Centraal Planbureau

Achterstand Europees aanbod | *Vergroot volume en vertrouwen*

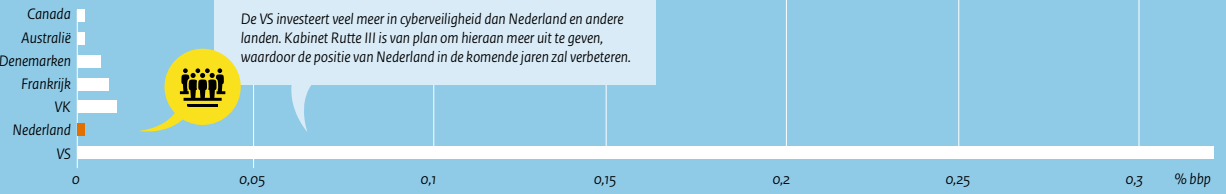
CPB Policy Brief | 2018/01

Knelpunten op de markt voor cyberveiligheid

Bastiaan Overvest
Anne Marieke Braam
Rinske Windig
Emilie Bartels

Knelpunten op de markt voor cyberveiligheid

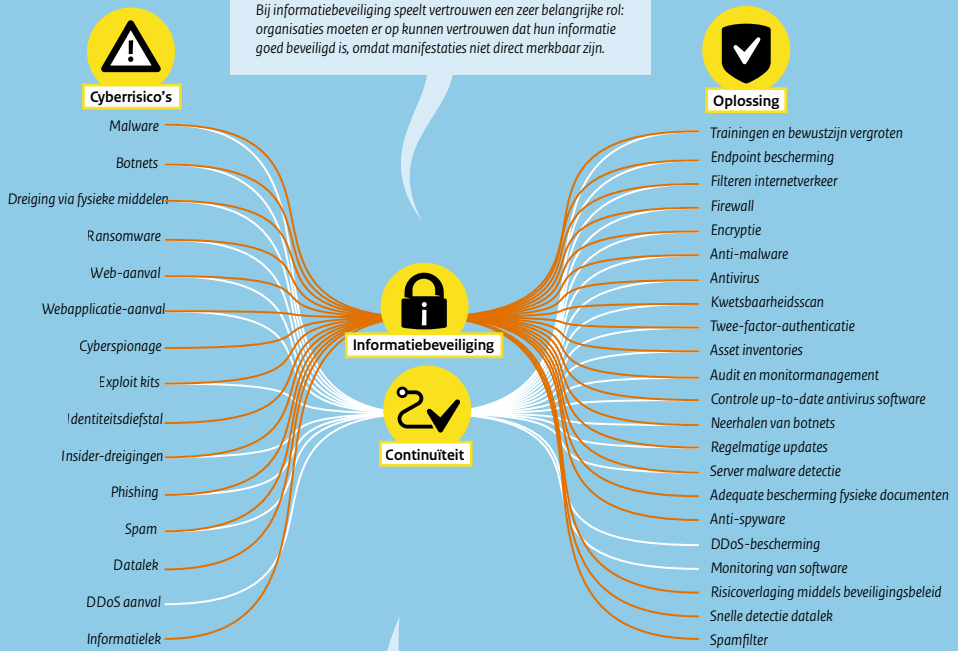
Hoe zorgen we voor een goed functionerende markt voor cyberveiligheid in Nederland en Europa?



De VS investeert veel meer in cyberveiligheid dan Nederland en andere landen. Kabinet Rutte III is van plan om hieraan meer uit te geven, waardoor de positie van Nederland in de komende jaren zal verbeteren.

1 Minder vertrouwen in buitenlandse cyberveiligheidsproducten

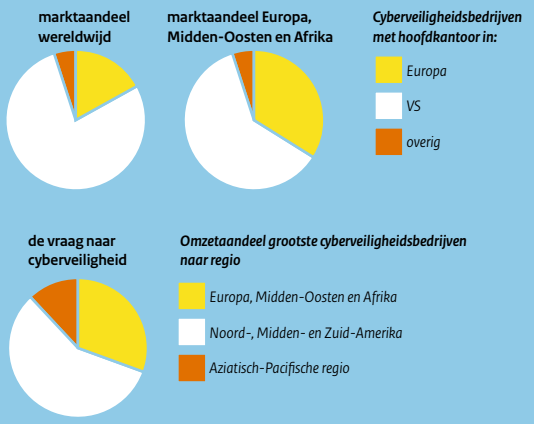
Bij informatiebeveiliging speelt vertrouwen een zeer belangrijke rol: organisaties moeten er op kunnen vertrouwen dat hun informatie goed beveiligd is, omdat manifestaties niet direct merkbaar zijn.



*Cyberdreigingen en oplossingen bestaan grofweg uit twee categorieën: ze vormen een gevaar voor de **informatiebeveiliging** of voor de **continuïteit** van een systeem.*

Er is sprake van informatie-asymmetrie: afnemers weten vaak niet goed welk product of welke dienst het best beschermt door de grote verscheidenheid aan dreigingen en oplossingen.

Deze investeringsvoorsprong vertaalt zich in een dominant marktaandeel van de VS, zowel wereldwijd als in Europa, Midden-Oosten en Afrika. Ook de vraag naar cyberveiligheidproducten is veel groter in de VS. Dat levert schaalvoordeel op. Nederland en andere Europese landen kunnen minder goed gebruik maken van schaalvoordelen.



2 Schaalvoordelen worden niet optimaal benut

Producten en diensten uit de VS kunnen door hun schaalvoordeel een stuk goedkoper zijn. Dit stelt afnemers van hoogwaardige informatiebeveiliging voor een dilemma: kiezen zij voor vertrouwde, nationale maar duurdere aanbieders, of voor goedkopere producten waarvan de betrouwbaarheid moeilijker gecontroleerd kan worden?

Om vertrouwen te vergroten kunnen in Europa (internationale) afspraken worden gemaakt over cyberveiligheid, zoals een digitale variant op de Geneefse Conventies. Hierin kunnen bijvoorbeeld afspraken worden gemaakt over het gebruik van 'zero-days' en achterdeurtjes door inlichtingendiensten.

De bewustwording over cybergevaren, en daarmee de vraag naar cyberveiligheidsproducten, kan worden vergroot door bedrijven bijvoorbeeld een 'cyberveiligheidsparagraaf' in hun jaarverslag te laten opnemen. Een grotere markt stelt Europese cyberveiligheidsbedrijven meer in staat te profiteren van schaalvoordelen.

Samenvatting

In Europa werkt de markt voor cyberveiligheid nog niet optimaal. Het gevolg is dat afnemers de keuze hebben tussen dure, maar gecontroleerde nationale oplossingen en relatief goedkope, maar moeilijk controleerbare buitenlandse producten. Voor een goed functionerende markt zijn er verschillende beleidsrichtingen. Zo kunnen (internationale) afspraken gemaakt worden over cyberveiligheid. Hierbij kan bijvoorbeeld gedacht worden aan afspraken over het gebruik van 'zero-days' en achterdeurtjes. Ook kan de bewustwording en daarmee de vraag naar cyberveiligheidsproducten worden vergroot door bedrijven een 'cyberveiligheidsparagraaf' in hun jaarverslag te laten opnemen.

