijn duidelijk gekoppeld aan het te realiseren effect dat in de (hoofd- en sub)doelstellingen beschreven staat.

De acties uit het actieplan worden onder andere gefinancierd uit de middelen die in het coalitieakkoord extra zijn vrijgemaakt voor cybersecurity. Een nadere uitsplitsing hiervan is te vinden in de budgettaire paragraaf van de Nederlandse Cybersecuritystrategie.

### Ex-durante fase

De Kamer zal jaarlijks worden geïnformeerd over de voortgang van de Nederlandse Cybersecuritystrategie. Er bestaat ook de mogelijkheid om bij de voortgangsrapportage acties aan te vullen of te wijzigen op basis van nieuwe inzichten en ontwikkelingen, die bijvoorbeeld kunnen blijken uit het nieuwe CSBN. Om de voortgang van de maatregelen in de tijd te kunnen volgen zal er in opdracht van het WODC een nulmeting worden uitgevoerd. Doel van de nulmeting is om duidelijk te krijgen wat de vertreksituatie is voordat de beleidsmaatregelen van start gaan. Deze informatie dient ook om de voortgang van de maatregelen te kunnen volgen in de tijd.

### Ex-post fase

De looptijd van de Nederlandse Cybersecuritystrategie is in principe zes jaar. Er zal in elk geval een evaluatieonderzoek plaatsvinden in 2025, halverwege de looptijd van deze strategie. Deze evaluatie heeft als doel om lessen op te leveren die kunnen worden meegenomen in beleidsvorming voor de toekomst.

Om goed aan te kunnen sluiten bij de actuele kennisbehoefte, zal er op een later moment een besluit worden genomen over de invalshoek van de evaluatie. Vanwege de breedte van deze strategie en de variatie in acties levert een evaluatie van alle doelen en maatregelen uit deze strategie en het actieplan waarschijnlijk weinig concrete aanbevelingen op. Er kan daarom gekozen worden voor één of meerdere relevante deelonderwerpen, bijvoorbeeld een onderwerp waarover weinig bekend is van de beleidstheorie of een onderwerp dat in de toekomst aan belang toeneemt.

Een volgend kabinet kan uiteindelijk een beslissing nemen over de uiteindelijke doorlooptijd en eventuele eindevaluatie van de Nederlandse Cybersecuritystrategie.

*Thuiswinkelen groeit nog steeds explosief. Door de coronamaatregelen werden in 2020 ruim 100% meer pakketten bezorgd. Voor het bestellen en afleveren van al deze bestellingen zijn digitale systemen onmisbaar.*


# Bijlagen

## Financiële onderbouwing

Dit kabinet heeft evenals het vorige kabinet structurele middelen vrijgemaakt die specifiek zijn gelabeld voor het verhogen van de digitale weerbaarheid. Het vorige kabinet heeft 95 miljoen structureel geïnvesteerd in de versterking van digitale weerbaarheid.[48] Dit kabinet investeert een extra 111 miljoen euro structureel in cybersecurity, de verdeling per departement is hieronder weergegeven. Deze middelen maken deel uit van een bredere structurele investering van 300 miljoen waarmee onder andere de AIVD en MIVD worden versterkt en investeringen worden gedaan op het gebied van economische veiligheid en de vitale infrastructuur.

De structurele investering van 111 miljoen draagt bij aan het uitvoeren van de verschillende acties die de departementen ondernemen ten behoeve van de realisatie van de doelen uit de strategie.[49] Daarnaast is digitale weerbaarheid onderdeel van andere investeringen die dit kabinet doet onder andere in digitalisering in brede zin, de versterking van de eigen ICT-infrastructuur of investeringen op specifieke beleidsterreinen. Voorbeelden hiervan zijn de versterking van het postennetwerk, hier zitten bijvoorbeeld ook cyberdiplomaten bij of de versterking van Defensie waarvan een deel ook geïnvesteerd zal worden in cybercapaciteit. Waar geen additionele investeringen mogelijk zijn en toch een opgave ligt zal herprioritering binnen de eigen begrotingen plaatsvinden. Tenslotte wordt er nog gekeken naar de mogelijkheid om aanvullende activiteiten te financieren via de Europese digitaliseringsfondsen. Daarnaast kunnen generieke nationale fondsen zoals het groeifonds ook ingezet worden voor digitale weerbaarheid. Naast middelen zijn er ook andere kritieke randvoorwaarden waar aan moet worden voldaan voor het realiseren van de acties. Hierbij behoeft voldoende capaciteit op de arbeidsmarkt met name de aandacht.

