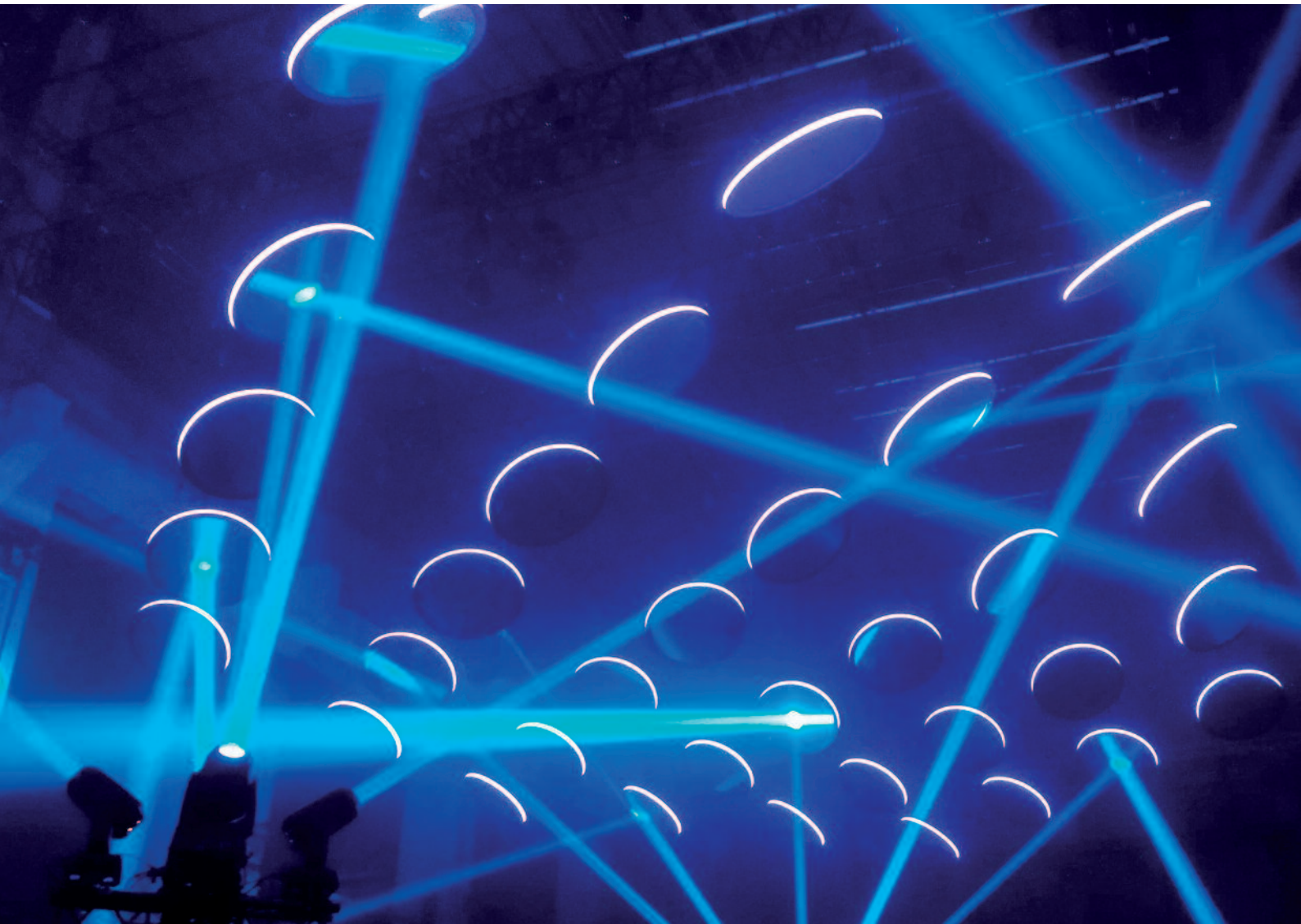
Nederlandse Cybersecurity Agenda

Nederland digitaal veilig



Inhoudsopgave

Voorwoord

Veiligheid in het digitale domein is voor het kabinet een topprioriteit. Daarom hebben we in het regeerakkoord een structurele investering van 95 miljoen euro in cybersecurity vastgelegd. De afgelopen maanden is door verschillende departementen, in nauwe samenwerking met partijen uit de publieke én private sector, de wetenschap en de samenleving, hard gewerkt aan een ambitieuze kabinetsbrede Nederlandse Cybersecurity Agenda. Als coördinerend minister voor cybersecurity ben ik trots om het product van deze vruchtbare samenwerking te mogen presenteren!

We hebben zeven stevige ambities opgesteld, die in samenhang zullen bijdragen aan een veilig digitaal Nederland. Cruciaal in dit geheel is dat Nederland zijn digitale slagkracht op orde heeft. Overheidspartijen en private organisaties in Nederland moeten goed samenwerken aan een integrale aanpak van cybersecurity. Als alle partijen hun verantwoordelijkheid nemen en over adequate capaciteiten en middelen beschikken, kunnen we daadkrachtig reageren op digitale dreigingen.

Voor de overheid betekent dat vooral: een krachtige regierol, stimuleren en voorwaarden scheppen. Zodat bedrijfsleven en burgers hun eigen digitale veiligheid en weerbaarheid kunnen vormgeven. Want daar blijven ze uiteraard zelf verantwoordelijk voor. Om de kansen van digitalisering te kunnen blijven benutten, is het noodzakelijk dat we ons veilig in de digitale wereld kunnen bewegen. Cybersecurity is het fundament voor succesvol ondernemen en besturen en voor het vertrouwen in het digitale domein: dit gedeelde belang maakt dat we wederzijds afhankelijk zijn en een gezamenlijke verantwoordelijkheid dragen voor de nationale veiligheid. Omdat landsgrenzen in de cyberwereld nauwelijks een rol spelen, zal die aanpak ook sterk internationaal georiënteerd moeten zijn. Ook in EU- en NAVO-verband blijft Nederland daarom werken aan versterking van de digitale veiligheid.

De komende maanden zullen we de ambities uit de Nederlandse Cybersecurity Agenda, in nauwe samenwerking met de betrokken departementen en overige partners, nader uitwerken in concrete maatregelen.

En uiteraard is deze agenda niet in beton gegoten. De komende jaren blijft het zaak de vinger goed aan de pols te houden en technologische en maatschappelijke ontwikkelingen nauwgezet te volgen, om te zien waar zich mogelijk nieuwe digitale kwetsbaarheden en dreigingen voordoen.

We zetten met de presentatie van deze Nederlandse Cybersecurity Agenda een cruciale stap naar een veiliger digitaal Nederland. De basis waarop we verder kunnen bouwen aan een veilig cyberdomein, waarin burgers, bedrijfsleven en overheden de economische en maatschappelijke kansen die de digitalisering biedt, ook echt kunnen verzilveren!

Ferd Grapperhaus
Minister van Justitie en Veiligheid

Samenvatting

Nederland beschikt over een uitstekende uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. Tegelijkertijd nemen kwetsbaarheden en dreigingen in het digitale domein toe. De dreiging vanuit beroepscriminelen groeit en blijft zich verder ontwikkelen. Statelijke actoren richten zich op digitale economische en politieke spionage en het treffen van voorbereidingen op digitale sabotage. Niet alleen het aantal landen dat digitale aanvalscapaciteiten ontwikkelt neemt toe, de ingezette aanvallen worden ook steeds complexer. Dit vormt een directe dreiging voor onze economische belangen en de nationale veiligheid.

Dit vraagt om extra inspanningen om de cybersecurity aanpak te versterken en zo de vitale belangen van Nederland beter te beschermen. In de Nederlandse Cybersecurity Agenda (NCSA) worden de kaders gesteld voor de volgende noodzakelijke stap in cybersecurity. De gezamenlijke koers wordt aangegeven en verschillende maatregelen worden in samenhang bezien. Dit versterkt de impact van publieke en private acties. Hierbij zijn de volgende uitganspunten leidend:

- Cybersecurity is onlosmakelijk verbonden met nationale veiligheid: door digitalisering zijn nationale veiligheidsbelangen kwetsbaar voor digitale aanvallen.
- Veiligheid in het digitale domein kan alleen in samenwerking met en deels ook door het bedrijfsleven worden vormgegeven. Publiek-private samenwerking staat daarom aan de basis van de Nederlandse cybersecurity aanpak.
- De overheid is er voor de publieke belangen: een digitaal veilig Nederland, door onderkenning van dreigingen tegen vitale belangen en versterking van de weerbaarheid. Bedrijfsleven en burgers worden gestimuleerd om zo goed mogelijk hun eigen verantwoordelijkheid en veiligheid vorm te geven. Ook is de overheid, als publiek orgaan, gehouden de cybersecurity van de eigen processen op orde te hebben en als *launching customer* het goede voorbeeld te geven.
- Kennis is cruciaal voor cybersecurity: het publiek en privaat delen van beschikbare kennis en het bevorderen van informatiedeling is nodig om cybersecurity in de breedte te versterken. Daarnaast is het noodzakelijk om zowel fundamenteel als toegepast onderzoek naar cybersecurity te (blijven) entameren, om de Nederlandse cybersecurity kennispositie te ontwikkelen.
- Het *mainstreamen* van cybersecurity is het doel: de digitale veiligheid moet in iedere organisatie onderdeel zijn van de dagelijkse processen.
- Het digitale domein is niet gebonden aan landsgrenzen. Een Nederlandse aanpak voor cybersecurity moet zich rekenschap geven van de internationale dimensie van data, verbindingen, internet *governance* en actoren die digitale aanvallen uitvoeren. Een veiliger digitaal domein is daarom een van de speerpunten van Nederland in onder meer NAVO- en EU-verband.
- Tot slot: waardenspanning tussen vrijheid, veiligheid en economische groei is inherent aan de ontwikkeling van cybersecurity. Door ons hier rekenschap van te geven willen we dilemma's in cybersecurity scherper wegen, en op basis van transparante en gefundeerde besluitvorming richting bepalen.

De NCSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: ***Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.***

1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software.
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur.
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime.
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling.
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

Deze zeven ambities zijn uitgewerkt in doelstellingen en maatregelen, die in nauwe publiek-private samenwerking zullen worden uitgevoerd. Hiertoe wordt een cybersecurity alliantie gesloten, met overheidspartijen en bedrijven die zich committeren aan het gezamenlijk versterken van de cybersecurity aanpak in Nederland.

Cybersecurity

het fundament voor economische kansen en maatschappelijke waarden in het digitale domein

Nederland is een van de meest gedigitaliseerde landen ter wereld. We beschikken daarmee over uitstekende voorwaarden om internationaal koploper te zijn, in het veilig en in vrijheid snel nieuwe technologieën uitrollen en gebruiken. Die nieuwe technologieën spelen een steeds belangrijkere rol in ons dagelijks leven. Denk bijvoorbeeld aan *e-commerce*, maar ook aan digitale communicatie met de dokter, de school en de overheid. Verdergaande digitalisering in de zorg (*e-health*), mobiliteit (*e-automotive*), toename van gebruiksvoorwerpen met een internetverbinding (*Internet of Things*), sleuteltechnologieën als *big data*, 5G, kwantumcomputers, en kunstmatige intelligentie zorgen er bovendien voor dat het cyberdomein en het fysieke domein meer met elkaar vervlochten raken. Deze ontwikkelingen brengen ook ethische kwesties aan het licht ten aanzien van privacy en omgang met data. Het beschermen van waarden en grondrechten in het digitale domein is eveneens een belangrijk onderdeel van cybersecurity. Burgers moeten er op kunnen rekenen dat hun grondrechten zowel online als offline gewaarborgd zijn en dat hun privacy ook in het digitale domein gegarandeerd is.

Met deze technologische en maatschappelijke ontwikkelingen zijn ook de kwetsbaarheden in het digitale domein toegenomen, een trend die zich naar verwachting de komende jaren zal voortzetten. Juist omdat elk aspect van de samenleving - maatschappelijk en economisch - in toenemende mate afhankelijk is van digitale processen, kunnen digitale aanvallen directe schade toebrengen aan onze economie en de nationale veiligheid bedreigen. Maatschappelijke processen kunnen immers makkelijker op grote schaal verstoord raken. De toegenomen kwetsbaarheid blijkt uit de opeenvolgende Cybersecuritybeelden Nederland, waarin Nederlandse inlichtingen- en veiligheidsdiensten, de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Nationaal Cybersecurity Centrum (NCSC) en de politie een zorgwekkende toename van digitale dreigingen signaleren. Bovendien blijft de weerbaarheid achter ten opzichte van de ontwikkeling van de dreiging. Deze situatie vraagt om extra inspanningen van overheden, bedrijfsleven en burgers om de belangen van Nederland te beschermen en de Nederlandse cybersecurity aanpak te versterken ten behoeve van de nationale veiligheid.

Definitie van cybersecurity
Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.

