De economische en maatschappelijke noodzaak van meer

CYBER SECURITY

Nederland digitaal droge voeten

De economische en maatschappelijke noodzaak van meer

CYBER SECURITY

Nederland digitaal droge voeten

‘Digitalisering biedt enorme kansen voor de samenleving en economie van de 21ste eeuw’

Voorwoord

Cybersecurity: voorwaarde voor succes van digitalisering

Nederland loopt wereldwijd voorop in de digitalisering. We hebben het grootste internetknooppunt ter wereld, de *Amsterdam Internet Exchange (AMS-IX)*, en diverse razendsnelle, breedbandige telecomnetwerken. Hierdoor zijn we een van de meest ICT-intensieve economieën van Europa. Onze digitale infrastructuur vormt, naast Schiphol en de Rotterdamse haven, de derde mainport van ons land.

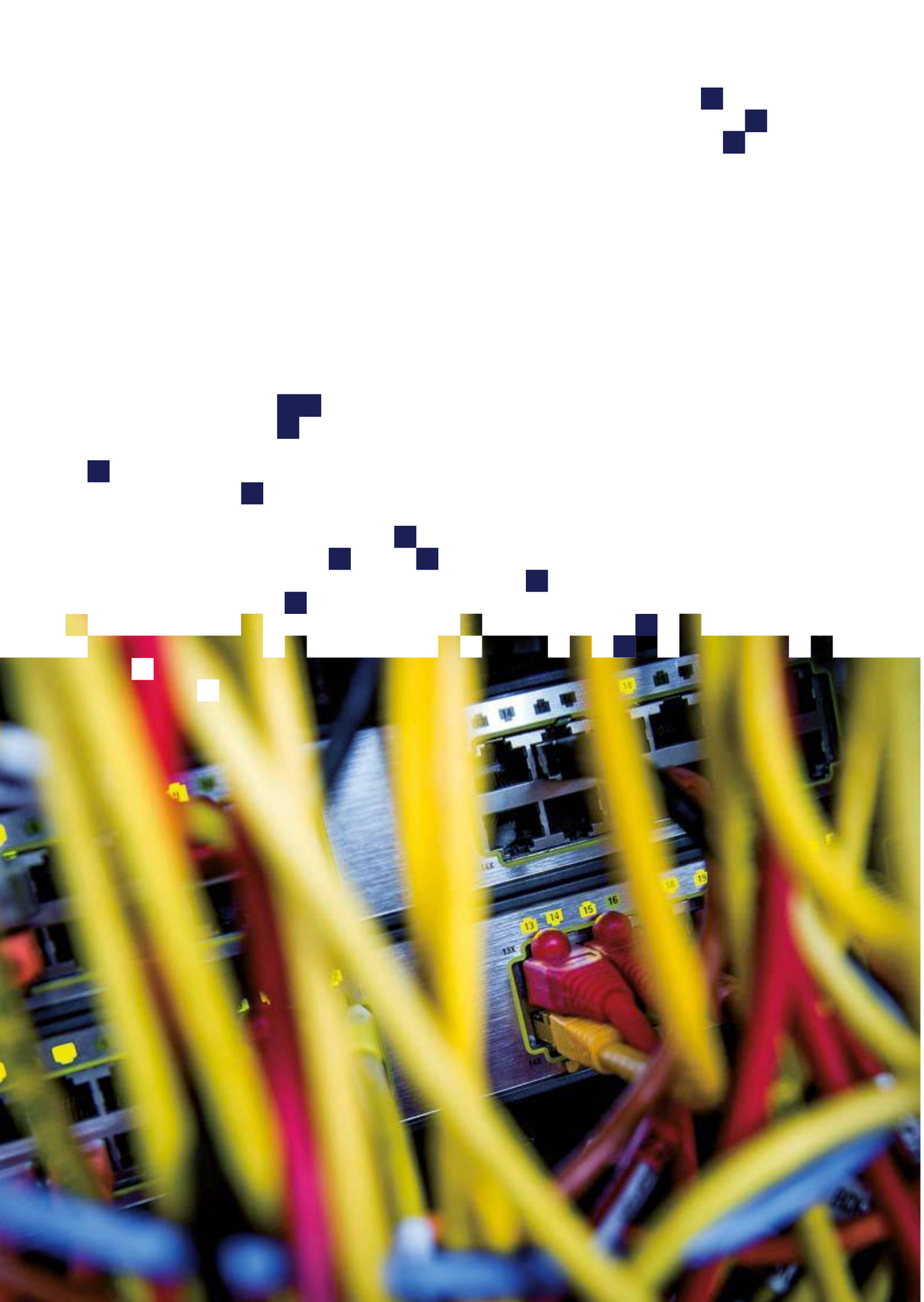
De digitalisering brengt grote economische en maatschappelijke kansen met zich mee. Om die kansen te kunnen blijven benutten, is het noodzakelijk dat we vertrouwen hebben in de digitale wereld en ons er veilig kunnen bewegen.

Uit dit advies blijkt dat cybercriminaliteit groeit en een steeds grotere bedreiging vormt voor onze veiligheid en voor onze economie. Het versterken van cybersecurity in Nederland is geen luxe, maar noodzaak. De burger moet veilig en vertrouwd kunnen leven in een digitale wereld, het bedrijfsleven moet goed zaken kunnen doen en van de overheid mogen we bepaalde waarborgen voor die veiligheid verwachten. Dat begint met meer aandacht voor cybersecurity: in de Tweede Kamer, de bestuurskamer en de huiskamer.

De urgentie is helder. We moeten nú versneld in actie komen voor meer cybersecurity. Dit advies bevat daarom concrete aanbevelingen voor wat overheid, bedrijven en mensen thuis kunnen doen. De belangrijkste adviezen en acties gaan over digitale vaardigheden, de rol van de overheid, de rol van de private sector en de samenwerking tussen beide.
Zo zorgen we er samen voor dat we de cybersecurity in Nederland versterken. En dat de digitale infrastructuur zo veilig en betrouwbaar mogelijk blijft. Wanneer burgers en bedrijven daarop vertrouwen, kunnen we de economische kansen van digitalisering ten volle benutten.

Dit advies is tot stand gekomen na vele gesprekken met experts. Ik dank al deze mensen voor hun nuttige inzichten, suggesties en adviezen. Essentieel waren ook de bijdragen van Donna, Gerrie, Patricia en Simon.

Herna Verhagen
CEO PostNL



Inhoud

Samenvatting

Internet en ICT zijn niet meer weg te denken uit ons dagelijks leven. Dat geldt voor de hele wereld, maar zeker voor Nederland. Ons land loopt voorop in de digitalisering. In bijna alle maatschappelijke sectoren is digitale technologie het belangrijkste middel om informatie te verwerken, te verzenden of het primaire bedrijfsproces aan te sturen.

Nieuwe digitale samenleving en economie

Nederland heeft zich ontwikkeld tot één van de meest ICT-intensieve economieën van Europa, dankzij onze uitstekende digitale infrastructuur. Denk aan het Amsterdam Internet Exchange (AMS-IX), het grootste internetknooppunt ter wereld, en onze razendsnelle, breedbandige telecomnetwerken. Dat brengt ons veel goeds. Zo is Nederland een aantrekkelijk vestigingsland voor ICT-bedrijven en multinationals. E-commerce genereert nieuwe economische activiteiten en werkgelegenheid. Slimme digitale toepassingen dragen bij aan innovatie en vooruitgang in tal van sectoren. Burgers communiceren steeds vaker digitaal met de overheid en krijgen steeds meer slimme meters en apparatuur in huis.

De afgelopen 25 jaar zorgde digitale bedrijvigheid voor ruim een derde van alle economische groei. Ruim 5 procent van ons BNP wordt inmiddels verdiend met ICT. De digitale economie vormt inmiddels een derde mainport, naast Schiphol en de Rotterdamse haven. Een mainport die bovendien sneller groeit dan andere economische sectoren.

Kansen en kwetsbaarheid

Digitalisering biedt dus enorme kansen voor de samenleving en economie van de 21e eeuw. Maar dan is het wel zaak te zorgen dat de digitale wereld veilig en vertrouwd blijft. Of het nu gaat om innovatie, de bescherming van bedrijfsgevoelige informatie, privacy of onze nationale veiligheid: cybersecurity is een basisvoorwaarde voor een welvarende en veilige samenleving in de 21e eeuw. Net zoals we ons land beschermen tegen overstromingen, zullen we ook in de digitale wereld onze dijkbewaking op orde moeten brengen. Alleen zo houden we digitaal droge voeten en kunnen we alle kansen die digitalisering ons land biedt, volop benutten.

Zorgelijke toename cyberdreigingen

Dat is niet vanzelfsprekend, want cyberdreigingen nemen fors toe. Kwetsbaarheden in ICT-systemen, zoals een tekortschietende beveiliging of verouderde software, vormen de achilleshiel van onze digitale veiligheid. *Cybercrime* vormt in Nederland nu al een schadepost van 10 miljard euro. Het Cyber Security Beeld Nederland 2016 (CSBN 2016) schetst een zorgelijk beeld van de veiligheidssituatie in het digitale domein. De dreigingen zijn gericht op diefstal van geld en kostbaar intellectueel kapitaal. Ook het verstoren en saboteren van diensten en processen bij overheden en cruciale maatschappelijke organisaties komt voor.[1] Grootschalige maatschappelijke ontwrichting kan het gevolg zijn, bijvoorbeeld als energiecentrales, transportsystemen of waterkeringen aangevallen worden.

Cybersecurity met spoed versterken

Het is daarom dringend noodzakelijk om de cybersecurity in Nederland te versterken. Dat begint met meer aandacht: in de Tweede Kamer, de bestuurskamer en de huiskamer. We vinden het allemaal vanzelfsprekend dat er regels, stoplichten en rotondes zijn om het verkeer veilig te houden. En dat bedrijven betrouwbare, veilige apparaten, voedsel en drinkwater leveren aan consumenten. De veiligheid van de digitale wereld moet net zo belangrijk

[1] Beleidsreactie op het Cyber Security Beeld Nederland 2016, Ministerie van Veiligheid en Justitie, 7 september 2016

worden als de veiligheid van de wereld om ons heen. Want criminaliteit, (bedrijfs)spionage en terrorisme vormen online net zo'n bedreiging als 'op straat'. De burger moet veilig en vertrouwd kunnen leven in een digitale wereld, het bedrijfsleven moet goed zaken kunnen doen en de overheid zorgt voor de randvoorwaarden om dat mogelijk te maken. Op alle drie de fronten is werk aan de winkel.

Sturing en samenwerking

Om onze welvaart en ons welzijn voor de toekomst veilig te stellen, is naast aandacht voor cybersecurity en bewustwording vooral sturing nodig. Sturing die overheid, politiek en private partijen verbindt op het hogere doel van een digitaal veilige leef- en werkomgeving. Dat cybersecurity per definitie ook een (lands)grensoverschrijdende en internationale component kent, wordt volledig onderkend. Niettemin richt dit adviesrapport zich op verbeteringen en acties die in Nederland kunnen worden genomen om de cybersecurity te verstevigen. Waar relevant wordt ook gewezen op internationale of Europese discussies, wetten en initiatieven.

De belangrijkste acties voor meer cybersecurity

Dit advies bevat een analyse van de belangrijkste kansen en bedreigingen die digitalisering ons land biedt. En het bevat concrete aanbevelingen voor acties bij de overheid, in het bedrijfsleven en bij mensen thuis. Cruciaal is de samenwerking tussen de publieke en private sector.

Om de cybersecurity te versterken en de digitale weerbaarheid te vergroten is een meerjarig actieprogramma inclusief investeringsagenda noodzakelijk. Dit programma zou door een nieuw kabinet in samenwerking met het bedrijfsleven en decentrale overheden opgesteld moeten worden. Voor de uitvoering van dit actieprogramma zou een hoge functionaris moeten worden benoemd, die onder directe verantwoordelijkheid van het kabinet opereert. De overheid zou daarnaast het goede voorbeeld kunnen geven door veiligheid en privacy bescherming een speerpunt te maken in de digitale bedrijfsvoering.

Zorg voor meer sturing vanuit overheid:

- Eenduidige politieke aansturing van de digitale mainport via een onderraad van de Ministerraad
- Aanstellen van een hoge functionaris voor het opstellen en uitvoeren van een meerjarig actieprogramma cybersecurity inclusief investeringsagenda
- Op orde brengen van de eigen digitale infrastructuur en bedrijfsvoering
- Moderniseren van de bevoegdheden van de Nederlandse opsporings-, inlichtingen- en veiligheidsdiensten, met oog voor *checks & balances*
- Toekomstbestendige wetten en regels maken

Stimuleer de eigen verantwoordelijkheid bij de private sector:

- Basis op orde hebben; voldoen aan randvoorwaarden voor cybersecurity
- Invulling geven aan zorgplicht op het gebied van cybersecurity
- Ketens veiliger maken door het invoeren van een ketenverantwoordelijkheid
- Inzet van een accreditatie- of certificeringssystematiek

Verstevig de samenwerking tussen de private en publieke sector:

- Onderzoek naar cyberaanvallen intensiveren voor snellere respons en betere preventie, door uitbreiding van de Information *Sharing and Analysis Centres* (ISAC's), het Nationaal Detectie Netwerk (NDN) en het Nationaal Respons Netwerk (NRN)
- Sturing en coördinatie op publiek-private samenwerking door hoge functionaris en cybersecurity-programma
- Borgen van impactvolle advisering door (geëvolueerde) Cyber Security Raad (CSR)
- Investeren in cybersecurity volgens de '10 procent-maatstaf'

Maak Nederland digitaal vaardig

- Versneld opnemen van digitale geletterdheid, inclusief cybersecurity, in het kerncurriculum voor basis- en voortgezet onderwijs
- Kennisontwikkeling op het gebied van cybersecurity stimuleren
- Doelgerichte voorlichtingscampagnes voeren over cybersecurity voor specifieke doelgroepen (waaronder mkb-bedrijven) en het brede publiek

Hoofdstuk 1

Digitalisering en vooruitgang

1.1 De nieuwe digitale samenleving en economie

Internet en ICT zijn sinds het einde van de 20e eeuw niet meer weg te denken uit ons dagelijks leven. Dat geldt voor vrijwel de hele wereld, maar zeker voor Nederland. In bijna alle maatschappelijke sectoren is de digitale technologie het belangrijkste middel om informatie te verwerken, te verzenden of het primaire bedrijfsproces aan te sturen.