De belangrijkste twee knelpunten waardoor de markt nog niet optimaal werkt, zijn onvoldoende vertrouwen in het aanbod van buitenlandse cyberveiligheidsbedrijven en onvoldoende mogelijkheden voor Europese aanbieders om schaalvoordelen te creëren. Om het (internationale) vertrouwen te vergroten zijn afspraken nodig over het gedrag van landen in het 'cyberdomein' (IT-netwerken zoals het internet, het telefonienetwerk en gesloten netwerken).

Om schaalvoordelen te creëren, moet de markt voor cyberveiligheid 'volwassen' worden. Hiervoor is meer informatie nodig over de kosten en baten van cyberveiligheid. Dit kan door bedrijven te stimuleren om een 'cyberveiligheidsparagraaf' in hun jaarverslagen op te nemen en door het verzamelen van meer Europese statistieken. Verder is het belangrijk dat de overheid op het terrein van cyberveiligheid een goede opdrachtgever is. Hierbij hoort ook adequaat toezicht op de cyberveiligheid van vitale processen.

Nu ontbreekt vertrouwen in buitenlandse cyberveiligheidsoplossingen. Hierdoor hebben Nederlandse aanbieders soms moeite om over de grens te verkopen. Dit vertrouwenstekort speelt vooral bij afnemers met een behoefte aan hoogwaardige cyberveiligheid. Dit zijn bijvoorbeeld bedrijven die beschikken over gevoelige informatie. Het vertrouwenstekort wordt daarnaast gevoed door incidenten waaruit blijkt dat inlichtingendiensten ook bevriende landen bespioneren. Schaalvoordelen ontbreken in Nederland, en mogelijk in Europa, doordat de markt voor cyberveiligheid hier relatief klein is en later op gang kwam dan in de VS. Het creëren van schaalvoordelen is dan ook nodig om te kunnen concurreren met de grote (met name) Amerikaanse aanbieders. Dit vergroot het vertrouwen in, en de kwaliteit van het Europese cyberveiligheidsaanbod.

De beleidsopties in deze *Policy Brief* kunnen helpen om de markt voor cyberveiligheid beter te laten functioneren. Hierdoor neemt uiteindelijk het algemene niveau van cyberveiligheid toe en kunnen we de economische vruchten van de digitalisering plukken.

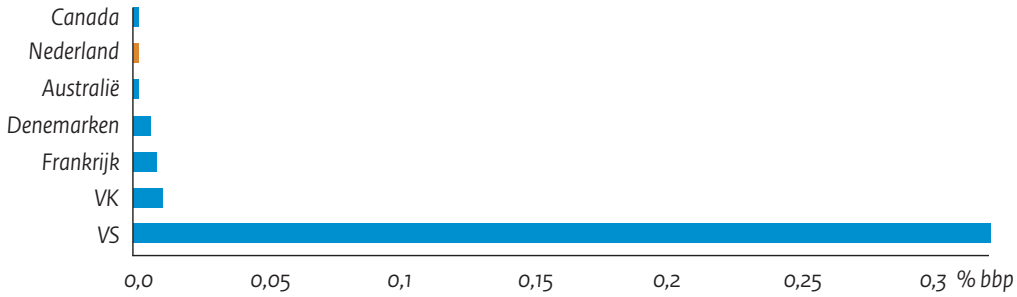
1. Marktwerking voor meer cyberveiligheid

In 2015 berichtte de Nederlandse chipmachinefabrikant ASML te zijn aangevallen door Chinese staatshackers. Hierbij hebben hackers mogelijk bedrijfsgeheimen over nieuwe technologieën buitgemaakt. De economische gevolgen van een hack kunnen groot zijn. Zo legde de gijzelsoftware 'non-Petya' in juni 2017 een containerterminal van AMP Terminals enkele dagen plat. De schade voor het bedrijf liep op tot 300 miljoen dollar.

Deze incidenten laten zien dat ICT kwetsbaar is. Dit is verontrustend, omdat onze economie en dagelijkse levens steeds meer digitaliseren. Digitalisering biedt kansen, maar het potentieel ervan kunnen we alleen optimaal benutten als we weerbaar zijn. Daarvoor moet de markt voor cyberveiligheid goed functioneren.

Hoe goed werkt die markt? Onvoldoende – volgens verschillende recente rapporten. Munnichs et al. (2017) concluderen bijvoorbeeld dat huishoudens, bedrijven en de overheid in Nederland te weinig investeren in cyberveiligheid en dat ze zich onvoldoende bewust zijn van het belang van cyberveiligheid. En Rademaker et al. (2016) wijzen op de relatief lage uitgaven van de Nederlandse overheid (zie figuur 1).

Figuur 1 De Nederlandse overheid investeert relatief weinig in cyberveiligheid



Bron: Rademaker et al. (2016).

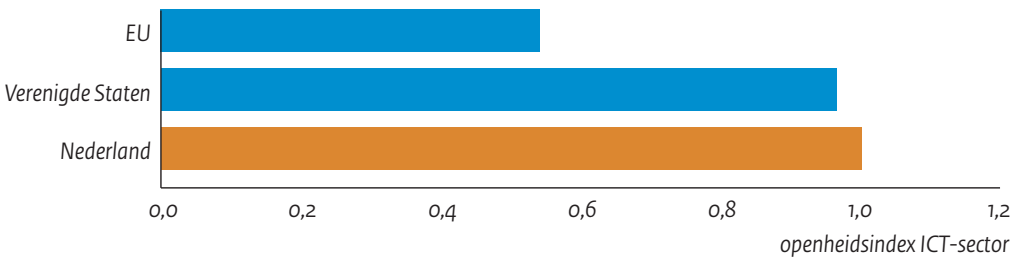
De Nederlandse uitgaven aan cyberveiligheid bedroegen in 2016 0,002 procent van het bbp.[1] In de Verenigde Staten lag dit percentage op 0,3 – hoger dan in een aantal Europese landen.

Momenteel werkt de Europese markt voor cyberveiligheid nog niet optimaal. Dit leidt tot een ongunstige *trade-off* tussen relatief dure maar betrouwbare producten en producten met een gunstige prijs-kwaliteitsverhouding, maar waarvan de betrouwbaarheid lastig te controleren valt. Deze *Policy Brief* geeft inzicht in de knelpunten op de markt voor cyberveiligheid en doet beleidsvoorstellen. Voor dit onderzoek hebben we gesprekken gevoerd met verschillende experts uit zowel het bedrijfsleven als de publieke sector (zie bijlage A).