Tegelijkertijd biedt cybersecurity als sector ook economische en maatschappelijke kansen: een sterke Nederlandse cybersecurity sector stimuleert kennisontwikkeling, de arbeidsmarkt en werkgelegenheid, en draagt bij aan het internationale profiel van Nederland op economisch, militair en veiligheidsgebied. Bovendien draagt een sterke

Nederlandse cybersecurity sector bij aan digitale autonomie: overheden en bedrijfsleven kunnen rekenen op eigen oplossingen voor digitale veiligheid en stimuleren door afname van cybersecurity dienstverlening voor de eigen processen ook digitale veiligheid in den brede. Deze stimulans bevordert bovendien de export van Nederlandse waarden als een open, vrij en veilig internet. Nederland versterkt op deze wijze ook internationaal zijn positie als gekende en erkende samenwerkingspartner en cybersecurity autoriteit.

DE SCOPE VAN CYBERSECURITY: NEDERLAND DIGITAAL VEILIG

De minister van Justitie en Veiligheid is coördinerend bewindspersoon voor cybersecurity en voert regie op de uitvoering van de NCSA. Daarbinnen houdt iedere partij zijn eigen taken en verantwoordelijkheden. Daarbij geldt dat ook in het digitale domein 100% veiligheid niet realistisch is. Deze brede Nederlandse cybersecurity aanpak krijgt vorm als onderdeel van het beschermen van de nationale veiligheid, dat gecoördineerd wordt door de NCTV.

BELEIDSVERANTWOORDELIJKHEDEN IN HET DIGITALE DOMEIN

Het beleidsterrein cybersecurity richt zich op het voorkomen van schade door verstoring, uitval en misbruik van ICT. Hieraan zijn verschillende beleids-thema's verwant die onder verantwoordelijkheid van andere bewindspersonen worden vormgegeven. In het bijzonder gaat het om het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) vanwege de verantwoordelijkheid voor de digitale overheid en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), het ministerie van Economische Zaken en Klimaat (EZK) in verband met digitalisering, het ministerie van Buitenlandse Zaken (BZ) vanwege de coördinerende rol op internationale vrede en veiligheid en tot slot het ministerie van Defensie (Def), aangaande de grondwettelijke taken van de krijgsmacht in het digitale domein. De NCSA is nauw verbonden met de volgende strategische documenten: de Digitaliseringsstrategie (in wording), de Brede Agenda Digitale Overheid (in wording), de Defensienota en de Geïntegreerde Buitenland- en Veiligheidsstrategie en de Internationale Cyberstrategie en Defensie Cyberstrategie (in wording).

Van Nationale Cybersecurity Strategie 2011 tot Nederlandse Cybersecurity Agenda 2018

De NCSA bouwt voort op de effecten die gerealiseerd zijn bij de eerdere Nationale Cybersecurity strategieën uit 2011 en 2013. De visie uit deze strategieën blijft leidend: *"Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt, volop worden benut, waarin aan dreigingen het hoofd wordt geboden en waarin fundamentele rechten en waarden worden beschermd."* De agenda geeft een gezamenlijke koers aan, waardoor het voor overheids- en private partijen inzichtelijker wordt waarop zij hun (afgestemde) activiteiten kunnen richten. De NCSA beziet verschillende maatregelen in samenhang, verbindt ze in richtinggevende doelstellingen en versterkt zo de impact ervan.

Spionage, sabotage en beroepscriminaliteit

dreigingen in het digitale domein

Digitale sabotage of verstoring kan direct leiden tot aantasting van de nationale veiligheid. De grootste dreiging op het digitale vlak wordt gevormd door criminelen en statelijke actoren. Digitalisering is doorgedrongen tot in de haarvaten van de Nederlandse maatschappij en economie. Hierdoor is onze samenleving volledig afhankelijk geworden van digitale middelen. Het ongestoord functioneren van deze middelen is essentieel voor vitale processen binnen bedrijfsleven en overheid, het verdienvermogen van ondernemingen en het dagelijks leven van burgers. Incidenten in de afgelopen jaren hebben duidelijk gemaakt dat digitale aanvallen een grote impact op de samenleving kunnen hebben en kunnen leiden tot aantasting van de fysieke en nationale veiligheid. De dreiging vanuit beroepscriminelen neemt toe en blijft zich verder ontwikkelen. Hierbij worden succesvolle criminele verdienmodellen, zoals *ransomware* verder ontwikkeld en uitgebreid. De vrijwel kosteloze schaalbaarheid van digitale aanvallen is extra interessant voor criminelen.

Niet alleen consumenten zijn het slachtoffer. Ook bedrijven en financiële instellingen zijn het doelwit van criminelen. Complexere aanvalsmethoden worden steeds breder beschikbaar, onder meer door ontwikkelingen als *cybercrime-as-a-service*. Hierdoor kunnen steeds meer actoren met beperkte kennis en middelen aanvallen uitvoeren die in voorkomende gevallen direct maatschappelijke effecten hebben.

Nederlandse overheidsinstellingen en in Nederland gevestigde bedrijven zijn structureel doelwit van digitale spionage door statelijke actoren. Zo zijn bijvoorbeeld multinationals en onderzoeksinstellingen in de energie-, *hightech*-, en chemische sector het slachtoffer geworden van digitale spionage. Bij deze digitale inbraken zijn *terabytes* aan vertrouwelijke gegevens gestolen die een substantiële economische waarde vertegenwoordigen. Statelijke actoren richten zich op digitale economische en politieke spionage, en treffen voorbereidingen op digitale sabotage. Niet alleen het aantal landen dat digitale aanvalscapaciteiten ontwikkelt neemt toe, de gebruikte aanvallen worden ook steeds complexer. Daarnaast hebben statelijke actoren zich het afgelopen jaar ook gericht op digitale beïnvloeding van democratische processen voor geopolitiek gewin. Om geopolitieke belangen te behartigen investeren staten in civiele en militaire cybercapaciteiten.

Voorbeeld: *Cybercrime-as-a-service* en *ransomware*
Cybercriminelen voeren lang niet alle stappen van een aanval zelf uit. Vaak kopen ze diensten en expertise bij elkaar in. Een voorbeeld daarvan is *ransomware*: een type schadelijke software dat systemen en/of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt. Als een crimineel *ransomware* wil verspreiden, betaalt hij bijvoorbeeld iemand om die te ontwikkelen en iemand anders om de *ransomware* via e-mail onder miljoenen geadresseerden te verspreiden. Deze diensten worden zeer professioneel en compleet geleverd: van technische hulpmiddelen tot infrastructuur en helpdeskfunctionaliteit.

Cyberaanvallen hebben hun weerslag op onze maatschappij. Burgers krijgen bijvoorbeeld te maken met de gevolgen van identiteitsdiefstal of het verlies van persoonlijke foto's door een *ransomware* besmetting. In potentie ondermijnt dit het vertrouwen in de digitale samenleving. Cyberaanvallen door criminele of statelijke actoren kunnen de Nederlandse economie ondermijnen door diefstal van gevoelige of kostbare informatie en daarmee het vertrouwen in het economisch verkeer schaden.

Voorbeeld: *NotPetya*
De casus *NotPetya* is een voorbeeld van een digitale aanval met aanzienlijke gevolgen voor Nederlandse bedrijven. In juni 2017 werden organisaties wereldwijd het slachtoffer van een aanval met *ransomware*. In Nederland heeft deze *ransomware* onder meer de bedrijfsvoering van de containerterminal van APM en pakketbezorger TNT aangetast. Bij APM heeft de afhandeling van containers dagenlang stilgelegen. Ook TNT heeft door de aanval vertragingen bij de bezorging gekend. Hoewel Oekraïne het primaire doelwit van deze aanval leek te zijn, waren de gevolgen voor Nederlandse bedrijven aanzienlijk.

Strategische uitgangspunten

Een effectieve cybersecurity aanpak houdt rekening met de dynamiek die het digitale domein eigen is. Dit vraagt om strategische uitgangspunten voor het bepalen van de ambities en maatregelen.

CYBERSECURITY IS INTEGRAAL ONDERDEEL VAN DE NATIONALE VEILIGHEID

Cybersecurity is onlosmakelijk verbonden aan nationale veiligheid en het ongestoord functioneren van de maatschappij. Door digitalisering wordt de maatschappij kwetsbaar voor verstoringen door digitale aanvallen. Door de connectiviteit van de digitale samenleving kunnen eenvoudige digitale aanvallen snel digitale processen verstoren. Om de weerbaarheid hiertegen te vergroten is een basisniveau van cybersecurity noodzakelijk. Burgers, bedrijven en overheden moeten inspanningen leveren om hun digitale veiligheid te vergroten. Ook moet de overheid zijn beschermende taak in het digitale domein kunnen waarmaken. Capaciteiten en middelen om dreigingen het hoofd te bieden op orde te zijn. Tot slot dient ook nationale veiligheid en cybersecurity een basisoverweging te zijn bij verdere ontwikkeling van digitale processen van de overheid. Dit betekent dat de overheid nadere cybersecurity eisen zal ontwikkelen voor inkoop van eigen ICT-middelen. Bij deze eisen zullen ook economische veiligheidsoverwegingen worden meegenomen om de weerbaarheid tegen statelijke actoren te verhogen.

PUBLIEKE-PRIVATE SAMENWERKING IS DE BASIS

Veiligheid in het digitale domein kan alleen in samenwerking met, en voor een belangrijk deel ook door, het bedrijfsleven worden vormgegeven. Publiek-private samenwerking staat daarom aan de basis van de Nederlandse cybersecurity aanpak. De huidige praktijk van deze samenwerking laat zien dat er behoefte is aan een heldere verdeling van verantwoordelijkheden in het digitale domein. Deels zullen die verantwoordelijkheden hun basis hebben in de bestaande wet- en regelgeving over veiligheid, leveringszekerheid en marktordening. Echter, er ontstaan ook nieuwe vraagstukken waar de verantwoordelijkheden tussen overheid, bedrijfsleven en burger (opnieuw) bepaald moeten worden. Daarom zet deze agenda in op een integrale cybersecurity aanpak, die gezamenlijke inzet vraagt van het bedrijfsleven, maatschappelijke organisaties en van verschillende overheidspartijen.

OVERHEID STAAT VOOR DE PUBLIEKE BELANGEN, STIMULEERT DE EIGEN VERANTWOORDELIJKHEID EN GEEFT HET GOEDE VOORBEELD

Een kerntaak van de overheid is het voortouw te nemen bij het streven naar een veilig en stabiel Nederland door dreigingen tegen vitale belangen te onderkennen en de weerbaarheid van die belangen te versterken. Dat betekent dat de overheid zorgt voor een adequate aanpak van en voorbereiding op crises en incidenten, waar de maatschappelijke continuïteit in het geding is. Hoewel 100% veiligheid ook in het digitale domein onmogelijk is. Van de vitale infrastructuur is circa 80% in private handen. De overheid wil daarom het bedrijfsleven en burgers stimuleren om zo goed mogelijk hun eigen verantwoordelijkheid en veiligheid vorm te geven. Waar nodig worden er stimuli geboden of kaders ingericht om de randvoorwaarden te scheppen voor veilig gedrag in het digitale domein. Het open karakter van het internet kan leiden tot wijdverspreide kwetsbaarheden. Daar waar misbruik van producten, diensten of processen de continuïteit van de maatschappij in gevaar kan brengen, stelt de overheid bijzondere eisen aan producenten, afnemers, consumenten en dienstverleners. Tot slot is de overheid, als publiek orgaan, gehouden de cybersecurity van de eigen processen op orde te hebben en daarmee ook als *launching customer* het goede voorbeeld te geven.

KENNISONTWIKKELING EN INFORMATIEDELING IS CRUCIAAL

Kennis is cruciaal voor cybersecurity: het publiek en privaat delen van beschikbare kennis en het bevorderen van informatiedeling is nodig om breed de weerbaarheid op cybersecurity te versterken. Daarnaast is het noodzakelijk om zowel fundamenteel als toegepast onderzoek naar cybersecurity te (blijven) entameren, om de Nederlandse cybersecurity kennispositie te ontwikkelen. Wanneer we kunnen beschikken over eigen hoogwaardige wetenschappelijke kennis en toepassingen dan draagt dit bij aan de digitale autonomie van Nederland en/of Europa.