| Departement | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 en verder |
|---|---|---|---|---|---|---|
| EZK | 2,1 | 6,6 | 13,5 | 13,5 | 13,5 | 16,1 |
| IenW | 0,5 | 1,1 | 2,3 | 2,3 | 2,3 | 2,8 |
| JenV | 8,7 | 14,8 | 29,5 | 29,5 | 29,5 | 35,5 |
| Waarvan NCSC | 6,6 | 13,7 | 27,5 | 27,5 | 27,5 | 33 |
| BZK | 5,9 | 13,5 | 27,2 | 27,2 | 27,2 | 32,6 |
| Waarvan AIVD | 3,8 | 7,9 | 15,9 | 15,9 | 15,9 | 19,1 |
| BZ | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,7 |
| DEF | 3,4 | 7,1 | 14,2 | 14,2 | 14,2 | 17 |
| Waarvan MIVD | 3,4 | 7,1 | 14,2 | 14,2 | 14,2 | 17 |
| OCW | 0,5 | 1,3 | 2,7 | 2,7 | 2,7 | 3,2 |
| VWS | 0,5 | 1,3 | 2,7 | 2,7 | 2,7 | 3,2 |
| **TOTAAL** | **22,1** | **46,2** | **92,6** | **92,6** | **92,6** | **111** |

## Afkortingen

| | |
|---|---|
| AI | Artificiële intelligentie |
| AIVD | Algemene Inlichtingen- en Veiligheidsdienst |
| CERT | Computer Emergency Response Team |
| CDINEV | Commissie Defensie, Internationale, Nationale en Economische Veiligheid |
| CSBN | Cybersecuritybeeld Nederland |
| CSIRT | Computer Security and Incident Response Team |
| CSR | Cyber Security Raad |
| DOCS | Directeuren overleg Cybersecurity |
| DSP-CSIRT | Cyber Security Incident Response Team voor digitale dienstverleners |
| DTC | Digital Trust Center |
| ECCC | European Cybersecurity Competence Centre |
| EU | Europese Unie |
| FIOD | Fiscale Inlichtingen- en Opsporingsdienst |
| GGE | Group of Governmental Experts |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICT | Informatie- en communicatietechnologie |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IOCS | Interdepartementaal overleg cybersecurity |
| MIVD | Militaire Inlichtingen- en Veiligheidsdienst |
| NCC | Nationaal Crisiscentrum |
| NCSA | Nederlandse Cybersecurity Agenda 2018 |
| NCSC | Nationaal Cyber Security Centrum |
| NCTV | Nationaal Coördinator Terrorismebestrijding en Veiligheid |
| NLCS | Nederlandse Cybersecuritystrategie |
| NIB2 | Netwerk- en Informatiebeveiligingsrichtlijn (herziening) |
| OEWG | Open Ended Working Group |
| OM | Openbaar Ministerie |
| PoA | Program of Action |
| RDINEV | Raad Defensie, Internationale, Nationale en Economische Veiligheid |
| SEA | Strategische Evaluatie Agenda |
| VN | Verenigde Naties |
| Wbni | Wet Beveiliging Netwerk en Informatiesystemen |



## Begrippenlijst

Op basis van het CSBN zijn de belangrijkste begrippen als volgt gedefinieerd:

**Belang**: waarden, verworvenheden, materiële en immateriële zaken waaraan schade kan ontstaan als een cyberincident zich voordoet en het gewicht dat de maatschappij of een partij aan de verdediging ervan toekent. In het CSBN ligt de focus op nationale veiligheidsbelangen.