[1] Overigens is het kabinet Rutte III van plan om hieraan meer uit te geven: structureel 95 miljoen euro vanaf 2021. Hierdoor verbetert de positie van Nederland in de komende jaren.

Daarnaast hebben we de markt in kaart gebracht op basis van cijfers uit jaarverslagen van de 21 grootste cyberveiligheidsaanbieders.

Figuur 2 ICT-sectoren Europese landen over het algemeen geslotener dan in de VS



Bron: UNCTAD World Development Indicators, bewerking CPB. NB. De figuur geeft de mate van openheid per land van de ICT-sector, gecorrigeerd voor de omvang van de economie en de openheid van andere sectoren in het land volgens de *Relative Comparative Advantage* maatstaf van Vollrath (1991).

Op basis van de gesprekken en onze eigen analyse hebben we zes mogelijke knelpunten geïdentificeerd: 1) handelsbarrières, 2) onvoldoende ICT-afgestudeerden, 3) onvoldoende bewustwording van cyberveiligheidsrisico's, 4) ongunstige randvoorwaarden, 5) onvoldoende mogelijkheden om schaalvoordelen te creëren, 6) onvoldoende vertrouwen in (met name) buitenlands aanbod. Als fundamentele knelpunten zien we *onvoldoende vertrouwen* en *onvoldoende schaal*.

Handelsbarrières, zoals importheffingen, kunnen een hindernis vormen voor de internationale markt voor cyberveiligheid. Specifiek voor cyberveiligheid kan het Wassenaar Arrangement een barrière vormen. Volgens deze regeling is voor producten zowel civiel als militair gebruikt kunnen worden (*dual-use*) een exportvergunning nodig. Hieronder vallen ook sommige cyberveiligheidsproducten. In de gesprekken met experts werden dergelijke handelsbarrières echter niet als knelpunt gezien.[2] Dit beeld wordt bevestigd door figuur 2.**Error! Reference source not found.** Deze geeft voor de VS, de EU en Nederland de relatieve openheid van de ICT-sector weer. Nederland heeft een relatief open ICT-sector. Opvallend is dat de EU als geheel in vergelijking met de VS een gesloten ICT-sector heeft.

Een veelgenoemd knelpunt in de gesprekken met experts is een tekort aan ICT- of cyberveiligheidsafgestudeerden. Dit knelpunt hangt samen met het feit dat de grootste werkgevers voor deze afgestudeerden in de VS (*Silicon Valley*) en, in toenemende mate, in Duitsland (zoals het *Helmholtz-Zentrum f IT-Sicherheit*) zitten. Deze grote organisaties bieden hogere salarissen en hebben meer ontwikkelingsmogelijkheden dan relatief kleine Nederlandse organisaties. Een tekort aan ICT'ers *an sich* lijkt daarom niet het probleem. Ook veel genoemd is een gebrek aan '*awareness*'. Het Nederlandse mkb zou bijvoorbeeld cyberveiligheidsrisico's te laag inschatten. Uiteindelijk beperkt dit de vraag naar cyberveiligheid. Paragraaf 3 gaat dieper in op de vraagzijde. Verder zijn volgens experts de randvoorwaarden voor startende (cyberveiligheids-)bedrijven in Nederland relatief

[2] Door beveiligingsonderzoekers wordt het Wassenaar Arrangement wel gezien als barrière bij het internationaal delen van kennis over softwarekwetsbaarheden.

ongunstig. Voor deze bedrijven is er bijvoorbeeld te weinig financiering beschikbaar in de vorm van durfkapitaal om een goede start te maken.[3] Goede randvoorwaarden zijn belangrijk voor een dynamisch ondernemingsklimaat, maar niet specifiek voor cyberveiligheid en komen daarom in dit stuk verder niet aan de orde.

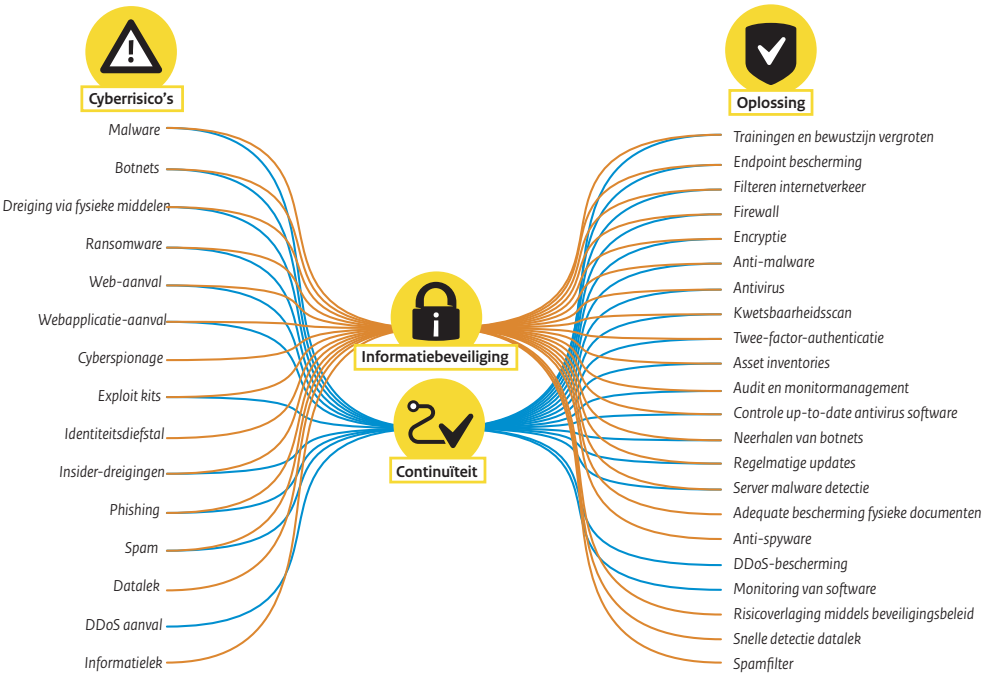
Om de markt voor cyberveiligheid beter te laten functioneren, zou het beleid zich meer kunnen richten op de twee fundamentele knelpunten: vergroten van het (internationale) vertrouwen in het cyberveiligheidsaanbod en creëren van schaal aan de aanbodzijde. Het internationale vertrouwen kan omhoog door afspraken te maken over statelijke verantwoordelijkheden en bevoegdheden. Ook kan gedacht worden aan een evaluatie van het Nederlandse certificeringssysteem voor hoogwaardige oplossingen (zoals beveiliging van staatsgeheimen) en een verdere harmonisatie van Europese certificeringssystemen. De mogelijkheden om schaal te creëren kunnen worden vergroot door te zorgen voor een maatschappelijk optimale vraag naar cyberveiligheid. Dit kan via goed opdrachtgeverschap van de overheid[4] en een stevig toezicht op de cyberveiligheid van vitale processen. Daarnaast kunnen bedrijven meer openheid geven in een ´cyberparagraaf´ in het jaarverslag.