MAINSTREAMEN VAN CYBERSECURITY IS EEN VOORWAARDE

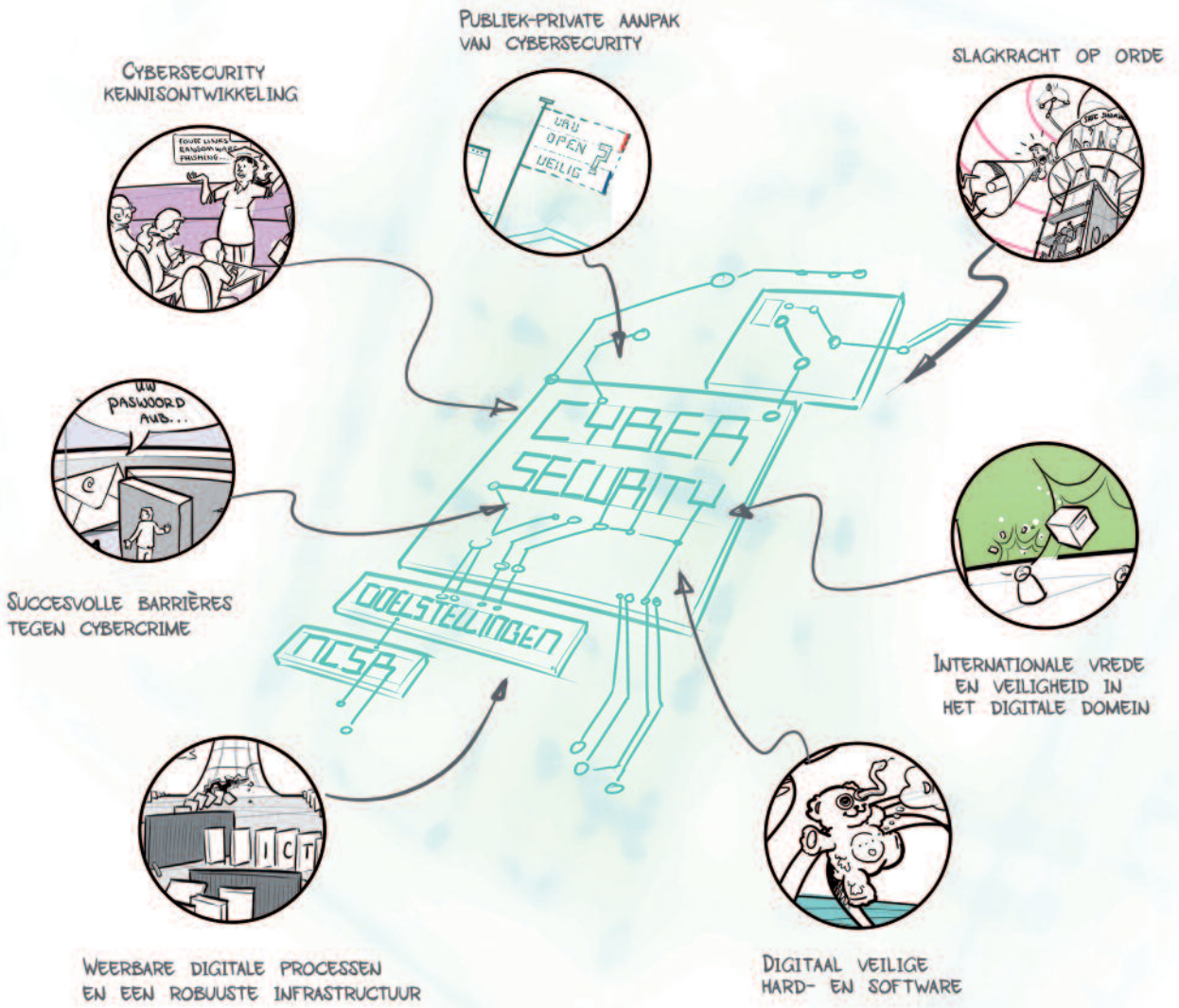
Digitalisering dringt door in alle facetten van de maatschappij. Cybersecurity staat aan de basis van succesvol ondernemen, besturen en veilig deelnemen aan het maatschappelijke verkeer. Het is noodzakelijk dat overheden en bedrijven beter in staat zijn of worden gesteld om hun digitale veiligheid te organiseren en die digitale veiligheid onderdeel maken van hun dagelijkse processen, producten en diensten (het *mainstreamen* van cybersecurity). Ook burgers en/of eindgebruikers hebben een verantwoordelijkheid in het beschermen van hun eigen digitale veiligheid: in het dagelijks leven hoort een basisniveau van cybersecurity onderdeel te zijn van veilig gedrag.

HET DIGITALE DOMEIN IS NIET NATIONAAL BEGRENSD

Het digitale domein is per definitie niet gebonden aan landsgrenzen. Een Nederlandse aanpak voor cybersecurity moet zich rekenschap geven van de internationale dimensie van data, verbindingen, internet *governance* en actoren die digitale aanvallen uitvoeren. Daarom is een veiliger digitaal domein een van de speerpunten van Nederland in EU- en NAVO-verband. Een bondgenootschap dat zijn collectieve verdedigingstaak ook vorm kan geven in het digitale domein, levert immers een directe en essentiële bijdrage aan de nationale (digitale) veiligheid van de lidstaten. Daarnaast zal een aantal doelstellingen van de NCSA slechts bereikt kunnen worden door middel van internationale wetgeving, coalitievorming of internationale ontwikkeling van normen en standaarden, in het bijzonder in Europees verband. Het grensoverschrijdende karakter van dreigingen maakt het noodzakelijk sterk in te zetten op internationale samenwerking. De Nederlandse Cybersecurity Agenda zal, in verbinding met de Geïntegreerde Buitenland- en Veiligheidsstrategie en de Defensienota, bij de verdere uitwerking dan ook richtinggevend zijn voor de Nederlandse inzet in internationale gremia. Enerzijds geldt dat voor die effecten en resultaten die alleen in internationaal verband kunnen worden bereikt, anderzijds zullen de internationale ontwikkelingen ook in acht worden genomen bij het effectief vormgeven van het Nederlandse beleid. Belangrijke voorbeelden zijn de Europese ontwikkelingen op het gebied van certificering, standaard-ontwikkeling en het stimuleren van de Europese Digitale Eengemaakte Markt, waarvan cybersecurity een onderdeel is. Nederland blijft op onderwerpen als fragiliteit van vrije software zijn rol als internetpionier vervullen.

WAARDENSPANNING VRAAGT OM ZORGVULDIGE WEGING

De verregaande digitalisering zet regelmatig de balans tussen de kernwaarden veiligheid, vrijheid en economische groei onder druk. Nederland zet in op een heldere afweging van de belangen bij het maken van (beleids)keuzes en betracht hierover transparantie. In brede maatschappelijke en politieke debatten over digitalisering, wordt cybersecurity niet geïsoleerd benaderd maar nadrukkelijk bezien in samenhang met onderwerpen als fundamentele rechten en waarden en maatschappelijke groei. Een duidelijke en transparante afweging van waardenspanning leidt tot betere besluitvorming.



Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen

De Nederlandse Cybersecurity Agenda

De Nederlandse aanpak van cybersecurity heeft het volgende doel:
Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.

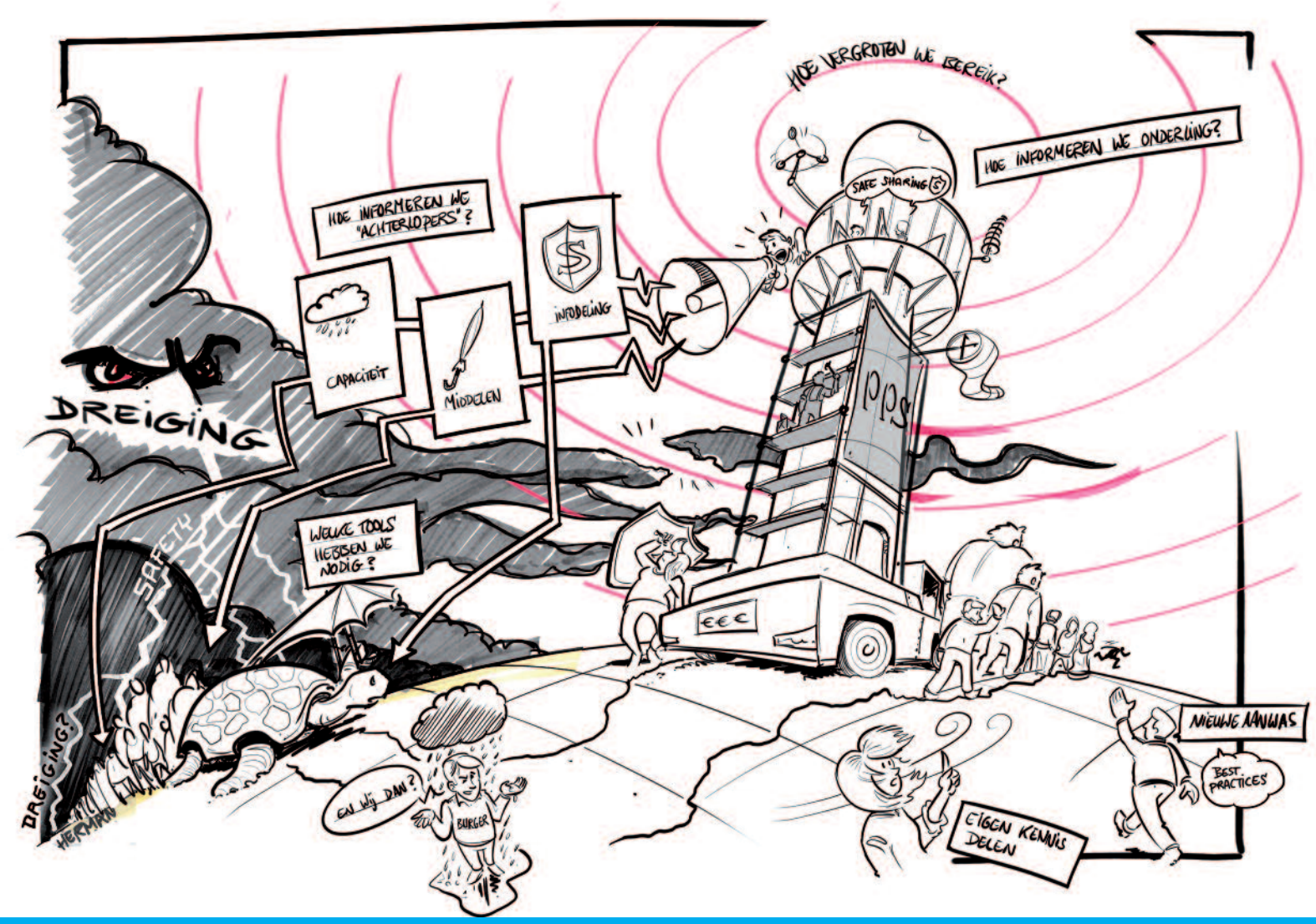
We zetten daarbij in op de volgende ambities:
1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software.
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur.
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime.
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling.
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

De impact van technologische en maatschappelijke ontwikkelingen en digitale dreiging, ontwikkelt zich met verschillende snelheden en vraagt om een dynamische meerjarige cybersecurity aanpak. Veel van deze maatregelen vragen om overheidsinzet. Sommige andere maatregelen kunnen alleen met of door marktpartijen worden vormgegeven. Dit vraagt om nauwe samenwerking in de uitwerking van de NCSA. De maatregelen zijn niet uitputtend. Er is ruimte voor aanvulling. Daarmee ontstaat er een dynamische aanpak die aangepast kan worden aan de ontwikkeling van de dreiging. Daarom zal jaarlijks bij het 'Cybersecuritybeeld Nederland' bezien worden of deze aanpak herijking behoeft en of beleidsinstrumenten bijdragen aan de verwezenlijking van de ambities. In 2021 wordt de agenda geëvalueerd en waar nodig herzien.

Regeerakkoord
Er wordt een ambitieuze cybersecurity agenda opgesteld met onder meer standaarden voor *Internet of Things* apparaten, software aansprakelijkheid, versterken van het NCSC, het stimuleren van cybersecurity onderzoek en het verbeteren van voorlichtingscampagnes.

Er wordt structureel 95 miljoen euro gereserveerd voor cybersecurity. De middelen worden onder andere ingezet voor de uitbreiding van personele capaciteit en ICT-voorzieningen en verdeeld over de departementen Justitie en Veiligheid (NCTV), Defensie (MIVD), Binnenlandse Zaken en Koninkrijksrelaties (AIVD), Buitenlandse Zaken, Infrastructuur en Milieu en Economische Zaken.

De structurele cybersecurity intensivering is geïntegreerd in de maatregelen van deze NCSA.



Nederland heeft zijn digitale slagkracht op orde

1. Slagkracht op orde

Om daadkrachtig te kunnen reageren op de toename van de digitale dreiging, moeten overheidspartijen en private organisaties in Nederland samenwerken en beschikken over adequate capaciteiten en middelen. Die capaciteiten zijn bij tal van deze organisaties nog volop in ontwikkeling, waarbij een verschillend niveau van volwassenheid zichtbaar is. Waar sommige (grotere) bedrijven en organisaties een eigen *security operations center* of computercrisisteam organiseren, zijn andere (kleinere) bedrijven of organisaties zich nog maar net of nog niet in voldoende mate bewust van digitale risico's. De beveiliging van de eigen digitale systemen en informatie van publieke en private partijen is daar nog niet vanzelfsprekend en basale beveiligingsvoorschriften zijn nog niet geïmplementeerd.