Internet en digitale processen zijn vervlochten geraakt met ons sociale leven, betaalgedrag en consumptie, contacten en relaties, werk, gezondheid en communicatie met de overheid. Naast de fysieke wereld is de laatste decennia een nieuwe wereld ontstaan: de digitale of *cyber*wereld. En net zoals de industriële revoluties van de 18e en 19e eeuw heeft de digitale revolutie[2] grote gevolgen voor onze maatschappij en economie.

In de periode 1990-2013 kwam 36 procent van de economische groei in Nederland voor rekening van digitale bedrijvigheid.[3] Nederland heeft inmiddels, samen met Groot-Brittannië, de meest ICT-intensieve economie van Europa. Ruim 5 procent van ons Nationaal Inkomen werd in 2015 verdiend met ICT.[4] De *Amsterdam Internet Exchange (AMS-IX)* is het grootste internetknooppunt ter wereld en Nederland beschikt over razendsnelle en breedbandige telecomnetwerken. Deze uitstekende digitale infrastructuur vormt, naast Schiphol en de Rotterdamse haven, de derde mainport van ons land.[5]

[2] The Digital Revolution is the change from mechanical and analogue electronic technology to digital electronics which began with the adoption and proliferation of digital computers and digital record keeping that continues to the present day. Implicitly, the term also refers to the sweeping changes brought about by digital computing and communication technology during (and after) the latter half of the 20th century. Analogous to the Agricultural Revolution and Industrial Revolution, the Digital Revolution marked the beginning of the Information Age.Central to this revolution is the mass production and widespread use of digital logic circuits, and its derived technologies, including the computer, digital cellular phone, and the Internet. Wikipedia.

[3] De impact van ICT op de Nederlandse Economie, Dialogic, 2014

[4] ICT, kennis en economie 2015, CBS, 2015

[5] In navolging van de motie Verhoeven. Kamerstukken 34300, nr. 45.

‘Nederland heeft zich ontwikkeld tot een van de meest gedigitaliseerde landen ter wereld’

Nederland heeft zich ontwikkeld tot een van de meest gedigitaliseerde landen ter wereld: 97 procent van de huishoudens en 91 procent van de bedrijven heeft toegang tot vast snel internet (30 megabits per seconde (Mbps) of meer).[6]
De hosting- en housingsector behoort tot de top van Europa en heeft grote invloed op de aantrekkelijkheid van ons vestigingsklimaat voor buitenlandse bedrijven. Het belang van digitalisering voor Nederland houdt bovendien niet op bij de landsgrenzen. Nederland is, door de AMS-IX, dé *Digital Gateway to Europe* en voor veel bedrijven ook de *Gateway to the World*. Een groot deel van het wereldwijde internetverkeer loopt immers via dit internetknooppunt.

Van de buitenlandse investeringen in Nederland is 25 procent gerelateerd aan ICT, wat aansluit bij de Nederlandse ambitie om een aantrekkelijk, betrouwbaar en veilig vestigingsklimaat te bieden. De Nederlandse hostingindustrie heeft een internationaal sterke positie. Die is te danken aan de relatief grote bandbreedte. Bovendien is overal ter wereld sprake van dalende kosten van opslag, transport en verwerking en de exponentiële groei van hoeveelheid data. Nederland staat de laatste jaren steeds in de top 10 van meest concurrerende en innovatieve economieën wereldwijd (Global Innovation Index).[7]

De ICT-sector voegt jaarlijks zo’n 34 miljard euro, oftewel 5,3 procent, toe aan het bnp. Ter vergelijking: de haven van Rotterdam en luchthaven Schiphol voegen respectievelijk 2,3 en 2,1 procent toe aan de werkgelegenheid.[8] De digitale economie groeit harder dan de traditionele economie en biedt Nederland daarom enorme kansen voor de toekomst.

Dat Nederland een aantrekkelijk land is voor ICT-bedrijven, blijkt niet alleen uit het feit dat multinationals zoals Microsoft en Google grote nieuwe datacenters bouwen in de Wieringermeer en de Eemshaven en dat een groot aantal internationale spelers hun hoofdkantoor in Nederland hebben. Het blijkt ook uit de snelle groei van succesvolle, innovatieve startups. Zo is de van oorsprong Nederlandse hotelreserveringssite Booking.com, opgericht begin jaren 90, binnen enkele jaren uitgegroeid van eenmanszaak tot wereldwijde speler. In diezelfde tijd richtten slimme studenten Coolblue op, dat inmiddels bestaat uit 319 specialistische webshops, 7 fysieke winkels en ruim 1.500 medewerkers. Een ander toonaangevend voorbeeld is dat van het Amsterdamse Adyen, inmiddels wereldwijd een van de grootste online betalingsproviders, met klanten als Facebook, Spotify en Airbnb. Talloze andere Nederlandse e-commercebedrijven zijn gevolgd, veelal internationaal georiënteerd. Ook voor veel traditionele retailbedrijven zijn online verkoopkanalen onmisbaar geworden.

Nederland kent een aantal top-securitybedrijven met hoogwaardige specialistische kennis op het terrein van cybersecurity, zoas FoxIT en Deloitte Nederland.[9] Die Nederlandse cybersecuritymarkt is ook een economische groeikans.[10]

De digitale economie biedt enorme kansen aan innovatieve startups en toonaangevende mkb-bedrijven. Overal in het land zijn rondom universiteiten en hogescholen startup-incubators ontstaan. Op hightech-campussen wordt aan nieuwe innovaties gewerkt. Voor de werkgelegenheid van nieuwe generaties Nederlanders is het daarom belangrijk dat er ook in het (beroeps) onderwijs meer aandacht komt voor digitalisering en ICT.

6 Ontwikkelingen omtrent snel internet in het buitengebied, Kamerbrief 19 mei 2016, Ministerie van Economische Zaken
7 Global Competitiveness Reports, 2014, 2015, 2016, World Economic Forum, 2016
8 Rapport werkgroep Digitale Economie ten behoeve van de Studiegroep Duurzame Groei, Ministerie van Economische Zaken, juli 2016
9 Deloitte Nederland won op 14 september 2016 voor de vijfde keer de ‘Global CyberLympics Security Challenge’ die dit jaar in Atlanta (VS) werd gehouden.
10 Economische kansen Nederlandse cybersecurity-sector, SEO/Verdonck Klooster i.o.v. Ministerie van Economische Zaken, 17 mei 2016

1.2 Het dreigingsbeeld is ronduit zorgelijk

De digitalisering brengt grote economische en maatschappelijke kansen met zich mee. Om die kansen te kunnen blijven benutten, is het noodzakelijk dat we vertrouwen hebben in de digitale wereld en ons er veilig kunnen bewegen.

Kwetsbaarheden in ICT-systemen, zoals lekken, programmeerfouten en tekortschietende beveiliging vormen de achilleshiel van digitale veiligheid. Dit brengt de bescherming van persoonsgegevens en bedrijfsgegevens in gevaar. Systemen raken snel verouderd en updates worden soms te laat geïnstalleerd. Het bereik en de impact van cyberaanvallen, waar ook ter wereld, wordt nog eens vergroot doordat in toenemende mate bestaande apparatuur via bestaande netwerken aan internet wordt gekoppeld. Het gevaar van zwakke schakels in de digitale keten neemt toe. De ketenafhankelijkheden en connectiviteit van industriële controlesystemen maken dat de vitale processen in Nederland kwetsbaar zijn. Ketens zijn zo sterk als de zwakste schakel.[11]

Cybersecurity is een basisvoorwaarde voor een welvarende en veilige samenleving in de 21e eeuw. De afgelopen jaren zijn belangrijke stappen gezet om deze risico's beter in kaart te brengen. Op basis van recente analyses van de Nationale Politie en Nederlandse inlichtingen- en veiligheidsdiensten moeten we erkennen dat het dreigingsbeeld ronduit zorgelijk is. De actuele dreiging is weergegeven in het Cyber Security Beeld Nederland 2016 (CSBN 2016) van het ministerie van Veiligheid en Justitie. Daarin is de toegenomen dreiging in het afgelopen jaar zichtbaar gemaakt op een aantal verschillende thema's en worden ontwikkelingen en trends naar de toekomst geschetst. De dreigingen zijn gericht op diefstal van geld en kostbare commerciële informatie maar richten zich ook op de ondermijning van politiek en bestuur en het verstoren of saboteren van diensten en processen waar overheden en de samenleving van afhankelijk zijn voor hun functioneren.[12] Er is sprake van zeer reële en toenemende kwetsbaarheden en dreigingen tegen Nederlandse belangen, zowel economische, maatschappelijke als geopolitieke.

Cybercriminaliteit

Nederland is door zijn uitstekende internetinfrastructuur en grote aantal hostingbedrijven en providers helaas ook steeds aantrekkelijker voor cybercriminelen. Cybercriminaliteit komt voor in allerlei vormen (onder andere hoogwaardige *malware, ransomware, phishing, bad hosting*) en wordt bovendien steeds vernuftiger en professioneler. Slachtoffers kunnen zich moeilijker beschermen en de aangerichte schade wordt omvangrijker. Zorgelijk is bovendien dat er een criminele dienstensector rond *cybercrime* is ontstaan. Hierdoor kan iedereen complexe cyberaanvallen uitvoeren door deze 'in de markt' in te kopen of uit te besteden, zogeheten *cybercrime as a service*.

Deze geavanceerde criminele activiteiten richten zich vooral op het bedrijfsleven, van mkb-bedrijven tot multinationals. De wereldwijde schade van *cybercrime* werd in 2014 op ongeveer 400 miljard euro geschat. De becijferde schadepost voor Nederland als gevolg van *cybercrime* en spionage is jaarlijks 10 miljard euro, circa 1,5 procent van het bnp. Door de groei van de digitale economie neemt dit toe.[13] Onderzoek laat zien dat een significant deel van de schade als gevolg van cyberrisico's daarnaast niet opgemerkt of gedetecteerd is. Een schatting van die schade is nog eens 4,6 miljard euro.[14] Een ander voorbeeld van cybercriminaliteit die toeneemt is *bad hosting*, het fenomeen waarbij servers worden gebruikt voor het hosten van *cybercrime*. Het komt voor dat hostingbedrijven niet weten dat hun servers en diensten voor *cybercrime* worden ingezet.

[11] CSBN 2016, Nationaal Cyber Security Center, Ministerie van Veiligheid en Justitie, september 2016
[12] Beleidsreactie op het Cyber Security Beeld Nederland 2016, Ministerie van Veiligheid en Justitie, 7 september 2016
[13] Digitale agenda, Vernieuwen, vertrouwen, versnellen, Ministerie van Economische Zaken, 2016
[14] Cyber Value at Risk in the Netherlands, Deloitte, 2016

Tegelijkertijd zijn er ook hostingbedrijven die er actief bij betrokken zijn. Bad hosting is een negatief bijproduct van de degelijke digitale infrastructuur in Nederland.
Het Team High Tech Crime (THTC) van de Nationale Politie ziet een verschuiving van veelplegers van het fysieke domein (huisinbraken, diefstal, plofkraken) naar de digitale wereld, omdat daar makkelijker en anoniemer geld te verdienen valt. Het aantal meldingen van cybercrime was in 2015 al hoger dan het aantal gemelde fietsdiefstallen (98.916).[15] Het Openbaar Ministerie (OM) voorziet dat over vijf jaar 50 procent van het aantal te behandelen zaken een vorm van cybercrime betreft.[16]

De opsporing van internetcriminelen (wereldwijd) wordt moeilijker door het bestaan van Tor, een afkorting voor *The onion router*. Het Tor-netwerk vermomt iemands identiteit door het omleiden van internetverkeer over verschillende Tor-servers, en het versleutelen van het verkeer, zodat het niet naar een persoon is te herleiden. Het systeem is ontwikkeld om bijvoorbeeld politieke dissidenten te helpen om hun mening te uiten, zonder dat zij het risico lopen om gearresteerd te worden. Helaas is een neveneffect dat gebruikers van internet met kwade bedoelingen 'anoniem' hun gang kunnen gaan.

Cyberspionage en chantage

Nederlandse overheidsinstellingen en in Nederland gevestigde bedrijven zijn structureel doelwit van digitale spionage door onder andere Rusland en China. We weten dat verschillende staten gerichte campagnes en aanvallen uitvoeren om planmatig hoogwaardige kennis en bedrijfsinformatie (intellectueel eigendom) van Nederland te stelen. Het doel is om de nationale economie en concurrentiepositie te versterken en de eigen militaire slagkracht in het digitale domein te vergroten.[17] Inmiddels heeft de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) kunnen vaststellen dat bedrijven uit de topsectoren high tech, energie, water, chemie, life sciences & health, agri & food en tuinbouw te maken hebben (gehad) met digitale spionage. Verschillende bedrijven zijn bij herhaling door verschillende actoren aangevallen.