**Aanval**: moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van één of meer digitale processen.

**Cybercriminaliteitsbestrijding**: bestrijding van criminaliteit waarbij een computersysteem wordt aangevallen of misbruikt voor criminele activiteiten. Cybercrimebestrijding is een integraal onderdeel van de cybersecurity aanpak.

**Cyberincident**: (samenhangende set van) gebeurtenissen of activiteiten die kunnen leiden tot verstoring van één of meer (digitale) processen. Dit omvat zowel een cyberaanval (moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van een of meer digitale processen) als uitval als gevolg van bijvoorbeeld natuurlijke of technische oorzaken of menselijke fouten.

**Cybersecurity**: het geheel aan maatregelen om relevante risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risico-afweging.

**Digitale veiligheid**: het ongestoord functioneren van informatie-en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen.

**Digitaal proces (hierna: proces)**: een proces dat geheel of gedeeltelijk wordt uitgevoerd door de complexe en onderling samenhangende interactie tussen mensen en vele componenten van hardware, software en/of netwerken. Volledig geautomatiseerde processen, zoals procesbesturingssystemen, vallen ook onder het begrip.

**Digitale ruimte**: de complexe omgeving die het resultaat is van onderling verweven digitale processen, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT)-apparaten en verbonden netwerken. De digitale ruimte wordt vanuit drie invalshoeken of lagen benaderd: 1) digitale processen uitgevoerd (of in gang gezet) door mensen, 2) de technische laag (van IT en OT) die de digitale processen mogelijk maakt, 3) risicomanagement- en/of governance laag die de twee andere lagen bestuurt.

**Dreiging**: een cyberincident dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten.

**Maatschappelijke organisaties**: Maatschappelijke organisaties functioneren in een spanningsveld tussen overheid, markt en gemeenschap. Maatschappelijke organisaties zijn in de regel organisaties met een maatschappelijke doelstelling en geen winstoogmerk. In deze strategie worden hier o.a. stichtingen en samenwerkingsverbanden mee bedoeld die een bijdrage leveren aan het verhogen van cybersecurity in Nederland en daarbuiten.

**Medeoverheden**: bestaat uit provincies, gemeenten en waterschappen.

**Multi-factor authenticatie**: Methode om vast te stellen of een gebruiker of digitaal systeem wel is wie of wat hij zegt te zijn. Je gebruikt hiervoor verschillende manieren. Bijvoorbeeld een wachtwoord en een code die de gebruiker per sms krijgt. Of een combinatie van een vingerafdruk en een wachtwoord.

**Organisaties**: het geheel van overheidsorganisaties, bedrijven, kennisinstellingen en maatschappelijke organisaties.

**Overheid**: de totale overheid bestaat uit de Rijksoverheid, provincies, gemeenten en waterschappen.

**Phishing**: Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.

**Publieke waarden**: een afspiegeling van wat een samenleving als belangrijke waarden beschouwt, zoals veiligheid, democratie, zelfbeschikking, non-discriminatie, participatie, privacy en inclusiviteit.
Rijksoverheid: De Rijksoverheid bestaat uit 12 ministeries, veel uitvoerende diensten, inspecties en de Hoge Colleges van Staat.

**Risico**: de kans dat een dreiging leidt tot een cyberincident en de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid.

**Security by default**: betekent dat de configuratie uitgaat van de meest veilige instellingen.

**Security by design**: betekent dat veiligheid wordt meegenomen al in de ontwerpfase.

**Uitval**: een situatie waarin één of meer digitale processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van menselijke fouten.

**Veiligheidsregio**: Een veiligheidsregio is een gebied waarin wordt samenwerkt door verschillende besturen en diensten ten aanzien van taken op het terrein van brandweerzorg, rampenbeheersing, crisisbeheersing, geneeskundige hulpverlening en handhaving van de openbare orde en veiligheid. Nederland kent 25 veiligheidsregio's.



**Verstoring**: een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(verwerking), dat wil zeggen, een verstoring in de technische laag van de digitale ruimte.