Voldoende slagkracht behelst ook de capaciteiten van veiligheidsorganisaties, die in staat moeten zijn om hun taken voor de nationale veiligheid ook in het digitale domein vorm te geven. Dit hangt nauw samen met de offensieve capaciteiten van Defensie, die ook onder ambitie 2 aan de orde komen.

Er is dringend behoefte aan opbouw van capaciteiten, aan meer en beter toegesneden informatie over digitale dreigingen, die sneller beschikbaar is voor overheidspartijen en private organisaties en aan handelingsperspectief om die dreigingen te mitigeren. De informatie-uitwisseling tussen organisaties en bedrijven is in Nederland de afgelopen jaren sterk verbeterd, door samenwerking bij incidenten of omdat de partijen elkaar hebben leren kennen en elkaar zijn gaan vertrouwen. Dat is een stap voorwaarts, maar het biedt nog niet voldoende garanties dat we nu en in de toekomst digitale dreigingen het hoofd kunnen bieden. De volgende stap is om informatie-uitwisseling en bestaande samenwerking structureel te borgen en tegelijkertijd breder in te richten, bijvoorbeeld door het bevorderen van cross-sectorale analyses. Het is noodzakelijk om de detectie- en responscapaciteiten van overheidsorganisaties en vitale aanbieders te versterken. Daarmee versterken we ook de digitale slagkracht van deze partijen. We moeten komen tot een praktijk waarin klanten en toeleveranciers elkaar onderling stimuleren om hun digitale veiligheid te organiseren. Zo werken we toe naar een cyber-ecosysteem waarin alle partijen capaciteiten opbouwen en informatie delen; van bedrijfsleven tot overheid en van burger tot informatiebeveiliger.

DOELSTELLINGEN

- Overheden en bedrijven zijn in staat een adequate respons te bieden op digitale dreigingen en aanvallen. Ze nemen hiervoor de benodigde (preventieve) maatregelen en ze hebben de basis op orde.
- Nederland is voorbereid op grootschalige cyberincidenten die de nationale veiligheid bedreigen.
- Organisaties die van vitaal belang zijn voor de nationale veiligheid hebben beter inzicht in digitale dreigingen en aanvallen, en zijn in staat om aanvallen die hen en daarmee de nationale veiligheid bedreigen, te detecteren.
- Er wordt een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden ingericht waarbinnen informatie over cybersecurity breder, efficiënter en effectiever wordt gedeeld tussen publieke en private partijen. Dit dekkende stelsel heeft tot doel de slagkracht van publieke en private partijen te versterken.
- Het juridisch instrumentarium om slagvaardig op te treden in het digitale domein blijft op orde en wordt geactualiseerd in het licht van de dreiging en de technologische ontwikkelingen.

MAATREGELEN

o Om snel te kunnen handelen bij ICT-inbreuken die de nationale veiligheid bedreigen, worden de incidentresponscapaciteiten van onder andere de inlichtingen- en veiligheidsdiensten, Defensie *Computer Emergency Response Team* (CERT), NCSC en

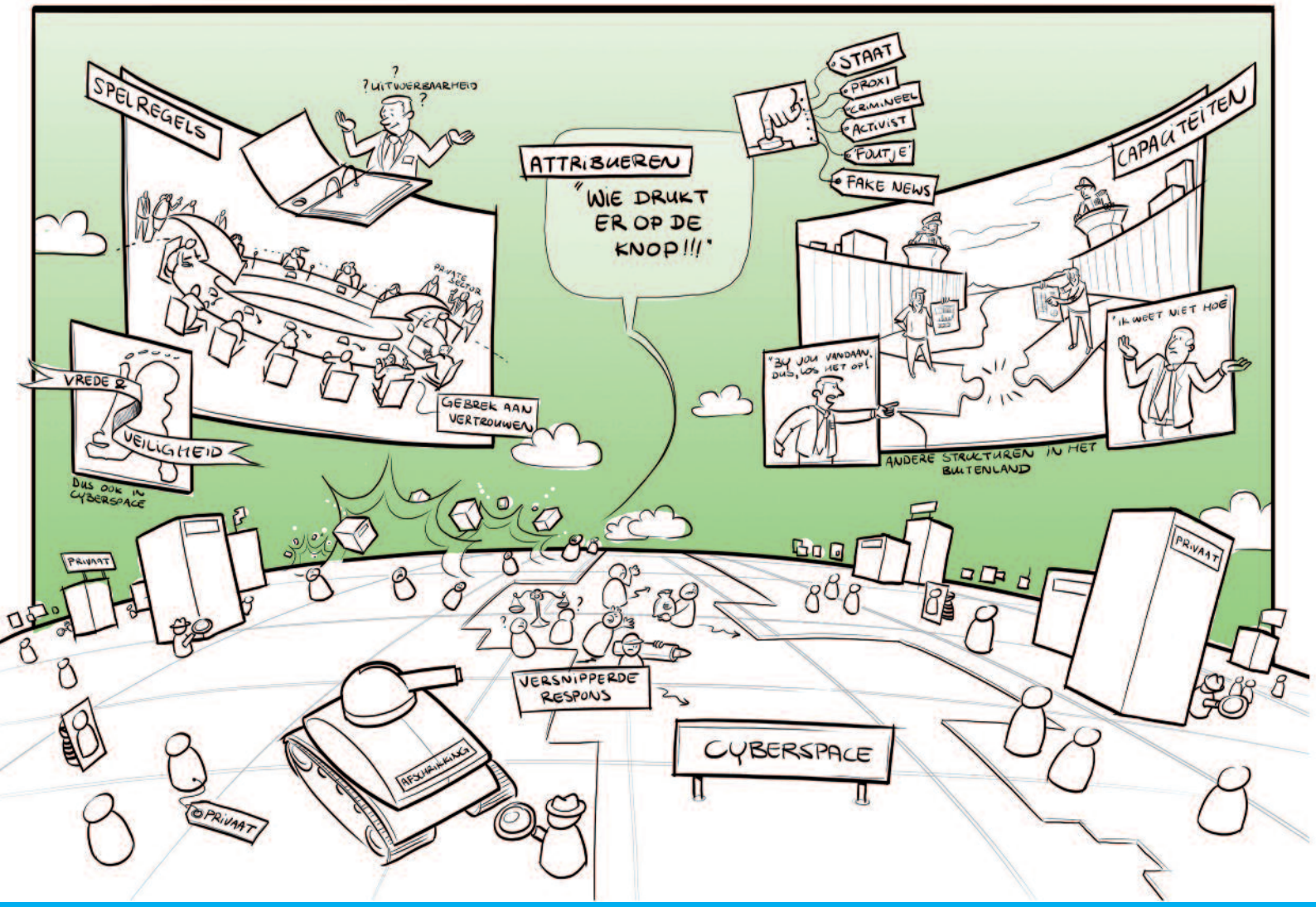
Rijkswaterstaat versterkt. Ook wordt de oprichting van meer private sectorale computercrisisteams aangemoedigd, zoals Z-CERT (voor de zorgsector) en I-CERT (voor de verzekeringssector).

- De vitale processen in onze samenleving vragen om extra bescherming en versneld herstel bij uitval of schade. Daarom is het belangrijk dat deze organisaties zorgen voor een eigen adequate responscapaciteit of dat ze hiervoor afspraken maken met een vertrouwde derde partij. Hiertoe zal met private partijen de ontwikkeling worden verkend van een certificeringsstelsel voor cybersecurity dienstverleners bij wie veilig dienstverlening kan worden afgenomen.[1]
- Nederland moet voorbereid zijn op grootschalige cyberincidenten die de nationale veiligheid bedreigen. Hiertoe wordt het Nationaal Crisisplan ICT geactualiseerd. Daarnaast zal een integraal ICT-crisisoefenbeleid worden opgesteld. Daarin worden afspraken gemaakt tussen overheidspartijen en private organisaties over een gezamenlijke oefenagenda en beschikbare capaciteiten hiervoor bij de betrokken partijen.
- De capaciteiten van de inlichtingen- en veiligheidsdiensten, DefCERT en het NCSC om inzicht te krijgen in dreigingen en digitale aanvallen, deze te signaleren, te verstoren en de weerbaarheid te verhogen, worden structureel versterkt. Hiertoe heeft het kabinet de afgelopen jaren en in het huidige regeerakkoord extra middelen vrijgemaakt. Het Nationaal Detectie Netwerk (NDN) zal de komende jaren nog verder worden versterkt zodat er een toekomstbestendig netwerk ontstaat.
- Het landelijk situationeel beeld wordt versterkt met de inrichting van een samenwerkingsplatform[2] met het oogmerk om binnen de wettelijke kaders meer en sneller handelingsperspectief met belanghebbende organisaties te kunnen delen. Hierbij dient ook aandacht te worden besteed aan de eisen op het gebied van informatiebeveiliging. Ontvangende partijen moeten een voldoende volwassenheidsniveau hebben om informatiedeling mogelijk te maken.
- Onder coördinatie van de NCTV worden rondetafelgesprekken georganiseerd waarmee het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden vorm kan krijgen. De ervaringen van bestaande publieke en private cybersecurity samenwerkingsverbanden worden hierbij betrokken.
- Het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Centre[3] (DTC) zullen de oprichting en doorontwikkeling van cybersecurity samenwerkingsverbanden voor overheden, het bedrijfsleven en maatschappelijke organisaties stimuleren, en – waar nodig – ondersteuning bieden. Ook wordt hierbij aandacht gegeven aan het opstellen van een set van basisbeveiligingsmaatregelen voor bedrijfsleven en maatschappelijke organisaties.
- Bezien wordt of de wetgeving gericht op het beschermen van nationale veiligheid voldoende handvatten biedt om deze veiligheid ook in het digitale domein te bevorderen, met behoud van fundamentele waarden en privacy.

1 Zie ook de doelstellingen en maatregelen op pagina 27-28.

2 De mogelijkheden met welke partijen en in welke vorm dit samenwerkingsplatform kan worden vormgegeven, worden nader onderzocht.

3 Kamerstuk 'Oprichting Digital Trust Centre' 23 september 2017.



Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein

2. Internationale vrede en veiligheid in het digitale domein

Statelijke actoren zetten steeds vaker digitale middelen in voor spionage-, beïnvloedings- en sabotagedoeleinden als integraal onderdeel van hun machtsinstrumentarium, of in concrete conflictsituaties. Ook is er een toename van het aantal landen dat aan een offensieve, militaire cybercapaciteit bouwt. Deze dreiging is de afgelopen jaren sterk toegenomen en vormt een ernstige internationale veiligheidsdreiging.

In internationaal verband is er sprake van scherpe tegenstellingen tussen verschillende landen in de benadering van het cyberdomein. Er bestaat verschil van inzicht over de toepassing van internationaal recht, (gedrags)normen in *cyberspace*, en de afhankelijkheid van en toegang tot digitale middelen. Het decentrale karakter van het internet en de mogelijkheden die het internet biedt voor anoniem optreden, bemoeilijken daarnaast het handhaven en controleren van gemaakte afspraken. Mede doordat attributie moeilijk is in het cyberdomein, kunnen dergelijke cyberoperaties de internationale rechtsorde bedreigen. Nederland dient ook zelf te beschikken over capaciteiten en instrumenten om digitale aanvallen op onze nationale belangen resoluut te kunnen afweren en – in het uiterste geval – proportioneel te kunnen vergelden.