2. Het belang van vertrouwen

Het vertrouwen in buitenlandse cyberveiligheidsoplossingen is soms laag – vooral als het om de staatsveiligheid gaat. Zo verbood de Amerikaanse overheid in september 2017 het gebruik van Russische beveiligingssoftware vanwege twijfels over de betrouwbaarheid. Ook zou de Amerikaanse inlichtingendienst NSA in Europa hebben gespioneerd, waaronder bij kanselier Angela Merkel en vliegtuigbouwer Airbus.[5] Dit soort incidenten vergroten de behoefte aan betrouwbare cyberveiligheidsoplossingen, liefst uit eigen land. Uit onze gesprekken met experts komt vertrouwen dan ook naar voren als een belangrijk knelpunt. Zonder buitenlands vertrouwen houdt voor Europese cyberveiligheidsbedrijven de groei op bij de landsgrens.

[3] Ook in Nederland is er durfkapitaal voor cyberveiligheidsbedrijven. In november 2017 werd bekend dat EclecticIQ een injectie kreeg van 14 miljoen euro. Straathof en Van Veldhuizen (2015) laten zien dat het volume van de Nederlandse durfkapitaalinvesteringen sinds 2010 sterk stijgt.
[4] Zie ook VKA/SEO (2016) voor suggesties rondom opdrachtgeverschap van de overheid.
[5] Zie bijvoorbeeld dit artikel in de Volkskrant.

Figuur 3 Cyberdreigingen en oplossingen



NB. De lijst van dreigingen en mogelijke oplossingen komt uit ENISA Threat Landscape Report 2016.

Op de markt voor cyberveiligheid bieden cyberveiligheidsbedrijven diverse oplossingen aan voor allerlei cyberdreigingen (zie figuur 3). Cyberdreigingen vormen een gevaar voor informatiebeveiliging en/of de continuïteit van de ICT van een afnemer.

In hoeverre vertrouwen voor een afnemer een rol speelt, is afhankelijk van meerdere factoren. Ten eerste is het belang van vertrouwen extra groot bij informatiebeveiliging, omdat het soms maanden of jaren kan duren voordat een informatielek wordt ontdekt, als het al wordt ontdekt. Dit in tegenstelling tot een verstoring van de continuïteit van een bedrijf – dat is meestal wel direct merkbaar. Wanneer er geen direct signaal is, is het belangrijk dat organisaties vertrouwen hebben dat de informatie goed is beveiligd.

Ten tweede verschilt het belang van vertrouwen per type afnemer. Voor sommige afnemers is de te beveiligen informatie bijzonder gevoelig of kostbaar. Denk hierbij aan staatsgeheimen of waardevolle *know-how*. Ook de continuïteit van systemen is soms essentieel. Bijvoorbeeld voor een vitaal proces als het betalingsverkeer, of de levering van stroom. Niet alleen zijn de behoeftes van deze afnemers anders dan van het gemiddelde huishouden, ook het dreigingsniveau verschilt per type gebruiker. Zo is een organisatie met gevoelige of verhandelbare informatie een aantrekkelijk doelwit voor een gerichte aanval. Deze afnemers hebben dus behoefte aan hoogwaardige cyberveiligheid. Tussen deze 'hoogwaardige' afnemers van cyberveiligheid en aanbieders speelt vertrouwen een essentiële rol.

Een gebrek aan vertrouwen hangt daarnaast samen met een gebrek aan informatie. Op de markt voor cyberveiligheid is sprake van informatieasymmetrie: Afnemers hebben meestal minder informatie over nut en noodzaak van een product dan aanbieders. Daarnaast is het verschil in beveiligingsniveau tussen producten voor afnemers moeilijk in te schatten. Een mogelijk gevolg van deze 'averechtse selectie' is dat alleen de goedkoopste aanbieders met de laagste kwaliteit overblijven – een *lemons market*. Aan de aanbodzijde bestaat het risico op moreel gevaar. Een buitenlands cyberveiligheidsbedrijf kan in het geheim samenwerken met een inlichtingendienst, of met een concurrent van de afnemer. In verschillende landen zijn bedrijven en burgers immers al verplicht om, al dan niet heimelijk, medewerking te verlenen aan inlichtingendiensten.

Afnemers en aanbieders gaan op verschillende manieren om met het vertrouwenstekort. Nationale overheden kunnen voor bepaalde producten controles verplichten of producten uit verdachte landen weren. In Nederland worden cyberveiligheidsproducten beoordeeld door de AIVD en de MIVD. Andere landen hebben vergelijkbare controles. Ook kunnen overheden controles en beperkingen instellen voor IT-bedrijven en voor de handel in veiligheidsproducten. De *International Traffic in Arms Regulations* (ITAR) en de *Export Administration Regulations* (EAR) zijn voorbeelden van Amerikaanse wetgeving voor import en export van veiligheidsproducten. In Duitsland kan de overheid een buitenlandse deelname van meer dan 25 procent in een IT-bedrijf blokkeren, met het *Außenwirtschaftsgesetz* . In Nederland gaan ook stemmen op voor een dergelijke wet sinds de overname van Fox-IT door een Brits bedrijf in 2015, maar deze wet bestaat nog niet. Een andere mogelijkheid is om zelf cyberveiligheidsoplossingen te (laten) ontwikkelen. In Nederland gebeurt dat sinds 2012 via de 'Small Business Innovation Research' regeling.[6] Het Verenigd Koninkrijk stimuleert bijvoorbeeld via *grand challenges* nieuwe cyberveiligheidsoplossingen[7] en in Duitsland wordt een groot onderzoekscentrum voor cyberveiligheid opgericht.

Aanbieders kunnen het vertrouwenstekort tegengaan door meer transparantie of zekerheden te bieden. Kaspersky heeft bijvoorbeeld in september 2017 aangeboden om voor het Amerikaanse Congres te getuigen en de software te laten controleren.[8] En Apple verklaarde in 2016 niet mee te werken aan een FBI-verzoek over het ontgrendelen van een iPhone van een terrorist. In Rusland weigerde chatapp Telegram publiekelijk medewerking aan de Russische inlichtingendienst FSB. Microsoft, als laatste voorbeeld, heeft een Duits cloudcentrum ondergebracht bij Deutsche Telekom. Hierdoor kan Microsoft niet of moeilijker meewerken aan Amerikaanse informatieverzoeken. Ook kunnen bedrijven investeren in het laten certificeren van hun producten. Een andere mogelijkheid is het onder opensource-licentie uitbrengen van technologie.

Uiteindelijk kan het vertrouwenstekort gevolgen hebben voor de markt voor cybersecurity als geheel. Als kwaliteit niet zichtbaar is, loont het voor aanbieders niet om te investeren in

[6] Zie bijvoorbeeld dit bericht van dcypher.
[7] Zie de National Cyber Security Strategy van het VK.
[8] Zie dit nieuwsbericht van Kaspersky.