Cyberspionage gaat direct ten koste van het Nederlandse verdienmodel. Dat gebeurt niet alleen bij grote bedrijven. Ook mkb'ers en startups, die innovatieve ideeën ontwikkelen, zijn regelmatig doelwit van cybercriminelen die intellectuele eigendommen willen stelen. Dit is des te schadelijker als we ons realiseren dat ons bedrijfsleven en onze export zeer kennisintensief zijn. Voor toonaangevende bedrijven in bijvoorbeeld de tuinbouw en uitgangsmaterialen (pootgoed, plantgoed en zaaizaad), bio- en life sciences, maar ook '*Dutch Design*', kan cyberspionage de kern van het verdienmodel raken. Bij ongeveer een derde van de bedrijven uit de *Research & Development* Top 25 van de afgelopen drie jaar heeft de AIVD geconstateerd dat zij doelwit zijn (geweest) van digitale spionage (bron: technisch weekblad). Hierbij zijn aanvallen waargenomen op diverse R&D-projecten van Nederlandse multinationals, die investeringen vertegenwoordigen van tientallen fte's en vele miljoenen euro's. Digitale spionage vormt dus een concrete dreiging voor het innovatie- en verdienvermogen van Nederland.

In circa twee derde van de gevallen waarin de AIVD contact opneemt met een aangevallen bedrijf, is dat zich niet bewust van de door de dienst waargenomen spionageactiviteiten.
De aangetroffen infectieduur varieert van enkele dagen tot ruim twee jaar. Daarbij lag het toegangsniveau van de actor op het niveau van domein administrator, wat wil zeggen dat ze de hoogste toegangsrechten hadden op de digitale infrastructuur van die bedrijven.

Daarnaast is het Nederlandse ambtelijke en politieke apparaat doelwit van gerichte digitale aanvallen. Dit vormt een aanzienlijke bedreiging voor de integriteit en effectiviteit van de Nederlandse rechtsstaat.

Cybersabotage

Naast criminaliteit en spionage vormt cybersabotage een groot risico voor Nederland. De gevolgen van moedwillige verstoring van vitale sectoren, denk aan energiecentrales, drinkwatervoorziening, betalingsverkeer of telecom, kan tot grote maatschappelijke en economische ontwrichting leiden. Een storing op Schiphol kan het luchtverkeer verstoren. Een aanval op de NS of ProRail kan het treinverkeer platleggen. Cybersabotage van energiecentrales kan de energievoorziening in gevaar brengen. Stuk voor stuk voorbeelden met grote maatschappelijke en economische schade voor Nederland. Een voorbeeld hiervan was DigiNotar, de grootste ICT-crisis waar de Nederlandse overheid ooit mee te maken heeft gehad. Het begon met een digitale inbraak, en had kunnen eindigen met het uitvallen van vitale overheids-ICT. Alleen snel en adequaat crisismanagement heeft deze uitkomst kunnen voorkomen. Door een inbraak bij DigiNotar (een partij die volledig vertrouwd werd door de overheid, en waarop veel aangesloten (overheids)systemen leunden), kon de vertrouwelijkheid van met de overheid uitgewisselde gegevens niet gegarandeerd worden.

Ook individuele bedrijven kunnen slachtoffer worden van cybersabotage, bijvoorbeeld door DDoS-aanvallen. Dergelijke aanvallen kunnen leiden tot uitval van websites en daarmee webshops, ernstige vertraging en verstoring van netwerken, en een grotere kans op hacken. We zien in de wereld, ver weg maar ook dichter bij huis, dat deze risico's reëel zijn. Aan de grenzen van Europa vinden hybride conflicten plaats waarbij cyberaanvallen worden ingezet voor zowel spionage- als sabotagedoeleinden in geopolitieke conflicten. Er zijn aanwijzingen dat ook Nederland een voorstelbaar doelwit is van sabotage-activiteiten via digitale kanalen.

Cybersecurity in vergelijking met andere dreigingen

In het concept Nationaal Veiligheidsprofiel (NVP)[18] zijn alle verschillende dreigingstypen in Nederland geïdentificeerd en door experts beoordeeld op hun 'waarschijnlijkheid' en 'impact'. Het NVP laat zien dat cyberspionage tegen de overheid een waarschijnlijk risico is, meer nog dan bijvoorbeeld epidemieën, natuurrampen en nucleaire ongevallen.
De (toenemende) cyberdreigingen gericht op verstoring van het internet, de telecomsector en spionage gericht op het bedrijfsleven hebben een fors hoge impact (potentiële maatschappelijke ontwrichting). Duidelijk mag zijn dat we cyberdreigingen niet meer kunnen onderschatten. Ze zijn net zo reëel en hebben minstens net zoveel impact als dreigingen in de fysieke wereld.

[15] http://stavc.nl/diefstalcijfers/fietsdiefstal/
[16] Uitspraak van procureur-generaal Gerrit van der Burg van het Openbaar Ministerie (OM) in Nieuwsuur van 16 juni 2016
[17] Jaarverslag 2015 Algemene Inlichtingen- en Veiligheidsdienst, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2015
[18] Nationaal VeiligheidsProfiel (NVP), 2016 (concept), Analystennetwerk Nationale Veiligheid

1.3 Vertrouwen en veiligheid in de digitale wereld

Om de kansen en mogelijkheden van de nieuwe digitale samenleving en economie optimaal te benutten, moeten we ervoor zorgen dat de digitale wereld veilig en vertrouwd blijft. Of het nu gaat om innovatie, de bescherming van bedrijfsgevoelige informatie, privacy, de digitale dienstverlening of onze nationale veiligheid: cybersecurity is een basisvoorwaarde voor een welvarende en veilige samenleving in de 21e eeuw.

In de 19e eeuw, ten tijde van de Industriële Revolutie, stimuleerde de 'koning-koopman'[19] de economie onder meer door het aanleggen en moderniseren van wegen, kanalen en spoorlijnen. Publieke investeringen in dat type infrastructuur zijn sinds die tijd een belangrijke pijler onder het economisch beleid van de overheid geweest. In de digitale wereld ligt dat anders. In tegenstelling tot onze water, spoor- en snelwegen is de digitale infrastructuur voor 80 procent in handen van private partijen. Snelle technologische veranderingen en innovaties zorgen bovendien voor een veel kortere levensduur van digitale infrastructuur. Een groot deel van de verantwoordelijkheid voor de veiligheid van de digitale wereld ligt daarom bij het bedrijfsleven. De rol van de overheid is daardoor anders, maar niet kleiner. De overheid heeft, net als in de fysieke wereld, de taak om de veiligheid van het digitale domein en de digitale infrastructuren te borgen.

Technologische ontwikkelingen onderstrepen alleen maar verder het belang van cybersecurity als we ons realiseren dat hierdoor:

- steeds meer informatie over onszelf digitaal beschikbaar is. Verschillende partijen gebruiken die informatie voor diverse (commerciële) doeleinden. Denk daarbij ook aan ontwikkelingen als *big data* en *quantum computing*.
- machines (computers) en robots standaard handelingen en activiteiten gaan overnemen van mensen (*machine learning*).
- voorwerpen en producten zelfstandig met ons en met elkaar gaan communiceren (*internet of things*).
- *industrial Control Systems en SCADA*[20] systems in toenemende mate via het internet worden ontsloten, hoewel ze hier niet voor ontworpen zijn. Bijvoorbeeld binnen de vitale infrastructuur gaan internetkoppelingen een steeds grotere rol spelen (te denken valt aan digitale processen binnen waterbeheer, de energievoorziening, luchtvaart, etc.).
- computers hun intrede doen in het menselijk lichaam (nanotechnologie, e-health).

Het is daarom evident dat cybersecurity een cruciale plaats verdient in de ontwikkeling en gebruik van de technologieën die dit mogelijk maken.

De overheid blijft verantwoordelijk voor de nationale veiligheid, het voorkomen en beperken van maatschappelijke ontwrichting, het borgen van de veiligheid binnen de digitale infrastructuur, veilig gebruik ervan en de bescherming van onze grondrechten. Ook in de digitale wereld zijn toegankelijkheid (non-discriminatie), privacy en gelijke behandeling essentiële Nederlandse waarden. De concrete vormgeving van deze waarden in wet- en regelgeving en het beschermen van de nationale veiligheid, blijven ook in de digitale wereld essentiële taken voor de overheid. De snelheid waarmee de digitalisering zich ontwikkelt vergt daarbij blijvende en voortdurende aandacht.

[19] nl.wikipedia.org/wiki/Willem_I_der_Nederlanden
[20] SCADA, afkorting van Supervisory Control And Data Acquisition, is het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen.

1.4 Van bewustzijn naar oplossingen

In de voorgaande paragrafen las u over de economische kansen van digitalisering, het belang van cybersecurity om die kansen te benutten, en de verschillende cyberdreigingen die we het hoofd moeten bieden. We hebben onze analyse en ideeën over oplossingen om de cybersecurity te verbeteren besproken met een groot aantal betrokkenen (zie bijlage 1 voor de onderzoeksopzet bij dit adviesrapport). De volgende punten kwamen in de gesprekken naar voren.

‘*Cybercrime* is niet iets wat alleen anderen overkomt’

Nederland heeft een aantrekkelijk vestigingsklimaat voor bedrijven
Nederland heeft een groot aantal informatieknooppunten, een hoge mate van connectiviteit en veel internationale spelers zijn in ons land actief. Minstens zo belangrijk voor het vestigingsklimaat is onze open en democratische samenleving. De overheid is transparant, zorgt voor naleving van wetten en regels, en toezicht is voorspelbaar en duidelijk. Het klimaat voor startups is goed, wat onder andere blijkt uit het feit dat Nederland op plaats vier staat in de ranking voor beste startup-ecosystemen in Europa.[21] Cruciaal voor het Nederlandse vestigingsklimaat is dat het internet open, veilig en vrij blijft, met voldoende waarborgen voor privacy, innovatie en veiligheid van burgers en bedrijven. Nederland kan zich in de toekomst internationaal blijven positioneren als een veilige en betrouwbare vestigingsplaats als de veiligheid en betrouwbaarheid van het digitale domein gegarandeerd zijn. Tegelijkertijd constateren we ook dat er een economische groeikans is voor de cybersecurity-sector.

Groter maatschappelijk bewustzijn nodig van het dreigingsbeeld en de noodzaak van cybersecurity
Cyberdreigingen nemen toe, zo signaleren de Nederlandse inlichtingen- en veiligheidsdiensten en bedrijven. In verschillende gesprekken kwam naar voren dat de risico’s en gevaren in de digitale wereld onderschat worden. De reële cyberdreiging is ernstiger dan veel bedrijven, burgers en ook overheidsorganen en -diensten zich realiseren. In tegenstelling tot het belang van fysieke veiligheid erkennen en herkennen de meeste mensen de noodzaak van cybersecurity veel minder snel. Dat levert onnodige risico’s op.

Het uitgangspunt zou moeten zijn dat cybercriminelen elk Nederlands bedrijf en elk netwerk als doelwit zien. *Cybercrime* en cyberspionage is niet iets wat alleen anderen overkomt. Wanneer bedrijven niet investeren in hun cybersecurity brengt dat op den duur hun bedrijfsprocessen en daarmee de eigen concurrentiepositie ontegenzeggelijk in gevaar. Security als randvoorwaarde of *license to operate* in het productieproces moet vanzelfsprekend worden. Voor veel grote bedrijven geldt dit al, zoals Amazon en Google, maar ook kleinere ondernemingen kunnen zich geen naïviteit veroorloven. Net zoals in de voedingsindustrie de voedselveiligheid cruciaal is, hoort de cybersecurity van producten, diensten en processen ook gegarandeerd te zijn. Het afgelopen jaar zijn veel digitale aanvallen waargenomen op bedrijven in Nederland, waarbij het motief economische spionage was. Twee derde van de getroffen bedrijven had deze aanvallen niet zelf waargenomen.[22]

[21] 2015 Global Startup Ecosystem Report, Compass, 2015
[22] CSBN 2016, Nationaal Cyber Security Center, Ministerie van Veiligheid en Justitie, september 2016

Het is noodzakelijk om (operationele) informatie te delen tussen publiek en privaat, bijvoorbeeld over getroffen maatregelen. Jaarlijks wordt door het ministerie van Veiligheid en Justitie het Cyber Security Beeld Nederland uitgegeven. Daarin worden de cyberdreigingen en belangen (tegengaan van maatschappelijke ontwrichting en schade in de samenleving) inzichtelijk gemaakt. Al enkele jaren wordt in deze publicatie geconstateerd dat er onvoldoende zicht is op de maatregelen die getroffen worden door publieke en met name private organisaties. Dit betekent dat we onvoldoende zicht hebben op de weerbaarheid van Nederland.

Meer stimulans nodig om legacy-problemen op te lossen

Legacy staat voor het probleem van verouderde versies van software die gebaseerd zijn op inmiddels achterhaalde technologie. Deze voldoen voor de gebruiker nog steeds, maar worden niet meer of minimaal onderhouden. Dit probleem speelt zowel bij mensen thuis als bij bedrijven en sommige overheden. Het komt regelmatig voor dat gebruikers of softwareproducenten onvoldoende prikkels hebben om legacy-problemen op te lossen. Maar wanneer software en systemen niet meer worden onderhouden, holt de cybersecurity hard achteruit. Zolang aan toekomstige diensten en software geen cybersecurity-eisen worden opgenomen, blijven legacy-problemen ontstaan en bestaan.