DOELSTELLINGEN

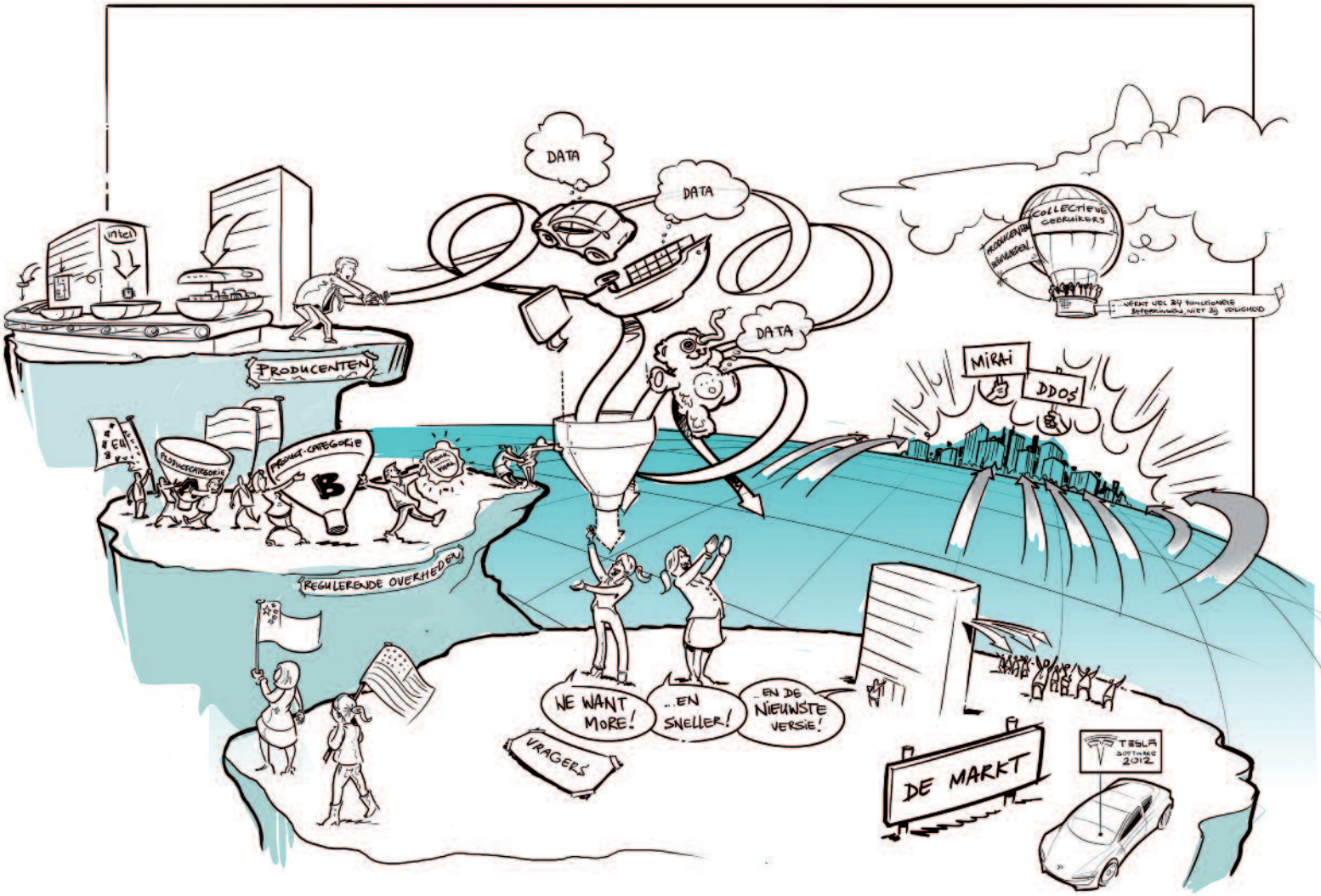
- Nederland bevordert de internationale rechtsorde in het digitale domein, waaronder de waarborging van mensenrechten.
- Nederland is in staat, al dan niet in coalitieverband, onverwijld en adequaat te reageren bij digitale aanvallen door statelijke actoren en beschikt over offensieve capaciteiten die een bijdrage leveren aan het vermogen tot afschrikking.
- Nederland draagt bij aan het mitigeren van cyberdreigingen afkomstig van criminele en statelijke actoren, door te investeren in capaciteitsopbouw van de mondiale cybersecurity keten.

MAATREGELEN

o Nederland zal de toepassing van het internationaal recht in *cyberspace* bestendigen, aanvullende normen stimuleren en vertrouwen tussen staten en andere partijen creëren. Nederland zet in op het vergroten van de internationale coalitie die de visie van een open, vrij en veilig internet onderschrijft. Dat zal Nederland doen door verdere interpretatie en toepassing van het internationaal recht in het digitale domein te stimuleren, bijvoorbeeld op het gebied van mensenrechten, humanitair recht en het kader voor bestrijding van cybercriminaliteit. En voor bescherming van telecommunicatie en kritieke infrastructuren. Daarnaast worden vertrouwenwekkende maatregelen tussen staten en verdere normontwikkeling gestimuleerd. De *Global Commission on the Stability of Cyberspace* heeft hier reeds een belangrijke bijdrage aan geleverd.

o Nederland ontwikkelt een breed strategisch kader ten behoeve van respons op digitale aanvallen. Daarin zijn alle beschikbare instrumenten opgenomen, waaronder (publieke) attributie, afschrikking, inzet van offensieve capaciteiten en bredere respons in het cyberdomein. Daartoe versterkt Nederland onder andere de diplomatieke en politieke reactie op verstorende of destructieve cyberoperaties van statelijke actoren. Het kader wordt opgevolgd met een geschikt instrumentarium voor een diplomatieke respons. Dit sluit aan op het cyberdiplomatennetwerk en de *toolbox* voor diplomatieke actie bij cyberincidenten, die door de Europese Unie is ontwikkeld. Nederland speelde hierin een voorstrekkersrol.

- Ter afschrikking van (potentiële) tegenstanders bouwt Nederland de offensieve cybercapaciteiten bij de krijgsmacht verder uit. Wij dragen zo ook bij aan het ontwikkelen en operationaliseren van het handelingsvermogen in NAVO- en EU-verband in het digitale domein. Hetgeen ook dient ter ondersteuning van militaire missies en operaties in het fysieke domein.
- Nederland levert een intensieve bijdrage aan een vrij, open en veilig internet, en bevordert een adequate bescherming van mensenrechten online, onder andere door normontwikkeling. Dit zal mede vorm krijgen door de doorontwikkeling van de *Freedom Online Coalitie*.
- Nederland versterkt de mondiale cybersecurity keten door het cybersecurity niveau van derde landen te verhogen en de digitale kloof tussen technologisch meer en minder ontwikkelde landen te verkleinen. Middels het *Global Forum on Cyber Expertise* (GFCE) worden strategische capaciteitsopbouw projecten gefaciliteerd en wordt de internationale multi-stakeholder coalitie voor een open, vrij en veilig internet verbreed.



Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software

3. Digitaal veilige hard- en software

Door de opmars van het *Internet of Things* worden steeds meer apparaten aan het internet verbonden. In 2020 gaat het naar verwachting om 20,4 miljard apparaten. Minstens 63% daarvan zullen consumentenapparaten zijn.[4] De overige 37% betreft apparaten die door bedrijven worden gebruikt en waarvan de impact (op eigen bedrijfsprocessen, maar ook verderop in de keten) bij verstoring of misbruik in potentie nog veel groter is dan bij particulier gebruik.

Het is belangrijk dat iedereen deze producten digitaal veilig en vertrouwd kan gebruiken, niet alleen voor de eigen digitale veiligheid, maar ook voor onze samenleving als geheel. Door kwetsbaarheden in hard- en software van een apparaat, kunnen kwaadwillende partijen zich daar namelijk eenvoudig toegang toe verschaffen, en via dat apparaat tot het netwerk waar het deel van uitmaakt.

Gebruikers en aanbieders van digitale producten houden vaak geen of onvoldoende rekening met de potentieel schadelijke effecten voor anderen, als gevolg van hun eigen handelen. Met alle gevolgen van dien, zoals het misbruik van het apparaat voor *DDoS*-aanvallen, het manipuleren van de werking van het apparaat of de diefstal van informatie die erop is opgeslagen.

Digitale veiligheid van hard- en software komt niet vanzelf tot stand. Aanbieders van hard- en software lossen niet altijd alle digitale veiligheidsrisico's op die met hun processen en productie gepaard gaan. Gebruikers hebben nauwelijks middelen om een goede inschatting te kunnen maken van het digitale veiligheidsniveau van een apparaat dat aan het internet is verbonden. Zelfs als ze deze kennis wel hebben, blijft het lastig om deze inschatting te kunnen maken. Het is voor gebruikers bijvoorbeeld moeilijk om de langetermijnimpact van hun beslissingen te overzien. Ook is er vaak specialistische kennis nodig om de digitale veiligheid van het apparaat te kunnen doorgronden. Gebruikers moeten daarom door middel van het bieden van instrumenten die inspelen op het gedrag van gebruikers, in staat worden gesteld ("*empowered*" worden) om de digitale veiligheid van hard- en software te kunnen doorgronden. Hierbij speelt onderzoek naar de effectiviteit van voorlichtingscampagnes op veilig gedrag van een gebruiker een belangrijke rol.

DOELSTELLINGEN

Om de digitale veiligheid van hard- en software te bevorderen is een samenhangende set van maatregelen nodig om de digitale veiligheid op een gebalanceerde wijze te bevorderen, waarbij diverse partijen een verantwoordelijkheid hebben. Daarom zet Nederland in op de (door)ontwikkeling en uitvoering van de Roadmap Digitaal Veilige Hard- en Software.[5] Daarbij gelden de volgende doelstellingen:

- Nederland zet in op het voorkomen van digitale veiligheidsrisico's in hard- en software door het stimuleren van standaardisatie- en certificeringsinitiatieven en het versterken van toezicht en handhaving.
- Nederland zet in op het detecteren van digitale veiligheidsrisico's, door het testen van digitale producten en het inzichtelijk maken van digitale veiligheidsrisico's.
- Nederland zet in op het mitigeren van digitale veiligheidsrisico's door het aansprakelijkheidsregime, en het versterken van het bewustzijn en handelingsperspectief voor burgers en bedrijven.
- Nederland zet in op het realiseren van een set van basisbeginselen om de digitale veiligheid van hard- en software te bevorderen.

4 https://www.gartner.com/newsroom/id/3598917.

5 Roadmap Digitaal Veilige Hard- en Software, ministerie van EZK 2018.

MAATREGELEN

- Standaarden en certificering leveren een belangrijke bijdrage aan de digitale veiligheid van hard- en software.
- Nederland dringt in de onderhandelingen in Brussel aan op snelle vaststelling van de *Cyber Security Act* (CSA), en een voortvarende ontwikkeling van een Europees raamwerk Beveiligingscertificering voor ICT-producten en -diensten. Op korte termijn dringt het kabinet aan op verplichte certificering vast te stellen voor specifieke productgroepen. Dat wil zeggen voor producten waarmee het risico het grootst is of waarmee veel problemen zijn in de praktijk. Op de langere termijn moet door geleidelijke uitbreiding een verplichte certificering of het voldoen aan een CE-markering voor alle met internet verbonden producten gaan gelden.
- Daarnaast stimuleert Nederland de toepassing van internationale standaarden, samenwerkingsverbanden en raamwerken. Nederland wil proactief op relevante Europese en mondiale standaardisatie- en certificatie-initiatieven aansluiten via het standaardisatieplatform NEN. Ook gaat Nederland werk maken van multilaterale samenwerking rond *Internet of Things*-standaardisatie, onder meer via het Global Forum on Cyber Expertise (GFCE).
- Het kabinet gaat met publieke en private partijen een monitor ontwikkelen met informatie over de digitale veiligheid van digitale producten, met specifieke aandacht voor *Internet of Things*-apparaten. Hierbij betrekt het kabinet internationale ervaringen.
- Het kabinet gaat in gesprek met de aanbieders van internettoegang over hoe zij - analoog aan de succesvolle aanpak van botnets - gaan bijdragen aan de bestrijding van onveilige *Internet of Things*-apparaten. Het testen van producten is cruciaal om zekerheid te verkrijgen over de digitale veiligheid daarvan. Er komt een pilot om aan de hand van diverse sectorale use cases ervaring en kennis op te doen met wat een gedeeld testplatform kan bieden.
- Het ontwikkelen en marktrijp maken van innovatieve oplossingen kan een belangrijke bijdrage leveren aan het digitaal veilig maken van hard- en software. Nederland zet in op het ontwikkelen van cybersecurity onderzoek via de NCSRA III (publicatie beoogd in 2018) dat zich richt op het ontwikkelen en marktrijp maken van innovatieve oplossingen. Ook lopen via de toepassing van het Small Business Innovation Research (SBIR)[6] verschillende tenders voor onderzoek die bijdragen aan nieuwe innovatieve, digitaal veilige hard- en software. Daarnaast stimuleert het kabinet open source encryptie door extra middelen hiervoor vrij te maken in het kader van de NCSRA III. Tot slot gaat het kabinet dialoogsessies organiseren over innovatieve oplossingen om hard- en software digitaal veilig te houden of af te voeren. Zie ook de doelstellingen onder ambitie 5.
- Aansprakelijkheid vormt een belangrijke financiële prikkel voor aanbieders om hun hard- en software veilig te maken én te houden. Het kabinet is met stakeholders en wetenschappers in gesprek over aandachtspunten rond de aansprakelijkheid bij digitaal onveilige hard- en software, en over welke verbeterpunten en oplossingen zij zien. Daarnaast neemt Nederland actief deel aan de expertgroep over aansprakelijkheid en nieuwe technologieën en betrekt daarbij de inbreng van Nederlandse stakeholders. Verder stelt Nederland in de onderhandelingen over het 'Richtlijnvoorstel digitale inhoud en digitale diensten', voor om in alle gevallen een verplichting op te nemen veiligheidsupdates te verplichten als het gaat om software die is geleverd aan een consument.
- Met het stellen van minimumveiligheidseisen kunnen onveilige producten van de markt geweerd worden. Het kabinet onderzoekt welke minimale veiligheidseisen kunnen worden gesteld aan apparaten via de Europese Radio Equipment Directive.[7]
- Het kabinet gaat onderzoeken welke aanvullende maatregelen nodig en gewenst zijn bij inkoop binnen de Rijksoverheid, voor de digitale veiligheid van hard- en software.
- Toezicht en handhaving geven aanbieders een prikkel om zich aan wet- en regelgeving te houden. Het kabinet organiseert een nationale dialoogsessie voor toezichthoudende instanties, om te bezien welke rol zij de komende periode kunnen spelen om de digitale veiligheid van hard- en software te bevorderen, synergie te creëren tussen de verschillende acties van toezichthouders en te kijken hoe samenwerking tussen toezichthouders kan worden verbeterd.