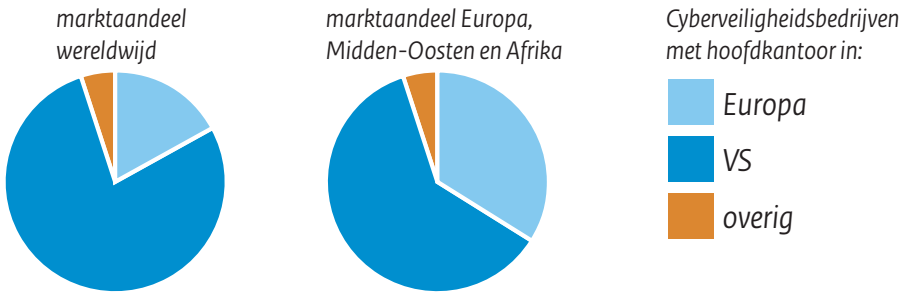
veiligere ICT-producten. Als binnenlandse aanbieders meer vertrouwd worden dan buitenlandse aanbieders, brengt dat een concurrentienadeel met zich mee voor cyberveiligheidsbedrijven met internationale ambities. Europese cyberveiligheidsbedrijven met een product waarbij vertrouwen essentieel is, kunnen dus relatief minder groeien. De markt voor dat type hoogwaardige oplossingen is dan mogelijk nationaal.

Een oplossing voor deze problemen ligt in het vergroten van het internationale vertrouwen in het cyberveiligheidsaanbod. Dit is vooral belangrijk voor producten waarbij vertrouwen een grote rol speelt, zoals technologie die gebruikt wordt voor staatsgeheimen, continuïteit van vitale processen en waardevolle bedrijfsgeheimen. Internationale afspraken over gedrag en taken van landen in het cyberdomein helpen hierbij. Deze en andere opties worden verder uitgewerkt in paragraaf 4.

3. Het belang van schaal

Als (internationaal) vertrouwen het belangrijkste knelpunt is, dan leidt dit tot nationaal afgebakende markten. Dat zien we echter niet. De helft van de grootste cyberveiligheidsbedrijven komt uit de Verenigde Staten. Het wereldwijde marktaandeel van Amerikaanse bedrijven is maar liefst 78 procent (zie figuur 4). Europese cyberveiligheidsbedrijven hebben een aandeel van 17 procent wereldwijd – en in Europa, het Midden-Oosten en Afrika 34 procent. Hoe kan het dat Amerikaanse bedrijven de internationale markt voor cyberveiligheid zo beheersen?

Figuur 4 De Verenigde Staten domineren de markt voor cyberveiligheid



NB. De figuur laat het marktaandeel zien van cyberveiligheidsbedrijven uit Europa, de VS en overige economieën. Het marktaandeel is weergegeven voor de wereldwijde markt en voor EMEAR (Europa, Midden-Oosten en Afrika). Marktaandelen zijn berekend met gegevens uit jaarverslagen van de 21 grootste aanbieders.[9] Cijfers zijn voor 2016 of meest recent beschikbaar.

[9] Deze lijst is samengesteld op basis van de concurrentieanalyse uit jaarverslagen, de Cybersecurity 500, een besluit van de Europese Commissie, en Worldwide Endpoint Security 2010-2014 Forecast. 'Multiple product' bedrijven waarbij het cyberveiligheidsaandeel niet is gespecificeerd, zijn weggelaten.

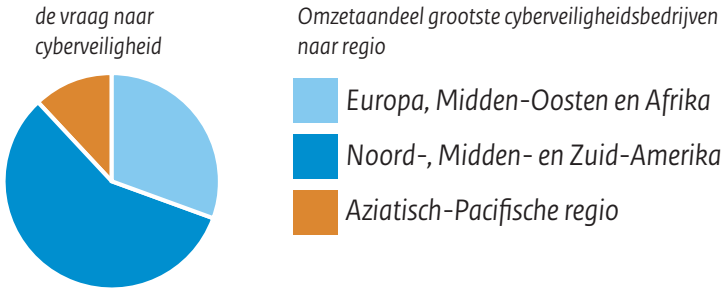
Het korte antwoord is: schaal.[10] Een bedrijf heeft schaalvoordelen als de gemiddelde kosten lager zijn naarmate het meer produceert. Software en digitale platformen zijn voorbeelden van producten met schaalvoordelen. De marginale productiekosten voor een softwarekopie zijn namelijk bijna nul. Ook bij cyberveiligheidsoplossingen – zoals antivirussoftware, monitoringsdiensten en gegevensbeheersystemen – zijn schaalvoordelen daarom belangrijk. Een extra reden waarom grotere bedrijven een voordeel hebben, is dat afnemers erop willen vertrouwen dat een aanbieder tijdens een crisissituatie voldoende menskracht heeft. Op zo'n markt kan slechts een handvol grote bedrijven overleven.

Waarom slagen Europese bedrijven er minder goed in om schaalvoordelen te creëren? Dit heeft meerdere oorzaken. Ten eerste hebben de Verenigde Staten een voorsprong: de ICT-sector is daar groter en de vraag naar cyberveiligheid kwam daar eerder op gang. Op het gebied van wetgeving in de ICT-sector zijn de Verenigde Staten ook een voorloper. Bedrijven zijn al vanaf 2003 wettelijk verplicht om een datalek te melden, terwijl in Nederland deze generieke verplichting er sinds 2016 is. Vanaf 25 mei 2018 gaat de Algemene verordening gegevensbescherming (AVG) in, waarmee in elke EU-lidstaat een meldplicht geldt.

Ten tweede is de Amerikaanse thuismarkt groter. De economieën in de afzonderlijke Europese lidstaten zijn kleiner dan de Amerikaanse economie. Cyberveiligheidsbedrijven in de VS kunnen daardoor laagdrempeliger groeien en schaalvoordelen behalen, zonder het product te moeten aanpassen.

Een derde verklaring is dat de vraag naar cyberveiligheid in de Verenigde Staten groter is. Figuur 1 laat al zien dat de Amerikaanse overheid daar relatief veel aan uitgeeft. En de omzet van de grootste cyberveiligheidsbedrijven wordt voor het grootste deel behaald in de "AMER"-regio; meer dan op basis van bbp verwacht mag worden (figuur 5).

Figuur 5 Vraag cyberveiligheid relatief hoog in Noord- en Zuid-Amerika



NB. Het diagram geeft het volumeaandeel van de top 21 cyberveiligheidsbedrijven in drie economische regio's.