Grote behoefte aan meer kennis en vaardigheden

Door de digitalisering van de economie en het toenemende belang van data wordt de behoefte aan mensen met ICT-competenties en specifieke kennis van cybersecurity groter. Dat geldt niet alleen voor hoger geschoold personeel, maar ook voor vakmensen met een beroepsopleiding. Voor vrijwel alle sectoren en beroepen is begrip van computers en ICT-vaardigheden vereist. Onlosmakelijk onderdeel daarvan is dan ook cybersecurity.

In alle interviews kwam steevast naar voren dat Nederland op een aantal plekken al over veel kennis beschikt. Neem bijvoorbeeld de ereplaatsen in de Cyberlympics van Deloitte en KPN. Ook zijn er de experts van het Nationaal Cyber Security Center (NCSC) van het ministerie van Veiligheid en Justitie en het THTC van de politie. Juist vanwege de uitstekende digitale infrastructuur zien Nederlandse experts en bedrijven veel misstanden en dreigingen voorbij komen. We moeten daarom blijvend investeren in ICT-kennis en vaardigheden op alle onderwijsniveaus, in alle lagen van de bevolking. Tegelijkertijd signaleren verschillende deskundigen dat er nu al sprake is van schaarste aan ICT-specialisten. Meer investeringen in specialistische en generieke opleiding en scholing is belangrijk om de ervaren tekorten nu en in de toekomst te voorkomen.

Kerntaken van overheid in digitale wereld even belangrijk als in fysieke wereld

De overheid draagt bij aan een veilig en stabiel Nederland door dreigingen van vitale belangen te onderkennen en de weerbaarheid en bescherming van die belangen te versterken. De gevolgen voor Nederland zijn bijvoorbeeld groot (voor burgers en sommige typen bedrijven) wanneer de (drink)watervoorziening in een groot gebied voor langere tijd wordt stilgelegd door in te breken in de gedigitaliseerde besturingsprocessen.
Mensen maken aanspraak op veiligheid. Thuis, op straat, maar ook in de digitale wereld. Mensen kunnen zelf veel doen om hun digitale veiligheid te vergroten. Net zoals goede sloten op huizen en bedrijfspanden vanzelfsprekend zijn, moet de beveiliging van computers en systemen goed

‘Door versnippering is onduidelijk welke partij voor welke taak verantwoordelijk is’

geregeld zijn. Maar er ligt in het digitale domein ook een nadrukkelijke taak voor de overheid waar het gaat om het maatschappelijk belang: het voorkomen en beperken van maatschappelijke ontwrichting in de samenleving, net zoals dat geldt voor de fysieke wereld en infrastructuur. Het is de taak van de overheid om te bewaken dat niemand wordt buitengesloten in de digitale wereld (non-discriminatie), om onze privacy te beschermen en ervoor te zorgen dat in algemene zin wetten en regels worden nageleefd. De concrete vormgeving van de bescherming van de persoonlijke levenssfeer (zoals vastgelegd in de Grondwet) of bescherming van persoonsgegevens in de snel veranderende digitale wereld, waarbij de infrastructuur ook nog eens grotendeels in private handen is, betekent dat de overheid voortdurend alert moet zijn en tijdig en adequaat moet inspelen op nieuwe ontwikkelingen. Het is daarbij van belang de balans tussen veiligheid en privacy te bewaken, met een reëel oog voor de toegenomen cyberdreigingen.

Coördinatie en sturing cruciaal, zowel bij de overheid zelf als voor publiek-private samenwerking

Dat de overheid een cruciale rol heeft in de digitale wereld is, zoals hierboven ook blijkt, voor iedereen duidelijk. Maar de invulling ervan is nog niet uitgekristalliseerd. Dat heeft geleid tot een beperkte coördinatie en sturing. Ook is er sprake van versnippering over een groot aantal ongelijksoortige partijen. De beleidsverantwoordelijkheid voor ICT en specifiek cybersecurity is verdeeld over ten minste vijf departementen:

- ICT en economie bij het ministerie van Economische Zaken;
- nationale veiligheid, het NCSC, opsporing en vervolging (Politie en Openbaar Ministerie) en coördinatie op crisisbeheersing bij het ministerie van Veiligheid en Justitie;
- de AIVD en ICT van de overheid bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties;
- onderwijs en kennisinnovatie bij het ministerie van Onderwijs, Cultuur en Wetenschap;
- inzet van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) bij het ministerie van Defensie.

Bovendien zijn tal van agentschappen, zelfstandige bestuursorganen (ZBO’s) en toezichthouders actief. Daarnaast heeft elke gemeente in Nederland een eigen ICT- en cybersecuritybeleid. Er is (politiek) geen eenduidig aanspreekpunt. In de uitvoering van het cybersecuritybeleid zijn verschillende partijen actief: departementen, opsporingseenheden van de politie, inlichtingendiensten, gemeenten, onderwijsinstellingen, ZBO’s, agentschappen en private ondernemingen. Daarnaast wordt ook op Europees niveau regelgeving gemaakt en hebben we te maken met internationale partners (ook buiten Europa).

Informatie-uitwisseling tussen overheidspartijen onderling en tussen private partijen en overheden is niet voldoende geborgd. Door versnippering verliest men zicht. Bovendien is onduidelijk welke partij voor welke taak verantwoordelijk is, en blijft vaak onzichtbaar wat gebeurt aan opvol-

ging. Budgetten zijn versnipperd. Op sommige terreinen ontbreken bevoegdheden of is wetgeving gedateerd, waardoor de overheid onvoldoende is uitgerust om te zorgen voor detectie en monitoring. Dat gaat ten koste van zowel onze veiligheid als innovatie en onze burgerrechten.

Voorbeelden van publiek-private samenwerking

Gelukkig zijn er ook veel goede voorbeelden, bijvoorbeeld de samenwerking tussen partijen in de financiële sector, het NCSC en de Nederlandse opsporings-, inlichtingen- en veiligheidsdiensten. Banken wisselen gegevens uit, waardoor het makkelijker wordt om criminelen te herkennen en sneller in te grijpen. De Nederlandse opsporings-, inlichtingen- en veiligheidsdiensten. doen dat ook. Op een praktische en pragmatische manier werken de veiligheidsdiensten en private sectoren samen. Ook binnen The Hague Security Delta wordt samenwerking gezocht: dat is een groeiend netwerk van bedrijven, overheden en kennisinstellingen in binnen- en buitenland die samenwerken om producten, diensten of kennis te ontwikkelen voor een veiligere wereld.

Tegelijkertijd is die samenwerking vrijblijvend en niet structureel geborgd. De huidige informatie-uitwisseling tussen bedrijven en overheid is gericht op het veilig houden en maken van internet. Het gebeurt aan de hand van incidenten of omdat de partijen elkaar kennen en vertrouwen. Dat is goed, maar biedt onvoldoende garanties voor de toekomst. We kunnen niet alleen op de waardevolle Nederlandse traditie van polderen en maatschappelijk overleg vertrouwen voor een veilige digitale wereld.

Een voorbeeld van meer structurele samenwerking tussen overheid en private partijen zijn de Information *Sharing and Analysis Centres* (ISAC's). Om dreigingen tegen vitale sectoren van de economie tegen te gaan zijn inmiddels zeventien ISAC's opgericht en zijn er twee in oprichting. Dit zijn publiek-private samenwerkingsverbanden waarin bedrijven onderling informatie en ervaringen uitwisselen over cybersecurity, bij elkaar gebracht door het NCSC. Bedrijven leren in een vertrouwde omgeving van elkaar en kunnen wederzijdse bijstand verlenen als zich (acute) problemen voordoen. De ISAC's zorgen voor meer schaalgrootte om verdediging te kunnen bieden tegen complexe aanvallen die voor individuele bedrijven niet haalbaar is. De ervaringen hebben geleerd dat het erg belangrijk is dat de partijen elkaar vertrouwen om informatie te kunnen en willen delen. Het opstellen van regels over vertrouwelijkheid heeft daar in een aantal ISAC's aan bijgedragen.
In succesvolle informatie-uitwisseling tussen de bankensector en het Openbaar Ministerie zijn opgestelde convenanten (waarin die samenwerking nader werd uitgewerkt) een goede basis gebleken voor meer structurele samenwerking.

Veel deskundigen adviseren om de ISAC-structuur voor de vitale sectoren uit te breiden naar andere delen van de economie, met name naar de kennisintensieve bedrijven. De aanwezige samenwerkingsstructuren die bestaan binnen de huidige Topsectoren en het innovatieve mkb bieden daartoe mogelijk een goede basis. Dit sluit aan bij het voornemen van het ministerie van Economische Zaken om hiertoe een verkenning uit te voeren.[23]

[23] Digitale agenda, Vernieuwen, vertrouwen, versnellen, Ministerie van Economische Zaken, 2016

Hoofdstuk 2

Aanbevelingen voor een actieprogramma

Nederland heeft een uitstekende uitgangspositie om de economische kansen van de digitale toekomst voluit te benutten. De mate van digitalisering, het vestigingsklimaat, de beschikbare infrastructuur: allemaal factoren die maken dat Nederland een koppositie inneemt. Het is daarom des te belangrijker dat we de randvoorwaarden voor economisch succes goed borgen: veiligheid, vertrouwen en betrouwbaarheid van de digitale wereld.
Om de cybersecurity in Nederland op een hoger niveau te krijgen – concreet: hoger vaardighedenniveau van burgers, bedrijven en overheid en strakkere sturing op digitale veiligheid – zijn investeringen, samenwerking en acties nodig. Het is noodzakelijk dat overheid, bedrijfsleven, burgers en onderwijsinstellingen de handen ineenslaan voor een gezamenlijk doel: Nederland digitaal vaardig, vertrouwd en veilig houden. Dit hoofdstuk benoemt de speerpunten die de hoogste prioriteit verdienen en schetst een concrete aanpak voor de belangrijkste problemen.

2.1 Maak Nederland digitaal vaardig

Het is belangrijk dat Nederland digitaal vaardiger wordt: burgers, bedrijven en overheden moeten begrijpen hoe de digitalisering ons leven beïnvloedt, dat naast talloze kansen ook nieuwe bedreigingen op ons af komen en dat we ons daartegen moeten beschermen.

‘Net zoals kinderen veilig leren fietsen, kunnen ze ook internet van jongs af aan veilig leren gebruiken’

Digitale vaardigheden versterken begint met het verhogen van kennis, kunde en vaardigheden, zodat iedereen op een veilige en vertrouwde manier kan deelnemen aan de digitale samenleving. Ook is meer publieke en politieke discussie nodig over zaken die door digitalisering in een nieuwe context komen te staan. Denk aan onderwerpen als openbare orde en veiligheid, privacy en het beschermen van je eigen omgeving. Zowel de bereidheid om zelf maatregelen te nemen als het begrip voor noodzakelijke maatregelen van overheid en bedrijfsleven nemen toe als het maatschappelijk bewustzijn groter wordt.

Stimuleren van ‘een leven lang leren’

Nieuwe generaties Nederlanders groeien op in een vergaand gedigitaliseerde samenleving. Digitale vaardigheden zijn inmiddels net zo belangrijk als lezen, schrijven en rekenen.[24] Dat begint op de basisschool en gaat via het voortgezet onderwijs naar het mbo, hbo en de universiteit. Net zoals kinderen veilig leren fietsen, is het veilig gebruik van internet iets wat kinderen van jongs af moeten leren. Daarbij hebben ouders natuurlijk een belangrijke rol, maar ook scholen. Digitale vaardigheden zijn steeds vaker vereist om een startkwalificatie te halen. Maar ook daarna, tijdens het werkzame leven, blijft aandacht voor digitalisering noodzakelijk.

De Cyber Security Raad (CSR) constateerde in haar advies van november 2015 al dat het belangrijk is dat Nederlandse jongeren goed voorbereid worden op hun digitale toekomst door digitale geletterdheid en cybersecurity onderdeel te laten uitmaken van het onderwijscurriculum. Het gaat dan om de gehele keten van basis- tot beroepsonderwijs.[24]

Ook het Platform Onderwijs2032 adviseerde het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) in januari 2016 om digitale geletterdheid op te nemen in het kerncurriculum voor het primair en voortgezet onderwijs[25]: *“Het werken en leren in de digitale wereld behoort tot de kern van toekomstgericht onderwijs. Dat betekent dat leerlingen ICT-basiskennis opbouwen, informatievaardigheid ontwikkelen, mediawijs worden en leren begrijpen hoe informatietechnologie werkt (computational thinking). Dit betreft niet alleen het gebruik van computers en ICT als consument, maar ook als producent.”*

[24] De robot de baas. De toekomst van werk in het tweede machinetijdperk. WRR, 2015
[25] http://onsonderwijs2032.nl/wp-content/uploads/2016/01/Ons-Onderwijs2032-Eindadvies-januari-2016.pdf

De digitale samenleving is vandaag de dag een feit. Als samenleving kunnen we het ons niet permitteren om nog langer te wachten op aanpassingen van de curricula. Het is van cruciaal belang om de aanpassing van curricula op korte termijn te gaan laten plaatsvinden.