6 SBIR benut de creativiteit van ondernemers om maatschappelijke problemen op te lossen en daagt ondernemers uit om nieuwe producten te ontwikkelen en op de markt te brengen, zie https://www.rvo.nl/subsidies-regelingen/sbir.

7 Kamerstuk 26643, nr. 467 en Kamerstuk 24095, nr. 415.

- Bewustwording en *empowerment* leveren een belangrijke bijdrage aan de digitale veiligheid van hard- en software, onder meer omdat aanbieders hierdoor rekening kunnen houden met digitale kwetsbaarheden en gebruikers zich bewust zijn van mogelijke risico's. Als onderdeel van de cybersecurity bewustwordingscampagnes van veiliginternetten.nl lanceert de overheid een of meer beleidsondersteunende publiekscampagnes voor digitaal veilige hard- en software.

10 Kamerstuk 26643, nr. 467 en Kamerstuk 24095, nr. 415

Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur

4. Weerbare digitale processen en een robuuste infrastructuur

ICT is steeds meer verweven met de Nederlandse samenleving. Een gevolg hiervan is dat bedrijven en overheden via slimme toepassingen in toenemende mate datagedreven gaan functioneren. Organisaties zijn vaak niet meer in staat om alle taken zelf uit te voeren. Zij opereren in ketens. Ze zijn afhankelijk van andere organisaties voor onder andere het leveren van de gegevens of voor het uitvoeren of ondersteunen van hun gegevensverwerking. Dat is niet zonder risico. Wanneer de gegevensuitwisseling met andere organisaties niet veilig en betrouwbaar verloopt, kan het bedrijfsproces verstoord raken. Wanneer dit gebeurt in de ketens van vitale aanbieders dan kan dit leiden tot verregaande uitval, aantasting van de fysieke veiligheid en maatschappelijke ontwrichting. Er kunnen problemen zijn met de fysieke infrastructuur of met de protocollen en de software voor de gegevensuitwisseling. Ten slotte kan de partij die voorziet in diensten ten behoeve van gegevensverwerking, wegvallen of tekortschieten.

Vanwege het belang van de beschikbaarheid (of continuïteit) van datacommunicatienetwerken worden specifieke eisen gesteld aan de aanbieders van zulke netwerken, onder meer via de Telecommunicatiewet en het wetsvoorstel voor de Cybersecuritywet (Csw).[8] Die zijn erop gericht dat dergelijke aanbieders hun systemen en netwerken weerbaar maken tegen verschillende dreigingen en incidenten, waaronder die, welke kunnen leiden tot uitval van fysieke infrastructuur. Met de Csw ontstaat daarnaast voor alle aanbieders van een essentiële dienst en digitale dienstverleners de verplichting om passende technische en organisatorische maatregelen te treffen. Op de invulling hiervan wordt toegezien door sectorale toezichthouders. Hiermee wordt het beveiligingsniveau van aanbieders verder verhoogd en ontstaat de mogelijkheid om stevig op te treden tegen kwetsbare (niet passend beveiligde) informatiesystemen. De Csw vervangt en vult aan op de reeds in werking getreden Wet gegevensverwerking en meldplicht cybersecurity (Wgmc), waarin onder meer al is geregeld dat de NCSC de taak heeft om het Rijk en de vitale aanbieders te adviseren over cybersecurity. Deze wet biedt ook de mogelijkheid om een vakminister te informeren in die gevallen waar door een rijksorgaan of vitale aanbieder niet adequaat wordt omgesprongen met adviezen van het NCSC. De Nederlandse overheid vraagt van alle organisaties om adequaat te kunnen reageren wanneer de continuïteit van hun dienstverlening in gevaar komt. Ook is het van belang dat verouderde soft- en hardware tijdig wordt vervangen (*legacy*-problematiek).

Voor effectieve en storingsvrije gegevensuitwisseling vereisen ook de software en protocollen voor wereldwijde gegevensuitwisseling aandacht en onderhoud. Vaak gaat het om zogenoemde vrije software, die in de regel wordt ontwikkeld door *communities* waarin vrijwilligers samenwerken. Daardoor ontbreken vaak de capaciteiten of middelen voor onderhoud en/of professioneel onderzoek naar de kwaliteit ervan. Ook andere softwareontwikkelaars gebruiken vrije software als bouwsteen voor hun werk, waardoor de afhankelijkheid van deze software verder toeneemt.

8 De Cybersecuritywet vloeit voort uit de NIB-richtlijn en is in februari 2018 aangeboden aan de Tweede Kamer.

De kwaliteit van niet-vrije software en de veiligheid van hardware-onderdelen is evenzeer belangrijk voor effectieve en storingsvrije gegevensuitwisseling. Dit komt aan de orde bij ambitie 3. Sommige populaire protocollen voor gegevensuitwisseling via het internet zijn decennia oud en niet meer bestand tegen hedendaagse aanvallen. Verbeterde versies van oude internetstandaarden (zoals IPv6 of HTTPS) worden zeer langzaam in gebruik genomen, waardoor de nadelen van oude versies (IPv4 en HTTP) nog lang blijven spelen.

Bedrijven en overheden zijn voor hun gegevensverwerking afhankelijk van andere organisaties, waaronder *cloud*leveranciers en hun klanten, overheden die open data beschikbaar stellen en certificaatleveranciers die de integriteit van gegevensuitwisseling garanderen. Nederland streeft ernaar belangrijke (keten)afhankelijkheden tussen organisaties inzichtelijk te krijgen, maar realiseert zich dat het onhaalbaar is om die altijd geheel in beeld te hebben. De Nederlandse overheid vraagt daarom van alle organisaties dat ze adequaat kunnen reageren wanneer de continuïteit van hun dienstverlening in gevaar komt. Het Digital Trust Centre in oprichting wil, in samenspraak met het NCSC, partijen, waaronder het midden- en kleinbedrijf, hierbij helpen, door het bewustzijn te vergroten en handelingsperspectief te bieden. En daar waar organisaties gebruik willen maken van de diensten van cybersecurity dienstverleners, is het van belang dat ook zij op professionele en integere wijze omgaan met computernetwerken en gevoelige informatie. Veel Nederlandse organisaties zijn afhankelijk van een beperkt aantal buitenlandse aanbieders van digitale infrastructuurdiensten, waardoor de impact bij verstoring groot is.

Voorbeeld: *Heartbleed*
Heartbleed was een kwetsbaarheid in de programmeerbibliotheek OpenSSL die in 2014 werd onthuld. De kwetsbaarheid was toen al twee jaar in deze veelgebruikte software aanwezig. Veel webservers, VPNservers, mailservers en andere applicaties maken gebruik van OpenSSL om beveiligde verbindingen op te zetten. Ook andere apparaten kunnen OpenSSL gebruiken. Voorbeelden zijn *appliances*, routers, WiFi-*accesspoints* en sommige applicaties op *client*systemen. Door misbruik te maken van *Heartbleed*, konden aanvallers op afstand het interne geheugen van systemen uitlezen. Dit voorbeeld onderstreept dat een kwetsbaarheid in vrije software grote gevolgen kan hebben voor de cybersecurity van bedrijfsleven, overheden en burgers.

DOELSTELLINGEN

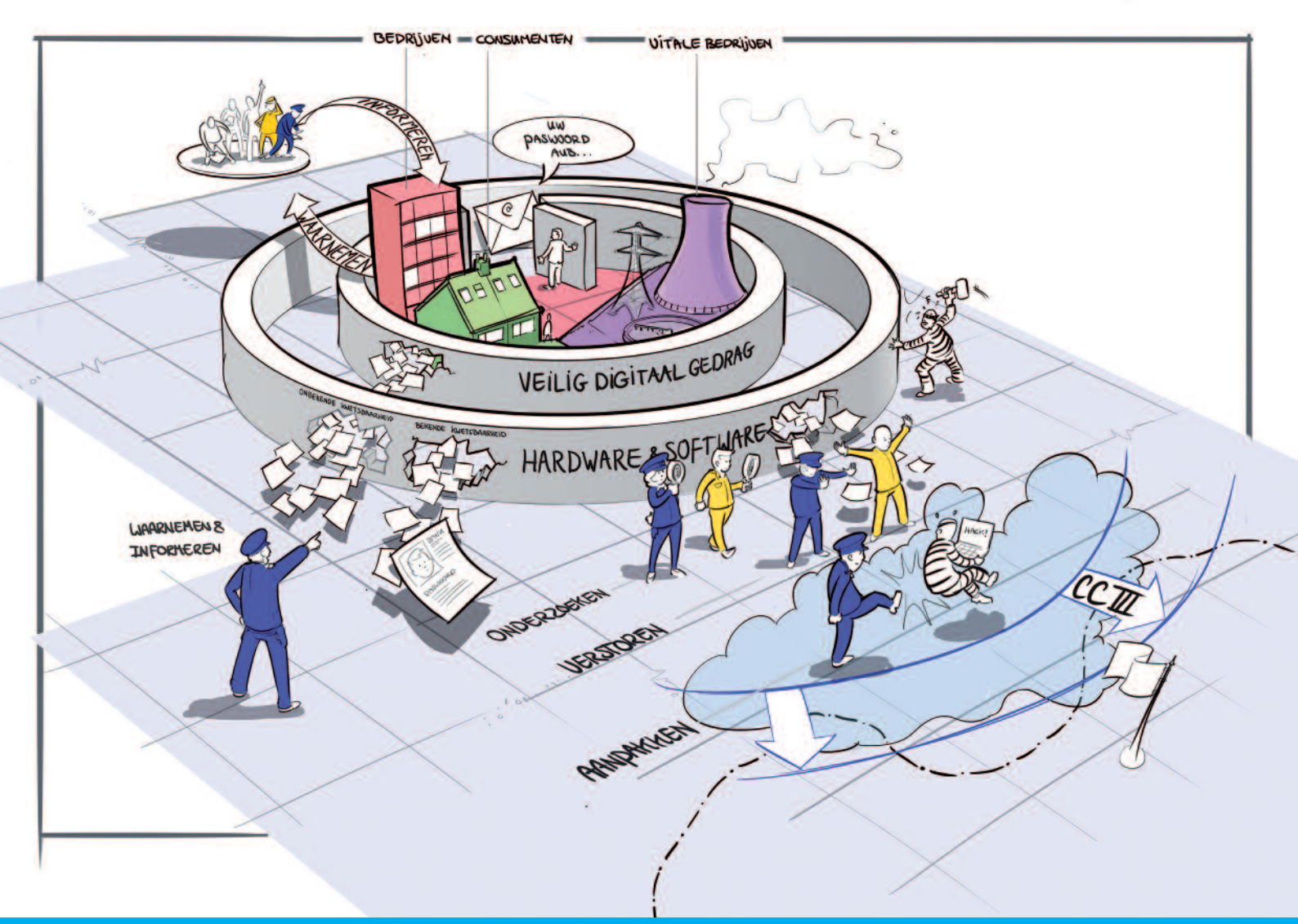
- Alle relevante partijen worden betrokken bij het waarborgen van de continuïteit en de digitale weerbaarheid van vitale processen, waardoor de weerbaarheid van de gehele keten wordt versterkt.
- Nederland zet in op het versterken van de kwaliteit van vrije software en de versnelde adoptie van moderne internetprotocollen en internetstandaarden.
- De Nederlandse overheid stimuleert een innovatief cybersecurity klimaat waarin veilige ICT-producten en -diensten worden ontwikkeld en gebruikt.

MAATREGELEN

o Naast de bestaande verplichtingen voor telecomaanbieders in de Telecommunicatiewet wordt met het voorstel voor de Cybersecuritywet het aantal vitale aanbieders dat zorg- en meldplichten krijgt, fors uitgebreid. Sectorale toezichthouders gaan toezien op de cybersecurity in sectoren in de vitale infrastructuur waar dat tot nu toe niet gebeurde en krijgen daarvoor de instrumenten aangereikt.

o Deze toezichthouders ontwikkelen in aanvulling op bovenstaande met de vakdepartementen een methodiek voor het identificeren van afhankelijkheidsrelaties van vitale aanbieders voor hun datagedreven bedrijfsprocessen.