Waarom de vraag naar cyberveiligheid in de Verenigde Staten groter is, kan ten eerste verklaard worden door de verschillen in wetgeving. Denk bijvoorbeeld aan het Amerikaanse productaansprakelijkheidsrecht. Deze verschillen leiden niet zozeer tot handelsbarrières, maar tot verschillen in omvang van de vraag. Ten tweede ervaren de Verenigde Staten (maar

[10] Ook VKA/SEO (2016), p. 53, wijst op het belang van schaalgrootte.

ook Israël) mogelijk een hoger dreigingsniveau dan Nederland en andere Europese landen. Amerikaanse overheden en bedrijven verwachten of ervaren bijvoorbeeld dreiging vanuit Noord-Korea, Rusland of terroristische groepen. De defensie-uitgaven van de VS zijn met 3,3 procent bbp dan ook hoger dan in Nederland of Duitsland (beide 1,2 procent bbp). Ten derde kan de vraag in Europa relatief laag zijn als ICT-gebruikers binnen huishoudens, bedrijven en overheden de cyberrisico's te laag inschatten. Vaak wordt het mkb gezien als een (te) weinig digitaal bewuste sector – cijfers die dit kunnen onderbouwen, zijn er echter nog niet. Mogelijk verandert dit met de Algemene verordening gegevensbescherming (AVG) die bedrijven dwingt om digitale (persoons-)gegevens goed te beveiligen.

De Amerikaanse 'dominantie' heeft belangrijke gevolgen voor de markt. Het grootste deel van de wereldwijde omzet komt namelijk bij Amerikaanse bedrijven terecht. Uit de gesprekken kwam naar voren dat zij hierdoor innovatiever zijn en gemiddeld een hogere kwaliteit kunnen bieden. Europese aanbieders hebben veelal onvoldoende schaal, waardoor ze relatief duur zijn en maar een beperkt aantal producten kunnen aanbieden. Voor grotere afnemers zijn deze kleine cyberveiligheidsbedrijven bovendien minder aantrekkelijk vanwege hun beperkte capaciteit.

Een ander gevolg van de verschillen in schaalgrootte is dat talent wegtrekt. Grote cyberveiligheidsbedrijven en kennisinstellingen zitten vooral in de Verenigde Staten, maar ook steeds meer in het Verenigd Koninkrijk of Duitsland. Deze organisaties bieden doorgaans hogere salarissen en betere opleidingsmogelijkheden dan kleine Nederlandse cyberveiligheidsbedrijven.

De twee knelpunten van vertrouwen en schaal samen hebben gevolgen voor de Nederlandse markt. De vraagzijde, en dan vooral afnemers met een hoogwaardige behoefte, staan namelijk voor een ongemakkelijke keuze: tussen enerzijds vertrouwde, maar relatief dure, nationale producten en anderzijds ogenschijnlijk kwalitatief hoogwaardige en gunstig geprijsde producten met onzekerheid over de betrouwbaarheid. Deze *trade-off* leidt tot een segmentering van de markt: hoe gevoeliger of hoogwaardiger de vraag, hoe hoger het marktaandeel van nationale aanbieders zal zijn.

Een vergroting van de vraag stelt Nederlandse cyberveiligheidsbedrijven in staat om schaalvoordelen te creëren. Of de vraag momenteel 'te laag' is weten we niet. Wel zijn er aanwijzingen dat de vraagzijde nog niet volwassen is. Meer informatie voor ICT-gebruikers over cyberrisico's vergroot mogelijk de vraag. Ook kan de vraag worden vergroot wanneer de overheid meer doet om cyberveiligheid van de eigen organisatie en van vitale processen te borgen.

4. Beleidsopties

Voor een goede werking van de markt voor cyberveiligheid zijn voldoende *schaal* en *vertrouwen* essentieel. Als de marktvraag onvoldoende volwassen is en als het vertrouwen in

buitenlandse producten (al dan niet terecht) ontbreekt, ontstaan onnodige risico's voor gebruikers van ICT en voor vitale processen die van ICT afhankelijk zijn.

Het huidige beleidspakket zorgt al grotendeels voor meer schaal en vertrouwen. Zo vergemakkelijkt de EU-Dienstenrichtlijn grensoverschrijdende dienstverlening en stimuleert de AVG organisaties om veilig met (digitale) persoonsgegevens om te gaan. Verder schrijft de Europese NIB-richtlijn beveiligingsvereisten voor, die momenteel worden omgezet naar nationaal recht met het wetsvoorstel voor de Cybersecuritywet. We zien een aantal opties om de markt nog beter te laten werken:

1. Maak internationale afspraken over statelijke verantwoordelijkheden en bevoegdheden in het cyberdomein.
2. Harmoniseer het Europese certificeringssysteem.
3. Evalueer het Nederlandse certificeringssysteem.

Om Nederlandse en andere Europese cyberveiligheidsbedrijven in staat te stellen om schaalvoordelen te creëren, zien we deze beleidsopties:

4. Stimuleer het opnemen van een 'cyberparagraaf' in jaarverslagen.
5. Verzamel Europese statistieken over cyberveiligheid bij bedrijven.
6. Vergroot cyberexpertise bij de overheid.
7. Denk goed na over benodigde kennis en producten ('vraagarticulatie').
8. Zorg voor een cyberveilige digitale overheidsinfrastructuur. Bijvoorbeeld via 'security by design' en/of als gunningscriterium bij de aanbesteding.
9. Zorg voor goede afstemming en organisatie van het toezicht op cyberveiligheid van vitale processen.

Deze beleidsopties helpen om de markt voor cyberveiligheid beter te laten werken. Positieve gevolgen daarvan zijn dat Nederlandse cyberveiligheidsbedrijven meer mogelijkheden krijgen om (internationaal) door te groeien. Ook krijgt de vraagzijde meer keuze, waardoor het algemene niveau van cyberveiligheid kan toenemen.

De negen opties worden hieronder verder uitgewerkt.

Ad 1) Het internationale vertrouwen kan worden vergroot door afspraken over de bevoegdheden en werkwijze van inlichtingen- en opsporingsdiensten in het cyberdomein. Hierbij kan worden gedacht aan een EU-standpunt over encryptie en de voorwaarden waaronder inlichtingen- en opsporingsdiensten digitaal onderzoek mogen doen. Staan we bijvoorbeeld toe dat inlichtingendiensten 'zero-days' (weeffoutjes in software die onbekend zijn bij de leverancier en waardoor digitaal kan worden ingebroken) of achterdeurtjes (bewust ingebouwde technieken om bijvoorbeeld een wachtwoord te omzeilen) in software mogen gebruiken? Afspraken hierover kunnen ook, als begin, bilateraal worden gemaakt of opgesteld als niet-bindende principes.[11] Om de naleving van internationale afspraken te

[11] Een voorbeeld van niet-bindende regelgeving is de Tallinn-handleiding. Deze bevat een richtinggevende analyse van de toepassing van het internationaal recht op het cyberdomein.

borgen kan een onafhankelijke autoriteit worden ingesteld – zoals de OPCW (chemische wapens) en de IAEA (atoomenergie).