Om zo innovatief mogelijk te blijven denken, is het belangrijk wetenschappelijke kennis op universiteiten en hogescholen bijeen te brengen. Dat geldt ook voor het stimuleren van kennis-ontwikkeling en -toepassing. Een goed en belangrijk voorbeeld hiervan is het *Dutch cybersecurity platform for higher education and research (dcypher)* dat is opgericht tijdens de One Conference van het NCSC.[26]

Bewustzijn vergroten

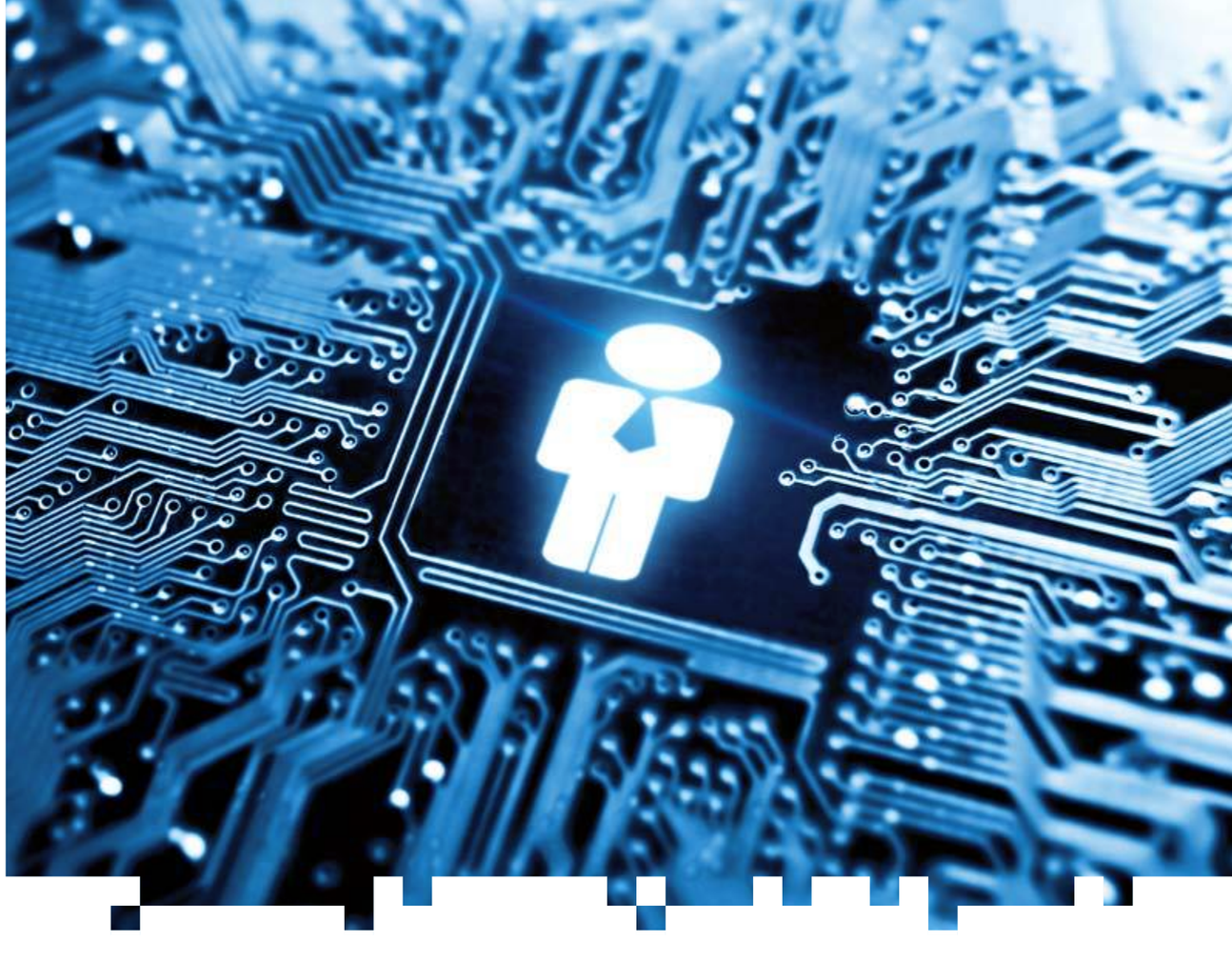
In Nederland bestaan al verschillende initiatieven om het online bewustzijn van burgers en bedrijven te vergroten. Voorbeelden zijn de landelijke overheidscampagne Alert Online en de 'Hang op! Klik weg! Bel uw bank!'-campagne waarmee banken consumenten bewustmaken van veilig online bankieren. In het Verenigd Koninkrijk is een dergelijke campagne opgezet met de titel '*Be Cyber Streetwise*'. Het is belangrijk om ook effectieve voorlichting te geven aan andere doelgroepen, zoals kleinere bedrijven en lokale middenstanders (mkb-bedrijven). Daarnaast zijn brede campagnes noodzakelijk om het bewustzijn van Nederlanders te vergroten, zoals er ook campagnes zijn op het gebied van veilig verkeer en verantwoord alcoholgebruik.

Samengevat

Maak Nederland digitaal vaardig

- **Versneld opnemen van digitale geletterdheid, inclusief cybersecurity, in het kerncurriculum voor basis- en voortgezet onderwijs**
- **Kennisontwikkeling op het gebied van cybersecurity stimuleren**
- **Doelgerichte voorlichtingscampagnes voeren over cybersecurity voor specifieke doelgroepen (waaronder mkb-bedrijven) en het brede publiek**

[26] Beleidsreactie Cyber Security Beeld Nederland 2016, Ministerie van Veiligheid en Justitie, september 2016,



2.2 Maak ruimte voor sturing vanuit de overheid

Het belang van de digitale mainport voor Nederland is inmiddels vergelijkbaar met dat van Schiphol en de Rotterdamse haven. De politieke verantwoordelijkheid voor deze digitale mainport is echter versnipperd. Het ontbreekt op dit moment aan eenduidige politieke coördinatie en sturing (doorzettingsmacht) ten aanzien van de verschillende elementen en belangen die deze digitale mainport raken. Daardoor gaat kostbare tijd verloren en zijn budgetten te versnipperd en niet toereikend.

‘Heldere politieke verantwoordelijkheid voor de digitale mainport is nodig’

Eenduidige politieke sturing op digitale mainport

Het economisch belang en de veiligheidsnoodzaak rechtvaardigen een eenduidige politieke sturing van de digitale mainport.[27] Een nieuw kabinet zou hiervoor een heldere structuur moeten kiezen in de vorm van een onderraad voor de digitale mainport en cybersecurity.[28] Deze structuur zorgt ervoor dat de direct betrokken ministers met een deelverantwoordelijkheid op cybersecurity of de digitale mainport beleid met elkaar afstemmen en tot een gecoördineerde, gezamenlijke aanpak komen.

Hoge functionaris en meerjarig actieprogramma

Naast heldere politieke verantwoordelijkheid voor de digitale mainport, is meer sturing in de uitvoering noodzakelijk. Hiervoor zou een hoge functionaris moeten worden benoemd, die een meerjarig cybersecurity-actieprogramma opstelt in samenwerking met het bedrijfsleven en lagere overheden. Het actieprogramma brengt ambities, bevoegdheden en geld samen en bevat een investeringsagenda om de cybersecurity structureel te verbeteren.
Verankering van de taak en opdracht door middel van een kabinetsbesluit stelt zeker dat de hoge functionaris voldoende bevoegdheden en doorzettingsmacht heeft om het actieprogramma succesvol uit te kunnen voeren. Het instellen van een Taskforce (onder leiding van de functionaris) is daarbij van groot belang om zowel horizontaal (binnen het Rijk) als verticaal (tussen de verschillende overheidslagen) betrokken partijen (private organisaties, bestuursorganen, en maatschappelijke organisaties) samen te brengen en zo een voortvarende aanpak te bevorderen. De hoge functionaris bevordert de totstandkoming en uitvoer van het cybersecurity-programma en zorgt dat er draagvlak voor maatregelen van het programma ontstaat.

De hoge functionaris:

- legt het actieprogramma en de investeringsagenda jaarlijks voor aan het kabinet (via de onderraad);
- bevordert het overleg tussen betrokken bestuursorganen, bedrijfsleven en maatschappelijke organisaties;
- bewaakt de voortgang van de uitvoering van het cybersecurity-programma en rapporteert en adviseert daarover aan het kabinet;
- En dient vanzelfsprekend de beschikking te hebben over voldoende mandaat, bij voorkeur door middel van een kabinetsbesluit waarin deze taken en bevoegdheden zijn vastgelegd.

Eigen ICT op orde brengen met duidelijke sturing

Voor succesvolle en grote bedrijven is een centrale aansturing van het securitybeleid vanzelfsprekend. Bij de Nederlandse overheid is dat nog niet het geval, zoals ook bleek uit het onderzoek van de Tijdelijke Commissie ICT van de Tweede Kamer: er is te weinig overkoepelend gezag en centrale sturing op overheids-ICT. De verantwoordelijkheden en besluitvorming over ICT zijn per departement geregeld en er is te weinig doorzettingsmacht van verantwoordelijke bewindspersonen en ambtenaren. De rijksbrede kostenbesparingen en maatschappelijke opbrengsten van het ICT-beleid zijn zo bijvoorbeeld moeilijk zichtbaar.[29]

Enerzijds is het wenselijk dat (cyber)veiligheid een integraal onderdeel is van alle ICT-aanbestedingen. Anderzijds is het nodig verouderde en onveilige ICT (legacy) te vervangen bij alle gebruikers binnen het gehele rijksdomein, inclusief uitvoeringsdiensten en lagere overheden. Er liggen grote kansen voor de overheid om meer te doen met minder kosten door de inzet van gedigitaliseerde standaardprocessen. Besparingen hieruit zijn te benutten voor benodigde investeringen in cybersecurity.

Het is aan te raden een rijksbreed beleid en samenhangend protocol voor cybersecurity vast te stellen. Vervolgens is het van belang dat de overheid in haar eigen ketens de ‘toeleveranciers’ verplicht om te voldoen aan cybersecurity-eisen. Die eisen moeten tegelijkertijd reëel zijn, om te voorkomen dat mkb-bedrijven worden buitengesloten.

Wetgeving moderniseren

De overheid, specifiek de Nederlandse opsporings-, inlichtingen- en veiligheidsdiensten, kunnen hun taken op het gebied van de nationale digitale veiligheid en de bescherming van privacy op dit moment moeilijk waarmaken. De wettelijke bevoegdheden voor de diensten schieten tekort en zijn nog gebaseerd op verouderde wetgeving, die geschreven is vóór de tijd van de digitale revolutie. De technologische ontwikkeling is sindsdien razendsnel gegaan, maar de wetgeving is achtergebleven. Gezien het dreigingsbeeld leidt dit tot risico’s voor de Nederlandse overheid, het bedrijfsleven en de burgerrechten van Nederlanders. De huidige Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) is dermate gedateerd dat inlichtingen- en veiligheidsdiensten geen mogelijkheden hebben tot brede monitoring en detectie van hedendaagse datastromen. Dit gaat om het grootste deel van alle online communicatie. Het is niet mogelijk om de cybersecurity in Nederland op peil te krijgen zonder modernisering van de WIV.

Daarnaast zijn er belangrijke wetsvoorstellen aanhangig in het parlement: het wetsvoorstel Computercriminaliteit III en het wetsvoorstel gegevensverwerking en meldplicht cybersecurity. Deze wetsvoorstellen zijn relevant voor de politie en nodig om cybercriminaliteit beter te kunnen bestrijden. Het huidige wettelijke kader en lopende trajecten rond de aanpassing van die wetgeving is in overzicht opgenomen in bijlage 2. Het blijven van een aantrekkelijke vestigingsplaats voor bedrijven valt of staat met een transparante, democratisch gelegitimeerde overheid en adequate wetgeving. Daarom is het noodzakelijk dat er altijd nadrukkelijk een

[27] Bijvoorbeeld bij elkaar brengen van verschillende beleidsterreinen: van BZK: overheids-ICT en lagere overheden, EZ: economische kansen en sectoren, industrie, en MKB, VenJ: veiligheid en veiligheidsdiensten OC&W: onderwijs, VWS: zorg, IenM: mobiliteitsbeleid.

[28] Een onderraad is een afzonderlijke vergadering van de Nederlandse ministerraad, waarin onderwerpen worden besproken door alleen de direct en indirect betrokken ministers. De voorzitter is de minister-president. Per onderraad is een coördinerend minister verantwoordelijk voor de voorbereiding en inbreng van de stukken.

[29] Parlementair onderzoek naar ICT-projecten bij de overheid, Rapport Commissie Elias, Tweede Kamer, vergaderjaar 2014–2015, 33 326, nr. 5

duidelijk doel is verbonden aan data-interceptie. Tegenover uitgebreidere bevoegdheden dient ook voldoende toezicht op het gebruik van die bevoegdheden te staan.

Regelgeving op Europees (en mondiaal) niveau

Vanwege het grensoverschrijdende karakter van alle vraagstukken rond digitalisering, en meer specifiek cybersecurity, worden in toenemende mate wetten en regels binnen Europees (EU-) of internationaal verband gemaakt. In dat licht wijzen wij ook op naderende Europese regelgeving op het terrein van zorgplichten en cybersecurity, in het bijzonder de richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn) en de EU-verordening ten behoeve van privacy die in 2018 van kracht wordt. Zie bijlage 2. Ook wordt gewerkt aan mondiale normen op het gebied van cybersecurity.