- Onderzocht wordt of aanvullende (Europese of internationale) maatregelen nodig zijn om de impact bij verstoring van de dienstverlening van een beperkt aantal buitenlandse aanbieders van digitale infrastructuur, waar veel Nederlandse organisaties van afhankelijk zijn, te beperken.
- Vrije software vervult een centrale rol in de gegevensuitwisseling tussen organisaties. Het ministerie van EZK zal, in nauwe samenwerking met het NCSC, bezien hoe de gemeenschappen die vrije software ontwikkelen en onderhouden kunnen worden ondersteund, om de kwaliteit daarvan te verbeteren.
- De overheid zorgt ervoor dat leveranciers moderne internetprotocollen en internetstandaarden toepassen in hun producten en diensten, mede door agendering in Europa.
- De overheid als *launching customer* hanteert cybersecurity vereisten bij de inkoop van ICT-producten en -diensten en geeft hierover dringend advies aan vitale aanbieders.
- Met private partijen wordt verkend hoe een certificeringsstelsel ontwikkeld kan worden voor cybersecurity dienstverleners, zodat overheid en private partijen weten bij wie ze veilig dienstverlening af kunnen nemen.



Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime

5. Succesvolle barrières tegen cybercrime

PROBLEEMVERKENNING

Criminelen ontplooien op grote schaal hun activiteiten via internet. Zo was 1 op de 9 personen in 2017 slachtoffer van *cybercrime*. Achter de term *cybercrime* gaat een grote variëteit aan verschijningsvormen schuil van zowel klassieke criminaliteit in digitale vorm als nieuwe criminaliteit. Het gaat bijvoorbeeld om het hacken van computers om geld naar criminele bankrekeningen over te schrijven, of het ongemerkt aanzetten van camera's en microfoons om mensen in hun eigen omgeving te kunnen bespioneren. Beroepscriminelen hebben het vooral gemunt op private organisaties en burgers voor de diefstal van gegevens die vervolgens kunnen worden doorverkocht of gepubliceerd.

Bedreigingen voor de nationale veiligheid in het kader van cybersecurity zijn vaak strafbare feiten gericht tegen de digitale infrastructuur en daarmee verbonden apparaten. De aanpak van deze feiten richt zich voornamelijk op nieuwe criminaliteit, of *cybercrime* in enge zin. De aanpak van *cybercrime* richt zich op het voorkómen en bestrijden van strafbare feiten en het beperken van slachtofferschap, daderschap en recidive. Daarbij gaat het om zowel *hightech crime* als veel voorkomende criminaliteit. Digitale opsporing is ook van belang voor meer klassieke strafbare feiten waarbij het internet steeds vaker een hulpmiddel is, zoals drugshandel en fraude. Dergelijke criminaliteit valt buiten het kader van deze strategie.

De versterking van cybersecurity en de aanpak van *cybercrime* worden in samenhang met elkaar vormgegeven. De verwevenheid is het sterkst op het gebied van preventieve maatregelen.

Veilige hard- en software vormen een belangrijke barrière in het voorkomen van digitale dreigingen. Wanneer door kwetsbaarheden deze hard- en software wordt misbruikt, speelt dit *cybercrime* in de hand. De veiligheid hiervan is van groot belang en hier zal samen met de aanbieders van hard- en software invulling aan gegeven moeten worden. Dit staat meer uitgebreid omschreven in ambitie 3 van de NCSA. Dat geldt evenzeer voor het veilige gebruik van burgers en bedrijven van dergelijke hard- en software. Dit staat ook beschreven in ambitie 6.

Hiernaast hebben het Team High Tech Crime van de politie en het Landelijk Parket van het Openbaar Ministerie de afgelopen jaren ruime ervaring opgedaan met het tegengaan van geavanceerde dreigingen voor nationale veiligheid. De door hen opgedane kennis en expertise zal worden benut ten behoeve van de aanpak van *cybercrime*. Cybercriminelen blijven hun werkwijzen ontwikkelen. Daar moeten de bevoegdheden van politie en Justitie gelijke tred mee kunnen houden.

DOELSTELLINGEN

- Er zijn effectieve barrières die cybercriminelen tegenhouden.
- De versterking van cybersecurity en de aanpak van *cybercrime* worden in samenhang met elkaar vormgegeven. Hiervoor is samenwerking van de overheid met het bedrijfsleven, burgers en maatschappelijke organisaties van groot belang.
- Voor cybersecurity is het van belang dat opsporingsbevoegdheden gelijke tred houden met de ontwikkelingen in de werkwijze van cybercriminelen zodat dreigingen voor de nationale veiligheid geadresseerd kunnen worden.

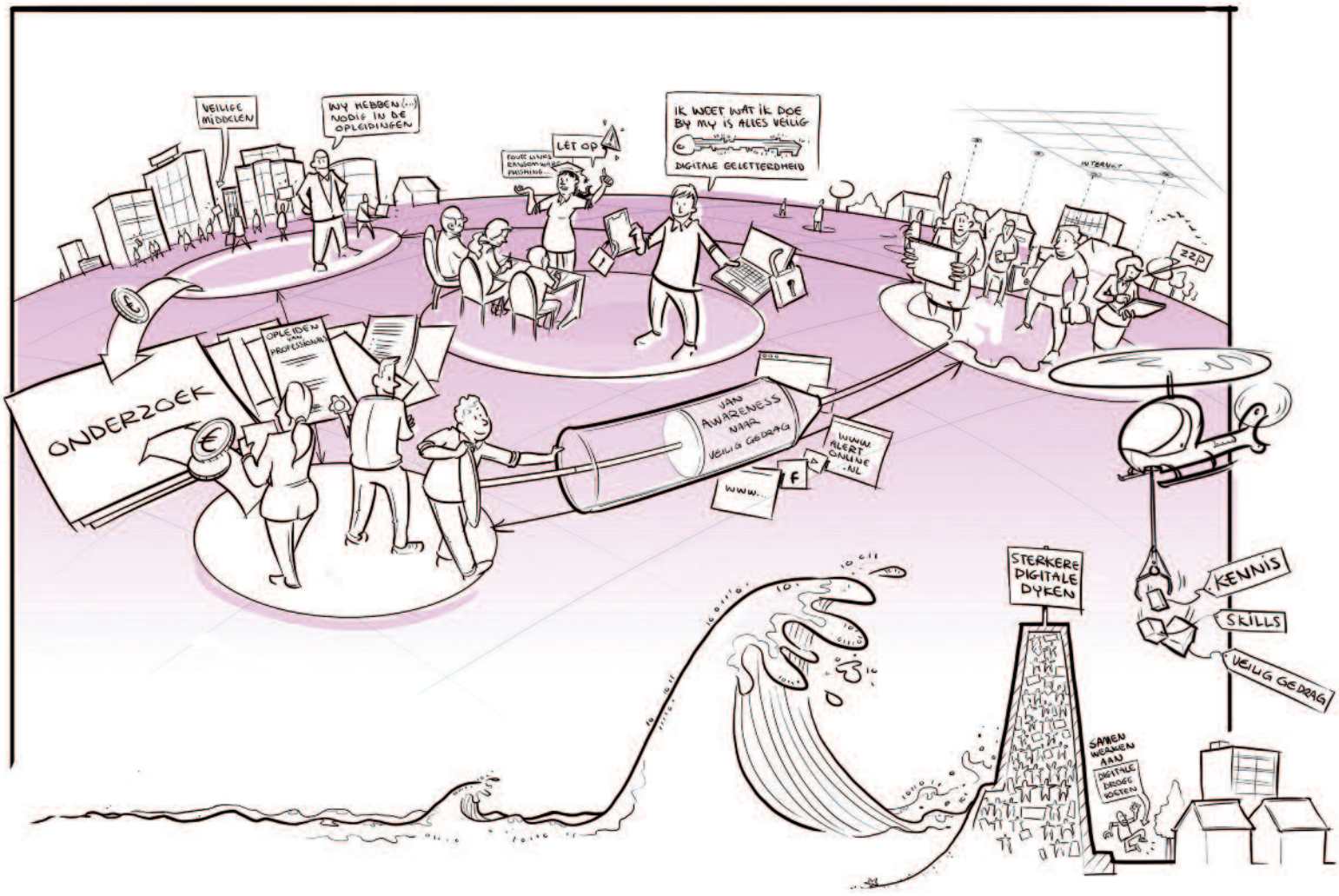
MAATREGELEN

o Na aanvaarding in de Eerste Kamer wordt de wet Computercriminaliteit III voortvarend geïmplementeerd. Daarmee worden de opsporingsmogelijkheden van politie en Justitie van digitale aanvallen, op bijvoorbeeld vitale sectoren, door criminelen versterkt. De wet wordt twee jaar na de inwerkingtreding geëvalueerd.

- Er worden voorstellen ontwikkeld om burgers en bedrijven digitaal meer vaardig te maken zodat cybercriminelen minder kans maken. Zie ook de doelstellingen en maatregelen bij ambitie 6.
- Het gebruik van veilige hard- en software wordt gestimuleerd om *cybercrime* te voorkomen. Zie ook de doelstellingen en maatregelen bij ambitie 3.

Integrale aanpak *cybercrime*

Het opsporen van cybercriminelen en het verstoren van hun verdienmodel draagt bij aan cybersecurity. De huidige aanpak van *cybercrime* richt zich op het opsporen, vervolgen en verstoren van strafbare feiten, preventie en het versterken van de wet- en regelgeving. Deze wordt voortgezet en geïntensiveerd. Daarnaast worden er nieuwe elementen aan toegevoegd, zoals preventieve maatregelen voor potentiële daders en slachtoffers, een mogelijk andere vorm van ondersteuning van slachtoffers, een aanpak van daders ter voorkoming van recidive en kennisontwikkeling voor beleidsvorming op de langere termijn.



Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling

6. Cybersecurity kennisontwikkeling

Kennis is in Nederland een groot goed. Onze maatschappij is afhankelijk van het ontwikkelen en toepassen van kennis. Dit geldt in het bijzonder voor een digitaal veilige maatschappij en daarom zijn ambities op het gebied van kennisontwikkeling onmisbaar in de NCSA.

Er is urgentie geboden om hoogwaardige cybersecurity kennisontwikkeling in Nederland in stand te houden en te verdiepen. Het versterken van voldoende en hoogwaardige ontwikkeling van zowel fundamenteel als toegepast cybersecurity onderzoek is hiervoor cruciaal. Cybersecurity kennisontwikkeling is nodig om maatregelen te kunnen treffen tegen bestaande en nieuwe digitale dreigingen. Bovendien voorkomt een hoogwaardige eigen autonome kennispositie een te grote afhankelijkheid van cybersecurity expertise en cybersecurity oplossingen uit andere landen. Cybersecurity kennisontwikkeling geldt niet alleen voor bètawetenschappen, maar ook voor alfa en gamma. Het gaat om zowel gericht als interdisciplinair onderzoek, waarbij wordt gekeken naar oplossingen voor de korte en de lange termijn en. Het is hierbij van het grootste belang dat wordt gekeken naar de gehele kennisketen.

Cybersecurity onderzoek in Nederland is van hoog niveau. Daarin wordt door meerdere partijen, zoals universiteiten, hogescholen, NWO, bedrijven en ook het Rijk, geïnvesteerd. Opeenvolgende edities van de Nationale Cyber Security Research Agenda (NCSRA) hebben de afgelopen jaren een belangrijk kader gevormd voor cybersecurity onderzoek. Door de investeringen in omringende landen in cybersecurity onderzoek, is het wenselijk dat er in Nederland een (meerjarige) impuls komt voor cybersecurity onderzoek om zo talent, en daarmee onze cybersecurity kennispositie, te behouden.

Daarnaast is er een groeiende vraag vanuit het bedrijfsleven en overheden naar innovatieve oplossingen op cybersecurity vraagstukken en goed opgeleid personeel. Deze krapte op de arbeidsmarkt leidt tot schaarse cybersecurity kennis bij organisaties die daardoor mogelijk onvoldoende weerbaar zijn tegen digitale dreigingen.

Het is evenzeer van belang dat ook burgers en bedrijven hun kennis blijven ontwikkelen om zich te kunnen beschermen tegen digitale dreigingen. Het in 2016 door de ministeries van JenV, OCW, EZK en NWO opgerichte dcypher[9] kreeg naast een opdracht op het gebied van cybersecurity onderzoek ook een cybersecurity hoger onderwijs opdracht mee. Het heeft het hoger onderwijs in Nederland in kaart gebracht, waardoor onderlinge vergelijking van opleidingen en beoordeling van vaardigheden mogelijk is van pas afgestudeerden die toetreden tot de arbeidsmarkt. Een volgende essentiële stap is een verschilanalyse van onderwijscurricula (aanbod) en behoefte aan goed opgeleid personeel (vraag). Europese samenwerking op dit terrein wordt nagestreefd. Voldoende doceercapaciteit (in alle betrokken disciplines) vergt bijzondere aandacht.

Digitale geletterdheid maakt inmiddels deel uit van het curriculum van het primair en voortgezet onderwijs maar gelet op de risico's voor (jonge) kinderen is het noodzakelijk dat het onderwijs hierop blijft vernieuwen en anticiperen. Samen met onderwijzers, leerlingen, ouders, het vervolgonderwijs en het beroepenveld wordt de afgesproken herziening van het curriculum (waarbij digitale geletterdheid één van de thema's is) doorgezet. Deze curriculumherziening wordt vanaf 2019 wettelijk verankerd.