**Weerbaarheid**: het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid, is de uitkomst van een risico-afweging. Die risico-afweging kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen.

Voor meer uitleg van cybersecurity termen verwijzen we u graag door naar het Cybersecurity Woordenboek van de Cybersecurity Alliantie.

# Noten

1 Hoofdlijnen beleid voor digitalisering (Kamerstukken II, 2021-22, 26 643, nr. 842 herdruk).
2 NCTV, 'Cybersecuritybeeld Nederland', 2022 en Glossary NIST Computer Security Resource Center.
3 NCTV, 'Cybersecuritybeeld Nederland', 2022.
4 Hoofdlijnen beleid voor digitalisering (Kamerstukken II, 2021-22, 26 643, nr. 842 herdruk).
5 De zes nationale veiligheidsbelangen, zoals beschreven in de Nationale Veiligheid Strategie (NVS) kunnen ieder worden geraakt via de digitale ruimte.
6 NCTV, 'Cybersecuritybeeld Nederland', 2021.
7 AIVD, 'Tweede Kamer geïnformeerd over prioriteiten en accenten AIVD voor 2022', 2021.
8 NCTV, 'Cybersecuritybeeld Nederland', 2018-2022; Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', 2021. Cyber Security Raad, 'Integrale aanpak cyberweerbaarheid', 2021.
9 Risicomanagement blijkt vaak organisatorisch complex te zijn. Pijnpunten zijn onder andere het in kaart brengen van informatiestromen, het bewaren van een overzicht van hardware en software, het bijhouden van ontwikkelingen, en het consequent actueel houden van risico's.
10 Voor het kabinet staat digitale autonomie van de EU voor het vermogen om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes haar publieke belangen in de digitale wereld te borgen en digitaal weerbaar te zijn in een onderling verbonden wereld (Kamerstukken II, 2021-22, 26 643, nr. 842).
11 Deze werksessies en de bijeenkomsten om met partijen specifieke doelen te formuleren, zijn begeleid door De ArgumentenFabriek (www.argumentenfabriek.nl).
12 De uitkomst van de enquête en sessies met belanghebbenden is gepubliceerd op www.nctv.nl
13 De term CSIRT wordt in deze strategie gebruikt om te refereren aan een CSIRT, zoals gedefinieerd in NIB1 en NIB2.
14 Zie voor een nadere detaillering van deze twee sporen de brief over de integrale aanpak cybercrime die in november 2022 naar de Tweede Kamer zal worden verstuurd.
15 Cyber Security Raad, 'Integrale aanpak Cyberweerbaarheid', 2021.
16 Zie ook de doelen in Pijler III.
17 Zie voor meer informatie over schakelorganisaties https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds en samenwerkingsverbanden https://www.digitaltrustcenter.nl/samenwerkingsverbanden.
18 De term CSIRT wordt in deze strategie gebruikt om te refereren aan een CSIRT zoals gedefinieerd in NIB1 en NIB2.
19 Voorstel Richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148;
Voorstel Richtlijn van het Europees Parlement en de Raad betreffende de veerkracht van kritieke entiteiten (CER-richtlijn).
20 Andere veelgebruikte termen voor operationele technologie zijn o.a. *Industrial Control Systems* (ICS), ICS *Supervisory Control and Data Acquisition* (SCADA), industriële controlesystemen en *Industrial Automation & Control Systems* (IACS).
21 Zie ook de doelen in Pijler II.
22 Zoals de Algemene Beveiligingseisen voor Defensieopdrachten 2019 (ABDO); het voorstel voor een herziene Network *Code for cybersecurity aspects of cross-border electricity flows* als verdere uitwerking van de Verordening van het Europees Parlement en de Raad betreffende de interne markt voor elektriciteit; het voorstel voor een verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector.
23 Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', 2021.
24 Zie ook de doelen in Pijler II.
25 Hier wordt het verhalen van schade bedoeld door de afnemer bij de leverancier als gevolg van het niet voldoen aan gestelde beveiligingsvereisten voor de veiligheid van hun product of dienst.
26 Zie ook het Evaluatierapport Roadmap Digitaal Veilige Hard- en Software (Kamerstukken II, 2021-2022, 26643, nr. 867).
27 Op basis van een gedelegeerde handeling onder de Europese richtlijn voor radio apparatuur, de *Radio Equipment Directive*, 2014/53/EU; De Europese cyberbeveiligingverordening, of *Cyber Security Act*, 2019/881; De uitvoeringswet cyberbeveiligingsverordening.
28 Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud; Op basis van de EU verordening voor medische apparatuur, 2017/745.
29 VN-Reglement nr. 155 — Uniforme bepalingen voor de goedkeuring van voertuigen met betrekking tot cyberbeveiliging en het beheersysteem voor cyberbeveiliging.
30 Met horizontale maatregelen worden niet-sector specifieke maatregelen bedoeld.



31 De nadruk binnen deze pijler ligt op het aanpakken van statelijke actoren en criminelen omdat hier de voornaamste dreiging voor Nederlandse belangen vanuit gaat. Dit laat onverlet dat ook andere kwaadwillende actoren een dreiging kunnen vormen, zoals hacktivisten. Waar relevant kunnen activiteiten die bijdragen aan het bereiken van doelen in deze pijler ook ten goede komen aan de aanpak van andere kwaadwillende actoren.
32 Zie ook de doelen in Pijler I.
33 Zie ook de doelen in Pijler I.
34 Naast de genoemde organisaties zijn er ook andere opsporingsdiensten die in specifieke gevallen een rol kunnen spelen om kwaadwillende actoren op te sporen, aan te pakken en te verstoren zoals de Douane, de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) en de Koninklijke Marechaussee.
35 Als het laatste redmiddel kan Defensie zowel onder normale als in buitengewone omstandigheden (extra) voortzettingsvermogen leveren ter ondersteuning van het civiele gezag.
36 Resolutie door de Algemene Vergadering van de Verenigde Naties (A/RES/53/70) over 'developments in the field of information and telecommunications in the context of international security', 1998.
37 Verenigde Naties, 'Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security', 2021; Verenigde Naties, 'Open-ended working group on developments in the field of information and telecommunications in the context of international security: final substantive report', 2021.
38 NCTV, 'Cybersecuritybeeld Nederland, 2022.
39 Behavioural Insights Netwerk Nederland, 'Gedragsadviezen Gedragswetenschappelijk perspectief op vijf grote maatschappelijke vraagstukken: klimaat, digitalisering, kansengelijkheid, wonen en niet-gebruik van voorzieningen', 2022.
40 Centraal Bureau voor de Statistiek, 'de Veiligheidsmonitor 2022', 2022.
41 Deze pijler hangt nauw samen met de bestrijding van cybercriminaliteit zoals ook in pijler 4 aan bod komt.
42 Cyber Security Raad, 'Integrale aanpak cyberweerbaarheid', 2021.
43 Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', 2021.
44 In lijn met motie van het lid Amhaouch c.s. over een analyse van de effectiviteit van initiatieven om personeelstekorten in de techniekssector op te lossen (Kamerstukken II, 2021-2022, 35925 XIII, nr. 38).
45 Cyber Security Raad, 'Advies inzake de focus en aanpak van het evaluatieonderzoek van de Nederlandse Cybersecurity Agenda (NCSA)', 2020.
46 https://www.toolboxbeleidsevaluaties.nl
47 Kamerstukken II 2020-2021, 26643, nr. 763.
48 Zie voor de verdeling per departement Budgettair overzicht bij het regeerakkoord 'Vertrouwen in de toekomst', 2017.
49 Een deel van de acties baseert zich op de implementatie van Europese regelgeving, zoals NIB2, CER en CRA, waarvoor de onderhandelingen nog lopen. De precieze benodigde investeringen voor deze trajecten zijn momenteel nog niet te overzien.

Oktober 2022

Deze publicatie is een uitgave van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) namens de Rijksoverheid.
**info@nctv.minjenv.nl**