Toekomstbestendige wetten en regels maken

Wetgeving moet niet alleen bij de tijd worden gebracht, maar ook gehouden. De ontwikkelingen op het gebied van cybersecurity en technologische ontwikkelingen in de digitalisering gaan zo snel, dat we ook het tempo van totstandkoming van (nieuwe) regels moeten opvoeren. Onder meer het Centraal Planbureau (CPB) wijst daarop in een recent advies.[30] Ook het kabinet onderkent het belang dat wet- en regelgeving voldoende ruimte biedt aan vernieuwing en innovatie[31] en noemt daarbij zelf al een aantal instrumenten: doelregulering, experimenteerruimte en *right to challenge*.
Dergelijke instrumenten zijn noodzakelijk, want digitale technologie ontwikkelt zich vaak sneller dan nieuwe wetgeving. De uitdaging voor de toekomst is om wetgeving te maken die enerzijds heldere kaders biedt ('horizonbepaling'), maar anderzijds ook voldoende ruimte laat om aanpassingen te doen die een kortere doorlooptijd hebben, zogenaamde techniek neutrale wet- of regelgeving. Dit geldt overigens niet alleen in Nederland, ook de landen om ons heen worstelen met diezelfde vraagstukken. In dat licht is het ook belangrijk om op Europees niveau actief bij te dragen aan beleidsvorming en wet- en regelgeving.

'Een meerjarig actieprogramma kan cybersecurity structureel verbeteren'

Samengevat

Zorg voor meer sturing vanuit overheid

- **Eenduidige politieke aansturing van de digitale mainport via een onderraad van de Ministerraad**
- **Aanstellen van een hoge functionaris, bij voorkeur door middel van een kabinetsbesluit (waarin taken en bevoegdheden zijn vastgelegd), en geld voor het opstellen en uitvoeren van een jaarlijks (voortrollend) cybersecurity-programma**
- **Op orde brengen van de eigen digitale infrastructuur met duidelijke sturing**
- **Moderniseren van de bevoegdheden van de Nederlandse opsporings-, inlichtingen- en veiligheidsdiensten, met oog voor checks & balances**
- **Toekomstbestendige wetten en regels maken**

[30] Marktordening bij nieuwe ICT-toepassingen CPB Policy Brief 2016/09, CPB, 11 augustus 2016
[31] Kamerstukken 33009, nr. 10

2.3 Stimuleer de verantwoordelijkheid van de private sector

Het is helaas een illusie om te denken dat cybercriminaliteit en spionage alleen grote bedrijven treft. Van eenmanszaak tot multinational, cybersecurity is een zaak voor iedere ondernemer.

‘Vooroplopende bedrijven hebben cybersecurity als eerste prioriteit gesteld’

Het bedrijfsleven heeft daarom ook een eigen verantwoordelijkheid om de digitale veiligheid te vergroten. Maar met name kleinere bedrijven hebben vaak onvoldoende middelen, kennis of toegang tot kennis om dreigingen te onderkennen en zich vervolgens weerbaar te maken. Daardoor kunnen primaire bedrijfsprocessen onder druk komen te staan en lopen ondernemers het risico om hun concurrentiepositie te verliezen ten opzichte van andere bedrijven in binnen- en buitenland.

Basis op orde hebben; voldoen aan randvoorwaarden voor cybersecurity

De basis op orde geldt daarom niet alleen voor de overheid, maar ook voor het bedrijfsleven. Het installeren van beveiligingssoftware, encryptie van de eigen informatie en het tijdig installeren van software-updates zijn basismaatregelen die iedere ondernemer kan nemen. In het digitale domein zijn dit feitelijk *health, safety & environment*- (HSE-)maatregelen, waar goed presterende bedrijven vaak trots op zijn. Het is belangrijk dat bedrijven hun eigen netwerken beschermen en zich weerbaar maken tegen cyberaanvallen. Dat is ook nodig om de belangen van klanten te beschermen. Security als randvoorwaarde of *license to operate* zou een vanzelfsprekend onderdeel van de *corporate governance* moeten zijn. Bedrijven hebben immers ook een zorgplicht naar hun klanten.

Invulling geven aan de zorgplicht

In de private sector zijn de grote ondernemingen veelal voldoende *cyber aware*. Bedrijven zoals Amazon hebben cybersecurity als eerste prioriteit gesteld en investeren er jaarlijks miljarden in. Het idee dat cybersecurity een randvoorwaarde is voor het voortbestaan van de onderneming, is daar zichtbaar in investeringen en maatregelen. Zoals gezegd geldt dat niet altijd voor alle bedrijven. Vanwege de toenemende connectiviteit en ketenafhankelijkheid zorgt dat voor een risico in de gehele keten. Het bundelen van krachten is daarom des te belangrijker. Bij een nadere invulling van de zorgplicht moet helder gemaakt worden wat een klant of consument mag verwachten van de aanbieder en welke maatregelen hij zelf wordt verwacht te treffen.
Het is daarnaast belangrijk dat er brede discussie wordt gevoerd over het invulling van de zorgplicht waar het gaat om leveranciers van hard- en software. Een voorbeeld hiervan is het toevoegen van veiligheidseisen aan software en hardware in de productaansprakelijkheid. Want cybersecurity leunt voor een belangrijk deel op de beveiliging van geleverde hard- en software. De Nederlandse overheid kan dit vraagstuk rond zorgplichten in de context van cybersecurity agenderen op internationaal niveau.

Ketens veiliger maken door het invoeren van een ketenverantwoordelijkheid

Een andere manier om in gezamenlijkheid nader invulling te geven aan die zorgplicht, is het aangaan van ketenverantwoordelijkheid. Als het gaat om de inkoop van (duurzame) grondstoffen, de herkomst van ingrediënten voor de voedingsindustrie of de inhuur van externe medewerkers bestaan al jaren goede voorbeelden van ketenverantwoordelijkheid. Vergelijkbare initiatieven zijn mogelijk voor digitale productieketens. Dat betekent dat alle toeleveranciers, onderaannemers en afnemers die betrokken zijn bij de productieketen, elkaar verantwoordelijk mogen en moeten houden voor een *cyber secure* keten. Zij kunnen elkaar regels opleggen en eisen stellen die specifiek gaan over de cybersecurity voor (een van de schakels) in de keten. Grote bedrijven kunnen daarin de kleine ondernemingen bij de hand nemen: Veel grote organisaties hebben vaker wel methodes ontwikkeld om toeleveranciers meer secure te laten werken, maar kleinere bedrijven kunnen hier vaak de tijd en het geld niet voor vrij maken. Het is belangrijk om alle partijen uit de productieketen bij het onderwerp ketenverantwoordelijkheid te betrekken en een effectief controlemechanisme in te stellen.

Accreditatie of certificering

Een voorbeeld om in gezamenlijkheid te komen tot een hoger niveau van cybersecurity is door het invoeren van een accreditatie- of certificeringssystematiek. Kleine ondernemers en mkb-bedrijven kunnen ondersteuning op cybersecuritygebied goed gebruiken. Op dit moment ontbreekt een betrouwbaar keurmerk of certificeringsysteem voor cybersecuritybedrijven. Er loopt in de EU wel een discussie op dit gebied, maar dat zal niet op korte termijn tot bruikbare resultaten leiden. Hierop vooruitlopend kan het Nederlandse bedrijfsleven natuurlijk wel zelf actie ondernemen en via zelfregulering tot een accreditatie- of certificeringssysteem komen van private dienstverleners op het gebied van cybersecurity. Het model dat in het Verenigd Koninkrijk werd opgezet, kan hierin als inspiratiebron dienen.[32]

Samengevat

Stimuleer de eigen verantwoordelijkheid bij de private sector

- **Basis op orde hebben; voldoen aan randvoorwaarden voor cybersecurity**
- **Invulling geven aan zorgplicht op het gebied van cybersecurity**
- **Ketens veiliger maken door het invoeren van een ketenverantwoordelijkheid**
- **Inzet van een accreditatie- of certificeringssystematiek**

[32] Binnen het Engelse model kunnen cybersecuritybedrijven binnenkort een accreditatie krijgen van de regering. Hierdoor kunnen kritieke bedrijven, zoals overheidsinstellingen, banken en ziekenhuizen, hun cybersecurity laten beheren door professionals die op een officiële manier erkent zouden worden. Dit bemoeilijkt het werk van hackers en vermindert aanzienlijk hun kansen op succes.

2.4 Verstevig de privaat-publieke samenwerking

Nieuwe technologie brengt ook nieuwe uitdagingen voor de veiligheid met zich mee. Cybersecurity vraagt om een nieuwe manier van samenwerking, vooral tussen publieke en private partners. Een samenleving die via netwerken verbonden is heeft ook een onderling verbonden securityaanpak nodig.

Samenwerken is daarom noodzakelijk. Tussen overheid en bedrijfsleven moeten effectievere en soms nieuwe partnerschappen ontstaan. Dit vraagt om heldere spelregels, vertrouwen en het delen van soms zeer gevoelige informatie. De Nederlandse traditie van veel overleg en compromis geeft Nederland een unieke positie ten opzichte van andere landen. Die samenwerking kunnen we versnellen en verdiepen, om effectief te zijn in het licht van snelle technologische ontwikkelingen. Daarmee verkleinen we de reactietijd, vergroten we informatie-uitwisseling en versnellen we opvolging en maatregelen. Het is van belang om in de operationele samenwerking een vertrouwelijke omgeving te creëren om kennis te delen. Essentieel is dat de partijen transparant zijn over hun gedeelde belang en er wederzijdse meerwaarde is.

Onderzoek naar cyberaanvallen intensiveren voor snellere respons en betere preventie

Samenwerking tussen bedrijven en overheid op het gebied van cybersecurity moet worden verstevigd en geïnstitutionaliseerd. Informatie-uitwisseling op het gebied van ongeoorloofd gebruik, kwetsbaarheden in systemen, criminaliteit of spionage in de digitale wereld moet worden bevorderd. Veiligheid borgen begint bij het monitoren van dreigingen en risico's[33], vervolgens voorkomen en eindigt bij het opsporen van criminele actoren en vervolging van criminelen.

Een essentiële eerste stap voor snelle, adequate reacties op misstanden of aanvallen (respons) en preventieve maatregelen is daarom detectie en onderzoek naar cyberaanvallen te intensiveren. Nederland moet in staat zijn snelle en accurate impactanalyses te maken om schade te beperken en succesvol attributie-onderzoek uit te voeren om daders te identificeren. Die operationele samenwerking is te bewerkstelligen door uitbreiding van de eerder genoemde structuur van ISAC's naar andere delen van de economie, met name naar de kennisintensieve bedrijven. Ook is het raadzaam om het Nationaal Detectie Netwerk (NDN) en het Nationaal Respons Netwerk (NRN) uit te breiden en meer te sturen op operationele samenwerking.

Uitbreiden Nationaal Detectie Netwerk (NDN)

In het verlengde van monitoring ligt de noodzaak tot betere detectie. Operationele samenwerking bevordert ook de detectiekansen. Operationele samenwerking kan door partijen bij elkaar te brengen in een virtueel cybercentrum, waar dreigingsinformatie samenkomt.
Een logische stap is om het huidige NDN[34] daartoe uit te bouwen. Het NDN is een samenwerkingsverband tussen overheden en private partijen voor het beter en sneller waarnemen van digitale gevaren en risico's. Het NDN verzamelt dreigingsinformatie van alle partijen over belangrijke, actuele dreigingen en stelt vast welke indicatoren van belang zijn om een aanval te herkennen. De opsteller van de informatie stelt de indicatoren op gestandaardiseerde en geautomatiseerde wijze beschikbaar aan de deelnemers van het NDN. Deze kunnen vervolgens de informatie gebruiken om zelf vast te stellen of ze te maken hebben met een digitale aanval, en direct passende tegenmaatregelen nemen. De deelnemers melden (al dan niet geanonimiseerd) of de indicatoren ook op hun systemen voorkomen, hetgeen kan duiden op een aanval. Door deze informatie te combineren ontstaat een duidelijker beeld van de actuele dreigingen die iedereen ten goede komt. Een aanval bij de een wordt hiermee een vroegtijdige waarschuwing voor de ander. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijkheid tijdig maatregelen nemen om schade door indringers te beperken of voorkomen. Het gaat om de informatie vanuit het NCSC, de MIVD, AIVD en THTC en opsporingsdiensten van de politie, aangevuld met talrijke nuttige informatiebronnen uit de private sector. Uiteindelijk is het doel alle rijksoverheidsorganisaties te betrekken bij het NDN en de belangrijkste organisaties in de vitale sectoren. In het ultieme geval gaat het om circa honderd organisaties.
In diverse gesprekken is de wens geuit om kennisdeling uit te breiden, ook naar organisaties en bedrijven die vallen buiten de 'vitale sectoren'.

> 'Als we dreigingsinformatie delen, kan een aanval bij de een voor de ander een vroegtijdige waarschuwing zijn'

Uitbreiden Nationaal Respons Netwerk (NRN)

Betere detectie leidt tot een versterkte en snellere respons op incidenten. Het NRN is een samenwerkingsverband, gefaciliteerd door het NCSC, met als doel de gezamenlijke respons op ernstige cybersecurityincidenten te versterken. Dit gebeurt door de krachten van verschillende responscapaciteiten te bundelen, wat zorgt voor meer samenhang en versterking van bestaande capaciteiten. Het NRN, opgericht in 2014, is een samenwerkingsverband tussen het NCSC en publiek-private ICT-responsorganisaties uit verschillende sectoren. Binnen het NRN kunnen deze organisaties kennis en ervaringen delen en bijstand verlenen. Het NRN richt zich zowel op het organiseren van bestaande responscapaciteit als het stimuleren van nieuwe responscapaciteit binnen de overheid en vitale sectoren. Het is raadzaam het NRN verder uit te bouwen, met additionele responsmogelijkheden en het aanhaken van private initiatieven. Hiervoor is wel een aanpassing nodig van de onderliggende 'lidmaatschapsregels' (getekende overeenkomsten tussen deelnemende partijen met afspraken over de samenwerking), zodat private partijen kunnen deelnemen.