9 Dcypher is het platform dat onderzoekers, docenten, producenten, gebruikers en beleidsmakers in Nederland verenigt om kennis en kunde over cybersecurity te verbeteren.

Voor de huidige generaties blijft een inhaalslag nodig. Uit onderzoek[10] blijkt dat burgers en bedrijven zich nog onvoldoende bewust zijn van de gevaren van digitaal handelen en de maatregelen die ze kunnen nemen om te voorkomen dat zij slachtoffer worden in het digitaal domein. In de afgelopen jaren hebben het bedrijfsleven en de overheid al stevig ingezet op bewustwording onder het algemeen publiek en kleinere bedrijven van digitale dreigingen, en zijn handelingsperspectieven aangereikt, onder meer via veiliginternetten.nl en Alert Online maar ook via campagnes als maakhetzeniettemakkelijk.nl (*'boefproof'*) of veiligbankieren.nl (*'hang op, klik weg'*). De effecten van de verschillende inspanningen kunnen worden verbeterd door meer publiek-private samenwerking en samenhang aan te brengen in communicatiecampagnes in het publieke domein. Dit geldt ook voor de inspanningen van werkgevers om hun werknemers digitaal vaardig te maken en up-to-date te houden. Daarbij is het noodzakelijk om zowel ten behoeve van burgers als kleinere bedrijven een handreiking te ontwikkelen met basisveiligheidsmaatregelen. Deze set van veiligheidsmaatregelen biedt geen bescherming tegen alle denkbare digitale dreigingen, maar is een belangrijke stap waarmee burgers en kleine bedrijven hun digitale vaardigheden verder kunnen ontwikkelen.

DOELSTELLINGEN

- Nederland verricht hoogwaardig cybersecurity onderzoek.
- Nederland beschikt over een meerjarig kennisontwikkelingsprogramma waarbinnen de wetenschap hoogwaardige kennis ontwikkelt en vergroot, en er voldoende wetenschappers beschikbaar zijn om een eigenstandige kennispositie op cybersecurity te verwerven.
- Burgers en bedrijven zijn in staat en zien het belang om veel voorkomende digitale dreigingen het hoofd te bieden en meer weerbaar te zijn tegen *cybercrime*.

MAATREGELEN

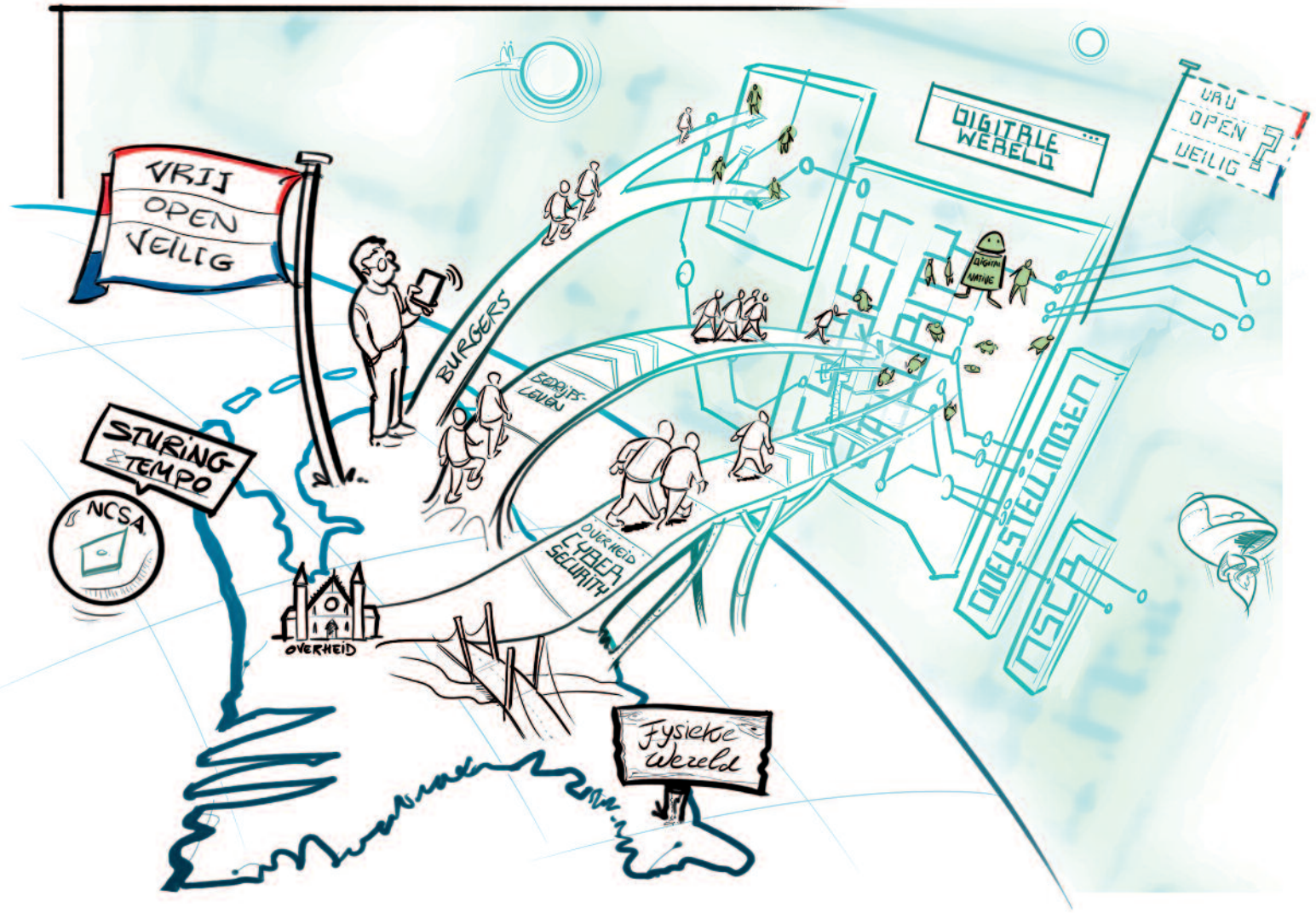
o Nederland zal structureel investeren in fundamenteel en toegepast cybersecurity onderzoek. Dit zal in een meerjarige publiek-private aanpak worden vormgegeven, als impuls voor hoogwaardige cybersecurity kennisontwikkeling. Hiertoe wordt verkend hoe verschillende initiatieven, trajecten en instrumenten met betrekking tot cybersecurity onderzoek beter op elkaar aan kunnen sluiten. Hierin zal de motie Verhoeven/Rutte[11] worden meegenomen. Vooruitlopend op de verkenning zal een eerste financiële impuls worden georganiseerd ten behoeve van cybersecurity onderzoek.

o Digitale vaardigheden, waaronder mediawijsheid en cybersecurity, zijn nadrukkelijk aandachtspunten in de integrale curriculumherziening in het primair en voortgezet onderwijs. In 2018 zullen hiervoor voorstellen worden ontwikkeld, die vanaf 2019 in wet- en regelgeving uitgewerkt zullen worden. Scholen worden door Kennisnet (dat wordt gefinancierd door het ministerie van OCW) ondersteund om hierop te anticiperen.

o De overheid stimuleert het bedrijfsleven en maatschappelijke organisaties om de digitale vaardigheden van burgers en werknemers verder te ontwikkelen, en zorgt voor continuïteit en samenhang tussen verschillende bewustwordingscampagnes om het effect daarvan te vergroten. Daarbij wordt rekening gehouden met de meest recente gedragswetenschappelijke inzichten.

10 Nationaal cybersecurity bewustzijnsonderzoek 2017, Alert Online en HM Government et. al. A call to action: The Cyber Aware perception gap, 2018.

11 De motie Verhoeven/Rutte verzoekt de regering de mogelijkheid te onderzoeken om een instituut voor onderzoek op het gebied van cybersecurity op te richten (Kamerstukken II, 2017/18, 34 775 VI, nr. 68).



Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity

7. Publiek-private aanpak van cybersecurity

Afgelopen jaren zijn vanuit publieke, private en de publiek-private sectoren diverse initiatieven genomen om cybersecurity in Nederland te versterken. Om die richting te bewaken is regie nodig op de koers en op de snelheid van de aanpak. Die regie kan en moet steviger en die ligt nadrukkelijk bij de overheid. De NCTV neemt als coördinator het voortouw om de versterking op cybersecurity op samenhangende wijze en in verbondenheid met alle betrokken partijen (overheid, bedrijfsleven, wetenschap, maatschappelijk middenveld) stevig vorm te geven. Tegelijkertijd geldt dat de overheid dit niet alleen kan doen. Voor een veilig klimaat in het digitale domein mag en moet van alle partijen verwacht worden dat zij hun verantwoordelijkheid nemen en hun bijdrage leveren om Nederland samen digitaal veilig te maken en te houden. De aanpak kan alleen succesvol zijn als zij in nauwe publiek-private samenwerking wordt vormgegeven, doorontwikkeld en geëvalueerd. De toenemende complexiteit en breedte van het cyberdomein vragen om continue verheldering van die rolverdeling en de verantwoordelijkheden. Het is daarbij zaak om de succesvolle marktinitiatieven ook in beeld te krijgen en aan deze agenda te verbinden. Zo is cybersecurity opgenomen in de *corporate governance code* en als zodanig onderwerp van audits en reviews. Ook aan private kant moet er meer in samenhang gewerkt (gaan) worden aan de integrale Nederlandse cybersecurity aanpak.

Het belang van informatiebeveiliging en cybersecurity bij de overheid neemt toe, doordat burgers en bedrijven de dienstverlening bij de overheid steeds meer digitaal afnemen. Uitval, sabotage of verstoring van de digitale dienstverlening zal daarom direct leiden tot aantasting van vitale dienstverleningsprocessen. Om de digitale dienstverlening door overheden aan burgers en bedrijven te optimaliseren en hoogwaardige dienstverlening te kunnen garanderen, is het zaak dat het openbaar bestuur blijvend investeert in informatiebeveiliging en cybersecurity. Het borgen van de beschikbaarheid en de continuïteit van dienstverlening hebben daarbij prioriteit. Digitalisering heeft naast dienstverlening ook een impact op de publieke waarden en de mensenrechten en de waarborging hiervan in de informatiesamenleving. Naast veilige dienstverlening aan burgers en bedrijven is het ook noodzakelijk de eigen informatiebeveiliging van de overheid op orde te hebben en te houden, en weerbaar te zijn tegen digitale aanvallen. In de brede agenda Digitale Overheid (BZK) wordt nader ingegaan op onder meer deze onderwerpen, alsook op de maatregelen om als overheid interbestuurlijk verder in te zetten op informatiebeveiliging en cybersecurity.

DOELSTELLINGEN

- De regierol van de overheid op de integrale aanpak van cybersecurity wordt versterkt.
- Nederlandse bedrijven, burgers en overheidsorganisaties geven invulling aan hun verantwoordelijkheden, rechten en plichten ten aanzien van cybersecurity.
- Voor informatiebeveiliging van de digitale overheid bestaat een samenhangend pakket van maatregelen, ter verhoging van de informatiebeveiliging van de digitale basisinfrastructuur, het verder uniformeren en harmoniseren van normenkaders op informatiebeveiliging, waaronder de totstandkoming en implementatie van een Baseline Informatiebeveiliging Overheid. Hierbij is aandacht voor het terugbrengen van de administratieve lasten voor gemeenten op informatiebeveiliging en het bundelen van audits en assessments in één verantwoordingstraject. Verankering van informatiebeveiliging en cybersecurity in de Wet Digitale Overheid is hier onderdeel van.

MAATREGELEN

- De versterkte regie op de integrale aanpak is belegd bij de NCTV.
- Er komt een cybersecurity alliantie, die publieke en private partijen verbindt om de maatregelen uit de NCSA vorm te geven.
- De voortgang van de cybersecurity aanpak zal onder coördinatie van de NCTV en in samenwerking met alle betrokken partijen worden gemonitord en waar nodig worden herijkt aan de hand van technologische en maatschappelijke ontwikkelingen. In 2021 wordt de uitvoering van de agenda integraal geëvalueerd.
- De samenwerking tussen overheid en bedrijfsleven wordt versterkt door de inrichting van het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden. Het groot-helpt-klein principe wordt hierin geoperationaliseerd. Er is ruimte voor verschillende modaliteiten in publiek-private samenwerking.
- Een samenhangend pakket van maatregelen voor informatiebeveiliging en cybersecurity in het openbaar bestuur wordt geadresseerd in de brede agenda Digitale Overheid. De sturing hierop vindt plaats vanuit het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO).

Deze publicatie is een uitgave van de NCTV namens de rijksoverheid.

info@nctv.minvenj.nl