Ad 2 en 3) Veel landen kennen een certificeringssysteem voor cyberveiligheidsproducten die zij gebruiken voor de bescherming van staatsgeheimen of defensiemiddelen. In Nederland worden cyberveiligheidsproducten beoordeeld door de AIVD en de MIVD. Het is belangrijk dat dit systeem goed werkt. Een strenge (en mogelijk langdurige) beoordeling voorkomt dat onbetrouwbare producten gebruikt worden, maar heeft ook het risico dat gebruikers van nuttige producten lang moeten wachten of dat het product technologisch achterhaald is op het moment dat de goedkeuring er is. Een goed certificeringssysteem maakt de maatschappelijk optimale afweging tussen deze voor- en nadelen.

Het zou nuttig zijn om te evalueren hoe de afweging tussen betrouwbaarheid en tijdigheid in het Nederlandse systeem wordt gemaakt. Hierbij kan ook worden gekeken naar aspecten als de toelating tot de beoordeling, de vergoeding van de kosten en de termijn waarbinnen het onderzoek is afgerond.

Een andere route is om het Europese stelsel van certificering verder te harmoniseren. Lidstaten vertrouwen nu vooral op eigen controles.[12] Als hetzelfde product meermaals gecertificeerd moet worden, en op steeds weer een andere manier, brengt dat extra kosten met zich mee. En als een bedrijf erin slaagt om een buitenlandse goedkeuring te krijgen betekent dat niet dat het product ook gekocht zal worden. De internationale effectiviteit van het certificeringssysteem kan worden vergroot door verdergaande harmonisatie.[13] Hierbij kan worden gedacht aan uniforme producteisen, een open toegang en, uiteindelijk, een 'Single Passport' – zoals dat al bestaat voor de bancaire sector op de Interne Markt.

Ad 4) Bedrijven zijn huiverig om openheid te geven over cyberincidenten. Om bedrijven aan te zetten tot meer transparantie kan overwogen worden om een 'cyberparagraaf' in het jaarverslag verplicht te stellen. In zo'n paragraaf geeft het bedrijf inzicht in de maatregelen die zijn genomen om cyberrisico's in te perken en welke incidenten zich hebben voorgedaan. Dit vergroot niet alleen het maatschappelijke inzicht in de cyberveiligheid, maar zet bedrijven er ook toe aan om bewust na te denken over cyberrisico's en interne maatregelen te nemen. Meer informatie over cyberveiligheid kan de vraag naar cyberveiligheid vergroten, waardoor uiteindelijk schaal wordt gecreëerd.

Op grond van de Wet gegevensverwerking en meldplicht cybersecurity zijn bedrijven die een vitaal proces aanbieden, verplicht om bij het Nationaal Cyber Security Centrum (NCSC) melding te doen van ernstige cyberincidenten. Deze meldingen helpen het NCSC om haar coördinerende en hulpverlenende rol goed in te vullen.

Ad 5) Op het niveau van bedrijven en overheden zijn geen cijfers over de frequentie en de aard van cybercriminaliteit en de kosten en baten van cyberveiligheidsmaatregelen beschikbaar. Om deze kennislacune op te vullen kan meer en gerichter statistisch onderzoek

[12] Het Verenigd Koninkrijk kent bijvoorbeeld de 'Commercial Product Assurance' en Frankrijk de Certification Sécuritaire de Premier Niveau.
[13] De Europese Commissie kondigde in september 2017 hiervoor voorstellen aan. [link]

gedaan worden. Het is wenselijk om dit voor een langere periode en op Europees niveau te doen. Het onderzoek kan niet alleen worden uitgevoerd onder bedrijven en huishoudens, maar ook via uitvragen bij cyberverzekeraars of ISACS (samenwerkingsverbanden tussen organisaties om informatie uit te wisselen). Beter statistisch onderzoek helpt bovendien om na te gaan in hoeverre de bewustwording binnen de samenleving onvoldoende is.

Ad 6, 7 en 8) Een aanbeveling voor goed opdrachtgeverschap door de overheid op het terrein van cyberveiligheid komt voort uit drie beleidsopties: 'Vergroot cyberexpertise bij de overheid', 'Denk goed na over benodigde kennis en producten (vraagarticulatie)' en 'Zorg voor een cyberveilige digitale overheidsinfrastructuur'. De overheid is een van de grootste vragers van ICT en zou daarom ook een van de grootste vragers moeten zijn van cyberveiligheidsoplossingen. Om een goede opdrachtgever te zijn, is voldoende kennis vanuit de overheid noodzakelijk. Deze expertise kan vervolgens worden ingezet om een duidelijke visie op te stellen en na te denken over welke kennis, diensten of producten nodig zijn; ook wel de vraagarticulatie genoemd. Verschillende ministeries zijn hier nu al actief mee bezig en hebben een 'Strategische Kennis- en Innovatieagenda' (SKIA) opgesteld, waarin onder andere de visie op veiligheid staat beschreven.[14]

De vraagarticulatie helpt vervolgens om doelgericht op een passende manier kennis of kunde in te kopen of zo nodig te laten ontwikkelen.[15] Bij het ontwikkelen van nieuwe producten kan gedacht worden aan instrumenten als SBIR, PCP of een innovatiepartnerschap.[16] Als ICT-diensten worden ingekocht dan is het belangrijk om al in een vroeg stadium na te denken over de cyberveiligheid. Bijvoorbeeld door te eisen dat het in te kopen product '*by design*' veilig is of door cyberveiligheid als expliciet criterium te laten meewegen bij de gunning[17]. Ook is het soms wenselijk om meerdere producten kleinschalig naast elkaar te testen.[18]

Ad 9) De cyberveiligheid van de vitale processen (zoals elektriciteits- en drinkwatervoorziening, of betalingsverkeer) is essentieel voor het goed functioneren van de maatschappij. Vitale bedrijven zijn in eerste instantie zelf verantwoordelijk voor hun cyberveiligheid. Het toezicht op de cyberveiligheid zal (volgens het wetsvoorstel Cybersecuritywet) sectoraal bij bestaande toezichthouders worden belegd. Het risico dat kan ontstaan, is dat vitale bedrijven onvoldoende investeren in cyberveiligheid en dat de sectorspecifieke toezichthouders dat onvoldoende zien of kunnen bijsturen, met als gevolg dat potentiële schaalvoordelen onbenut blijven.

Om dit risico te beperken hebben sectorale toezichthouders kennis en informatie nodig. Deze expertise kan worden opgebouwd door het aantrekken van cyberdeskundigen en door samenwerking met het NCSC en sectorspecifieke toezichthouders. Hierbij kan gedacht worden aan een werkgroep van toezichthouders en de publicatie van formele afspraken tussen het NCSC en toezichthouders. Zulke afspraken kunnen bijvoorbeeld duidelijk maken welke informatie wél en welke vooral níet gedeeld wordt.

---

[14] Zie bijvoorbeeld de SKIA's van het ministerie van Defensie en van Justitie en Veiligheid.
[15] Zie Van Elk et al. (2017) voor een kader voor doelgericht onderzoeksbeleid.
[16] De site van Pianoo geeft meer informatie over innovatiegericht inkopen.
[17] Een klassiek voorbeeld van hoe het mis kan gaan, is 'Diginotar'.
[18] Bij technologische onzekerheid en padafhankelijkheid is het optimale beleid een combinatie van vroegtijdig ingrijpen en ruimte voor experimenten. Zie Bijlsma et al. (2016).