Cyber Security Raad (CSR)

De CSR is een onafhankelijk adviesorgaan en geeft gevraagd en ongevraagd advies aan het kabinet. Daarnaast heeft de CSR als taak het toezien op de uitvoering van de Nationale Cybersecurity Strategie. De Raad is samengesteld uit vertegenwoordigers van wetenschap, publieke en private partijen. Die samenstelling maakt de CSR uniek. Dit jaar bestaat de CSR vijf jaar en heeft in die periode effectief gewerkt.

[33] Nederland loopt voorop in het signaleren van kwetsbaarheden in digitale processen binnen de overheid en vitale sectoren door bijvoorbeeld de inzet van Information *Sharing and Analysis Centres* (ISAC's).
[34] https://www.ncsc.nl/

Richting de toekomst is het belangrijk dat de CSR komt tot gezaghebbende adviezen, met impact in termen van bruikbaarheid en effectiviteit aan zowel het kabinet (via de onderraad) als aan de hoge functionaris.
Dit punt vraagt om aandacht in de evaluatie van de taakopvatting en samenstelling van de CSR (voorzien in het najaar van 2016).

Zorgen voor meer sturing op publiek-private samenwerking

Er is een breed scala aan overleggen en initiatieven tot samenwerking op het terrein van cybersecurity. Dat is een groot goed. Ondanks goede intenties, behoeven de initiatieven meer sturing. In gezamenlijkheid kunnen de partijen concrete kaders nader uitwerken en komen tot meer proactieve informatie-uitwisseling en betere samenwerking. Door meer sturing op de vele Privaat-Publieke Samenwerking (PPS)-initiatieven is het mogelijk nieuwe technologische ontwikkelingen sneller door te vertalen, en goede voorbeelden structureel en breder in te bedden. Ook kan het ene initiatief verder voortbouwen op (lessen uit) het andere. De coördinerende taak op PPS zou goed passen bij de hoge functionaris, zoals in 2.2 bedoeld. Diverse initiatieven en samenwerkingsverbanden kunnen worden ingezet ter bevordering van het cybersecurity-programma.

Samengevat

Verstevig de samenwerking tussen de private en publieke sector

- **Onderzoek naar cyberaanvallen intensiveren voor snellere respons en betere preventie, door uitbreiding van de Information *Sharing and Analysis Centres* (ISAC's), het Nationaal Detectie Netwerk (NDN) en het Nationaal Respons Netwerk (NRN)**
- **Sturing en coördinatie op publiek-private samenwerking door hoge functionaris en cybersecurity-programma**
- **Borgen van impactvolle advisering door (geëvolueerde) Cyber Security Raad (CSR)**

2.5 Financiële paragraaf: structurele en incidentele investeringen

De genoemde acties vragen (blijvende) investeringen van overheid en bedrijfsleven. Om een zo reëel mogelijk beeld te krijgen van die benodigde financiële middelen is onder andere gekeken naar de investeringen die worden gedaan door landen (overheden en bedrijfsleven) die vergelijkbaar zijn met Nederland in termen van digitalisering en economie.

‘Investeer 10 procent van het IT-budget in cybersecurity’

Dat zijn Estland, Singapore, het Verenigd Koninkrijk, de Verenigde Staten, Australië en Duitsland. Deze landen hebben specifieke aandacht voor cybersecurity en daarvoor ook specifieke budgetten beschikbaar gesteld. Ook is gekeken naar de potentiële economische schade als gevolg van cybersecurity. PWC deed daar op verzoek van de Europese Commissie onderzoek naar.

Structureel: 10 procent van IT-budgetten als maatstaf
De hoge mate van digitalisering heeft Nederland veel economische voordelen gebracht, maar maakt ons ook kwetsbaar voor cyberdreigingen. De komende jaren zijn daarom structurele, significante investeringen nodig om de cybersecurity in Nederland op peil te brengen en te houden. Op drie fronten: overheid, bedrijfsleven en burgers zelf. Van huiskamer naar bestuurskamer en tot in de Tweede Kamer, Provinciale Staten of gemeenteraad.

Overheid
Uit de analyse van vergelijkbare landen in Europa en elders in de wereld, blijkt dat het budget voor cybersecuritymaatregelen gemiddeld ongeveer 10 procent van het jaarlijkse IT-budget bedraagt. Wij stellen voor deze maatstaf over te nemen: 10 procent van het IT-budget van de Rijksoverheid zou specifiek aan digitale veiligheid en privacymaatregelen moeten worden besteed. Een (aanzienlijk) deel van deze gelden kan worden samengebracht in het budget van het cybersecurity-programma om collectief maatregelen te kunnen treffen. Deze maatstaf geeft vervolgens de (lokale) volksvertegenwoordiging een richtsnoer bij de besluitvorming over de begroting op rijks- of lokaal niveau. Besteedt het kabinet, provincie- of gemeentebestuur jaar na jaar minder dan 10 procent van de IT-budgetten aan veiligheid en privacy, dan is de kans groot dat de cybersecurity niet voldoende geborgd is.

Bestuurskamer
We zouden willen bepleiten dat deze ‘10 procent-maatstaf’ ook wordt overgenomen door private ondernemingen en publieke organisaties. Je zou zover kunnen gaan dat de overheid deze vuistregel als een *comply-or-explain* opneemt.

Huiskamer
Zelfs voor consumenten geeft deze maatstaf een eerlijk perspectief: bij bijvoorbeeld de aanschaf van een laptop van 500 euro, zou elke consument ervan uit moeten gaan dat daarvan 10 procent (50 euro) logischerwijze door hemzelf moet worden besteed aan het veilig houden van dit product. Bij het bouwen van een huis weet men dat het geld kost om te kunnen voldoen aan de veiligheidseisen en -voorschriften die horen bij veilig wonen. Diezelfde redenering gaat op voor het veilig bewegen in de digitale wereld. Als je een nieuwe computer van 500 euro koopt, houd dan rekening met ongeveer 50 euro voor een goed Internet cybersecurity-/antivirusabonnement.

Extra impuls voor komende jaren: investeringsagenda
Zoals in dit advies wordt betoogd, is een meerjarig actieprogramma met investeringsagenda geboden. Naast blijvende (financiële) aandacht voor cybersecurity in de vuistregel van 10 procent, is in dit adviesrapport geconstateerd dat op een aantal zaken een extra impuls noodzakelijk is. Dat betekent concreet dat de overheid op een aantal aspecten moet investeren. Het onderzoek dat is gedaan in de aanloop naar dit adviesrapport, rechtvaardigt dat in de investeringsagenda de volgende versterkingsmaatregelen worden opgenomen:

- Uitbreiding van de ISAC’s, het NDN en het NRN;
- Zorgdragen voor een veilige digitale infrastructuur bij de overheid, onder meer via regels voor aanbestedingen en ketenverplichting, accreditatie;
- Versneld opnemen van digitale geletterdheid, inclusief cybersecurity, in het kerncurriculum voor basis- en voortgezet onderwijs;
- Doelgerichte voorlichtingscampagnes voeren over cybersecurity, voor specifieke doelgroepen en het brede publiek.

Ter illustratie, investeringen in cybersecurity door de overheid van enkele vergelijkbare landen:
Singapore: Het land besteedt inmiddels 8 procent van het ICT-budget aan *cybersecurity* en geeft dit ook als streefcijfer aan bedrijven aan.
Duitsland: De Duitse overheid investeert 10 procent van het totale ICT-budget aan *cybersecurity.*
Verenigd Koninkrijk: De overheid in het VK heeft in de periode van 2011-2015 860 miljoen pond geïnvesteerd in het ‘*National Cyber Security Programme*’. Dat programma wordt verlengd met vijf jaar en voor de komende jaren investeert de overheid opnieuw 1,9 miljard pond en is dus meer dan verdubbeld, als onderdeel van de ‘*Second National Cyber Security Strategy*’. Naast dit programma investeert de overheid in het beschermen van het eigen netwerk, beveiliging van de *online services* en vergroten van de capaciteiten op *cybersecurity.* Het *cybersecurity-budget* van de Engelse overheid komt in totaal op 3,2 miljard pond.
Verenigde Staten: In het *Cybersecurity National Action Plan* (CNAP) van de VS van februari 2016 wordt in 2017 19 miljard dollar in cybersecurity geïnvesteerd, een toename van het budget van meer dan 35 procent ten opzichte van dat van 2016.
Australië: De Australische overheid investeert 230 miljoen dollar in de komende 4 jaar in *cybersecurity.* Dit is een aanvulling op de eerder toezegde versterkingsgelden *(2016 Defence White Paper, boosting Defence cyber capabilities by up to $400 million over the next decade.”).*

Samengevat
Financiële paragraaf: structurele en incidentele investeringen

- **Investeren in cybersecurity volgens de 10 procent-maatstaf**
- **Investeringsagenda vormgeven met versterkingsmaatregelen**

Bijlage 1

Onderzoeksopzet en -verantwoording

1. Onderzoeksopzet

1.1 Achtergrond

In juni 2016 heeft de Cyber Security Raad mij via haar beide voorzitters benaderd om te komen tot een onafhankelijk, publiek-privaat advies op het terrein van cybersecurity.
In het onderzoek dat ten grondslag ligt aan dit adviesrapport, heb ik het volgende onderzoeksvraagstuk uitgewerkt: Digitalisering is een onontkoombaar en onomkeerbaar proces. Gevolgen hiervan behelzen kansen en bedreigingen. Doel van het advies is om inzichtelijk te maken hoe we kansen kunnen benutten en dreigingen het hoofd kunnen bieden.

1.2 Centrale vraag

Het onderzoeksvraagstuk heb ik vertaald naar de volgende centrale vraag:
Nederland heeft een internationale koppositie waar het gaat om digitaal zakendoen, vanwege:

- een hoogwaardige digitale infrastructuur;
- een aantrekkelijk vestigingsklimaat;
- een snelle adoptie van nieuwe technologieën;
- oog voor duurzaamheid.

Wat zijn de volgende noodzakelijke stappen op het gebied van cybersecurity om die koppositie te beveiligen, versterken en uit te bouwen in onze steeds verder digitaliserende samenleving?

1.3 Verdieping naar vier deelvragen

1. Welke stappen zijn nodig voor een duurzaam digitaal veilig en versterkt aantrekkelijk economisch (vestigings)klimaat en hoogwaardige digitale dienstverlening?
2. Welke digitale infrastructuur hoort daarbij?
3. Hoe creëren we een digitaal zelfbewuste burger die zich thuis voelt in een digitale leefwereld, bewust handelt, en meegroeit met de ontwikkeling hierin?
4. Wat vraagt dit van privaat, van publiek (inclusief wetenschap en onderwijs) en hoe in gezamenlijkheid (publiek-private samenwerking)?

1.4 Resultaten

1. Een duurzaam digitaal aantrekkelijk, veilig en versterkt economisch (vestigings)klimaat en digitale publieke dienstverlening;
2. Hoogwaardige digitale infrastructuur;
3. Awareness: bewustwording en weerbaar maken;
4. Investeringen privaat, publiek (inclusief onderwijs en wetenschap) en in privaat/publieke samenwerking.

Om tot een goed inzicht te komen, is een groot aantal (wetenschappelijke, nationale en internationale) rapporten en publicaties betrokken. Daarnaast is over het onderzoeksvraagstuk en de verdiepende vragen gesproken met diverse experts vanuit verschillende invalshoeken, in binnen- en buitenland.
Ook heeft een groepssessie met vijftien experts op het terrein van cybersecurity plaatsgevonden.

2. Overzicht interviews

- AIVD , Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- MIVD, Ministerie van defensie
- NCSC, Ministerie van Veiligheid en Justitie
- FoxIT
- Cyber Security Raad
- Ministerie van Economische Zaken
- Team High Tech Crime, Politie
- Rabobank
- Schiphol
- KPN
- Philips Healthcare
- Professor Of Global Ict Law , Tilburg University
- Universitair Hoofddocent eLaw Universiteit Leiden
- Ministerie van Onderwijs, Cultuur en Wetenschap
- ACM
- Digicommissaris
- Hacking Community
- Amazon Web Services
- Euronext
- CIO Rijksoverheid / BZK
- The Hague Security Delta
- Digicommissaris
- Nederland ICT
- Deloitte
- VNO-NCW
- KPN
- Overheid Estland
- Overheid Verenigd Koninkrijk
- Deltacommissaris

3. Geraadpleegde rapporten

- 2015 Global Startup Ecosystem Report, Compass, 2015
- Cyber Security Beeld Nederland 2015 en 2016, NCSC
- Cyber Value at Risk in the Netherlands, 2016, Deloitte
- De impact van ICT op de Nederlandse Economie, Dialogic (2014)
- De publieke kern van het internet, naar een buitenlands internetbeleid, WRR, Amsterdam 2015
- De robot de baas. De toekomst van werk in het tweede machinetijdperk, WRR (2015)
- Digitale agenda, Vernieuwen, vertrouwen, versnellen, Ministerie van Economische Zaken (2016)
- Economische Kansen cybersecurity, SEO Economisch onderzoek, 11 april 2016
- Economische kansen Nederlandse cybersecurity-sector, SEO/Verdonck Klooster i.o.v. Ministerie van Economische Zaken, 17 mei 2016
- Handreiking cybersecurity voor de bestuurder, Cyber Security Raad (CSR), april 2015
- Global Competitiveness Report 2015-2016, World Economic Forum
- ICT, kennis en economie 2015, CBS, 2015
- Manifest voor de digitale economie 2017-2021, Groei door digitalisering, Nederland ICT, 29 juni 2016
- Marktordening bij nieuwe ICT-toepassingen, CPB Policy Brief 2016/09, 11 augustus 2016
- Nationaal Veiligheidsprofiel (NVP) 2016, concept, Ministerie van Veiligheid en Justitie
- Nationale Cybersecurity Strategie 2, 2013, Ministerie van Veiligheid en Justitie
- Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies,June 2014
- Ontwikkelingen omtrent snel internet in het buitengebied, Kamerbrief 19 mei 2016, Ministerie van Economische Zaken
- Rapport Jaarverslag Algemene Inlichtingen- en Veiligheidsdienst 2015, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Samenwerken met water. Een land dat leeft, bouwt aan zijn toekomst. Bevindingen van de Deltacommissie 2008
- The White House, 9 februari 2016, Fact Sheet: Cybersecurity National Action Plan
- Trusted Hulpverleners, 5 juli 2016, Ministerie van Veiligheid en Justitie
- Versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche, Brussel, 5.7.2016 COM(2016) 410 final, Europees Economisch en sociaal Comité van de regio's (EP, EU)

Bijlage 2

Wettelijk kader cybersecurity

Paragraaf 1 geeft een opsomming van bestaande, relevante wet- en regelgeving op het terrein van cybersecurity. In paragraaf 2 wordt een aantal wetten in ontwikkeling (toekomstige wetgeving) beschreven en paragraaf 3 somt de belangrijkste Europese regels op.