Bijlage A Gesprekspartners

Naam	Organisatie	Functie
Hans de Vries	Nationaal Cyber Security Centrum	Directeur
Hans van Loon	Van Loon Cyber	Strategy & business consultant
Hoi Wah Yip	AON	Manager
Jeremy Maginot	AON	Director
Mark Buningh	AON	Cyber Risk Practice Leader
Thijs de Boer	AON	Strategy director
Jan Piet Barthel	dcypher	Directeur
Kas Clark	Nationaal Cyber Security Centrum	Senior onderzoeker
Lars van Willigen	Ministerie van Economische Zaken	Beleidsadviseur
Maarten van Wieren	Deloitte	Senior manager
Maxwell Keyte	CapGemini	Lead cybersecurity
Michel Rademaker	The Hague Centre for Strategic Studies	Deputy director
Muhittin Hasancioglu	Shell	Vice president
Petra van Schayik	Compumatica	CEO
Sjoerd Peerlkamp	Alliander	CISO
Tim van Essen	Ministerie van Buitenlandse Zaken	Beleidsadviseur
Yori Kamphuis	CoBlue	Chief business development officer
Philip Meijer	Innovation Quarter	Account manager safety & security
Eric van Pelt	Netherlands Foreign Investment Agency	Senior project manager
Richard Franken	The Hague Security Delta	Directeur
Nathalie Falot	Considerati	Senior legal consultant
Marcel van Oirschot	Fox-IT	Commercieel directeur

Bijlage B Overzicht cybersecurity bedrijven

Bedrijfsnaam	Hoofdvestiging	Omzet (in mln.$)	Marktaandeel (%)
BAE Systems	Verenigd Koninkrijk	1.601,10	3,69
Booz Allen Hamilton	Verenigde Staten	5.804,28	13,38
CA Technologies	Verenigde Staten	4.036,00	9,30
Check Point Software Technologies	Israël	1.740,30	4,01
Cisco Systems	Verenigde Staten	1.969,88	4,54
CyberArk	Verenigde Staten	216,60	0,50
FireEye	Verenigde Staten	714,11	1,65
F-Secure	Finland	158,29	0,36
IBM Security	Verenigde Staten	7.192,71	16,57
Intel	Verenigde Staten	2.375,48	5,47
Kaspersky Lab	Rusland	644,00	1,48
Mimecast	Verenigd Koninkrijk	186,60	0,43
NCC Group	Verenigd Koninkrijk	241,90	0,56
Palo Alto Networks	Verenigde Staten	1.761,60	4,06
Rapid7	Verenigde Staten	157,44	0,36
Raytheon	Verenigde Staten	561,00	1,29
SecureWorks	Verenigd Koninkrijk	262,13	0,60
Sophos	Verenigd Koninkrijk	407,87	0,94
Symantec	Verenigde Staten	4.019,00	9,26
Thales	Frankrijk	8.186,75	18,87
Trend Micro	Japan	1.159,06	2,67

NB. * jaarverslag 2016, ** jaarverslag 2017. Sommige bedrijven zijn actief op meer markten dan alleen die voor cyberveiligheid: BAE Systems heeft een onderdeel *Cyber & Intellegence* (9%); Booz Allen Hamilton heeft *Cyber* als een van de vijf onderdelen; CA Technologies heeft de onderdelen *Mainframe Solutions* (54%), *Enterprise Solutions* (38%) en *Services* (8%) waar cyberveiligheid allemaal onder valt; Check Point Software Technologies is nagenoeg volledig gericht op cyberveiligheid; Cisco Systems heeft een onderdeel *Security* (4%); CyberArk is nagenoeg volledig gericht op cyberveiligheid; FireEye is nagenoeg volledig gericht op cyberveiligheid; F-Secure is nagenoeg volledig gericht op cyberveiligheid; IBM Security heeft een onderdeel *Cognitive Solutions* waar cyberveiligheid onder valt (12%); Intel heeft de *Data Center Group* (55%) en de *Security Group* (4%) waar cyberveiligheid onder valt; Kaspersky Lab is nagenoeg volledig gericht op cyberveiligheid; Mimecast is nagenoeg volledig gericht op cyberveiligheid; NCC Group is nagenoeg volledig gericht op cyberveiligheid; Palo Alto Networks is nagenoeg volledig gericht op cyberveiligheid; Rapid7 is nagenoeg volledig gericht op cyberveiligheid; Raytheon heeft het onderdeel *Forcepoint* waar cyberveiligheid onder valt (6%); SecureWorks is nagenoeg volledig gericht op cyberveiligheid; Sophos biedt hardware (20%), cyberveiligheidsproducten (77%) en overige diensten (3%) aan; Symantec is nagenoeg volledig gericht op cyberveiligheid; Thales heeft het onderdeel *Defence & Security* (55%) waar cyberveiligheid onder valt; Trend Micro is nagenoeg volledig gericht op cyberveiligheid.

Literatuur

Bijlsma, M., B.M. Overvest en S.M. Straathof, 2016, Marktordening bij nieuwe ICT-toepassingen, CPB Policy Brief.

Elk, R.A. van, A.M. Braam, B.M. Overvest en S.M. Straathof, 2017, Integraal onderzoeksbeleid: doelen en instrumenten, CPB Policy Brief.

ENISA, 2017, Threat landscape report 2016.

Ministerie van Defensie, 2016, Strategische kennis- en innovatieagenda 2016-2020.

Ministerie van Veiligheid en Justitie, 2013, Nationale cybersecurity strategie 2.

Ministerie van Veiligheid en Justitie, 2017, Strategische kennis- en innovatieagenda.

Munnichs, G., M. Kouw. en L. Kool, 2017, A never-ending race; On cyberthreats and strengthening resilience. Den Haag, Rathenau Instituut.

Rademaker, M., L. Faesen, K. van Lieshout en M. Abdalla, 2016, Dutch investments in ICT and cybersecurity. Putting it in perspective, The Hague Centre for Strategic Studies.

Straathof, S.M. en S. van Veldhuizen, 2015, Financiering van start-ups en venture capital, CPB Notitie.

United Kingdom Cabinet Office, 2017, National cyber security strategy 2016 to 2021.

Verdonk Klooster & Associates en SEO Economisch Onderzoek, 2016, Economische kansen Nederlandse cybersecurity-sector.

Vollrath, T.L., 1991, A theoretical evaluation of alternative trade intensity measures of revealed comparative advantage, *Weltwirtschaftliches Archiv*, vol. 127(2): 265-280.

Dit is een uitgave van:

Centraal Planbureau
Postbus 80510 | 2508 GM Den Haag
T (088) 984 60 00

Januari 2018