1. Wettelijk kader cybersecurity in Nederland:

Telecommunicatiewet (Tw) Aanbieders van communicatienetwerken en -diensten zijn onderworpen aan een zorgplicht om passende technische en organisatorische maatregelen te nemen ten behoeve van de veiligheid en de beveiliging van de door hen aangeboden netwerken en diensten (artikel 11a.1). Abonnees moeten hierover worden geïnformeerd. De Telecommunicatiewet (1998) heeft in artikel 11a.2 ook een meldplicht opgenomen. Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten moeten de minister onverwijld in kennis stellen van:

a. een inbreuk op de veiligheid;
b. een verlies van integriteit

waardoor de continuïteit (...) in belangrijke mate werd onderbroken. Op verzoek van de minister dient alle informatie die nodig is om de veiligheid en integriteit van hun netwerken en diensten te beoordelen, te worden verstrekt. Als openbaarmaking in het algemeen belang is, kan de minister informatie hieromtrent openbaar maken. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels hieromtrent worden gesteld. Toezicht vindt plaats door Agentschap Telecom en in bepaalde gevallen door de Autoriteit Consument en Markt of het CBP. De minister, ACM en CBP zijn bevoegd tot het opleggen van een last onder bestuursdwang.. Een bestuursorgaan dat bevoegd is om een last onder bestuursdwang op te leggen, kan in spoedeisende gevallen besluiten dat bestuursdwang zal worden toegepast zonder voorafgaande last (artikel 5:31 Algemene wet bestuursrecht). Dit is onder meer het geval indien het niet naleven van bepaalde bepalingen een ernstige en directe bedreiging vormt voor de openbare orde of veiligheid of volksgezondheid of ernstige economische of bedrijfstechnische problemen tot gevolg zal hebben (artikel 15.2 Tw).

Mainports Rotterdam en Schiphol

Sectorale wet- en regelgeving / Diverse Juridische kaders van toepassing.

Wet Luchtvaart (Wlv) De Wet Luchtvaart (1992) is de (stapsgewijze) vervanging van de Luchtvaartwet uit 1958. Wetgeving voor luchtvaartbedrijven is vastgelegd in de Luchtvaartwet (artikel 16), de Wet luchtvaart (artikel 4.1), het besluit vluchtuitvoering en de regeling vluchtuitvoering. Toezicht wordt uitgeoefend door de Inspectie Leefomgeving en Transport.

Besluit melding voorvallen in de burgerluchtvaart In dit besluit (2006) is een meldplicht opgenomen inzake voorvallen in de burgerluchtvaart.

Havennoodwet De Havennoodwet (1963) heeft betrekking op het gebruik van havens in geval van oorlog, oorlogsgevaar of daaraan verwante of daarmee verband houdende buitengewone omstandigheden. In deze noodwet is een verplichting opgenomen tot het verstrekken van inlichtingen aan de minister. In het aanwijzingsbesluit noodwetgeving Verkeer en Waterstaat wordt geregeld wie de autoriteiten zijn die in de Havennoodwet worden genoemd, die in buitengewone omstandigheden bevoegdheden van de minister kunnen uitoefenen in een bepaald gebied (van oudsher aangeduid als de rijksheren).

Financiën (betalingsverkeer)

Wet op het Financieel Toezicht (Wft) De Wet op het financieel toezicht (2006) regelt het toezicht op bijna de hele financiële sector van Nederland. Financiële instellingen kunnen zien aan welke eisen zij moeten voldoen en hoe het toezicht is geregeld.

Besluit Prudentiële Regels Wft (Bpr) De regels in dit besluit (2007) zijn van toepassing op vergunninghoudende en onder toezicht staande financiële ondernemingen die werkzaam zijn op de financiële markten.

Besluit Gedragstoezicht financiële ondernemingen Wft (Bgfo) In het Besluit Gedragstoezicht financiële ondernemingen Wft worden bepalingen van de wet op het financieel toezicht (deel 4) uitgewerkt. Bepalingen hebben onder meer betrekking op de zorgvuldige dienstverlening en meldingsplichten (hoofdstuk 9).

Algemene Wetgeving

Wet bescherming Persoonsgegevens (Wbp) Deze wet (2001) beschermt de persoonlijke levenssfeer van natuurlijke personen bij de verwerking van persoonsgegevens. De verplichtingen en aandachtspunten hieromtrent worden in deze wet geregeld. De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens. De Wbp regelt ook de taken en bevoegdheden van de Autoriteit persoonsgegevens (Nieuwe naam van CBP per 1 januari 2016). Belangrijkste bepalingen: verwerking persoonsgegevens alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier, verzameling persoonsgegevens alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden, betrokkene moet op de hoogte zijn en passende beveiliging. Organisaties die persoonsgegevens verwerken, zijn verplicht dit te melden bij de Autoriteit Persoonsgegevens. Organisaties kunnen ook een eigen interne toezichthouder aanstellen, de functionaris voor de gegevensbescherming (FG). De Wbp zal worden aangepast aan de nieuwe algemene verordening gegevensbescherming.

Algemene Verordening Gegevensbescherming (AVG) Op 25 mei 2016 is de Europese Algemene Verordening Gegevensbescherming in werking getreden. (Decentrale) overheden en bedrijven hebben tot 25 mei 2018 de tijd om aan de regels in de Verordening te voldoen. Deze nieuwe wetgeving moet zorgen voor harmonisatie van de huidige privacyregelgeving in Europa en verbetering van de privacy(bescherming) van burgers. Bij de nieuwe regelgeving gaat het vooral om het beschermen van persoonsgegevens in de digitale wereld.

Burgerlijk wetboek Relevant in situaties waarin de overheid of bedrijfsleven (een gedeelte van) het onderhoud of de hosting van haar informatiesystemen uitbesteedt aan een externe leverancier. Op contractuele afspraken is het burgerlijk wetboek van toepassing

Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) Deze wet omschrijft de taken en regelt de bevoegdheden van de AIVD en de MIVD. Binnen de kaders van hun taken en bevoegdheden zijn de AIVD en MIVD bevoegd inlichtingen en informatie te verzamelen met betrekking tot cybersecurity.

Wetboek van Strafrecht In het Wetboek van Strafrecht is een aantal specifieke strafbepalingen opgenomen die betrekking hebben op cybersecurity. Enkele voorbeelden hiervan zijn: Computervredebreuk (artikel 138ab): hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel, of
d. door het aannemen van een valse hoedanigheid.

Artikel 138b inzake (D)Dos en virusverspreiding.
artikel 139a en b: afluisteren
artikel 139c en d: aftappen

Verder nog bijvoorbeeld het bepaalde in artikel 161 sexies en 161 septies, inzake onder meer aantastingen van computersystemen. In deze artikelen is bepaald dat iemand die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, strafbaar is. Ook iemand aan wiens schuld dat te wijten is, is strafbaar.

Wetboek van Strafvordering In het Wetboek van Strafvordering zijn ook bepalingen opgenomen die betrekking hebben op cybersecurity, onder meer met bevoegdheden op het gebied van onderzoek van geautomatiseerde werken, doorzoeking ter vastlegging en inbeslagneming van gegevens; vordering tot verstrekking van telecommunicatieverkeersgegevens; opnemen van telecommunicatie; vordering tot verstrekking van gegevens ter zake van de gebruiker en de gebruikte communicatiedienst; en ontoegankelijk maken van gegevens.

Regelgeving

Voorschrift Informatiebeveiliging Rijksdienst (VIR) Dit besluit schrijft de technische en organisatorische maatregelen voor die getroffen worden ter bevordering van de beveiliging van binnen de Rijksdienst gedeelde informatie.

Voorschrift Informatiebeveiliging Rijksdienst – bijzondere informatie (VIR-BI) Dit besluit heeft betrekking op staatsgeheimen en overige bijzondere informatie waarvan kennisname door niet-gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van een of meer ministeries.

Beveiligingsvoorschrift Rijksdienst 2013 (BVR2013) Dit voorschrift is van toepassing op de integrale beveiliging van de Rijksdienst en geeft weer op welke wijze de verantwoordelijkheden voor de integrale beveiliging zijn verdeeld.

Baseline Informatiebeveiliging Rijksdienst (BIR) Deze baseline biedt een normenkader voor de beveiliging van de informatiehuishouding van de Rijksdienst. Om informatie-uitwisseling tussen organisaties binnen de Rijksdienst te vereenvoudigen, is er deze set rijksbrede beveiligingsnormen. Deze is in de plaats getreden van vijf interdepartementale normenkaders (voor DWR, Haagse Ring, Mobiele informatiedragers, Rijksweb en Departementaal vertrouwelijke webdiensten) en een groot aantal bestaande normenkaders bij ministeries en uitvoeringsorganisaties. De BIR bestaat uit een Tactisch Normenkader en een operationele baseline.

Algemene rijksvoorwaarden bij IT-overeenkomsten (ARBIT) De ARBIT zijn vooral bedoeld voor kleine en middelgrote IT-inkopen door de overheid.

2. Toekomstige wetgeving

Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) Dit wetsvoorstel introduceert een meldplicht voor ernstige ICT-inbreuken en stelt regels over het verwerken van gegevens ten behoeve van de taken van de minister van Veiligheid en Justitie op het terrein van cybersecurity. De meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving.

Wet computercriminaliteit III Dit wetsvoorstel zorgt ervoor dat de opsporing en vervolging van computercriminaliteit wordt versterkt. Dit is noodzakelijk vanwege technologische ontwikkelingen op internet en het gebruik van computers voor communicatie en de verwerking en opslag van gegevens. Ook worden burgers beter beschermd tegen bijvoorbeeld ‘grooming’ of de verspreiding van kinderpornografie, en tegen ernstige criminaliteit waarbij computers worden gebruikt. Politie en justitie mogen straks heimelijk en op afstand (online) onderzoek doen in computers. Dat kan een personal computer zijn, een mobiele telefoon of een server. Het geeft opsporingsambtenaren ruimte om verschillende onderzoekshandelingen toe te passen bij de opsporing van ernstige delicten. Zij kunnen gegevens ontoegankelijk maken of

kopiëren, maar ook communicatie aftappen of observeren. Politie en justitie hebben steeds meer last van versleuteling van elektronische gegevens. Internetgebruikers kunnen zelfs via bepaalde diensten gegevens anoniem transporteren. Dit speelt criminelen in de kaart.

NIB-richtlijn De richtlijn beoogt een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging te waarborgen. Lidstaten worden verplicht hun paraatheid te verbeteren en beter met elkaar samen te werken. Exploitanten van kritieke infrastructuur, essentiële aanbieders van informatiemaatschappijdiensten en overheden krijgen de verplichting opgelegd adequate maatregelen te nemen om beveiligingsrisico's te beheren en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporten. Vanaf het moment van publicatie (op 19 juli jl. in het publicatieblad van de EU) hebben de lidstaten een periode van 21 maanden, tot juni 2018, voor omzetting en implementatie van de richtlijn en een additionele zes maanden voor het identificeren van de partijen waarop de richtlijn van toepassing zal zijn.

Uitvoeringswetgeving: Europese verordening eIDAS Het wetsvoorstel strekt tot uitvoering van de EU-verordening over het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie. De voorgestelde uitvoeringswet bevat hiertoe wijzigingen van de Telecommunicatiewet, het Burgerlijk Wetboek, de Algemene wet bestuursrecht, de Wet bescherming persoonsgegevens en verscheidene andere wetten.

3. Opsomming van relevante EU-wet- en regelgeving

- Directive 2013/40/EU of 12 August 2013 on attacks against information systems
- Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)
- Regulation (EU) No 513/2014 of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management
- Regulation (EU) No 283/2014 of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure
- Regulation (EU) No 230/2014 of 11 March 2014 establishing an instrument contributing to stability and peace
- Regulation (EU) No 1291/2013 of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)
- Regulation (EU) No 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA