seo economisch onderzoek
amsterdam economics

VERDONCK KLOOSTER & ASSOCIATES

ECONOMISCHE KANSEN NEDERLANDSE CYBERSECURITY-SECTOR

Een verkenning

ECONOMISCHE KANSEN NEDERLANDSE CYBERSECURITY-SECTOR

Een verkenning

André Hendriks, Dick Brandt, Kim Turk (VKA) &
Viktoria Kocsis, Daan in 't Veld, Tom Smits (SEO Economisch Onderzoek)

DATUM	17 Mei 2016
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20152778

MANAGEMENTSAMENVATTING

Nederland heeft de ambitie om voorop te lopen in de ontwikkeling naar een steeds meer digitaliserende economie. Op veel ranglijsten staat Nederland al hoog, als het gaat om de mate van digitalisering van de economie. Echter, een grote mate van digitalisering creëert op hetzelfde moment een grote afhankelijkheid van goed werkende en veilige technologie.

Voor het vasthouden en mogelijk versterken van de digitale economie is vertrouwen -in die digitale economie- een belangrijke randvoorwaarde, waarbij het vertrouwen onder druk staat van een toenemend aantal cyberincidenten. De cybersecurity-sector levert een belangrijke bijdrage aan het borgen van het vertrouwen. Alhoewel ook door andere sectoren dan de ICT-sector, een bijdrage aan cybersecurity wordt geleverd, ligt in deze studie de focus op cybersecurity-diensten en producten binnen de ICT- sector.

Middels een enquête, die is uitgevoerd onder ongeveer 4000 ICT-bedrijven, is de omvang van de Nederlandse cybersecurity-sector binnen de ICT-sector bepaald. 270 bedrijven hebben uiteindelijk deelgenomen aan het onderzoek. Uit de enquête blijkt dat in 2014 ongeveer 10 procent van de omzet binnen de ICT-sector gekoppeld was aan cybersecurity-activiteiten.

In 2014 lag de omzet van de cybersecurity-sector (binnen de IVT-sector) tussen de € 6,9 en € 7,5 miljard. De toegevoegde waarde van de cybersecurity-sector was in datzelfde jaar € 3,8 á 4,1 miljard. In 2010 hebben bedrijven die cyberactiviteiten uitvoeren met ongeveer 0,4 procent bijgedragen aan het Nederlandse BBP. In 2014 is dit percentage gestegen tot ongeveer 0,6 procent. De cybersecurity-sector groeide daarmee veel sneller dan de ICT-sector zelf. In de periode 2010-2014 is de omzet en de toegevoegde waarde van cybersecurity binnen de ICT-sector jaarlijks met 14,5 procent toegenomen. De benaderde ICT-bedrijven in de enquête verwachten een jaarlijkse groei van omzet uit cybersecurity-activiteiten van ongeveer 7 procent.

In dit onderzoek is gekozen voor een enge afbakening van het begrip cybersecurity. Deze afbakening is gekozen om het onderzoek binnen de gestelde kaders haalbaar te maken. Daarnaast zien we dat wanneer in het dagelijks spraakgebruik de term cybersecurity wordt gebruikt, men ook een wat smallere interpretatie kiest.

Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT als gevolg van moedwillige activiteiten in het Cyberdomein en, indien er toch schade is ontstaan, het herstellen hiervan.

De cybersecuritysector creëert toegevoegde waarde door het aanbieden van producten en diensten die de cyberrisico's proberen te verminderen en schade efficiënt te herstellen. De rest van de economie betaalt voor deze producten en diensten en profiteert ervan.

Een precieze meting van de waarde van cybersecurity (de uitstralingseffecten van de cybersecurity-sector) voor de economie als geheel blijkt lastig. Deze studie schetst een aantal methoden voor het meten van deze waarde en kiest voor een schatting van de waarde door te kijken naar incidenten en de omvang van de schade. Echter, er geldt een aantal beperkingen bij het analyseren van incidenten en schade. Een daarvan is het ontbreken van een eenduidige definitie van cybersecurity-incidenten. Daarnaast zijn meetmethoden vaak niet transparant en is de data onvolledig en onvergelijkbaar. Vanwege deze beperkingen bleek het niet mogelijk om harde conclusies te trekken over de waarde van cybersecurity.

Enkele cijfers zijn wel beschikbaar. In 2014 en 2015 kwam ongeveer een kwart van het Nederlandse bedrijfsleven in aanraking met cyberincidenten, vooral met phishing, virussen en hacken. In Nederland raakt cybercrime de sectoren handel, financiële instellingen en de ICT-sector het meest. Betrouwbare informatie bleek beschikbaar voor de financiële sector, en dan vooral rondom online bank- en pasfraude. De schade daar wordtin 2014 geraamd op ruim 2 duizend euro per 1000 inwoners, en is de afgelopen jaren dalend. De Nederlandse overheid is vooral slachtoffer van informatielekkage. Consumenten komen vooral in aanraking met virussen, misbruik van persoonlijke gegevens, financiële verliezen en ongepaste websites voor kinderen.

In Nederland is de afgelopen jaren het aandeel virussen flink gedaald en ligt het percentage onder het Europese gemiddelde. De bovenstaande cijfers suggereren dat er een positieve ontwikkeling plaatsvindt wat enkele typen cyberincidenten en -schade betreft. Of er een correlatie is tussen deze ontwikkelingen en de groei van de sector is niet te concluderen op basis van de beschikbare informatie.

We concluderen dat de Nederlandse cybersecurity-sector een behoorlijke omvang heeft en bovendien snel groeiend is. Alleen het deel binnen de ICT-sector is reeds 0,6% van het BBP. Deze uitkomst is daarom een conservatieve schatting van de cybersecurity-sector. Immers, mogelijke activiteiten die onderdeel zijn van cybersecurity, maar buiten de ICT-sector vallen, zijn hierin nog niet meegenomen.

Met behulp van de input van een 30-tal deskundigen (middels interviews en ronde tafels) uit de sector, is een analyse gemaakt van de sterkten, zwakten, kansen en bedreigingen van de Nederlandse cybersecurity-sector.

Analyse Nederlandse cybersecurity-sector

Sterkten	*Zwakten*
• Verregaande digitalisering geeft relatief sterke/volwassen (systeem van bedrijven) in cybersecurity-sector • Goede reputatie • Politiek, neutrale wet- en regelgeving, toezicht • Goede samenwerking binnen ISAC's en met NCSC	• Onvoldoende specialisten/beschikbaarheid goed gekwalificeerde mensen • Investeringen en toegang tot (durf) kapitaal • Uitwisseling en samenwerking wetenschap, bedrijfsleven en overheid • Beperkt georganiseerde sector

• Goed informaticaonderzoek • Ligging, cultuur en ondernemersklimaat	• Nederland vooral diensten en groothandel, minder schaalbaar

Kansen	***Bedreigingen***
• Doorontwikkeling van de Nederlandse cybersecurity aanpak • Wetgeving • Betere uitwisseling bedrijfsleven-wetenschap • Groei awareness • Ontwikkeling domeinen	• Beschikbaarheid goed gekwalificeerde mensen • De thuismarkt is klein • Wetgeving • Kosten van beveiliging worden te hoog waardoor deze niet meer opwegen tegen de voordelen van gebruik digitale middelen. Met name voor MKB • Daling awareness • Kennis bij afnemers • Concurrentie van buitenlandse partijen en/of overnames

Doordat het niet mogelijk is om harde conclusies te trekken over de huidige waarde van cybersecurity, is het ook niet goed mogelijk om aan te geven welk potentieel gerealiseerd kan worden. Echter, er is een aantal knelpunten gesignaleerd. Uit de SWOT-analyse blijkt dat er sprake kan zijn van marktfalen: er gaat, ondanks de groei van de sector, iets mis in de markt, met name door asymmetrische informatie, kennis-spillovers en netwerkeffecten, marktmacht en het hold-up probleem) en andere knelpunten (bijvoorbeeld gedragsproblemen).

Bij de gesignaleerde knelpunten zijn in het onderzoek suggesties naar voren gebracht voor de aanpak van die knelpunten. De suggesties zijn onderverdeeld in een aantal thema's:

In het thema *Experts en expertise*, is een aantal suggesties opgenomen die inzetten op het gesignaleerde tekort aan hoog opgeleide experts, en op welke wijze onderzoek beter benut kan worden. De cybersecurity-sector is sterk gedreven door innovatie, waarbij onderzoek en kennisuitwisseling met de wetenschap nodig is om nieuwe producten en diensten te bieden die passen bij de steeds ontwikkelende cyberdreigingen.
Bij het thema *Geef goede voorbeeld*, is een aantal suggesties opgenomen die vooral betrekking hebben op de overheid zelf. In het cluster *Connect, Commit & Go for it!* hebben we een aantal suggesties opgenomen die vooral betrekking hebben op het in verbinding brengen van initiatieven, hier vervolgens focus op leggen en de noodzakelijke acties uitvoeren, indien nodig voorzien van financiering. Het cluster *Wet & Regelgeving* bevat suggesties waarbij vanuit wet- en regelgeving aan de cybersecurity-sector kan worden bijgedragen.

INHOUDSOPGAVE

1 INLEIDING

Het kabinet streeft ernaar om het structurele groeivermogen van Nederland te vergroten. Het proces van vernieuwing en innovatie levert hier een belangrijke bijdrage aan: oude technologieën, kennis, concepten en verdienmodellen maken plaats voor productievere, nieuwe vondsten. Aldus Minister Kamp in een brief uit 2015 naar de Tweede Kamer (EZ, 2015). En in 2013 schreef dezelfde minister: Informatie- en communicatietechnologie (ICT) is reeds enige tijd een drijvende kracht achter innovatie, productiviteitsstijgingen en daarmee ook de groei van onze economie als geheel. ICT initieert dwars door sectoren heen nieuwe mogelijkheden en is een belangrijke facilitator voor het oplossen van economische en maatschappelijke uitdagingen, bijvoorbeeld op het gebied van kwalitatief beter onderwijs, efficiëntere logistiek en duurzaam energiegebruik. ICT is daarmee onderdeel van het rijtje revolutionaire doorbraaktechnologieën als de stoommachine, de brandstofmotor en elektriciteit. Het is een motor voor innovatie, groei en banen in alle (top)sectoren van onze economie (EZ, 2013).

Onderzoek wijst uit dat ICT de afgelopen decennia in Nederland heeft gezorgd voor veel economische groei. Circa 36% van de economische groei van de afgelopen decennia zou door ICT veroorzaakt zijn (Brennenraedts et al., 2014).

Nederland heeft de ambitie om voorop te lopen in de ontwikkeling naar een steeds meer digitaliserende economie. Op veel ranglijsten staat Nederland al hoog, als het gaat om de mate van digitalisering van de economie. Echter, een grote mate van digitalisering creëert op hetzelfde moment een grote afhankelijkheid van goed werkende en veilige technologie.

Voor het vasthouden en mogelijk versterken van de digitale economie is vertrouwen een belangrijke randvoorwaarde. De cybersecurity-sector heeft een spilfunctie bij het borgen van dat vertrouwen. Vanuit inhoudelijke argumenten wordt deze spilfunctie door de overheid herkend. Er is zelfs een Nationale Cybersecurity Strategie 2 waarin is beschreven dat Nederland voorop wil lopen op het gebied van security-by-design en privacy-by-design (V&J, 2013).

Nationale Cybersecurity Strategie 2: Nederland is leidend op het terrein van cybersecurity:

1. De Nederlandse samenleving weet op een veilige manier optimaal gebruik te maken van de voordelen van digitalisering.
2. Het Nederlandse bedrijfsleven en de wetenschap lopen voorop op het gebied van security- en privacy-by-design.
3. Samen met zijn internationale partners vormt Nederland een vooruitstrevende coalitie voor het beschermen van fundamentele rechten en waarden in het digitale domein.

Het belang van ICT voor economische groei en innovatie staat vast, maar over het economisch belang van de Nederlandse cybersecurity-sector is een stuk minder bekend. EZ, CBS en TNO publiceren jaarlijks het rapport *ICT, kennis en economie* waarin de meest actuele gegevens over de

Nederlandse kenniseconomie zijn opgenomen. Het economische belang van de ICT-sector is een thema in dat rapport, waardoor we vooraf wisten dat in 2013 de ICT-uitgaven in Nederland bijna 45 miljard euro bedroegen (EZ et al. 2015).

In opdracht van The Hague Security Delta (HSD) is onderzoek gedaan naar de Nederlandse veiligheidssector. Hierdoor weten we dat het veiligheidscluster in Nederland goed is voor 61.500 werkzame personen en een omzet van 6 miljard euro. In het rapport wordt onderscheid gemaakt tussen de traditionele beveiligingssector (bijvoorbeeld persoons- en gebouwbeveiliging) en de niet-traditionele veiligheidssector (terrorisme, cyber, natuurrampen enz.).

Duidelijk is dat een aanzienlijk deel van de cybersecurity-sector zich binnen de ICT-sector bevindt. Maar hoe groot is nu die Nederlandse cybersecurity-sector? Voor het antwoord op deze vraag zijn nog weinig objectieve gegevens beschikbaar. Het CPB schrijft in 2015 dat ondanks het economische belang van cybersecurity, er weinig “harde” gegevens beschikbaar zijn (CPB, 2015, e-crime, 2015). Verschillende bronnen maken melding van de wereldwijde omvang van de cybersecurity-sector, maar in veel gevallen kunnen vraagtekens geplaatst worden bij de onafhankelijkheid en betrouwbaarheid van deze bronnen. Vaak gaat het dan om rapporten van bedrijven die ook oplossingen verkopen (bijvoorbeeld: Kaspersky Lab (2014) en Intel Security (2014)). Dit rapport schetst het resultaat van het eerste onafhankelijk onderzoek naar de omvang van de Nederlandse cybersecurity-sector.

Naast een kwantitatief beeld van de Nederlandse cybersecurity-sector geeft dit rapport inzicht in de sterke en zwakke kanten van de sector. De twee beelden samen vormen een goede basis voor analyse, en geven de situatie van vandaag weer.

Bij het ministerie van Economische Zaken bestaat echter ook de vraag in hoeverre een hoger niveau van cybersecurity in Nederland ook economische activiteiten aantrekt en de kansen voor het bedrijfsleven en werkgelegenheid biedt. Om meer zicht te krijgen op hoe groot deze economische potentie in Nederland is en hoe deze kan worden gestimuleerd, is het noodzakelijk begrip te krijgen van de ontwikkelingen (trends) en de kansen of bedreigingen die deze ontwikkelingen vormen. Aan het eind van dit rapport geven we een aantal suggesties aan de Nederlandse overheid, over de wijze waarop zij kan inspelen op bestaande sterkten, zwakten, kansen en bedreigingen.

1.1 Definitie Cybersecurity

Voor een definitie van cybersecurity wordt in Nederland vaak gebruik gemaakt van de definitie zoals deze in Nationale Cybersecurity Strategie is opgenomen: *Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan* (V&J, 2013).

Voor dit onderzoek bakenen wij dit nader af tot: *Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT als gevolg van moedwillige activiteiten in het cyberdomein en, indien er toch schade is ontstaan, het herstellen hiervan.*

Deze afbakening is gekozen om het onderzoek haalbaar te maken binnen de gegeven randvoorwaarden en om beter aan te sluiten bij het gebruik van het begrip cybersecurity in het dagelijks spraakgebruik. We hebben cybersecurity versmald tot activiteiten in het **cyberdomein**. Concreet denken we bij het cyberdomein aan de wereld van met elkaar verbonden IT-infrastructuren, waaronder het internet, telefonie-netwerken, IT-netwerken en SCADA-systemen.

Ten tweede wordt het element '**moedwillig'** toegevoegd aan de afbakening. Daarmee sluiten we schade door uitval als gevolg van bijvoorbeeld slijtage, onvolkomenheden in soft- of hardware, onoordeelkundig gebruik of natuurrampen uit. Dat neemt overigens niet weg dat maatregelen die de schade door verstoring, uitval of misbruik van ICT voorkomen of beperken, niet alleen worden genomen vanwege mogelijke moedwillige activiteiten in het cyberdomein, maar ook in het licht van continuïteitsbeheer.

Cybersecurity is dus nadrukkelijk meer dan alleen het voorkomen van binnendringen door hackers of virussen. De cybersecurity-sector is dan de verzameling van bedrijven die zich geheel of gedeeltelijk bezighouden met het leveren van cybersecurity-diensten en/of -producten.

Het hanteren van de afbakening in dit onderzoek, doet niets af aan de waarde van de bredere definitie. Immers organisaties zullen moeten nadenken over de bescherming tegen alle vormen van schade, ongeacht de oorsprong van die schade.

CYBERSECURITY EN ICT

Zoals de definitie suggereert, betreffen cybersecurity-activiteiten preventiemaatregelen, de opsporing van incidenten en het herstel daarvan. Omdat volgens de definitie van cybersecurity, het object ICT betreft, zien we dat vooral de ICT-sector zelf een groot aandeel heeft in het totaal van de activiteiten (zie Afbeelding 1). Denk aan het leveren van ICT-diensten en -producten, zoals virusscanners, VPN of ethical hacking.

Cybersecurity-activiteiten reiken echter verder dan alleen de ICT-sector. Ook vanuit andere sectoren wordt door het aanbieden van diensten en producten een bijdrage aan cybersecurity geleverd. Denk hierbij aan juridisch advies, sporenonderzoek, verzekeringen, certificaten en de communicatie rondom cyberincidenten. Het is dus niet alleen de ICT-sector die streeft naar het voorkomen van schade. Ook andere sectoren zijn betrokken bij het verminderen van cyberrisico's.

Afbeelding 1 Cybersecurity-activiteiten zijn breder dan alleen ICT-producten en -diensten.

Noot: de omvang van de blokken is illustratief, en vormen op geen enkele wijze een representatieve afspiegeling van de werkelijke omvang van sectoren.

1.2 Verantwoording en bronnen

Het onderzoek is uitgevoerd in opdracht van het ministerie van Economische Zaken, directie Energie, Telecom en Mededinging. Het onderzoek vond plaats in de periode november 2015-maart 2016 en is uitgevoerd door Verdonck, Klooster & Associates (VKA), in samenwerking met SEO Economisch Onderzoek. Deze laatste organisatie heeft binnen het onderzoek de economische analyses (omvang en uitstraling) voor haar rekening genomen. Voor de uitvoering van het onderzoek was een begeleidingscommissie ingesteld met deelnemers vanuit de ministeries van Buitenlandse Zaken, Economische Zaken, Veiligheid & Justitie en Binnenlandse Zaken en het CPB.

In het onderzoek is gebruik gemaakt van verschillende bronnen en instrumenten. Zo is gebruik gemaakt van een enquête onder 4.000 ICT-bedrijven en zijn interviews en ronde tafels gehouden met in totaal zo'n 30 deskundigen uit het Cybersecurity-domein. Daarnaast is deskresearch uitgevoerd en zijn diverse statistische bronnen geraadpleegd, waaronder CBS-microstatistieken.

Voor een volledig overzicht van de gebruikte bronnen verwijzen wij naar bijlage A. Voor een overzicht van de geïnterviewden en deelnemers aan de ronde tafels verwijzen we naar bijlage B.

1.3 Leeswijzer

In dit rapport wordt in hoofdstuk 2 eerst een schets gemaakt van de Nederlandse cybersecurity-sector. Het hoofdstuk sluit af met het eerste deel van de kwalitatieve analyse: de sterkten en zwakten van de sector. In hoofdstuk 3 presenteren we het eerste deel van de kwantitatieve analyse, waarin de omvang van de Nederlandse cybersecurity-sector aan bod komt. In hoofdstuk 4 is het tweede deel van de kwantitatieve analyse opgenomen. Dit deel gaat over de waarde van de cybersecurity-sector. Dit hoofdstuk eindigen we met een deel over het vestigingsklimaat. De kansen en bedreigingen, het tweede deel van de kwalitatieve analyse, is opgenomen in hoofdstuk 5. Het rapport sluit af met in hoofdstuk 6 de conclusies en suggesties.

2 DE NEDERLANDSE CYBERSECURITY-SECTOR

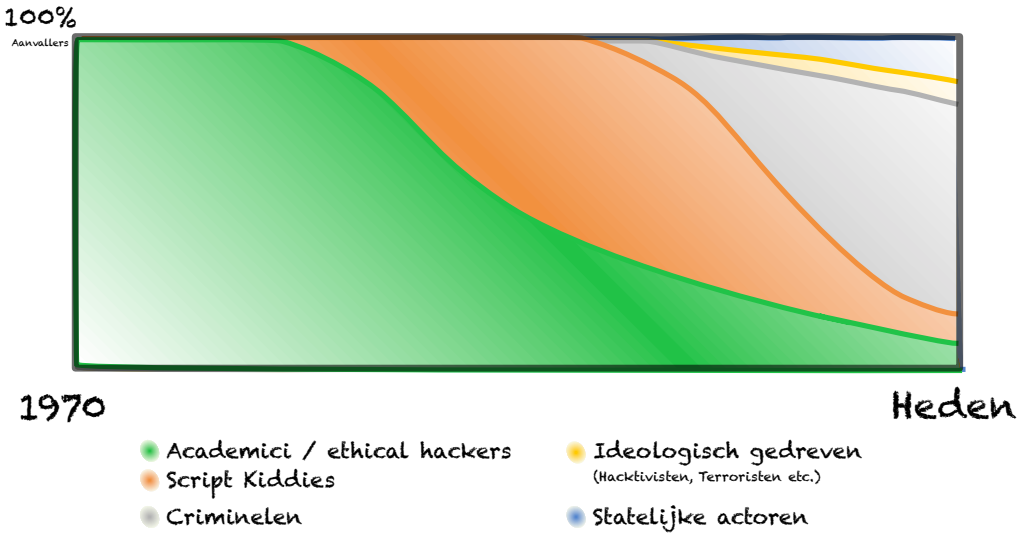
In dit hoofdstuk beschrijven we kort het ontstaan van de cybersecurity-sector, geven we een indeling van de verschillende cybersecurity-producten en diensten en beschrijven wij de sterke en zwakke punten van de Nederlandse cybersecurity-sector. We geven een aantwoord op de onderzoeksvraag: *Wat is de huidige uitgangspositie van Nederland voor het realiseren van economische kansen op cybersecurity-gebied?* In het volgende hoofdstuk beschrijven wij het economische omvang van de sector.

2.1 Ontstaan

Cyberdreigingen zijn er al sinds het eerste virus, begin jaren 70, op het ARPA-net werd 'vrijgelaten' en de boodschap "I'm the creeper, catch me if you can!" verspreidde. In die tijd was het allemaal nog vrij onschuldig, maar de laatste decennia is de impact ervan sterk toegenomen. In het begin was verspreiding alleen mogelijk via geheugendragers zoals floppydisks en duurde het maanden voordat verspreiding op enige schaal had plaatsgevonden. Met de opkomst van het internet zijn inmiddels nagenoeg alle computers met elkaar verbonden en kan wereldwijde verspreiding plaatsvinden binnen enkele seconden.

In onderstaande grafiek hebben we de ontwikkeling van het aandeel van de verschillende groepen aanvallers over de afgelopen 45 jaar afgebeeld als percentage van het totaalaantal aanvallers. Daarbij moet opgemerkt worden dat het aantal aanvallen over die periode van enkele stuks per jaar naar duizenden per seconde is gegroeid. Waarbij er elke seconde wereldwijd tientallen personen slachtoffer worden. Dit laatste is niet te zien in de grafiek.

Afbeelding 2 Ontwikkeling aandeel groepen aanvallers (Bron: VKA-analyse)



Met de opkomst van het internet ontstonden nieuwe dreigingen die de markt voor firewalls en andere netwerkbescherming liet ontstaan. Organisaties werden kwetsbaar voor inbrekers op hun netwerk. Hierbij ging het voornamelijk om partijen die door gebruik te maken van fouten in de configuratie van de apparatuur, nodig voor de verbinding met andere netwerken, toegang kregen tot bedrijfsgegevens. In het begin was dit vooral een intellectuele uitdaging voor academici, later bleek het ook interessant voor adolescenten die op websites hun eigen 'graffiti' achter lieten om indruk te maken op hun vrienden: de script-kiddies. Inmiddels hebben criminelen dit grotendeels overgenomen en gaat het om lucratieve activiteiten.

De dreigingsmatrix zoals ontwikkelde door het Nationaal Cyber Security Centrum (NCSC) maakt een combinatie tussen de bron van de dreiging, de doelwitten en de belangrijkste bedreigingen. Ook uit deze matrix blijkt dat het zwaartepunt van de oorsprong van dreigingen intussen ligt bij criminele organisaties en statelijke actoren.

Tabel 1 Cybersecurity-beeld Nederland 2015 (bron: NCSC, 2015)

Tabel 1 **Dreigingsmatrix**

	Doelwitten		
Bron van Dreiging	**Overheden**	**Private organisaties**	**Burgers**
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie ↘	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie
	Verstoring van ICT	Verstoring van ICT	Verstoring van ICT
	Overname van ICT	Overname van ICT ↘	Overname van ICT
Staten	Digitale spionage	Economische spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten ↗	
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal van informatie	Diefstal van informatie	Diefstal van informatie ↗
	Verstoring van ICT	Verstoring van ICT	
Hacktivisten	Diefstal en publicatie van verkregen informatie	Diefstal en publicatie van verkregen informatie	↘
	Defacement	Defacement	
	Verstoring van ICT	Verstoring van ICT	
	Overname van ICT	Overname van ICT ↘	
Interne actoren	Diefstal en publicatie of verkoop van verkregen informatie	Diefstal en publicatie of verkoop van verkregen informatie	
	Verstoring van ICT	Verstoring van ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal van informatie (bedrijfs-spionage)	Commercieel gebruik, misbruik of 'doorverkopen' van gegevens
Geen actor	Uitval van ICT	Uitval van ICT	Uitval van ICT

De groei van de cybersecurity-sector is mede te verklaren door te kijken naar de wetten van Moore (verdubbeling aantal transistors op chip elke 18 maanden), Gilder (totale bandbreedte van communicatie verdrievoudigt elke 12 maanden) en Metcalfe (de waarde van een netwerk is gelijkwaardig met het kwadraat van het aantal aansluitingen), die allen aangeven dat de belangrijke factoren die bepalen wat ICT kan, snel groeien met een constante snelheid (Kocovic, 2008). Als we Metcalfe's wet volgen is die groei meer dan lineair met het netwerk (Strategic Studies Institute, 2011).

Door het steeds krachtiger (en goedkoper) worden van chips krijgen wij steeds meer opslag- en verwerkingscapaciteit tot onze beschikking, waardoor steeds meer data verzameld en gebruikt kan worden. De big-dataontwikkeling geeft vele nieuwe kansen en mogelijkheden en ook hier spelen criminelen op in. Aan de ene kant is er meer informatie te halen waar (veel) geld mee verdiend kan worden en aan de andere kant maken criminelen slim gebruik van big-data om hun slachtoffers uit te zoeken en te belagen. Doordat de netwerkcapaciteit nog steeds groeit wordt het ook steeds makkelijker om snel, veel slachtoffers te bereiken.

De waarde en omvang van de ICT-infrastructuur neemt toe en daarmee ook onze kwetsbaarheid voor verstoring ervan. Bovendien, ook voor criminelen en andere actoren neemt de waarde en aantrekkelijkheid toe met de omvang van het netwerk en zij zullen dus meer middelen inzetten in een poging zich te verrijken.

Met het toenemen van enerzijds dreigingen en anderzijds het belang van ICT is er ook een economische sector ontstaan die gebruikers met cybersecurity-producten en -diensten bescherming biedt tegen de aanvallers. Dit blijkt een continue strijd tussen leveranciers en aanvallers te zijn, waarbij de aanvallers zeer innovatief zijn en steeds weer nieuwe zwakke plekken in de cyber-defensie weten te vinden. In deze strijd speelt schaalgrootte een belangrijke rol. Aanbieders waren lang kleine innovatieve start-ups die met originele oplossingen kwamen om het hoofd te bieden aan de dreigingen. Inmiddels zien we duidelijk schaalvergroting, waarbij de oplossingen van een aantal jaren geleden nu gemeengoed zijn geworden en consolidatie van aanbieders plaatsvindt.

Big data is ook voor de verdediging een duidelijke rol gaan spelen en daarmee hebben grotere partijen een voordeel. Partijen met meer data, zijn beter in staat om trends ten behoeve van beveiliging te ontdekken. Wij zien een duidelijke consolidatie van de ‘intelligence’ bij partijen die informatie verzamelen over aanvallers en over hoe ze de aanvallen uitvoeren. Overigens is het nog steeds een jonge industrie waarin ook nieuwe partijen ontstaan die specialistische en creatieve oplossingen hebben voor nieuwe dreigingen. Deze kleine partijen zorgen voor de noodzakelijke snelheid in de wedloop en zodra ze een bewezen werkende oplossing hebben die van enige importantie is worden ze in veel gevallen overgenomen door een grotere speler.

2.2 Recente en verwachte ontwikkelingen

De afgelopen jaren zien we bij onze klanten een trend van een groeiend aantal incidenten in het cyberdomein. Wij verwachten dat deze trend zich de komende jaren verder zal doorzetten, al was het alleen maar omdat de digitalisering nog verder zal toenemen. Met het Internet-of-Things (IoT) zal het aantal op internet aangesloten systemen de komende jaren sterk groeien. Het beeld is dat velen van die "nieuwe" systemen initieel onvoldoende beschermd zijn, resulterend in een toename van het aantal incidenten. Daarnaast zal deze toenemende digitalisering, en een groeiende afhankelijkheid van onze digitale hulpmiddelen, er voor zorgen dat het voor criminelen ook aantrekkelijker wordt om te proberen misbruik hiervan te maken. Om hier het hoofd aan te bieden zal ook het aanbod van beveiligingsdiensten en -producten groeien.
Voor het bedrijfsleven geldt daarbij dat de wet- en regelgeving rond cybersecurity (bijvoorbeeld de EU General Data Protection Regulation) zich verder ontwikkelt waardoor ook de niet ICT aspecten van cybersecurity meer aandacht zullen krijgen. Onze verwachting is dan ook dat dat gedeelte van de sector de komende jaren snel zal gaan groeien.

2.3 Indeling cybersecurity-sector

Er zijn veel manieren om de cybersecurity-sector in te delen. Wij hebben in dit onderzoek gekozen voor de indeling zoals die in de tweede National Research Agenda for Cyber Security (NCSRA II) is opgenomen (NCSRA, 2013). We veronderstellen een sterke koppeling tussen de research van vandaag en het ontstaan van nieuwe bedrijven en toepassingen morgen. Gebieden die nu nog vooral in de research-fase zitten, bieden kansen voor nieuwe toepassingen en bedrijven.

De NCSRA-II is een deelinvulling van de Nationale Cyber Security Strategie van de Nederlandse overheid. De agenda is opgesteld door ICT Innovatie Platform ‘Veilig Verbonden’ (IIP-VV). Dit platform bestaat uit onderzoekers vanuit industrie en kennisinstellingen, gebruikers en vertegenwoordigers van de overheid.

Voor de toepassing in ons onderzoek en de enquête onder ICT-bedrijven (zie hoofdstuk 3) hebben we de NCSRA II agenda aangevuld met Nederlandse omschrijvingen en zijn per categorie een aantal concrete voorbeelden van cybersecurity-producten en -diensten opgenomen.

Tabel 2 NCSRA indeling en vertaling naar cybersecurity-producten en -diensten (bron; NCSRA 2)

NCSRA-indeling	Omschrijving	Voorbeelden
Identity, privacy and trust management	Producten en diensten rondom veilige digitale toegang (verlening) tot en uitwisseling van informatie	Certificaten (incl. leveranciers, CA, etc.) Advies (incl. privacy & legal) Elektronische identiteiten Biometrie Secure communication (bv. VPN, Encryptie van communicatie)
Malware and malicious infrastructures	Verzamelen en verspreiden van informatie over dreigingen en kwetsbaarheden, en de organisaties daarachter.	Intelligence Honeypots Media (vakbladen, nieuwsbrieven, etc.) Secure Intelligent Sharing (platformen)
Attack detection, attack prevention and monitoring	Producten en diensten rondom preventie, detecteren en monitoren van digitale aanvallen.	Detectie- / Monitoringdiensten / SIEM Detectieproducten (virusscanners / IDS) Preventiediensten (PEN-Testen / ethical hacking) Preventieproducten (IPS / Firewalls)
Forensics and incident management	Producten en diensten rondom het vaststellen van sporen van aanvallen en/of fraude. Inclusief (crisis)beheersing en herstel na afloop.	Sporenonderzoek & analyse Fraudeonderzoek Opsporing CERT / Incident & Response Management Recovery
Data, Policy & Access Management	Producten en diensten rondom opslag en gebruik van data (inclusief regels/beleid), zo dat kan worden voldaan aan toepasselijke wet- en regelgeving en risicobeleid (compliance) en de beheersing daarvan.	Cybersecurity binnen hostingdiensten (cloud) Governance, Risk & Compliance diensten Secure Document Management Data-encryptie Juridisch advies rondom data-opslag Authenticatie/ autorisatie-producten (DC-kant) 'Outsourced' Security Management (SOC/ Updates & Patching /Professional Services) Awareness / Opleiden, trainen & oefenen
Risk Management, Economics & Regulation	Producten en diensten rondom gebruik van ICT-voorzieningen (inclusief regels/beleid), zo dat kan worden voldaan aan toepasselijke wet- en regelgeving en risicobeleid. Inclusief afhandeling excepties en bedrijfseconomische aspecten (aansprakelijkheid, risico vs. schade).	Certificeringen (ISO, Common Criteria, Privacy) Cyberverzekeringen Legal (aansprakelijkheid, corporate liability) Risk Management & Compliance BCM-/ en weerbaarheidsadvies Mobile Device Management
Secure Design and Engineering	Producten en diensten rondom het veilig (laten) ontwerpen en bouwen van ICT-voorzieningen (hard- en software).	Cryptografie Secure Software ontwerp en bouw Secure Hardware ontwerp en bouw Secure Operating Systems Beveiliging rondom SCADA/ PCS Internet of Things Security
Offensive Cyber capabilities	Producten en diensten rondom het pen-testen en aanvallen van ICT-voorzieningen (hard- en software)	Producten/diensten tbv Defensie-/Politie-/ Inlichtingen- en veiligheidsdiensten Spyshops

2.4 Sterkten en zwakten volgens deskundigen

In deze paragraaf beschrijven we de sterke en zwakke punten van de Nederlandse cybersecurity-sector. De analyse is gebaseerd op ons inzicht in de markt en een 30-tal deskundigen (middels interviews en ronde tafels) uit de sector. Zie bijlage B voor een overzicht van geïnterviewden en deelnemers aan de ronde tafels.
Het resultaat hiervan was een lange lijst met sterke en zwakke punten. Bij de analyse van de punten hebben we tevens onderzocht of op andere plaatsen aanknopingspunten te vinden zijn voor een bepaald falen. In welke mate de punten ook een aantoonbaar sterk of zwak punt zijn, en leiden tot een competitief na- of voordeel is niet onderzocht, noch is onderzocht wat de oorsprong is van deze punten.

De sterkten en zwakten zijn in onderstaande tabel opgenomen en worden vervolgens kort beschreven. De kansen en bedreigen, welke de SWOT-analyse[1] completeren, zijn opgenomen in paragraaf 5.1.

Tabel 3 Sterkten en Zwakten Nederlandse cybersecurity-sector volgens deskundigen uit de sector

Analyse Nederlandse cybersecurity-sector	
Sterkten	***Zwakten***
• Verregaande digitalisering geeft relatief sterke/volwassen (ecosysteem van bedrijven) in Cybersecurity-sector • Goede reputatie • Politiek, neutrale wet- en regelgeving, toezicht • Goede samenwerking binnen ISAC's en met NCSC • Goed informaticaonderzoek • Ligging, cultuur en ondernemersklimaat	• Onvoldoende specialisten/beschikbaarheid goed gekwalificeerde mensen • Investeringen en toegang tot (durf) kapitaal • Uitwisseling en samenwerking wetenschap, bedrijfsleven en overheid • Beperkt georganiseerde sector • Nederland vooral diensten en groothandel, minder schaalbaar

In onderstaande tekst lichten we de verschillende sterkten en zwakten kort toe.

2.5 Sterkten

VERREGAANDE DIGITALISERING

Nederland loopt voorop op het gebied van digitalisering. In Nederland is de internetpenetratie en kwaliteit van toegang (hoge snelheid van internetverbindingen) zeer goed. Volgens onderzoek van de Autoriteit Consument & Markt (ACM) heeft inmiddels twee derde van de Nederlandse huishoudens een snelheid van 30 Mbit/s of meer (ACM, 2016). Ook het internetgebruik onder de Nederlandse bevolking is zeer hoog; 93,2% van de bevolking maakt gebruik van internet. Daarmee zit Nederland volgens de Wereldbank in de top 3 van Europa. Alleen Noorwegen en Denemarken scoren iets hoger, respectievelijk 96,3% en 96%. (Wereldbank, 2016).

[1] SWOT-analyse, staat voor een analyse van Strengths, Weaknesses, Opportunities en Threats. In dit onderzoek: Sterkten, Zwakten, Kansen en Bedreigingen.

Volgens brancheorganisatie NederlandICT maken Nederlandse consumenten en bedrijven met zo'n 6,7 miljoen vaste breedbandaansluitingen en meer dan 10 miljoen mobiele breedbandaansluitingen veel gebruik van telecommunicatie. Zij stelt dat met één van de beste telecominfrastructuren ter wereld, twee belangrijke internetknooppunten en talloze datacenters en hostingbedrijven Nederland zich met recht de digitale poort naar Europa mag noemen (NederlandICT, 2016).

De verregaande digitalisering heeft overigens ook een keerzijde. De hoge dichtheid en kwaliteit van internetverbinding heeft ervoor gezorgd dat Nederland een belangrijk doelwit is geworden voor de beheerders van botnets. Een botnet, is een aantal op internet aangesloten computers, die zonder dat de eigenaar dat weet, voorzien zijn van kwaadaardige software. Zij worden vaak gebruikt om spam e-mail te versturen of deel te nemen aan een gedistribueerde denial -of- service (DDoS) aanval. Vanaf Nederlandse computers kunnen snel grootschalige DDoS-aanvallen worden opgezet. Nederland staat volgens een onderzoek van het Centraal Planbureau (CPB) op de derde plaats op de lijst met landen waar de meeste aanvallen vandaan komen (CPB, 2015). Het CPB beschrijft dat uit analyses blijkt dat DDoS aanvallen relatief vaak gelanceerd worden vanuit landen met veel internetters. Snel internet maakt een land aantrekkelijk voor hackers om een aanval vanuit te plegen, maar snel internet heeft geen significant effect op het aantal aanvallen dat een land te verduren heeft. De aanwezigheid van veel goed verbonden computers is een randvoorwaarde voor een werkend botnet.

Met de open houding van de Nederlandse bevolking ten opzichte van digitale ontwikkelingen loopt Nederland vaak voorop ten opzichte van andere landen. Voorbeelden hiervan zijn internetbankieren en digitaal zakendoen met de overheid. Mede hierdoor zullen ook dreigingen in het cyberdomein zich snel in Nederland manifesteren. Door de overheid en banken is de afgelopen jaren veel geïnvesteerd in het bewustzijn van de mogelijke dreigingen. Nederland wordt door sommige leveranciers ook gezien als een proeftuin voor Europa. Als een product of dienstverlening hier slaagt dan heeft dit ook een kans van slagen in de rest van Europa. Een voorbeeld hiervan is de samenwerking tussen Nederland en Canada waarbij Invest Ottawa, The Hague Security Delta, InnovationQuarter, De Kamer van Koophandel in Den Haag, de Nederlandse Ambassade in Ottawa en de Canadese Ambassade in Nederland het initiatief gelanceerd hebben voor een 'Canada-Netherlands Cyber & Security Technologies Soft Landing Platform' waarbij Canadese cybersecurity bedrijven Nederland gebruiken voor de start van hun oversteek naar Europa. In een interview met een leverancier van cybersecurity-producten en -diensten werd aangegeven dat dit element ervoor gezorgd heeft dat zij in geen ander Europees land zo succesvol hadden kunnen groeien als in Nederland.

GOEDE REPUTATIE

Alhoewel we dit aspect niet verder onderzocht hebben werd in een aantal interviews aangegeven dat de Nederlandse Cybersecurity-sector een relatief goede reputatie heeft in het buitenland. Wij zien dat bedrijven als Fox-IT en Compumatica intussen een behoorlijk deel van hun omzet uit het buitenland halen.

POLITIEK, NEUTRALE WET EN REGELGEVING, TOEZICHT

De Nederlandse overheid hecht waarde aan een veilig internet en zet cybersecurity hoog op de agenda. Zo wordt, op het moment van schrijven van dit rapport, door het kabinet gewerkt aan de doorontwikkeling van de Nederlandse cybersecurity aanpak. Maar ook middels wetgeving werkt de overheid aan een veiliger internet, en bescherming van privacy. De meldplicht datalekken is daar een voorbeeld van, maar vooral het kabinetsstandpunt rondom encryptie. In dit laatste kabinetsstandpunt is opgenomen dat het niet nodig is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. Dit betekent dat de opname van een zogenaamde *backdoor,* niet wettelijk vereist wordt. Dit beleid zal ook internationaal worden uitgedragen (V&J, 2016).

De Nederlandse overheid in het algemeen en het NCSC in het bijzonder, stimuleert organisaties om een beleid van responsible disclosure te voeren. Hierin staan randvoorwaarden en afspraken beschreven voor goedwillende hackers en beveiligingsonderzoeker om kwetsbaarheden in informatiesystemen te melden aan organisaties.
Nederland loopt voorop ten opzichte van andere landen met deze open houding ten opzichte van goedwillende (ethical) hackers. Deze vooruitstrevende houding is ook bekend in het buitenland. Door deze houding van de overheid zijn ook andere sectoren, zoals financiële instellingen, bereid om gebruik te maken van goedwillende hackers om hun eigen informatiebeveiliging verder te verbeteren. Tot slot, kan als voorbeeld genoemd worden dat Nederland in 2015 de Internationale Global Cyber Space Conference georganiseerd heeft.

GOEDE SAMENWERKING BINNEN ISAC'S EN MET NCSC

Het NCSC deelt kennis en informatie over kwetsbaarheden met de overheid en vitale sectoren. Voorbeelden van vitale sectoren zijn: elektriciteit, gas, kernenergie, drinkwater, telecom, transport (mainports Rotterdam en Schiphol), financiën en overheid. Voor de aanpak van cyberdreigingen en kwetsbaarheden zijn diverse Information Sharing and Analysis Centres (ISAC's) opgericht. ISAC's zijn publiek-private samenwerkingsverbanden en zijn per sector georganiseerd. Hier wisselen de deelnemers onderling informatie en ervaringen uit over cybersecurity. Ook worden analyses gedeeld over de *situational awareness* in de desbetreffende sectoren. Dit gebeurt met name op tactisch niveau. Het NCSC verzorgt voor deze ISAC's het secretariaat en neemt zelf ook deel als kennispartner. De voorzittersrol wordt altijd door een private deelnemer ingevuld.

De kruisbestuiving tussen de publieke en private sector levert waarde voor alle deelnemers. Een belangrijke meerwaarde voor alle deelnemers is het opbouwen van een permanent netwerk (NCSC, 2016).

GOED INFORMATICAONDERZOEK

De visitatiecommissie Informatica is zeer lovend over het informaticaonderzoek in Nederland. Ze noemt het onderzoek "van hoge kwaliteit, breed en met een hoge impact in internationaal perspectief". Voor de evaluatie werden de informatica-afdelingen van negen Nederlandse

universiteiten en drie Nederlandse onderzoeksscholen beoordeeld op onderzoekskwaliteit, levensvatbaarheid en maatschappelijke relevantie. De onafhankelijke visitatiecommissie voor Nederlands informaticaonderzoek 2009-2014 bestond uit vooraanstaande onderzoekers uit Nederland, Duitsland, Engeland en de Verenigde Staten. Ook een recente Canadese studie van de top-20 landen in ICT, plaatst Nederland in de kopgroep. Alleen de Verenigde Staten en Zwitserland scoren hoger (NWO, 2016).

LIGGING, CULTUUR EN ONDERNEMERSKLIMAAT

In veel gesprekken wordt het Nederlandse ondernemersklimaat, de cultuur en de ligging genoemd als een van de sterkten. Veel aspecten van het ondernemersklimaat hebben betrekking op het vestigingsklimaat en gelden breder dan alleen voor de cybersecurity-sector.

Aspecten van het vestigingsklimaat die specifiek genoemd zijn, zijn zaken als het fiscale klimaat, een goed opgeleide beroepsbevolking en een stabiel politiek klimaat. Ten aanzien van het ondernemersklimaat, werd aangegeven dat het voor startups relatief eenvoudig is om toegang tot bestaande netwerken te krijgen. Organisaties als The Hague Security Delta (HSD), Innovation Quarter en RVO zijn behulpzaam en helpen bedrijven bij vestiging en profilering, bijvoorbeeld in handelsmissies. De The Hague Security Delta, in het bijzonder biedt startups en buitenlandse bedrijven in het cybersecurity-domein, een landingsplek waarbij nauw samen wordt gewerkt met bedrijfsleven, overheid en kennisinstituten. In paragraaf 4.4 gaan we nog wat dieper in op het vestigingsklimaat.

In het Startup Nation Scoreboard van het European Digital Forum (EDF) uit 2016 wordt geconcludeerd dat van alle landen in de EU Nederland zijn beleid de afgelopen jaren het best in dienst heeft gesteld van startups. Volgens het rapport blinkt Nederland uit in het verbinden van grote bedrijven met kleinere starters. Het rapport is gebaseerd op het aantal aanbevelingen dat EU-landen hebben overgenomen uit het Europese ‘Startup Manifesto’ van 2013. Nederland scoort een gemiddelde van 85%, gevolgd door Italië (82%) en het Verenigde Koninkrijk (77%) (EDF, 2016).

Ook wordt ook de gunstige ligging van Nederland ten opzichte van andere landen genoemd als sterkte. Grote Europese steden zoals Londen, Parijs en Berlijn zijn goed en snel te bereiken. In een straal van 500 kilometer zijn 170 miljoen consumenten te bereiken (NFIA, 2013). Daarnaast is de DACH-regio (Duitsland, Oostenrijk en Zwitserland) van belang als min of meer samenhangende markt. Ook deze zijn goed en snel bereikbaar.

Tolerantie en vrijheid zitten diepgeworteld in de Nederlandse cultuur. Die wortels toegevoegd aan handelsgeest geven de ruimte aan innovatieve, ondernemende mensen om nieuwe producten of diensten te ontwikkelen. In de cybersecurity-sector komen we veel "karakters" tegen, die zich beter thuis voelen bij tolerantie dan bij gesloten, intolerante samenleving.

2.6 Zwakten

In een analyse van het NFIA uit 2013 werden reeds een aantal zwakten van de Nederlandse ICT-sector gemeld, die ook in 2016 nog voor de cybersecurity-sector gelden. Het betreft onder andere het tekort aan geschoold personeel, het gebrek aan groeikapitaal, en problemen met het aantrekken en behouden van talent. Daarnaast meldt NFIA dat in verhouding tot de landen om ons heen Nederlandse ICT-bedrijven relatief weinig spenderen aan onderzoek en ontwikkeling. Daarnaast zijn de afgelopen twee decennia een fiks aantal private onderzoekslaboratoria uit Nederland verdwenen. (NFIA, 2013).

ONVOLDOENDE SPECIALISTEN/BESCHIKBAARHEID GOED GEKWALIFICEERDE MENSEN

In de praktijk blijkt dat er een krapte is op de arbeidsmarkt voor *information security professionals*. Studenten die in dit vak afstuderen hebben vaak al ver voor hun afstuderen een baan en docenten op het HBO zijn moeilijk te krijgen. Uiteindelijk worden vacatures wel ingevuld, maar neemt de werkgever er genoegen mee dat een kandidaat (nog) niet volledig gekwalificeerd is en nog verder training on-the-job nodig heeft. Te verwachten is dat deze vraag in de toekomst nog verder zal toenemen. Het beschikbaar hebben van voldoende gekwalificeerd personeel wordt ook als een van de belangrijke factoren voor vestiging genoemd. Overigens is er op dit moment ook nog geen zicht op grotere aantallen opgeleiden die de komende jaren door Universiteiten en Hogescholen afgeleverd worden.

In Nederland geldt dat het UWV in 2015 signaleerde dat voor informaticaberoepen de arbeidsmarkt zeer krap is: *In de ICT zijn vooral vacatures op hoog en wetenschappelijk niveau moeilijk in te vullen. Daarbij gaat het vooral om developers/programmeurs in specifieke talen,* ***security-specialisten*** *of business analisten. Ook op de middellange termijn zal deze krapte in techniek en ICT blijven bestaan. Met een groeiende economie zal ook de vraag naar technici en ICT'ers immers verder aantrekken* (UWV, 2015). In een wereldwijd onderzoek van de Information Systems Audit and Control Association (ISACA), een onafhankelijk en non-profit opleidingsonderzoek, gaven 86% van de respondenten aan, dat er een ernstig tekort is aan goed opgeleid cybersecurity-personeel (ISACA, 2016). In een onderzoek van Frost & Sullivan wordt aangegeven dat 62% van de organisaties nu (eind 2014) een tekort heeft aan *security professionals.* (Frost & Sullivan, 2015).

De programma manager Cyber Security Research bij de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) signaleert bovendien dat het onderwijs onvoldoende aansluit op het bedrijfsleven: “We kijken met enige zorg naar de ontwikkelingen in het onderwijs. Wat de opleidingen opleveren sluit te vaak niet aan op de wensen vanuit het bedrijfsleven. Dat komt deels omdat er te weinig mensen afstuderen in ICT-vakken, zeker op het gebied van cyber security, en dat komt deels doordat de door het bedrijfsleven gewenste kennis niet gedoceerd wordt.”

Het verbeteren van die aansluiting moet volgens de programmamanager mede gebeuren door de oprichting van een nieuw *research and (higher) education platform* waar de agendering van onderzoek en onderwijs bottom up wordt gerealiseerd. “Door op een centrale plek onderzoeks- en

onderwijsinitiatieven met elkaar te verbinden, kunnen we voorkomen dat dingen nodeloos dubbel gedaan worden, bijvoorbeeld binnen verschillende Topsectoren of routes van de Nationale Wetenschaps Agenda (Dutch Digital Delta 2016). Dat platform is er intussen. Op 5 april is dcypher, het Dutch Cybersecurity Platform for Higher Education and Research, gelanceerd. De missie van dcypher is (bottom-up) agendering en coördinatie van zowel wetenschappelijk als praktijkgericht cybersecurity-onderzoek en – hoger onderwijs.

De oorzaak van dit tekort is mogelijk het gevolg van asymmetrische informatie maar mogelijk ook door elementen uit de gedragseconomie. Wanneer (aankomende) studenten niet goed op de hoogte zijn van de carrièrekansen in de sector, of een studie cybersecurity gewoonweg niet aantrekkelijk vinden, wordt de richting te weinig gekozen. Ook het aanbod zou zoals hierboven geschetst een oorzaak van het probleem kunnen zijn.

Dat dit tekort op korte en middellange termijn verder toeneemt, is opgenomen als bedreiging voor de sector in paragraaf 5.4.

INVESTERINGEN EN TOEGANG TOT (DURF) KAPITAAL

In een aantal gesprekken werd aangegeven dat het voor ondernemers in de cybersecurity-sector lastig is om aan durfkapitaal te komen. Dit beeld wordt onder meer bevestigd in de analyse van de NFIA voor de ICT-sector "Nederland kent een groot aantal technologie startups. Nederland genereert ongeveer 10% van de snelst groeiende technologie startups in Europa. Slechts een klein aantal ICT-start-ups groeit door naar Europees of wereldniveau. De oorzaken hiervoor zijn gebrek aan groeikapitaal, en problemen met het aantrekken en behouden van talent"(NFIA, 2013). In Nederland blijken die financieringsproblemen groter te zijn dan in andere Noordwest-Europese landen. Een belangrijke verklaring hiervoor is dat er in Nederland te weinig durfkapitaal (*venture capital*) beschikbaar is voor het financieren van de opstartfase. In die fase loopt publieke financiering doorgaans af, maar zijn bankkredieten nog niet te verkrijgen omdat de risico's hiervoor nog te groot zijn. Vooral het zogeheten late-fase durfkapitaal – dat starters het laatste zetje moet geven om in de uitrolfase terecht te komen – is problematisch. De financieringsketen werkt dus niet goed in Nederland; er vallen gaten. Het gevolg is dat de kans op marktintroductie en uitrol vaker dan elders onbenut blijft. De Nederlandse economie profiteert daardoor minder dan mogelijk is van de kansen die innovatie biedt (Vooren, A. et al., 2015).

Ook zien we dat succesvolle startups in de cybersecurity-sector, snel door grotere buitenlandse aanbieders en investeerders worden opgepikt. In paragraaf 5.4 geven we een aantal voorbeelden.

Overigens speelt geld in de onderzoek- en ontwikkelfase ook al een rol. Nederland geeft minder uit aan R&D dan veel van de ons omringende landen (FD, 2015 en NFIA, 2013). Met de goedkeuring van het nieuwe WBSO, zijn volgens verschillende partijen ook de mogelijkheden voor subsidie in het ICT-domein ingeperkt. Nederland ICT liet weten dat de nieuwe regeling een kaalslag betekent voor innovatieve softwareontwikkeling. Nederland wordt volgens de sector minder aantrekkelijk als vestigingsland (ICT Magazine, 2015).

Marktfalen was voor de Europese Commissie een belangrijke reden voor de invoering in 2006 van de Communautaire kaderregeling inzake staatssteun voor onderzoek, ontwikkeling en innovatie. Krachtens het Verdrag betreffende de werking van de Europese Unie is het bevorderen van onderzoek, ontwikkeling en innovatie (O&O&I) een belangrijke doelstelling van gemeenschappelijk belang (SER, 2010).

Van Dijk et al beschrijven het fenomeen als volgt: Verschillende instanties (inclusief OECD, DNB, SER, AWTI) en vanuit diverse economische onderzoeken geven hetzelfde beeld: de financiering van innovaties in het MKB vertoont knelpunten. De factoren die hiertoe leiden variëren en bestaan uit:
- risico-restricties bij banken en institutionele investeerders,
- intransparantie van de private financieringsmarkt,
- een kleinschalige venture capital-markt in Nederland,
- een grote mate van onzekerheid,
- beperkt zicht op cash-flow,
- relatief hoge transactiekosten voor vaak kleinere investeringsaanvragen,
- onduidelijke exit-mogelijkheden,
- etc.

Per saldo krijgen MKB-bedrijven onvoldoende kapitaal beschikbaar voor de nodige investeringen in innovaties. Als achterliggende redenen voor dit marktfalen, en een daaruit volgende legitimatie van een rol voor de overheid, is op basis van de deskresearch en de interviews het knelpunt ‘informatieasymmetrie’ centraal komen te staan als verklaring voor het onvoldoende beschikbaar zijn van kapitaal (Van Dijk et al., 2015).

UITWISSELING EN SAMENWERKING WETENSCHAP, BEDRIJFSLEVEN EN OVERHEID

Op verschillende momenten werd in het onderzoek aangegeven dat de aansluiting tussen wetenschap en bedrijfsleven in het cybersecurity-domein nog te zwak is en beter kan. Het domein is sterk gedreven door innovatie en hiervoor is kennis uit de universiteiten nodig. Wetenschappelijk onderzoek eindigt vaak slechts in publicaties en wordt in Nederland onvoldoende in de praktijk benut. Eerder deden 11 grote Nederlandse ondernemingen al een oproep om een uitdagende gezamenlijke agenda op te stellen waarin het wetenschaps- en innovatiebeleid aan elkaar gekoppeld worden. De aanbeveling was toen om gezamenlijk een onderzoeksagenda te ontwikkelen waarin maatschappelijke uitdagingen, topsectorenbeleid en wetenschapsagenda bij elkaar komen. 'Zo een agenda inspireert, versterkt de topsectorenaanpak en verbindt de industrie, wetenschap en overheid nog nauwer met elkaar', aldus de 11 grote Nederlandse ondernemingen (VNO NCW, 2014).

Maar ook de uitwisseling, over en weer, van kennis tussen bedrijfsleven en overheid in het cybersecurity-domein vindt in Nederland nog te weinig plaats. In de VS zien we dat er veel meer werknemers overstappen van overheid (bijvoorbeeld vanuit defensie) naar bedrijfsleven en vice

versa. En ook in Israël zien we dat het leger ook een bron is van specifieke technologieën die de basis kunnen vormen voor innovatieve startups. Mede door deze 'kennis-spillovers' uit het leger zijn Israëlische startups toonaangevend op het gebied van bijvoorbeeld drones en cyber security (FD, 2016).

Goede vormen van bestaande samenwerking in dit domein zijn er ook. Wij denken hierbij aan de samenwerking tussen NCSC en de ISAC's (zie paragraaf 2.5) en de Cyber Security Raad (CSR). De CSR is een onafhankelijk adviesorgaan. De Raad is samengesteld uit vertegenwoordigers van publieke en private partijen en vertegenwoordigers uit de wetenschap. Deze samenwerkingsverbanden zijn echter minder gericht op innovatie en valorisatie.

BEPERKT GEORGANISEERDE SECTOR

De cybersecurity-sector is nog jong en nauwelijks georganiseerd en bestaat vooral uit wat kleinere organisaties en uit activiteiten die een deel uit maken van ene grotere onderneming. Een typische organisatievorm als een brancheverenigingontbreekt nog. Door deze lage organisatiegraad heeft de sector nog geen aanspreekpunt of stem in een debat.

NEDERLAND VOORAL DIENSTEN EN GROOTHANDEL, MINDER SCHAALBAAR

Uit een studie van Dialogic naar de import en export van ICT blijkt dat vrijwel alle IT-hardware in Nederland wordt geïmporteerd. Daarnaast blijkt uit dezelfde studie dat software sterker plaatsgebonden is dan IT-hardware en dat het aandeel van de gehele softwaresector in de export bescheiden is. Tot slot bleek dat vooral de groothandel een belangrijk onderdeel uitmaakt van de export (Brennenraedts et al., 2014). Kortom, binnen de ICT-sector in Nederland gaat het vooral om diensten en ook bij de export van ICT gaat het vooral om groothandel. Het beeld is dat dit ook voor de cybersecurity-sector geldt. Gevolg van deze samenstelling is wel dat de (internationale) schaalbaarheid van ICT- en cybersecurity-bedrijven beperkt is. Immers, hardware kan bij succes snel op grote schaal geproduceerd worden, terwijl dat voor diensten lastiger is.

Partijen uit landen met een grotere maakindustrie zullen in delen van de cybersecurity-sector een voordeel hebben. Het gaat dan vooral om de hardware die worden toegepast. Fabrikanten van hardware zijn bij succes in staat de productie snel op te schalen en te profiteren van schaalvoordelen. Fabrikanten uit landen met een grote(re) maakindustrie hebben voordelen (kennis, ervaring, infrastructuur) die kunnen resulteren in marktmacht (schaalgrootte).

3 DE ECONOMISCHE OMVANG VAN DE NEDERLANDSE CYBERSECURITY-SECTOR

In dit hoofdstuk wordt een antwoord geformuleerd op de volgende onderzoeksvraag: *Wat is het verdienpotentieel van cybersecurity voor Nederland en het bedrijfsleven?*

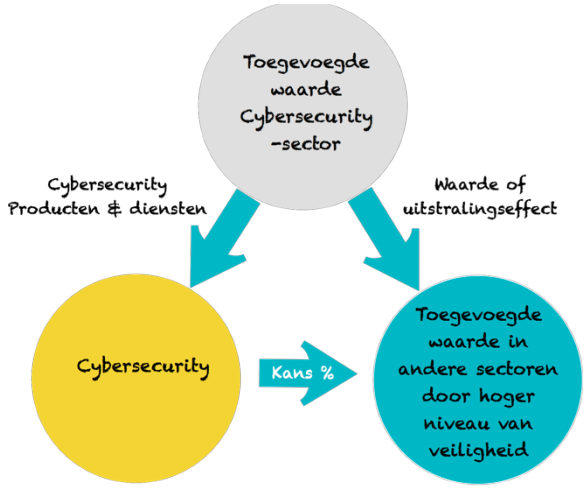
Dit hoofdstuk begint met een denkkader dat de omvang van de cybersecurity-sector koppelt aan de waarde die de sector creëert. De door de cybersecurity-sector gecreëerde waarde wordt beschreven in hoofdstuk 4. In sectie 3.2 wordt de ICT-sector gedefinieerd. Daarnaast is het aandeel binnen de ICT-sector gemeten door een enquête. In secties 3.3 en 3.4 presenteren we de huidige omvang van de cybersecurity-sector. In paragraaf 3.5 kijken we naar de potentiële omvang. Voor een uitgebreide beschrijving van de data en voor de vragenlijst verwijzen wij naar de verantwoording in de bijlage C.

3.1 Denkkader: omvang van en waarde door de cybersecurity-sector

Wat cybersecurity betreft kunnen we de economie in twee delen opsplitsen: de sector die bezig is met het verhogen van cybersecurity door het leveren van producten en diensten aan gebruikers, ook genoemd de cybersecurity-sector, en de rest van de economie (dus inclusief de afnemers van de cyberproducten en -diensten).

De cybersecurity-sector creëert toegevoegde waarde door het aanbieden van producten en diensten die de cyberrisico's proberen te verminderen.[2] De rest van de economie betaalt voor deze producten en diensten en profiteert ervan.

Afbeelding 3 Economische betekenis van cybersecurity voor de economie



[2] De berekening van het cyberrisico valt buiten de scope van dit onderzoek.

De rest van de economie kan te maken hebben met cyberincidenten (verstoring, uitval of misbruik van ICT) en kan profiteren van veiligere ICT-producten. Door een hoger niveau van cybersecurity kunnen bedrijven productiever worden, omdat bijvoorbeeld een ICT-systeem van een bedrijf minder vaak uitvalt. Daarnaast kan cybersecurity, zoals bijvoorbeeld digitalisering dat ook kan, een technologische vooruitgang bewerkstelligen. Bijvoorbeeld, door de ontwikkeling van een digitale handtekening kunnen nu ook digitaal veilige rechtsgeldige handelingen worden verricht. Hierdoor wordt productie in de rest van de economie efficiënter. Om beide redenen groeit de economie en neemt welvaart toe.

Waarde kunnen we omvatten door de begrippen van omzet, kosten en toegevoegde waarde. De omzet is de inkomsten (of baten) van bedrijven die ze realiseren door het leveren van producten en diensten. Deze baten zijn gerealiseerd tegen de gemaakte kosten. Het verschil tussen omzet en kosten is de winst (of verlies). De toegevoegde waarde is het verschil tussen de omzet en het aankoopbedrag (de waarde van ingekochte producten). Op macro-economisch niveau wordt de toegevoegde waarde gemeten via het bruto binnenlandse product (BBP). Afhankelijk van het type markt waar cybersecurity- producten en - diensten zijn aangeboden bestaan er verschillende relaties tussen de omzet, de kosten en de toegevoegde waarde van cybersecurity-bedrijven en de afnemers.

Stel dat een bedrijf één miljoen euro aan baten kan realiseren door een investering in een hoger niveau van cybersecurity. Baten duiden hier op een mogelijk financieel voordeel, bijvoorbeeld in de vorm van lagere kosten - minder netwerkuitvallen, gecrashte computers enzovoort. In dit geval is het bedrijf bereid om maximaal één miljoen euro te betalen voor cybersecurity. Als de leverancier van de cybersecuritydiensten en –producten de betalingsbereidheid van dit bedrijf kent – dit wordt verondersteld in een markt met eerste graad prijsdiscriminatie – dan zal de leverancier exact 1 miljoen euro vragen als vergoeding voor zijn diensten. De winst of toegevoegde waarde van de transactie slaat in dit geval volledig neer bij de leverancier.

Er zijn echter factoren waardoor de prijs die een cyberbedrijf vraagt niet overeenkomt met de betalingsbereidheid van afnemers. Producten en diensten worden niet per se efficiënt aangeboden en leiden niet per se tot hogere cybersecurity (of een lager cyberrisico). Marktmarkt en informatieproblemen kunnen ervoor zorgen dat vraag en aanbod in een markt niet perfect op elkaar aansluiten. De cybersecuritymarkt kan geconcentreerd zijn, bijvoorbeeld vanwege schaaleffecten, waardoor slechts een klein aantal grote spelers de markt domineert. Dit werkt prijsopdrijving in de hand waardoor sommige bedrijven niet investeren in cybersecurity, terwijl ze dat bij een lagere prijs wel zouden doen. De prijsopdrijving veroorzaakt daardoor een welvaartsverlies.

Afnemers zijn niet altijd in staat om op een mogelijk cyberincident (volledig) te anticiperen (cybercriminelen zijn een stap vooruit). Als gevolg kunnen cyberincidenten niet volledig voorkomen worden en zal schade het gevolg zijn. Bedrijven houden met deze mogelijke schade, rekening bij het bepalen van hun betalingsbereidheid in betere cybersecurity. Aan deze maximale

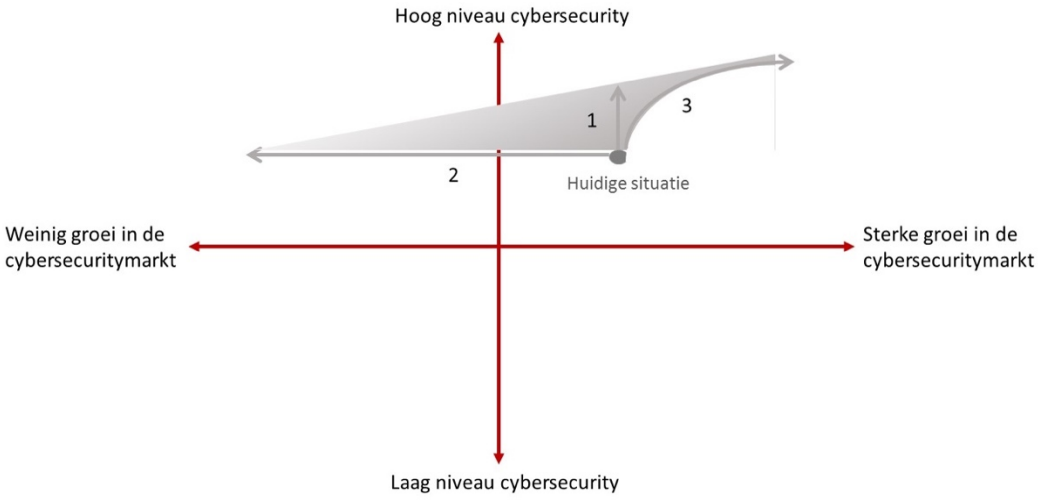
waarde zitten echter beperkingen. De potentiele schade kan bijvoorbeeld inhouden dat het bedrijf failliet gaat. De betalingsbereid wordt dus mede beperkt door de liquiditeit en solvabiliteit van de investerende partij en niet alleen door het risico op onveilige cybersituaties.

In zulke gevallen is de omzet en de toegevoegde waarde in de cybersecuritysector lager dan het potentieel en trekken de afnemers een deel van de toegevoegde waarde naar zich toe. Deze waarde kunnen afnemers investeren om hun eigen efficiëntie en productiviteit te verhogen. Daarnaast realiseren afnemers een lager dan gewenst niveau cybersecurity.

Stel dat de economie zich in een situatie vindt waar verbeteringen - in de maatschappelijke zin - mogelijk zijn. Deze verbeteringsmogelijkheden betekenen een hoger niveau van efficiëntie. Afbeelding 4 illustreert drie mogelijke veranderingen ten opzichte van de huidige situatie.

Ten eerste is het mogelijk dat met inzet van dezelfde middelen (arbeid, kapitaal) in de cybersecurity-sector een hoger niveau cybersecurity (of een lager cyberrisico) tot stand komt. Dit wordt geïllustreerd door de pijl omhoog (nr. 1) in Afbeelding 4. Ten tweede, stel dat het niveau van cybersecurity constant blijft bij afnemende inzet van cybersecurity-diensten (i.e., in een kleinere cybersecurity-sector). Dit zou een toename van de efficiëntie impliceren. Deze besparing kan de rest van de economie besteden aan investeringen in andere producten of diensten (de pijl naar links, nr. 2). Ten derde, als de technologie verandert, kan de cybersecuritysector een hoger niveau van cybersecurity aanbieden door het gebruik van dezelfde input (pijl recht om hoog, nr. 3).

Afbeelding 4 Verbeteringsmogelijkheden liggen naar boven en naar links van de huidige situatie.



Het niveau van cybersecurity wordt, naast de activiteiten van de cybersecurity-sector en technologische ontwikkeling, ook bepaald door andere factoren. Voorbeelden zijn: gedragingen van ICT-gebruikers (*security awareness*) en gedragingen van cybercriminelen en statelijke actoren. Met andere woorden, meer uitgaven aan cybersecurity leiden niet altijd tot een lager cyberrisico, en *vice versa*. Uiteindelijk zijn de uitgaven aan cybersecurity minder van belang dan het niveau in cybersecurity dat wordt verwezenlijkt.

3.2 De ICT-sector

Omdat het is te verwachten dat de ICT-sector het grootste aandeel heeft in de cybersecurity-sector, ligt de focus van dit deel van de studie op de ICT-sector. De afbakening van de ICT-sector komt overeen met de afbakening van het ministerie van Economische Zaken (EZ), het Centraal Bureau voor Statistiek (CBS) en TNO (EZ et al. 2015; Tabel 4). De uitkomst is daarom een conservatieve schatting van de cybersecurity-sector: mogelijke activiteiten die relevant zijn voor cybersecurity, maar buiten de afbakening vallen, zijn niet meegenomen.

Tabel 4 De afbakening van ICT-activiteiten (EZ et al., 2015)

SBI-codes	Activiteiten
	Leveren van ICT-goederen
26.1 t/m 26.4, 26.8	Vervaardiging van elektronische componenten en printplaten / ICT-goederen
	Leveren van ICT-diensten
46.5	Groothandel in ICT-apparatuur
*58.2	Uitgeverijen van software
61	Telecommunicatie
62	Dienstverlenende activiteiten op het gebied van informatietechnologie
63.11	Gegevensverwerking, webhosting en aanverwante activiteiten
95.1	Reparatie van computers en communicatieapparatuur

* Onder 58.2 valt een klein aantal bedrijven. Daarom zijn bedrijven met deze SBI-code omwille van vertrouwelijkheid van de data buiten beschouwing gelaten in de berekening.

De omvang is geschetst aan de hand van een aantal economische basiskenmerken, zoals toegevoegde waarde, omzet, omzet uit export en werkgelegenheid. Daarnaast is gekeken naar de internationale positie van de Nederlandse ICT-sector op basis van de handelsbalans. Voor deze kenmerken worden CBS-statistieken gebruikt.

Vóór dit onderzoek was het onbekend hoe groot cybersecurity is binnen de ICT-sector. Het aandeel is geschat middels een webenquête. Er is gekozen voor een webenquête omdat de vraagstelling relatief eenvoudig is en door een enquête een grotere steekproef kan worden bereikt dan met interviews.

De analyse bestond uit twee stappen:

- Het bepalen van aandeel cybersecurity: het nemen van een steekproef; webenquête; en de analyse van de resultaten;
- Berekening van economische kenmerken op basis van CBS-microstatistieken.

De analyse houdt een momentopname van de omvang de cybersecurity-activiteiten in, welke voor het eerst op deze manier is gemaakt voor Nederland. Er zijn twee meetmomenten gekozen: 2010 en 2014. Daarnaast betreft de vraag ook het verdienpotentieel van bedrijven die cyberproducten en –diensten aanbieden. Dit potentieel is gemeten middels de verwachte toekomstige groei van de omzet door cyberactiviteiten binnen de ICT-activiteiten.

3.3 Aandeel cybersecurity

Om een inschatting te maken van het aandeel cybersecurity binnen de ICT-sector is een enquête gehouden onder ICT-bedrijven. De enquête werd aangekondigd per e-mail en daarnaast op de website van branchevereniging Nederland ICT. Alleen bedrijven die aangaven in de ICT-sector werkzaam te zijn werden tot de vragenlijst toegelaten. Tijdens de aankondiging en werving van respondenten werd niet gemeld dat het onderzoek betrekking had op cybersecurity – dit werd pas duidelijk na aanvang van de enquête.

De respondenten komen uit het bedrijvenpanel van Kompass met bedrijven met 5 fte of meer. Van de 3.868 bedrijven[3] die een uitnodiging ontvingen, vulden 266 de enquête volledig of bijna volledig in: een respons van 6,9 procent. Voor sommige specifieke vragen kan de respons lager zijn dan dit aantal van 266; zie Bijlage A.2 voor de volledige vragenlijst. Van de 266 ICT-bedrijven selecteerden 115 bedrijven (43 procent) één of meer cybersecurity-producten en/of -diensten uit de opgestelde lijst; de resterende 151 bedrijven (57 procent) geven aan geen specifieke cybersecurity-producten of -diensten aan te bieden.[4]

REPRESENTATIVITEIT

In onze enquête geeft 43 procent van de ondervraagde ICT-bedrijven aan in enige mate omzet uit cybersecurity te behalen. In hoeverre het antwoord van 43 procent gehanteerd kan worden voor de ICT-sector als geheel, hangt af van de representativiteit van de steekproef.

Aan het eind van 2015 waren ongeveer 66.600 ICT-bedrijven geregistreerd bij de KvK (zie CBS Statline, 2015Q4). De ICT-sector wordt gekenmerkt door een groot aantal zzp'ers (ca. 53.900, 81 procent van het totaalaantal bedrijven). Echter realiseren de 5.700 bedrijven, die 5 fte of meer hebben (8,5 procent van het totale aantal), ongeveer 80 procent van de totale omzet van de sector. Het belangrijkste doel van de enquête was een inschatting te maken van het aandeel in de omzet dat cybersecurity representeert. Daarom werd voor dit onderzoek gekozen om te focussen op bedrijven met 5 fte of meer. Het bedrijfspanel van Kompass dekt deze populatie.

De verdeling van het aantal werknemers voor bedrijven met 5 fte of meer verschilt in de steekproef sterk ten opzichte van de gehele populatie (zie Afbeelding 5). Het aantal bedrijven in de categorie 20 tot 50 fte en in de categorie 100 of meer fte zijn substantieel hoger binnen de

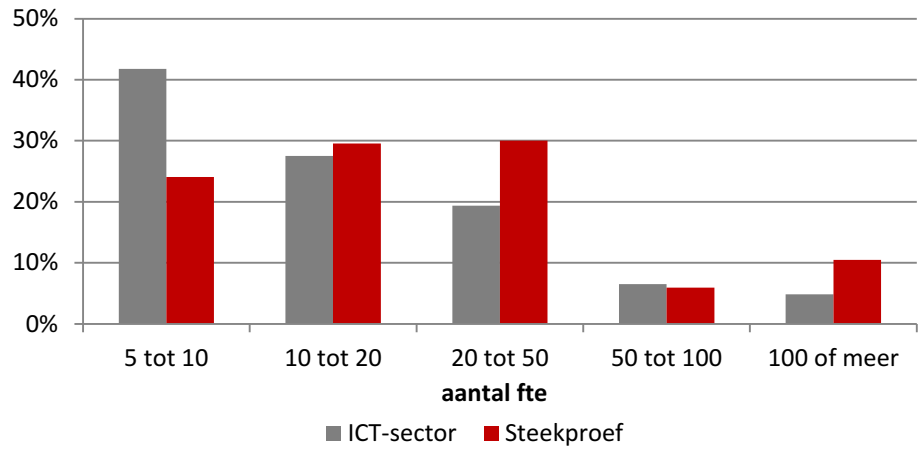
---

[3] Het Kompass-panel heeft ongeveer 6.000 ICT bedrijven waarvan voor 3.868 (67 procent) ook een emailadres bekend is.

[4] Naast de 266 bedrijven in de steekproef (waarvan 115 cybersecuritybedrijven en 151 niet-cybersecuritybedrijven) zijn er ook 24 bedrijven die weliswaar aangaven cybersecurityproducten en/of -diensten te leveren, maar geen enkele activiteit noemden. Aangezien de activiteit een verplichte vraag was, konden deze bedrijven ook latere vragen niet invullen. Deze bedrijven zijn niet meegenomen in de analyse.

steekproef dan bij de totale populatie. De categorie 5 tot 10 fte is in de steekproef juist ondervertegenwoordigd.[5]

Afbeelding 5 De steekproef omvat bedrijven met relatief veel werknemers.



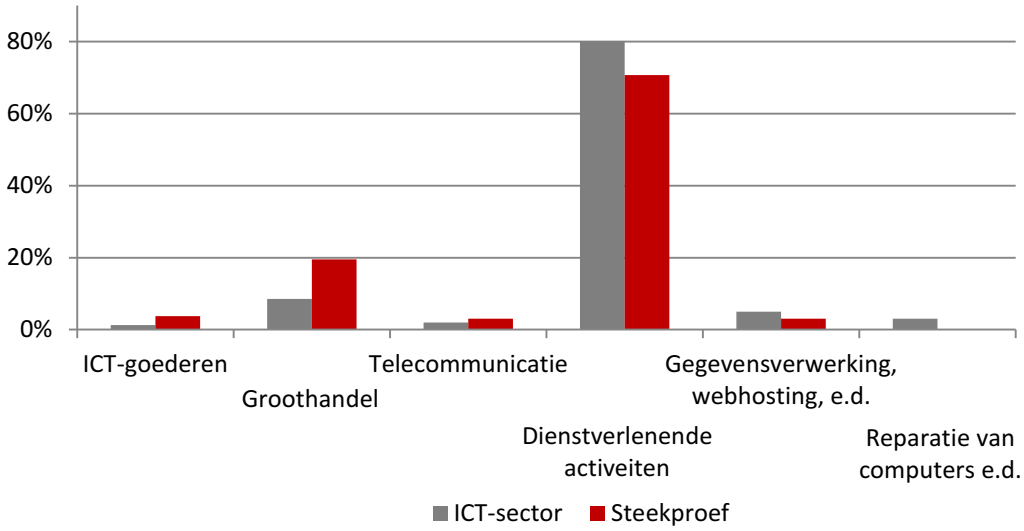
Bron: Steekproef: VKA/SEO Economisch Onderzoek, n=243. Gehele ICT-sector met 5 of meer fte: CBS (2015Q4). De grafiek toont aantallen bedrijven met 5 tot 10 fte e.d. als percentage van het totaal met 5 of meer fte.

Hoewel de steekproef iets verschilt van de ICT-sector als geheel wat betreft het aantal werknemers, geeft de enquête wel een goed beeld in termen van omzet. Met name dekken ICT-bedrijven met 5 fte of meer, ongeveer 80 procent van de omzet in de ICT-sector. Bovendien blijkt de mate waarin bedrijven omzet halen uit cybersecurity in onze steekproef niet samen te hangen met de bedrijfsomvang (in termen van omzet dan wel fte).

De representativiteit van de steekproef gaat bovendien verder dan de grootte van de ICT-bedrijven: een ander belangrijk kenmerk is het type activiteiten dat ICT-bedrijven verrichten. Zoals hierboven vermeld worden de activiteiten ingedeeld aan de hand van SBI-codes. Voor de SBI-code is een primaire bron bekend, aangezien deze informatie ook door Kompass geleverd kon worden. Afbeelding 6 geeft aan dat het overgrote merendeel van de ICT-bedrijven gecategoriseerd is met SBI-code 62 (‘Dienstverlenende activiteiten op het gebied van informatietechnologie’), volgens het CBS 80 procent. Dit geldt ook voor de steekproef, al is het aandeel van SBI-code 62 hier iets lager, te weten 71 procent.

[5] Vanwege de samenstelling van het bedrijvenpanel van Kompass bevat de steekproef in principe alleen bedrijven met 5 of meer fte. Er waren desalniettemin 23 (van de 266) bedrijven die aangaven 1, 2, of 3 fte in dienst te hebben.

Afbeelding 6 **De steekproef verschilt weinig van de gehele populatie wat betreft ICT-activiteiten.**



Bron: Steekproef: VKA/SEO Economisch Onderzoek, n=266, o.b.v. gegevens Kompass. ICT-sector: CBS (2015Q4).

Samenvattend kan worden gesteld dat de steekproef relatief iets meer grote bedrijven bevat, maar representatief is wat betreft de spreiding in ICT-activiteiten. Hierbij dient wel opgemerkt te worden dat – gegeven de respons van 266 – het aantal waarnemingen voor sommige ICT-activiteiten laag is (te weten ICT-goederen, telecommunicatie en gegevensverwerking, webhosting en aanverwante activiteiten). Binnen de deelsector van bedrijven die computers en communicatieapparatuur repareren waren in het geheel geen respondenten. Het is daarom niet mogelijk het aandeel cybersecurity in te schatten voor verschillende deelsectoren binnen de ICT-sector.

ENQUÊTE-UITKOMSTEN: HET AANDEEL CYBERSECURITY IN DE OMZET

De centrale vraag in de enquête luidde: *Ongeveer welk deel (in percentage) van de netto omzet van uw organisatie in 2014 heeft uw organisatie verkregen door cybersecurity-activiteiten?* Deze vraag werd voorgelegd aan respondenten die in de voorafgaande vraag van de enquête een of meer cybersecurity-activiteiten hadden aangekruist. Voor bedrijven aangeduid als niet-cybersecurity, is het aandeel per definitie gelijk aan nul.

Afgezien van het niveau van het aandeel cybersecurity, is het ook van belang in welke richting dit aandeel zich ontwikkelt, zowel in het verleden als naar de toekomst (naar verwachting van de respondenten). Om deze reden zijn twee aanvullende vragen gesteld. Voor het verleden werd gevraagd naar het aandeel van Cybersecurity in de totale omzet in 2010 (vraag 5 in Bijlage A.2), voor de toekomst is respondenten gevraagd een inschatting te maken van de jaarlijkse groeiverwachting de komende 3 tot 5 jaar (vraag 6 in Bijlage A.2).

Door deze wegingen zijn er twee waarden voor het aandeel cybersecurity binnen de ICT-sector berekend (Tabel 5). Volgens deze twee meetwaarden lag het aandeel cybersecurity lag in 2014 bij 9,5 en 10,3 procent binnen de omzet van de ICT-sector. Dit aandeel is jaarlijks 0,5%-punt gestegen tussen 2010 en 2014.
Tabel 5 geeft de resultaten weer voor het gerapporteerde aandeel cybersecurity in 2010 en 2014. Er zijn twee wegingen gebruikt: op basis van de hoofd-ICT-activiteit (SBI-code) en op basis van alle ICT-activiteiten, die bedrijven naast hun hoofdactiviteit hebben aangegeven. Een beperking van de SBI-codes is dat elk bedrijf slechts één hoofdactiviteit kan noemen bij de registratie bij de Kamer van Koophandel. In de praktijk ontwikkelen bedrijven meerdere activiteiten en zouden dus verspreid moeten zijn over meerdere SBI-codes. Om deze beperking op te vangen is in de enquête bedrijven zelf gevraagd welke ICT-activiteiten ze verrichten, waarbij meerdere mogelijkheden konden worden aangekruist.[6]

Door deze wegingen zijn er twee waarden voor het aandeel cybersecurity binnen de ICT-sector berekend (Tabel 5). Volgens deze twee meetwaarden lag het aandeel cybersecurity lag in 2014 bij 9,5 en 10,3 procent binnen de omzet van de ICT-sector. Dit aandeel is jaarlijks 0,5%-punt gestegen tussen 2010 en 2014.

Tabel 5 Het aandeel cybersecurity binnen de omzet van de ICT-sector is jaarlijks 0,5%-punt gestegen tussen 2010 en 2014.

	2010	2014
Gewogen o.b.v. hoofd-ICT-activiteit (SBI-codes)	7,5 %	9,5 %
Gewogen o.b.v. alle ICT-activiteiten (zelf-gerapporteerd)	8,4 %	10,3 %

Bron: VKA/SEO Economisch Onderzoek; n(SBI)=266 en n(alle)=246 (in 2014) en n(SBI)=248 en n(alle)=229 (in 2010).

Voor een juiste interpretatie van het resultaat is het van belang enkele onderliggende aannames te benoemen die zijn gemaakt in Tabel 5. Neem ter illustratie 9,5 procent o.b.v. hoofd-ICT-activiteit in 2014. Hoewel dit getal is berekend op de totale respons van 266 waarnemingen, zijn er slechts 49 bedrijven die daadwerkelijk een omzetpercentage cybersecurity in het eigen bedrijf hebben genoemd. Van de 115 cybersecurity-bedrijven hebben er 66 geen omzetpercentage ingevuld (keuze ‘onbekend’). Voor deze bedrijven wordt aangenomen dat het aandeel cybersecurity gelijk is aan het gemiddelde percentage voor bedrijven met eenzelfde SBI-code. Deze 115 bedrijven samen halen gemiddeld 22,2 procent van hun totale ICT-omzet uit cybersecurity. Om aan het totale aandeel van de gehele ICT-sector te komen, moet rekening gehouden met niet-cybersecurity-bedrijven (57 procent van de populatie). Dit levert 22,2 * 0,43 + 0 * 0,57 = 9,5 procent, zoals in Tabel 5.

[6] In de enquête hebben 20 bedrijven alleen de 'overige ICT-activiteiten' aangevinkt en activiteiten genoemd die niet op een duidelijke manier onder SBI-codes gecategoriseerd kunnen worden. Bij deze weging zijn deze 20 bedrijven buiten beschouwing gehouden.

In de tweede regel in Tabel 5 zijn de resultaten weergegeven wanneer wordt gewogen naar alle zelfgerapporteerde ICT-activiteiten. In tegenstelling tot de eerste indeling (alleen hoofdactiviteit gebruikt) kunnen dit dus meerdere activiteiten zijn. Een opgegeven omzetpercentage wordt gelijk verdeeld over de door hetzelfde bedrijf gerapporteerde ICT-activiteit; elke respondent houdt een totale weging gelijk aan 1 in de berekening. Het is een vereenvoudiging omdat de omzetcijfers per ICT-activiteit niet bekend zijn.

Voor de resultaten voor 2010 zijn minder waarnemingen gebruikt dan voor 2014, te weten 248 in plaats van 266. Dit komt doordat de vraag met betrekking tot 2010 niet van toepassing is voor bedrijven die in 2010 nog niet bestonden. Van de 115 cybersecurity-bedrijven in de steekproef waren er 18 die voor 2010 'niet van toepassing' hebben gekozen. We gaan daarom uit van een instroom van 16 procent cybersecurity-bedrijven in 2014 ten opzichte van 2010. Om een eerlijke vergelijking mogelijk te maken, wordt voor niet-cybersecurity eveneens een instroom van 16 procent aangenomen.[7]

Een laatste voorbehoud dient nog gemaakt te worden bij de cijfers in Tabel 5. De opgegeven percentages cybersecurity zijn hier *niet* gewogen naar omzet. In de enquête werd gevraagd naar omzet, maar slechts 136 van de 266 bedrijven in de steekproef heeft de omzet daadwerkelijk opgegeven. Weging naar omzet op basis van dusdanig weinig waarnemingen zou geen betrouwbare uitkomsten opleveren. Er zijn overigens geen aanwijzingen dat de weging naar omzet significant andere resultaten zou opleveren. De correlatie tussen opgegeven omzet en opgegeven deel aan cybersecurity is -0,1, oftewel vrijwel geen samenhang.

Vanwege het relatief lage aantal waarnemingen in de steekproef is het aandeel cybersecurity alleen berekend voor de gehele ICT-sector, en niet uitgesplitst naar gedeelte van de sector. Er is bijvoorbeeld geen onderscheid gemaakt naar grotere en kleinere bedrijven in termen van fte. De correlatie van het opgegeven deel aan cybersecurity met opgegeven fte is (evenals met omzet) ongeveer gelijk aan -0,1. Er is ook geen indeling gemaakt van aandelen cybersecurity naar ICT-activiteit, of naar cybersecurity-activiteit.

3.4 Cybersecurity-activiteiten in de Nederlandse economie

Om met behulp van het aandeel cybersecurity in de totale ICT-sector de omvang van cybersecurity-sector in kaart te brengen, dient eerst de omvang van de ICT-sector te worden bepaald. Hiervoor zijn microdatabestanden van het CBS gebruikt. Met hulp van het algemene bedrijvenregister (ABR) zijn bedrijven uit verschillende ICT-sectoren geïdentificeerd, te weten die

[7] Er wordt dus aangenomen dat instroom van ICT-bedrijven niet afhangt van het wel of niet verrichten van cybersecurityactiviteiten. Bedrijven die in 2010 wel bestonden, maar in 2014 niet meer (bijvoorbeeld door faillissement), komen vanzelfsprekend niet in onze steekproef terecht. Bij aanname van gelijke uitstroom van ICT-bedrijven met en zonder cybersecurityactiviteiten, heeft dit geen invloed op onze resultaten.

bedrijven met de SBI-codes genoemd in Tabel 4. Van deze bedrijven is de omzet en export bepaald (m.b.v. het BTW-bestand van het CBS) alsook de werkgelegenheid binnen deze bedrijven (o.b.v. polisbestanden van het CBS). Voor een uitgebreide beschrijving van de CBS-statistieken: zie Bijlage C1.zie Bijlage C1).
Tabel 6 laat de berekende aantallen bedrijven, omzet, toegevoegde waarde, omzet uit export en werkgelegenheid zien in de Nederlandse ICT-sector. De berekeningsmethode voor deze tabel is weergegeven in Bijlage A.1. Omdat de BTW-bestanden voor 2014 nog niet beschikbaar zijn, is 2013 het meest recente jaar waarvoor de omvang van de ICT-sector met behulp van de microdata-bestanden kon worden bepaald. Voor 2014 zijn de aantallen bedrijven via CBS StatLine beschikbaar. Overige statistieken voor 2014 zijn gebaseerd op een schatting aan de hand van omzet, export en werkgelegenheid binnen SBI-subsecties (2-cijferig) waaronder de onderliggende bedrijven vallen. Ook de toegevoegde waarde is geschat op basis van SBI-subsecties (zie ook zie Bijlage C1).

Tabel 6 Groei van de Nederlandse ICT-sector in de afgelopen jaren.

Omvang ICT in Nederland	2010	2013	2014*
Aantal bedrijven (x1000)	51	63	66
Omzet (€ mld.)	€ 57	€ 71	€ 73
Toegevoegde waarde (€ mld.)*	€ 31	€ 38	€ 40
% van het BBP	4,9%	5,8%	6,0%
Omzet uit export (€ mld.)	€ 18	€ 26	€ 27
Werkgelegenheid (fte, x1000)	161	165	166

Bron: SEO Economisch Onderzoek o.b.v. CBS (BTW-bestand 2010 en 2013); Euro's in basisprijzen;

* Eigen berekening o.b.v. CBS StatLine.

In de periode 2010-2014 is de omzet en de toegevoegde waarde jaarlijks met 6,8 procent toegenomen. Voor de werkgelegenheid is dit percentage 0,9.[8] Dit houdt een sterke productiviteitsgroei in in de ICT-sector. Het zijn vooral veranderingen in investeringen in ICT-kapitaal die daar een groot effect op hebben gehad. Deze investeringen zijn tussen 2008 en 2010 afgenomen en sinds 2010 neemt de productiviteit door ICT-kapitaal weer toe (zie Brennenraedts et al., 2014). In 2010 was de toegevoegde waarde van de ICT-sector 4,9 procent van het Nederlandse BBP. Dit percentage is tot 6 procent gestegen in 2014.

Door de omvang van de ICT-sector te vermenigvuldigen met de twee eerder berekende meetwaarden voor het aandeel cybersecurity binnen de ICT-sector, kan een schatting worden gemaakt van de omvang van cybersecurity in Nederland. Tabel 7 laat de berekeningen middels deze twee meetwaarden zien voor de jaren 2010 en 2014. Om naast de omzet ook de omzet uit export, de toegevoegde waarde en de werkgelegenheid van cybersecurity te kunnen bepalen, wordt aangenomen dat het omzetaandeel van cybersecurity representatief is voor omzet uit

[8] NB: Het aantal werknemers betreft alleen mensen in dienst. Zzp'ers zijn niet inbegrepen.

export, toegevoegde waarde en de werkgelegenheid. Nader onderzoek is nodig om te bepalen of deze aanname juist is.

Tabel 7 De toegevoegde waarde van cybersecurity bedroeg in 2014 ongeveer € 4 miljard tegenover € 2,5 miljard in 2010.

Omvang cybersecurity in Nederland	2010 Hoofd ICT-activiteit	2010 Alle ICT-activiteiten	2014 Hoofd ICT-activiteit	2014 Alle ICT-activiteiten
Omzet (€ mld.)	€ 4,3	€ 4,8	€ 6,9	€ 7,5
Toegevoegde waarde (€ mld.)	€ 2,3	€ 2,6	€ 3,8	€ 4,1
% van het BBP	0,36%	0,41%	0,57%	0,62%
Omzet uit export (€ mld.)	€ 1,3	€ 1,5	€ 2,6	€ 2,8
Werkgelegenheid (fte, x1000)	12,0	13,5	15,7	17,1

Bron: VKA/SEO Economisch Onderzoek; Euro's in basisprijzen.

Het aantal bedrijven dat cybersecurity-producten of -diensten levert is in onze steekproef 43 procent. Het aandeel bedrijven met minder dan 5 werknemers is echter veel groter dan het aandeel bedrijven met meer dan 5 werknemers. Omdat onze steekproef uitsluitend op de laatste groep is gebaseerd, kan er geen zuivere schatting worden gemaakt van het totaalaantal cybersecurity-ondernemingen. Het aantal bedrijven met 5 of meer fte dat cybersecurity-producten of -diensten levert in Nederland is naar verwachting 2.450 ondernemingen (van de 5.700 ICT-bedrijven met meer dan 5 fte).

In de periode 2010-2014 is de omzet en de toegevoegde waarde betreffende cybersecurity binnen de ICT-sector jaarlijks met 14,5 procent toegenomen[9]. In 2014 lag de omzet tussen € 6,9 en € 7,5 miljard. Deze stijging is het gevolg van twee factoren: de sterke groei van omzet in de ICT-sector (Tabel 6) en het jaarlijkse 0,5 procentpunt groei in het aandeel cybersecurity binnen de omzet van de ICT-sector.

Binnen de ICT-sector, was de de toegevoegde waarde van de cybersecurity-sector in dat jaar € 3,8 á 4,1 miljard. In 2010 hebben bedrijven die cyberactiviteiten uitvoeren met ongeveer 0,4 procent bijgedragen aan het Nederlandse BBP. In 2014 is dit percentage gestegen tot ongeveer 0,6 procent. Het aantal mensen in dienst binnen de ICT-sector dat zich bezighoudt met cyberactiviteiten is gestegen van 12,7 duizend in 2010 tot ongeveer 16,4 duizend in 2014. Dit betekent een gemiddeld jaarlijkse groei van 7 procent in deze periode.

[9] Een jaarlijks groeipercentage tussen 2010 en 2014 betekent in dit hoofdstuk niet dat er in de praktijk sprake was van een constante groei. Het gaat om een gemiddelde groei tussen de 2 meetmomenten.

HANDEL IN ICT-GOEDEREN

Met behulp van de omzet uit export van het BTW-bestand en de handelsbalans van het IHG-microdatabestand (Internationale Handel Goederen) van het CBS is tevens de internationale handel door Nederlandse bedrijven in ICT-goederen in kaart gebracht. In het BTW-bestand is de omzet uit export van alle Nederlandse bedrijven gemeten. Dit bestand geeft een volledig beeld van de export van ICT-goederen en -diensten (zie Tabel 8) Het IHG-bestand en dus Tabel 8 bevat alleen ICT-goederen. Om te bepalen welke goederen ICT-goederen zijn, is gekeken naar de koppeling van de productcodes van alle goederen in het IHG-bestand met een bepaalde ICT-code. Wanneer een product een koppeling heeft met een SBI-code binnen de ICT-sector, wordt deze meegenomen in de analyse. Tabel 8 laat de totale invoer, uitvoer en wederuitvoer van ICT-goederen door alle bedrijven in Nederland zien.

Tabel 8 De handelsbalans in ICT-goederen werd wat positiever tussen 2010 en 2013.

Handel in ICT-goederen	**2010**	**2013**
Invoer incl. wederuitvoer (€ mld.)	€ 31,9	€ 27,0
Uitvoer incl. wederuitvoer (€ mld.)	€ 23,4	€ 20,0
Handelsbalans incl. wederuitvoer (€ mld.)	**- € 8,5**	**- € 7,0**
Wederuitvoer (€ mld.)	€ 20,1	€ 17,1
Invoer excl. wederuitvoer (€ mld.)	€ 11,8	€ 10,0
Uitvoer excl. wederuitvoer (€ mld.)	€ 3,3	€ 2,9
Handelsbalans excl. wederuitvoer (€ mld.)	**- € 8,5**	**- € 7,0**
Aantal Nederlandse bedrijven betrokken in handel (x1.000)	**214,5**	**217,2**

Bron: SEO Economisch Onderzoek o.b.v. CBS (IHG-bestand 2010 en 2013); euro's in basisprijzen.

In de voorgaande sectie is de omzet uit export berekend voor Nederlandse bedrijven die actief zijn op het gebied van cybersecurity (zie Tabel 7). In 2014 was de exportwaarde van cybersecurity-diensten en -producten ongeveer 2,7 miljard euro. Ten opzichte van 2010 (1,4 miljard euro) betekent dit een gemiddelde jaarlijkse groei van ongeveer 22 procent.

De groei van export is opvallend en grotendeels een gevolg van de exportgroei in de ICT-sector. Export uit ICT-dienstverlening, die ongeveer 18 procent van de totale ICT-export in 2013 voor haar rekening neemt, is het meest gestegen: jaarlijks met gemiddeld 30 procent tussen 2010 en 2013. Groothandel leverde 68 procent van de export in 2013 en liet jaarlijks gemiddeld 13 procent groei zien tussen 2010 en 2013. Volgens Brennenraedts et al. is Nederland een exporteur van software. Dit feit kan de geschetste ontwikkeling mogelijk verklaren. Brennenraedts et al concluderen ook dat hardware (i.e. ICT-goederen) vooral uit het buitenland wordt geïmporteerd. De export van ICT-goederen vormde slechts 10 procent van de totale export in 2013. De export van ICT-goederen liet geen groei zien tussen 2010-2013 (zie ook Tabel 7). (Brennenraedts et al., 2014). Er is nog aanvullend onderzoek nodig om over de samenstelling van export nadere conclusies te trekken.

Het bepalen van het aandeel cybersecurity binnen de totale handelsbalans in ICT-goederen is echter niet mogelijk, om twee reden. Ten eerste, de handelsbalans betreft alleen ICT-goederen. In de enquête is er slechts een klein aantal waarnemingen voor ICT-goederen beschikbaar. Daarom is er geen apart aandeel berekend voor ICT-goederen. Ten tweede, de aandelen zijn bepaald in de Nederlandse ICT-sector. Binnen de handelsbalans kan alleen het gedeelte 'uitvoer' toegerekend worden aan Nederlandse bedrijven. Voor het bepalen van invoer is geen informatie beschikbaar over het gedeelte cybersecurity binnen de ICT-sector in andere landen.

3.5 Potentiële omvang

De laatste vraag van de enquête over het aandeel cybersecurity heeft betrekking op de toekomst, te weten de verwachte jaarlijkse verandering in de omzet vanuit cybersecurity. Alle respondenten die een cijfer gaven voor hun percentage aan cybersecurity in de omzet van 2014, maakten ook een inschatting van de te verwachten groei in de sector. Tabel 9 geeft de resultaten voor deze verwachte groei van omzet uit cybersecurity-activiteiten. Opgemerkt dient te worden dat deze percentages niet vergeleken kunnen worden met de percentages uit Tabel 5, omdat deze laatste het aandeel binnen de totale ICT-omzet geven.

Verder is het onbekend hoe de structuur van de sector nu eruitziet en zal in de toekomst ontwikkelen. Bijvoorbeeld, als de concurrentie tussen cyberbedrijven nu al sterk is of in de toekomst zou toenemen, zou een toenemende omzet voor een bedrijf een afnemende omzet kunnen betekenen voor een ander bedrijf. Als gevolg van concurrentie zouden de prijzen dalen waardoor de totale omzet in de sector zou ook afnemen. Deze ontwikkelingen beïnvloeden de groei van de sector en zijn niet in de cijfers meegenomen.

De berekeningswijze van de cijfers in Tabel 9 is conform aan de wijze zoals bij Tabel 5 beschreven. Aangenomen is dat bedrijven zonder cybersecurity-activiteiten op het moment van de enquête verwachten ook in de toekomst deze activiteiten niet te ontplooien.

Tabel 9 De verwachte jaarlijkse groei van omzet uit cybersecurity-activiteiten is ongeveer 7%.

	Verwachte toekomstige jaarlijkse groei
Gewogen o.b.v. hoofd-ICT-activiteit (SBI-codes)	6,9 %
Gewogen o.b.v. alle ICT-activiteiten (zelf-gerapporteerd)	7,4 %

Bron: VKA/SEO Economisch Onderzoek, n(SBI)=266 en n(alle)=246.

De verwachte jaarlijkse groei van omzet uit cybersecurity-activiteiten is ongeveer 7 procent. Dit percentage betreft het ICT-deel van de cybersecurity-sector. Nader onderzoek is nodig om de groei van andere cybersecurity-activiteiten (zie Afbeelding 1) te bepalen.

3.6 Conclusie

De cybersecuritysector creëert toegevoegde waarde door het aanbieden van producten en diensten die de cyberrisico's proberen te verminderen en schade efficiënt herstellen. De rest van de economie betaalt voor deze producten en diensten en profiteert ervan.

Middels een enquête is de omvang van de Nederlandse cybersecurity-sector binnen de ICT-sector bepaald. Uit de enquête blijkt dat in 2014 ongeveer 10 procent van de omzet binnen de ICT-sector gekoppeld was aan cybersecurity-activiteiten.

Dit aandeel cybersecurity is gebruikt om de totale omzet, omzet uit export, toegevoegde waarde en werkgelegenheid te bepalen binnen de ICT-sector.
In de periode 2010-2014 is de omzet en de toegevoegde waarde betreffende cybersecurity binnen de ICT-sector jaarlijks met 14,5 procent toegenomen. In 2014 lag de omzet tussen € 6,9 en € 7,5 miljard. De toegevoegde waarde van de cybersecurity-sector was € 3,8 á 4,1 miljard in datzelfde jaar. In 2010 hebben bedrijven die cyberactiviteiten uitvoeren met ongeveer 0,4 procent bijgedragen aan het Nederlandse BBP. In 2014 is dit percentage gestegen tot ongeveer 0,6 procent. De cybersecurity-sector groeide daarmee veel sneller dan de ICT-sector zelf.

De benaderde ICT-bedrijven in de enquête verwachten een jaarlijkse groei van omzet uit cybersecurity-activiteiten van ongeveer 7 procent.

Conclusie is dat de Nederlandse cybersecurity-sector een relevante omvang heeft en bovendien snel groeiend is.

4 UITSTRALING EN VESTIGINGSKLIMAAT

4.1 Inleiding

In dit hoofdstuk wordt een antwoord geformuleerd op de volgende onderzoeksvraag: *Welke uitstralingseffecten zou een sterke cybersecurity-sector kunnen hebben voor de ontwikkeling naar een digitale economie in Nederland?* Meer achtergrondinformatie bij de onderzoeksaanpak en meer resultaten zijn opgenomen in bijlage D.

Idealiter zou het denkkader geschetst in sectie 3.1 een precieze meting van de waarde van cybersecurity (de uitstralingseffecten van de cybersecurity-sector) voor de economie als geheel weergeven. Voor de ICT-sector in de periode 1990-2013 werd zo'n berekening gemaakt (Brennenraedts et al, 2014). Deze berekening werd mogelijk door de bestaande uitsplitsing van de economie naar het ICT- en niet-ICT-deel (zie CBS). Economische groei betreffend ICT komt vooral door een toename van ICT-kapitaal (investeringen) en technologische veranderingen. Met name is ICT gezien als een *general purpose technology* die de hele economie doordringt.

Deze statistische uitsplitsing bestaat niet voor cybersecurity en daarom is het meten van de toegevoegde waarde moeilijk. Daarom is er een aantal methoden voor het meten van de waarde van cybersecurity geformuleerd, zoals (1) de betalingsbereidheid van de afnemers van cyberproducten en -diensten, een soort verzekeringspremie, (2) de investeringen in cybersecurity en (3) het aantal cyberincidenten en -schade. De eerste twee methoden zijn gekoppeld aan de waardering van de afnemers van cyberproducten en -diensten voor de vermindering van het cyberrisico. Er is echter weinig onderzoek beschikbaar met deze methoden. De derde methode is gebaseerd op daadwerkelijke incidenten en schade. Voorafgaand aan deze studie leek deze methode een haalbare proxy te geven voor de waarde van cybersecurity.

In de volgende sectie worden de eerste twee methoden kort beschreven. De derde methoden volgt in sectie 4.3. Conclusies over het vestigingsklimaat zijn getrokken in sectie 4.4. Meer achtergrondinformatie over de methoden en de beschikbare metingen zijn opgenomen in bijlage D.

4.2 Betalingsbereidheid en investeringen in cybersecurity

Een eerste methode waarmee de waarde van cybersecurity kan worden bepaald is de betalingsbereidheid (*willingness to pay*, WTP) voor maatregelen die de cybersecurity verhogen (zie voor een overzicht van waarderingsmethoden in de context van leveringszekerheid Van der Noll *et al*., 2010). Er zijn verschillende methoden om de betalingsbereidheid voor veiligheid te bepalen.

De betalingsbereidheid kan door een “uitgesproken voorkeur” gemeten worden. Er is slechts één studie bekend die de uitgesproken voorkeuren betreffend cybersecurity meet. Rowe et al. (2011) vragen consumenten hoeveel ze zouden betalen voor verbeteringen in het ISP-veiligheidsbeleid, of, als alternatief, met hoeveel ze zouden moeten worden gecompenseerd om ongunstige

wijzigingen in het ISP-beleid te accepteren. De studie laat zien dat Amerikaanse consumenten bereid zijn om tussen 2,94 en 6,51 dollar per maand te betalen voor internettoegang met een hoger niveau van cybersecurity.

Daarnaast kan betalingsbereidheid gezien worden als een vorm van preventie om cyberschade door cyberonveiligheid te voorkomen. Dit is een soort verzekeringspremie. Cyberverzekering bestaat al langer (OECD, 2015, Anderson et al. 2013, RAND Europe, 2015). Een vorm van verzekering is dat bedrijven het risico, gekoppeld aan technologische ontwikkeling, een onderdeel maken van hun risicomanagementstrategieën. De verzekeringsmarkt ontwikkelt zich in deze richting.

Een tweede methode is om te kijken naar investeringen in cybersecurity. Deze investeringen zijn ook een proxy voor de waarde van de vermindering van het cyberrisico. Daarnaast signaleren deze investeringen de verantwoordelijkheid die de economie neemt voor de vermindering van de kansen op cyberincidenten. Er is op dit moment slechts één studie bekend die de investeringen in cybersecurity in kaart probeert te brengen. RAND Europe (2015) kijkt naar investeringen in cybersecurity door het bedrijfsleven in 12 vitale sectoren. Volgens RAND (2015) is de angst voor reputatieschade de belangrijkste reden voor investeringen. Ook zijn bedrijven bang voor mogelijke rechtszaken vanwege aansprakelijkheid. Daarnaast investeren bedrijven in cybersecurity om de kans op een cyberaanval en schade daarvan te verminderen. Het meten van de hoogte van de investeringen bleek ook in deze studie echter moeilijk.

4.3 Cyberincidenten en -schade als proxy

Een derde methode is gebaseerd op daadwerkelijke incidenten en schadekosten door onvoldoende cybersecurity.[10] Voor de analyse zijn verschillende bronnen gebruikt, namelijk studies, statistieken en een mediasearch via LexisNexis.[11]

De analyse van incidenten en schade kent echter een aantal beperkingen. Ten eerste, er is géén eenduidige definitie van cybersecurity-incidenten. Om een overschatting van incidenten en schade te voorkomen, kiest deze studie voor een conservatieve aanpak wat betreft de afbakening van cybercrime. Conservatief houdt in dat in de afbakening slechts de meest voorkomende digitale vormen van criminaliteit de lading zullen dekken, conform de aanpak van het NCSC (2015). Daarnaast kijkt deze studie alleen naar de frequentie of omvang van bepaalde cybercrime middelen, zonder iets te kunnen zeggen over een totaal van de categorieën bij elkaar. Ten tweede, verschillende statistieken meten slechts een deel van deze middelen dus er is geen volledig beeld beschikbaar.

---

[10] Het is gebruikelijk om preventiekosten en schadekosten als maatstaf te gebruiken voor het kwantificeren van uitstralingseffecten. Het milieubeleid is hiervan een voorbeeld. Zie bijvoorbeeld CE Delft (2010).

[11] LexisNexis is een databank met archieven van bijna 10.000 dagbladen en tijdschriften.

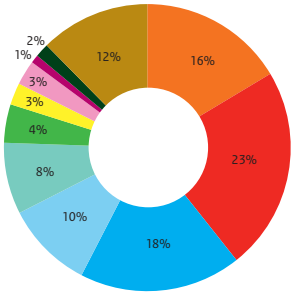
Uiteindelijk kennen meetmodellen een aantal beperkingen waardoor de schade te laag of te hoog wordt ingeschat. Meetmethoden zijn vaak niet transparant waardoor vergelijk niet mogelijk is. Daarnaast zijn de meest gebruikte methoden gebaseerd op enquêtes die vaak slechts een klein aantal waarnemingen voor een groep of zelfs voor een land bevatten. In dit geval levert de extrapolatie naar de hele populatie onbetrouwbare gegevens, vooral als er *outliers* in de data zitten. Onwetendheid door slachtoffers en prikkels voor meer of juist minder schade te rapporteren leiden ook tot over- of onderrapportage. Een uitgebreide analyse en aanbevelingen voor het (betere) meten van cyberincidenten en -schade is terug te vinden in Bijlage D en in het rapport van e-crime (2015).

Vanwege de bovenstaande beperkingen is het niet mogelijk om harde conclusies te trekken voor de waarde van cybersecurity.

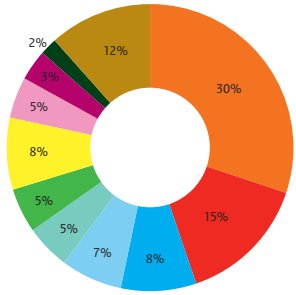
Enkele cijfers zijn wel beschikbaar. Volgens PWC (2015) is 23 procent van bedrijven de laatste 24 maanden geconfronteerd met cybercrime. In de rest van de wereld ligt het percentage van bedrijven op negen procent. De Nederlandse overheid is vooral slachtoffer van informatielekkage (NCSC, 2015; Afbeelding 7). Het Nederlandse bedrijfsleven en consumenten komen vooral in aanraking met phishing, virussen en hacken (zie Ponemon Institute, 2015 en PWC, 2014). In Nederland raakt cybercrime handel, financiële instellingen en de ICT-sector het meest (zie Afbeelding 8).

Afbeelding 7 **De overheid is slachtoffer van informatielekkage, private partijen van phishing**

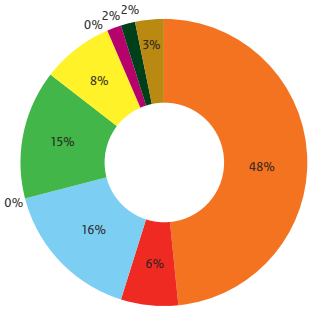
Figuur 19 **Type incidenten waarbij een overheidspartij betrokken was**



Figuur 20 **Type incidenten waarbij een private partij betrokken was**



Figuur 21 **Type incidenten waarvoor het NCSC een internationaal hulpverzoek ontving**



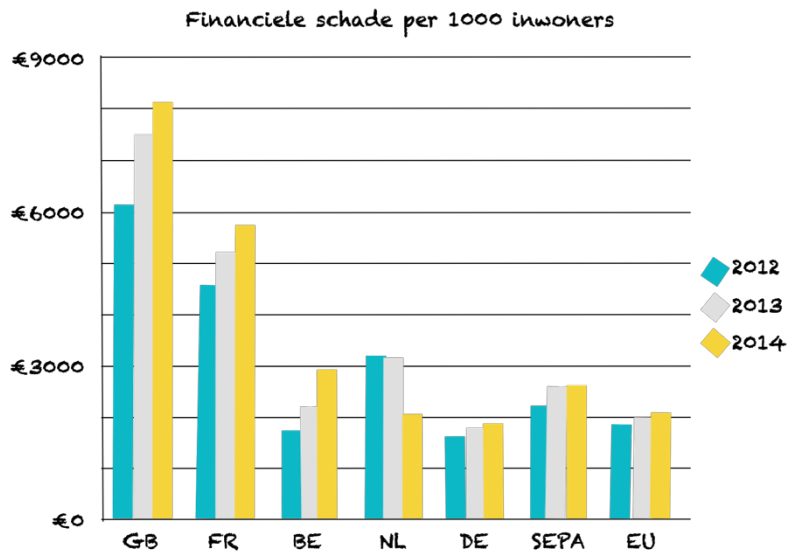
Bron: NCSC (2015).

Afbeelding 8 **In Nederland raakt cybercrime handel, financiële instellingen en de telecom/ICT-sector**

Bron: PWC (2014); Percentage functioneel belast met de aanpak, het voorkomen of in kaart brengen van economische criminaliteit, uitgesplitst naar sector en naar cybercrime expertise.

In de lijst van middelen zijn incidenten betreffende online bank- en pasfraude het best gerapporteerd. Ondanks de stijging in Europa neemt het aantal frauduleuze transacties af in Nederland. Volgens de DNB en ECB daalt de financiële schade substantieel in Nederland in de periode 2012 en 2014 (van 3.183 euro naar 2.046 euro per 1000 inwoners) en komt dichterbij het Europese gemiddelde (zie Afbeelding 9).

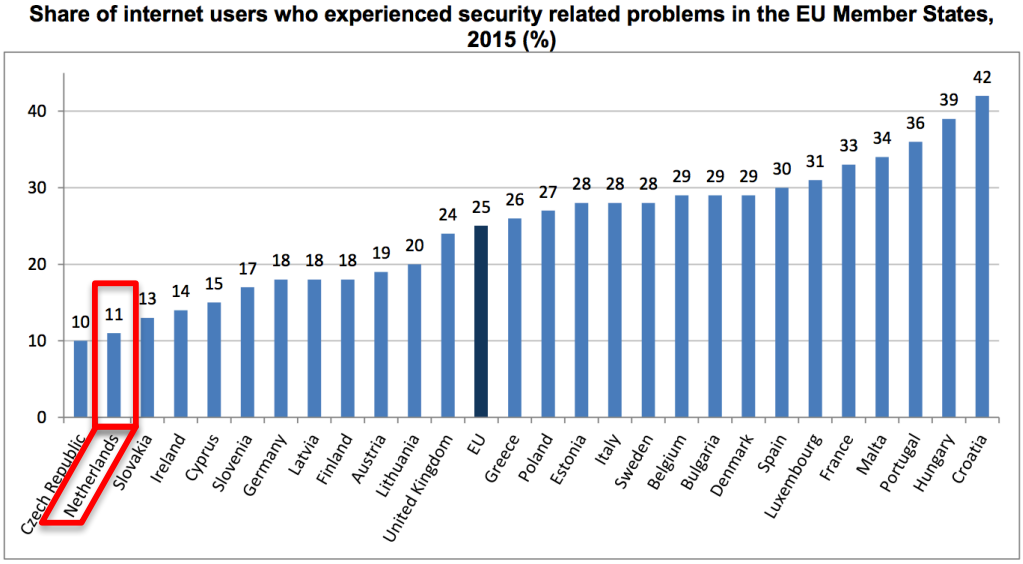
Afbeelding 9 De financiële cyberschade in Nederland daalt en komt dichterbij het Europese gemiddelde



Bron: ECB (2013, 2014, 2015)

Een recente studie van Eurostat (zie Eurostat, 2016) analyseert in hoeverre particuliere internetgebruikers cyberincidenten ervaren. De cijfers van Eurostat zijn gebaseerd op de veiligheidsmonitoren van verschillende landen, gerapporteerd door de nationale bureaus voor de statistiek.

Afbeelding 10 Aandeel internetgebruikers met security-problemen



Bron: Eurostat (2016)

In 2015 heeft 25 procent van Europese internetgebruikers problemen ervaren die gerelateerd zijn aan cyberincidenten. In Nederland is dit percentage 11 procent, de op Tsjechië na, laagste binnen de EU. We moeten echter een vraagteken plaatsen bij de vergelijkbaarheid van deze cijfers, vooral omdat de methodologie in de veiligheidsmonitor van verschillende landen onbekend is.

De meest voorkomende incidenten zijn virussen, misbruik van persoonlijke gegevens, financiële verliezen en ongepaste websites voor kinderen. In de afgelopen jaren is het aandeel van virussen flink gedaald in Nederland: van 23 procent in 2010 naar 6 procent in 2015. Dit percentage ligt onder het Europese gemiddelde (respectievelijk 31 procent in 2010 en 21 procent in 2015). Maar ten minste 20 procent van de Nederlandse internetgebruikers wil niet online winkelen, online bankieren of zet hun mobiele toestellen niet op een wifi-netwerk vanwege bezorgdheid over de veiligheid. Dit betekent dat Nederlanders voorzichtiger zijn dan het Europese gemiddelde.

4.4 Cybersecurity en Vestigingsklimaat

Nederland staat hoog op de ranglijsten met vestigingsklimaat. KPMG beschrijft bijvoorbeeld in haar onderzoek *Competitive Alternatives* dat Nederland van de West-Europese landen het meest aantrekkelijk is om er een onderneming te vestigen. Buitenlandse bedrijven zijn in Nederland aanzienlijk goedkoper uit dan in Duitsland, Frankrijk, Groot-Brittannië en Italië.
In het onderzoek is gekeken naar onder meer naar de kosten voor huisvesting, arbeid, transport, energie en de fiscale kosten. KPMG geeft aan dat Nederland aantrekkelijk is voor bedrijven die actief zijn in onderzoek en ontwikkeling, met name vanwege fiscale stimuleringsmaatregelen (KPMG, 2016).
Ook op de Global Competitive Index van het World Economic Forum staat Nederland op dit moment hoog, namelijk op plaats 5, de hoogste notering ooit. (World Economic Forum, 2015).

In verschillende wereldwijde ranglijsten op het gebied van cybersecurity staat Nederland steeds bij de top 6. Bijvoorbeeld in de International Telecommunication Union (ITU) and ABI Research, Global Cybersecurity Index, 2014 (ABI, 2014), de Melissa Hathaway, Cyber Readiness Index 1.0, 2013 (Hathaway, 2013) en de Security and Defence Agenda (SDA), Cyber-security: The vexed question of global rules, An independent report on cyber-preparedness around the world (SDA, 2012).

Ernst & Young concludeerde in 2011 dat veiligheid en betrouwbaarheid van de ICT-infrastructuur voor bedrijven die overwegen zich te vestigen in Nederland geen doorslaggevende factor is, bij deze beslissing. Veiligheid en betrouwbaarheid van de ICT-infrastructuur speelt op de achtergrond wel een rol, maar andere factoren zoals politieke stabiliteit, de beschikbaarheid van geschoold personeel en het rechtsbestel, maar ook de snelheid van ICT-verbindingen spelen een grotere rol (Ernst & Young, 2011).

4.5 Conclusies

In de statistieken is er nog geen uitsplitsing voor cybersecurity en daarom is het meten van de waarde van de sector lastig. Daarom is er een aantal methoden voor het meten van de waarde van cybersecurity geformuleerd, zoals (1) de betalingsbereidheid van de afnemers van cyberproducten en -diensten, een soort verzekeringspremie, (2) de investeringen in cybersecurity en (3) het aantal cyberincidenten en -schade. De eerste twee methoden zijn gekoppeld aan de waardering van de afnemers van cyberproducten en -diensten voor de vermindering van het cyberrisico. Er blijkt weinig onderzoek beschikbaar met deze methoden. De derde methode is gebaseerd op daadwerkelijke incidenten en schade. Theoretisch leek deze methode een haalbare proxy te geven voor de waarde van cybersecurity en binnen dit onderzoek is een poging gedaan om hiervoor betrouwbare data te verzamelen.

Voor de analyse van incidenten en de omvang van de schade zijn verschillende bronnen gebruikt, namelijk studies, statistieken en een mediasearch via LexisNexis. Er geldt een aantal beperkingen bij het analyseren van incidenten en schade. Eén daarvan is het reeds genoemde ontbreken van de eenduidige definitie van cybersecurity-incidenten. Daarnaast zijn meetmethoden vaak niet transparant en de data is onvolledig en niet te vergelijken. Voor nadere analyses is er een systematische verzamel- en aggregatiemethode nodig. Vanwege deze beperkingen bleek het niet mogelijk om harde conclusies te trekken over de waarde van cybersecurity. Enkele cijfers zijn wel beschikbaar.

Volgens PWC (2015) is 23 procent van bedrijven de laatste 24 maanden geconfronteerd met cybercrime. In de rest van de wereld ligt het percentage van bedrijven op negen procent. Het Nederlandse bedrijfsleven komt vooral in aanraking met phishing, virussen en hacken. In Nederland raakt cybercrime handel, financiële instellingen en de ICT-sector het meest. Betrouwbare informatie bleek beschikbaar voor de financiële sector, en dan vooral rondom online bank- en pasfraude (ECB-rapporten). De schade daar in 2014 wordt geraamd op ruim 2 duizend

euro per 1000 inwoners, en is de afgelopen jaren dalend. De Nederlandse overheid is vooral slachtoffer van informatielekkage (NCSC, 2015).

Bij consumenten zijn volgens de veiligheidsmonitor van het CBS (Eurostat, 2016), de meest voorkomende cyberincidenten virussen, misbruik van persoonlijke gegevens, financiële verliezen en ongepaste websites voor kinderen. In de afgelopen jaren is het aandeel virussen hierbinnen flink gedaald in Nederland en het percentage ligt onder het Europese gemiddelde. Maar volgens de monitor zijn Nederlandse consumenten voorzichtiger dan het Europese gemiddelde met online winkelen, online bankieren of het gebruik van een wifi-netwerk voor hun mobiele toestellen.

De bovenstaande cijfers suggereren dat er een positieve ontwikkeling plaatsvindt wat enkele typen cyberincidenten en -schade betreft. Of er een correlatie is tussen deze ontwikkelingen en de groei van de sector is niet te concluderen op basis van de beschikbare informatie.

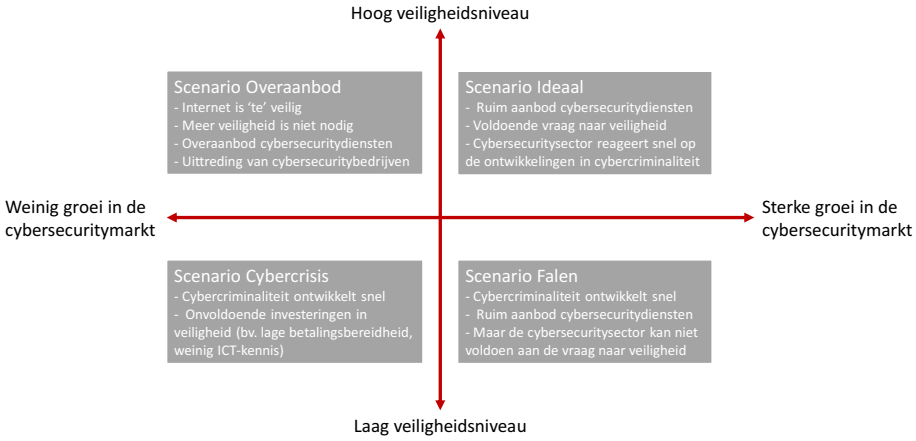
5 KANSEN EN BEDREIGINGEN CYBERSECURITY-SECTOR

Dit hoofdstuk starten we met een analyse van scenario's voor de cybersecurity-sector. Daarna completeren we de SWOT-analyse door in te gaan op de kansen en bedreigingen.

5.1 Scenario's

In welke mate de gesignaleerde kansen en bedreigingen voor de cybersecurity-sector zich ook daadwerkelijk manifesteren is onzeker. Een manier om gestructureerd na te denken over kansen en bedreigingen is door gebruik te maken van scenario's.
Op basis van de onderzoeksvraag waren er twee belangrijke indicatoren die de scenario's kunnen bepalen: de groei van de cybersecuritysector en het niveau van veiligheid.

Afbeelding 11 Vier scenario's voor de uitstalingseffecten



We kunnen deze indicatoren als twee dimensies gebruiken waardoor vier scenario's worden bepaald (zie Afbeelding 11). Op de verticale as zien we de mate van veiligheid van het cyberdomein variëren van laag tot hoog. In de onderste helft van de afbeelding is het veiligheidsniveau laag, zijn er veel incidenten en schade. In de bovenste helft van de afbeelding is er sprake van een hoog niveau van veiligheid.

Op de horizontale as zien we de groei van cybersecuritysector. Aan de linkerzijde is er weinig of geen groei, of mogelijk zelfs sprake van krimp. Aan de rechterzijde is sprake van sterke groei van de sector. De combinatie van de twee assen geeft de volgende vier scenario's.

1. Scenario Overaanbod
2. Scenario Ideaal
3. Scenario Cybercrisis

4. Scenario Falen

Hieronder werken we de vier scenario's verder uit.

In het *scenario Overaanbod* zien we dat afnemers het Cyberdomein als (te) veilig beschouwen. Er zijn weinig grote incidenten, waardoor afnemers niet bereid zijn veel geld te besteden aan cybersecurity-producten en diensten. De gesignaleerde bedreiging Daling awareness (paragraaf 5.4 sluit hier op aan. Het gevolg van een veilig cyberdomein is een overaanbod aan cybersecurity-producten en diensten en het uittreden van aanbieders van cybersecurity-producten en diensten.

Het *scenario Ideaal* beschrijft een situatie waarin er een ruim aanbod aan cybersecurity-producten en diensten, gecombineerd met voldoende vraag. Afnemers kunnen goed het aanbod van cybersecurity-producten en diensten goed op waarde inschatten. Er zijn incidenten, maar de het aanbod van cybersecurity-producten en diensten biedt afnemers de mogelijkheid om zich tegen aanvaardbare kosten (gelet op de meerwaarde van het gebruik maken het cyberdomein) te beschermen tegen schade door verstoring, uitval of misbruik van ICT als gevolg van moedwillige activiteiten.

In het *scenario Cybercrisis* wint de cybercriminaliteit het van de cybersecurity. Er wordt onvoldoende geïnvesteerd in de ontwikkeling van cybersecurity-producten en diensten, bijvoorbeeld doordat afnemers niet bereid blijken te zijn de toenemende kosten te dragen, omwille van marktfalen zoals het hold-up probleem of asymmetrische informatie (zie ook paragraaf 6.2).

Tot slot, het *scenario Falen*, beschrijft ook een situatie waarin de cybersecurity-sector zich door toenemende vraag snel ontwikkelt, echter de cybercriminaliteit ontwikkelt zich sneller, waardoor per saldo de veiligheid in het cyberdomein lager wordt.

Dat de cybersecurity behoorlijk groeit is reeds duidelijk geworden in hoofdstuk 3. Hiermee komen we dus aan de rechterkant van Afbeelding 11. Uit de analyse van sterkten en zwakten halen we elementen die erop wijzen dat Nederland mogelijk in de huidige situatie in het *scenario Falen* zitten (rechtsonder). Er is volgens de deskundigen sprake van een tekort aan specialisten en toegang tot (durf) kapitaal. Alhoewel sommige studies wijzen op een groei van het aantal cyberincidenten en de schade (Ponemon, 2015), wijzen andere studies juist weer op een daling. In paragraaf 4.3 lieten we in dit kader al zien dat volgens DNB en ECB de financiële schade in Nederland substantieel daalt. Dit zou kunnen betekenen dat we ons op dit moment juist meer rechtsboven in Afbeelding 11 bewegen.

5.2 Analyse van kansen en bedreigingen

In deze paragraaf beschrijven we de kansen en bedreigingen van de Nederlandse cybersecurity-sector. Net als de analyse van sterkten en zwakten is deze analyse gebaseerd op ons inzicht in de

markt, de input van een 30-tal deskundigen (middels interviews en ronde tafels) uit de sector. Zie bijlage B voor een overzicht van geïnterviewden en deelnemers aan de ronde tafels.
De kansen en bedreigingen zijn in onderstaande tabel opgenomen en worden vervolgens kort beschreven. De sterkten en zwakten, welke de SWOT-analyse completeren, waren eerder te vinden in paragraaf 2.4.

Tabel 10 Analyse kansen en bedreigingen

Analyse Nederlandse cybersecurity-sector	
Kansen	***Bedreigingen***
• Doorontwikkeling van de Nederlandse cybersecurity aanpak • Wetgeving • Betere uitwisseling bedrijfsleven-wetenschap • Groei awareness • Ontwikkeling domeinen	• Beschikbaarheid goed gekwalificeerde mensen • De thuismarkt is klein • Wetgeving • Kosten van beveiliging worden te hoog waardoor deze niet meer opwegen tegen de voordelen van gebruik digitale middelen. Met name voor MKB • Daling awareness • Kennis bij afnemers • Concurrentie van buitenlandse partijen en/of overnames

In onderstaande tekst lichten we de verschillende kansen en bedreigingen kort toe.

5.3 Kansen

DOORONTWIKKELING VAN DE NEDERLANDSE CYBERSECURITY AANPAK

Op het moment van schrijven van dit rapport, wordt door het kabinet gewerkt aan de doorontwikkeling van de Nederlandse cybersecurity aanpak. Alhoewel de contouren van deze doorontwikkeling nog niet duidelijk zijn, kan mogelijk inspiratie gevonden worden bij het Amerikaanse Cybersecurity National Action Plan, dat door President Obama in februari 2016 is gepresenteerd (Obama, 2016). In het plan, waarvoor 19 miljard dollar in het budget 2017 is vrijgemaakt, is onder andere de focus gelegd op het tot stand brengen van multi-factor authenticatie. In de National Cybersecurity Awareness Campagne, zal in samenwerking met de National Cyber Security Alliance (technologiebedrijven zoals Google, Facebook, DropBox, en Microsoft en financiële dienstverleners als MasterCard, Visa, PayPal, en Venmo) gewerkt gaan worden aan veiliger toegang en transacties. Binnen het Amerikaanse plan wordt er een *Commissie ter verbetering van de Nationale Cybersecurity* aangesteld.

Een kans die in dit kader ook genoemd is het verder bundelen van cyber-security-activiteiten binnen de overheid. Operationeel bijvoorbeeld in een gemeenschappelijk Security Operations Center. Tactisch bijvoorbeeld door meer bundeling van inkoop. Beide concentraties zorgen voor schaalvergroting en door de schaalvergroting die optreedt zal er een plek ontstaan waar kennis samenkomt, die voor de experts interessant is, waardoor ook verdere ontwikkeling van kennis zal

plaats vinden. Doordat bij de huidige (gefragmenteerde) inkoop de kwaliteit van een product of dienst door de inkopende organisatie (nog) niet op waarde kan worden geschat, kan sprake zijn van asymmetrische informatie en meer bijzonder, adverse selectie.

WETGEVING

Wanneer de Nederlandse overheid in het cyberdomein strenge wetgeving introduceert en toezicht houdt op de naleving, bijvoorbeeld rondom datalekken kan dit vertrouwen geven aan gebruikers. Aspecten die in dit kader genoemd worden:

- Bevoegdheden in het kader van nieuwe wetgeving (Wet computercriminaliteit III & Wiv), biedt ook kansen vanuit business-overweging, levert naar verwachting vraag naar specialisten op.
- De Wiv kan volgens sommigen een goede bijdrage leveren aan een veiliger internet. De pakkans van cybercriminelen zou hiermee kunnen worden vergroot.

Op 1 januari 2016 is de Wet Meldplicht Datalekken in werking getreden. Kern van de wet is de introductie van een brede meldplicht voor private en publieke organisaties, en de mogelijkheid forse boetes op te leggen wanneer een datalek dat niet gemeld wordt aan de verantwoordelijke en niet gemeld wordt aan de betrokkenen terwijl dat wel had gemoeten. Vanuit verschillende kanten werd aangegeven dat de wetgeving nog veel onduidelijkheden bevat, en dat het niet mogelijk is om op voorhand situaties aan de Autoriteit Persoonsgegevens (AP), ten einde uitsluitsel te krijgen over de mate waarin getroffen beveiligingsmaatregelen afdoende zijn. Meer duidelijkheid en een mogelijkheid om een "ruling" op voorhand te verkrijgen over een bepaalde (beveiligings)oplossing, zouden kansen kunnen betekenen voor de Nederlandse cybersecurity-sector.

Een steeds strenger wordende wetgeving voor het cyberdomein wordt niet direct gezien als een bedreiging door alle geïnterviewden. Een aantal respondenten gaf aan dat, indien strikte wetgeving rondom bijvoorbeeld privacy in Nederland in het buitenland goed ‘verkocht wordt’, dus ook als een voordeel gezien kan worden door afnemers in het buitenland.

BETERE UITWISSELING BEDRIJFSLEVEN-WETENSCHAP

In paragraaf 2.6 is al aangegeven dat volgens geïnterviewden de aansluiting tussen wetenschap en bedrijfsleven in het cybersecurity-domein beter kan. De cybersecurity-sector is sterk gedreven door innovatie en hiervoor is kennisuitwisseling met de wetenschap nodig. Een goed ontwikkeld ecosysteem waarin wetenschap en bedrijfsleven samen optrekken, kennis delen en elkaar versterken wordt als cruciaal gezien om ervoor te zorgen dat Nederland voorop loopt op dit gebied.
Dat Nederland wat betreft het benutten van wetenschappelijk kennis internationaal onder het gemiddelde scoort wordt herkend. In dit kader heeft het ministerie van Economische Zaken het Valorisatieprogramma opgezet dat ondersteunt bij het vormgeven van activiteiten op het gebied van ondernemerschapsonderwijs en kennisvalorisatie (RVO).

De Adviesraad voor Wetenschap- en technologiebeleid (AWT) concludeerde eerder: Het innovatie- en groeivermogen van ondernemingen wordt bepaald door vele interne en externe factoren, zoals een goede strategie, toegang tot nieuwe kennis, een goede organisatie, toegang tot financiering en toegang tot internationale markten. Op veel van deze aspecten zullen groeibriljanten tegen problemen aanlopen, die ze uiteindelijk zelf moeten kunnen oplossen. Bij het oplossen van deze problemen, hebben groeibriljanten veel baat bij een goed functionerend ecosysteem, waarin zij snel de juiste partners kunnen vinden; partners die hen kunnen helpen bij het verkrijgen van kennis, verkrijgen van financiering, vinden van goede mensen, vergaren van informatie over marktkansen, toegang krijgen tot internationale netwerken, etcetera. De raad focust in dit advies daarom op het versterken van het ecosysteem als belangrijk beleidsdoel. Het ecosysteem in Nederland kan versterkt worden door (innovatie)samenwerking tussen groeibriljanten en (internationale) klanten, 'complementoren' en concurrenten te stimuleren. Hierbij spelen universiteiten, Topconsortia voor Kennis en Innovatie, instituten voor toegepast onderzoek en hogescholen een belangrijke rol (AWT, 2014).

Rondom het punt van uitwisseling van kennis tussen wetenschap en bedrijfsleven zijn indicaties van marktfalen te vinden. Het gaat dan om de al het al vaak beschreven bestaan van positieve externaliteiten (kennis-spillovers) van innovatie.

Daarnaast is er al veel geschreven over de vorming van ecosystemen rondom universiteiten. Zo geven Van Oort et al. aan dat het op orde brengen van regionale productiestructuren, via huisvesting, informatieverstrekking, financiering en de toegankelijkheid van de afzet- en arbeidsmarkt, is te classificeren als noodzakelijke voorwaarden voor de ontwikkeling van een innovatief academisch ondernemerschap. Daadwerkelijk succes berust op pad-afhankelijke netwerken en geschreven en ongeschreven regels tussen onderzoekers, bedrijven en kennisinstellingen – de zachte kant van een ecosysteem (Van Oort et al., 2014).

In navolging van de Adviesraad voor wetenschap, technologie en innovatie (AWTI): *Stimuleer samenwerking tussen groeibriljanten en (internationale) klanten, complementoren en concurrenten. Snijd het instrumentarium hiervoor toe op de wensen en behoeften van groeibriljanten: snel, flexibel en efficiënt. De raad denkt hierbij aan flexibele arrangementen zoals 'open innovatie'-omgevingen en regionale groeiversneller programma's.*

GROEI AWARENESS

Veel geïnterviewden gaven aan dat een mogelijke toename van incidenten, al dan niet met een boete voor datalekken als gevolg, zullen zorgen voor een groei van de cybersecurity-sector. Toenemende *awareness* bij bestuurders en toezichthouders als gevolg van incidenten, zal de vraag naar cybersecurity-producten en -diensten doen toenemen.

ONTWIKKELING DOMEINEN

In ons onderzoek zijn op verschillende momenten binnen de cybersecurity-sector bepaalde producten of diensten, of categorieën van producten of diensten genoemd, waarvan de

respondenten de komende tijd veel verwachten. De meest genoemde producten zijn geplot op de NCSRA-indeling uit hoofdstuk 2.

Tabel 11 Groeidomeinen binnen de cybersecurity-sector

NCSRA-indeling	Voorbeelden
Identity, privacy and trust management	Authenticatie/ autorisatie-producten Secure communication (bv. VPN, Encryptie van communicatie)
Attack detection, attack prevention and monitoring	Detectie- / Monitoringdiensten / SIEM Detectieproducten (virusscanners / IDS) Preventiediensten (PEN-Testen / ethical hacking)
Forensics and incident management	CERT / Incident & Response Management
Data, Policy & Access Management	Cybersecurity binnen hostingdiensten (cloud) Juridisch advies rondom data-opslag 'Outsourced' Security Management Awareness / Opleiden, trainen & oefenen
Secure Design and Engineering	Beveiliging rondom SCADA/ PCS Internet of Things Security

Met name de "managed services", waarbij een dienstverlener een aantal taken binnen cybersecurity van een organisatie overneemt wordt als groeidomein geïdentificeerd. Vooral MKB-organisaties, zullen als gevolg van groeiende awareness, zoeken naar aanbieders die niet alleen producten leveren, maar de organisatie ontzorgen. De kosten van cybersecurity-oplossingen kunnen in zo'n model ook over meerdere organisaties worden verdeeld, en komen zo ook binnen handbereik van kleinere organisaties.

Dit zien we ook terug in internationale studies naar de groeikansen voor de cybersecurity-sector. Forbes haalt een onderzoek van Allied Market Research aan, waarin is beschreven dat de wereldwijde managed services markt een omvang van zo'n 30 miljard dollar zal bereiken in 2020, met een gemiddelde jaarlijkse groei van bijna 16% (Forbes, 2015).

5.4 Bedreigingen

BESCHIKBAARHEID GOED GEKWALIFICEERDE MENSEN

Veruit de meest genoemde bedreiging voor de cybersecurity-sector is het verwachte tekort aan goed gekwalificeerd personeel. Dat het tekort vandaag al actueel is hebben we reeds beschreven in paragraaf 2.6.

Maar de komende jaren zal de vraag naar cybersecurity-professionals nog verder toenemen. Het Platform Opleiding, Onderwijs en Organisatie (PLATO) van de Universiteit Leiden heeft een onderzoek naar dit tekort uitgevoerd in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC) van het ministerie van Veiligheid en Justitie. Hierin wordt beschreven dat het aantal zichtbare vacatures momenteel nog bescheiden is, maar dat op basis van de omgevingsanalyse (het maatschappelijk belang en de rol van incidenten nemen toe) wordt verwacht dat de vraag naar Cyber Security Professionals zal stijgen. Het onderzoek stelt: *Enerzijds neemt de urgentie van het inzetten van kennis en kunde op dit terrein toe. Anderzijds wordt het*

cybersecuritydomein steeds meer ook als een organisatievraagstuk gezien en breder opgevat (multidisciplinair) (Plato, 2014).

Uit de studie blijkt dat veel bredere HBO- en WO-opleidingen relevant aanbod van studierichtingen hebben voor de cybersecuritysector, maar dat en er (nog) weinig specialistische cybersecurityopleidingen zijn.

Ook de CSR trok aan de bel naar aanleiding van dit onderzoek en schreef een advies aan de staatssecretarissen van Veiligheid en Justitie en Onderwijs, Cultuur en Wetenschap (CSR, 2015). Alhoewel in de Nationale Cybersecurity Strategie 2 (een brede kabinetsvisie uit 2013) reeds een Taskforce cyber security onderwijs werd aangekondigd, lijkt dit tot op heden nog niet van de grond te komen.

DE THUISMARKT IS KLEIN

Nederland is een relatief klein land, waardoor ook de markt voor cybersecurity-producten en -diensten relatief klein is. Dit maakt het voor Nederlandse bedrijven niet eenvoudig om een behoorlijke schaalgrootte te bereiken. Leveranciers op bijvoorbeeld de Engelse, of nog groter, de Amerikaanse markt, hebben een veel grotere thuismarkt te bedienen en kunnen hierdoor sneller schaalvoordelen bereiken. Omdat schaalgrootte van belang is voor het opbouwen en bijhouden van de laatste inzichten in het cybersecurity-domein, zijn grotere spelers in het voordeel. Nederlandse cybersecurity-bedrijven zoeken in de praktijk snel internationale expansie. Het aantrekken van de benodigde middelen voor die expansie door innovatie startup in cybersecurity blijkt niet altijd eenvoudig.
Wanneer schaalvergroting leidt tot marktmacht, kunnen bedrijven een hogere prijs berekenen dan het efficiënte niveau of minder investeren dan maatschappelijk gezien wenselijk is. De welvaartswinst slaat dan alleen bij producenten neer en komt niet ten goede aan de consument. Een voorbeeld van marktfalen, door marktmacht.

WETGEVING

Op verschillende momenten in het onderzoek en vanuit verschillende hoeken werd gewezen op het feit dat er bedreigingen voor de cybersecurity-sector uitgaan van wet- en regelgeving. Met name de nieuwe wet Wet Computercriminaliteit (WCC III) en de nieuwe Wet op de inlichtingen en Veiligheidsdiensten (Wiv) worden in dit kader zowel bij de kansen als bij bedreigingen genoemd. Ook in de media verschijnen reacties van grote partijen als Google & Microsoft op deze nieuwe wetgeving (RTLZ, 2015). Buitenlandse afnemers van producten of diensten van Nederlandse cybersecurity-bedrijven zouden die bedrijven mogelijk links laten liggen wanneer deze bedrijven werken vanuit Nederland, of beoordelen Nederland als minder aantrekkelijke vestigingsplaats.

Ook zien partijen de ontwikkeling dat Europese landen steeds verder uiteen lopen op het vlak van privacywetgeving als bedreiging voor de cybersecurity-sector. Tot slot ervaren partijen de gevolgen van *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* als beperkend voor de export van goederen. Meer specifiek, op de lijst

van goederen staan sinds begin 2013 ook Internet monitoring systemen en intrusion software. Door opname van de lijst wordt voorkomen dat bedrijven deze systemen verkopen aan landen die op de verboden lijst staan. Echter, verschillende partijen geven ook aan dat de reikwijdte van de maatregelen te breed is, waardoor de cybersecurity-sector minder goed in staat is om kwetsbaarheden te identificeren en op te lossen. Ook hier geldt dat grote partijen als Google en Facebook hebben aangegeven dat hierdoor beperkingen ontstaan op activiteiten als PEN-testen, en delen van informatie over kwetsbaarheden en zogenaamde *bug bounty* programma's (Google, 2015) en (Facebook, 2015).

KOSTEN VAN BEVEILIGING WORDEN TE HOOG

Een bedreiging voor de cybersecurity-sector kan ook worden gevormd door een ontwikkeling waarbij de kosten van connectiviteit (o.a kosten van beveiliging en schade door cyber incidenten) niet meer opwegen tegen de voordelen van het elektronisch zakendoen. Dit scenario wordt bijvoorbeeld geschetst in een rapport van verzekeraar Zurich en een onderdeel van de onafhankelijke Amerikaanse denktank *Atlantic Council*. Alhoewel bij de onderzoeksaanpak wordt aangegeven dat het erg lastig was om betrouwbare gegevens te vinden voor zowel de kosten als de nadelen, wordt in het rapport geschetst hoe de jaarlijkse kosten van cybersecurity in westerse landen nu reeds de jaarlijks voordelen van connectiviteit overstijgen. Acties van overheden, bedrijven, non-gouvernementele zijn nodig om een aantal zwartere scenario's die de onderzoekers schetsen te voorkomen.

De auteurs wijzen erop dat de jaarlijkse voordelen van aansluiting wel weer daarna jaarlijks terugkomen, waardoor de cumulatieve voordelen uiteindelijk nog steeds groter zijn dan de kosten (Atlantic Council, 2015). Dit zou de groei van de cybersecurity-sector kunnen remmen.

DALING AWARENESS

Wanneer de komende jaren er weinig (vooral) grote incidenten zijn, kan de perceptie ontstaan dat de dreiging is gedaald, met als gevolg dat er minder wordt besteed aan cybersecurity. Een dergelijk effect is daarmee niet toe te schrijven aan een bepaald type marktfalen, maar is veel meer een aspect van gedragseconomie.

KENNIS BIJ AFNEMERS

In samenhang met het voorgaande wordt ook gesignaleerd dat het op dit moment nog moeilijk om als afnemer van producten of diensten, zeker een afnemer binnen het MKB, kwaliteit in de markt te herkennen. Hierdoor worden mogelijk minder producten of diensten afgenomen. Standaarden en accreditatie kunnen helpen om marktfalen door deze vorm van asymmetrische informatie op te lossen. In het Verenigd Koninkrijk zijn er accreditatieschema's opgezet voor onder meer *PEN-testen*, *monitoring* en *incident response*. Vanaf oktober 2014, verplicht de Engelse overheid dat inschrijvers op contracten waarin zij in aanraking komen met persoonsgegevens gecertificeerd zijn tegen het *Cyber Essentials scheme* (UK, 2014).

In het kader van voorzitterschap NL EU heeft NCTV aangekondigd 2 speerpunten te hebben: standaardisering & certificering en Ethical hacking (WEF, 2016).

CONCURRENTIE VAN BUITENLANDSE PARTIJEN EN/OF OVERNAMES

De verwachting van verschillende deskundigen is dat de komende jaren het aanbod van cybersecurity-producten en diensten vanuit met name de VS zal groeien. Het gaat daarbij bijvoorbeeld monitoring (SIEM) van infrastructuren en netwerken. Deze partijen hebben vaak een veel grotere schaalgrootte en beschikken over relatief veel kapitaal. Hiermee concurreren is bijna onmogelijk voor Nederlandse bedrijven, en zeker innovatieve startups. Schaalgrootte hebben we hierboven reeds genoemd als mogelijk indicatie van marktfalen.

Ook zien we dat succesvolle startups in de cybersecurity-sector snel door grotere buitenlandse aanbieders en investeerders worden opgepikt. Voorbeelden van jonge Nederlandse bedrijven die recent zijn overgenomen zijn bijvoorbeeld Surfright (opgericht in 2006) dat is ingelijfd door Sophos en het 4 jaar oude Authasas dat is overgenomen door het Britse Micro Focus (Nu.nl, 2016) en (FD, 2015-2).

Een negatief gevolg van veel overnames is dat de horizontale markt meer geconcentreerd raakt en de prijzen stijgen. In plaats daarvan kunnen deze bedrijven eerst ook een lagere prijs berekenen, waarmee ze concurrerende bedrijven van de markt kunnen uitsluiten, waardoor de concentratie nog hoger wordt. Een voorbeeld van marktfalen door marktmacht. Voordeel van een toename van overnames is wel dat de aantrekkelijkheid van de sector voor ondernemers toeneemt, waardoor ook het aantal ondernemingen waarschijnlijk zal toenemen.

5.5 Conclusie

Kijkend naar de kansen maar vooral de bedreigingen, gecombineerd met de groeiverwachtingen van de sector zelf, zien we de meeste aanknopingspunten aan de rechterkant van Afbeelding 11: de sector zal blijven groeien. Ook de ICT-aanbieders verwachten dat de omzet van cybersecurity-producten en -diensten de komende jaren nog verder zal groeien (zie paragraaf 3.5).

Of we vervolgens naar boven of beneden in Afbeelding 11 bewegen, hangt af van de mate waarin de structurele kenmerken (arbeid, kapitaal en technologie) zich ontwikkelen: zal er sprake zijn van (toenemend) falen, of komt het aanbod van cybersecurity-producten en -diensten op het niveau van de vraag. Kijkend naar de bedreigingen zien we dat de experts verwachten dat het tekort aan hoog opgeleide specialisten en de beperkte toegang tot durfkapitaal en de komende 3-5 jaar zullen blijven bestaan. Daarnaast is schaalgrootte een aantal malen door de experts genoemd als belangrijk element voor aanbieders van cybersecurity-producten en -diensten, ten einde steeds voldoende informatie over dreigingen te hebben. Wanneer aanbieders met een bepaalde schaalgrootte aldus veel voordelen hebben ten opzichte van kleinere aanbieders is ook sprake van een vorm van marktfalen.

6 CONCLUSIES EN SUGGESTIES

6.1 Conclusies

Nederland heeft de ambitie om voorop te lopen in de ontwikkeling naar een steeds meer digitaliserende economie. Op veel ranglijsten staat Nederland al hoog, als het gaat om de mate van digitalisering van de economie. Echter, een grote mate van digitalisering creëert op hetzelfde moment een grote afhankelijkheid van goed werkende en veilige technologie.

Voor het vasthouden en mogelijk versterken de digitale economie is vertrouwen -in die digitale economie- een belangrijke randvoorwaarde. Het zorgen van vertrouwen in de digitale economie is het onderwerp van de cybersecurity-sector.

Er is al veel onderzoek gedaan naar het belang van de ICT-sector. Zowel naar de omvang van de sector zelf, als naar de rol die ICT speelt voor andere sectoren en de economie als geheel. Maar hoe groot is nu die Nederlandse cybersecurity-sector? Voor het antwoord op deze vraag zijn nog weinig objectieve gegevens beschikbaar. Dit rapport schetst het resultaat van het eerste onafhankelijk onderzoek naar de omvang van de sector.

In dit onderzoek hanteren wij een enge afbakening van het begrip cybersecurity. Deze afbakening is gekozen om het onderzoek binnen de gestelde kaders (tijd en geld) beter haalbaar te maken. Daarnaast zien we dat wanneer in het dagelijks spraakgebruik de term cybersecurity wordt gebruikt, men ook een wat smallere interpretatie kiest.

Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT als gevolg van moedwillige activiteiten in het Cyberdomein en, indien er toch schade is ontstaan, het herstellen hiervan.

Omdat volgens de definitie van cybersecurity, het object ICT betreft, zien we dat vooral de ICT-sector zelf een groot aandeel heeft in het totaal van de activiteiten. Denk aan het leveren van ICT-diensten en -producten. Cybersecurity-activiteiten reiken echter verder dan alleen de ICT-sector. Ook vanuit andere sectoren wordt door het aanbieden van diensten en producten een bijdrage aan cybersecurity geleverd.

Uit onderzoek naar de oorsprong en aard van moedwillige activiteiten (met schade door verstoring, uitval of misbruik van ICT als gevolg) blijkt dat het zwaartepunt van de oorsprong van dreigingen ligt bij criminele organisaties en statelijke actoren.

Met het toenemen van enerzijds dreigingen en anderzijds het belang van ICT is er ook een economische sector ontstaan die gebruikers met cybersecurity-producten en -diensten bescherming biedt tegen de aanvallen en helpt bij het herstellen van schade.

De cybersecuritysector creëert toegevoegde waarde door het aanbieden van producten en diensten die de cyberrisico's proberen te verminderen en schade efficiënt herstellen. De rest van de economie betaalt voor deze producten en diensten en profiteert ervan.

Middels een enquête is de omvang van de Nederlandse cybersecurity-sector binnen de ICT-sector bepaald. Uit de enquête blijkt dat in 2014 ongeveer 10 procent van de omzet binnen de ICT-sector gekoppeld was aan cybersecurity-activiteiten.

Dit aandeel cybersecurity is gebruikt om de totale omzet, omzet uit export, toegevoegde waarde en werkgelegenheid te bepalen binnen de ICT-sector. Hiervoor zijn ook microstatistieken van het CBS gebruikt. In onderstaande tabel staan de belangrijkste uitkomsten.

Tabel 12 De toegevoegde waarde van cybersecurity binnen de ICT-sector bedroeg in 2014 ongeveer € 4 miljard tegenover € 2,5 miljard in 2010.

Omvang cybersecurity in Nederland	2010 Hoofd ICT-activiteit	2010 Alle ICT-activiteiten	2014 Hoofd ICT-activiteit	2014 Alle ICT-activiteiten
Omzet (€ mld.)	€ 4,3	€ 4,8	€ 6,9	€ 7,5
Toegevoegde waarde (€ mld.)	€ 2,3	€ 2,6	€ 3,8	€ 4,1
% van het BBP	0,36%	0,41%	0,57%	0,62%
Omzet uit export (€ mld.)	€ 1,3	€ 1,5	€ 2,6	€ 2,8
Werkgelegenheid (fte, x1000)	12,0	13,5	15,7	17,1

Bron: VKA/SEO Economisch Onderzoek; Euro's in basisprijzen. Twee meetwaarden: 'hoofd ICT' is gebaseerd op de SBI-codes van bedrijven en 'alle ICT' is gebaseerd op alle activiteiten die bedrijven rapporteerden.

In de periode 2010-2014 is de omzet en de toegevoegde waarde betreffende cybersecurity binnen de ICT-sector jaarlijks met 14,5 procent toegenomen. In 2014 lag de omzet tussen € 6,9 en € 7,5 miljard. De toegevoegde waarde van de cybersecurity-sector was € 3,8 á 4,1 miljard in datzelfde jaar. In 2010 hebben bedrijven die cyberactiviteiten uitvoeren met ongeveer 0,4 procent bijgedragen aan het Nederlandse BBP. In 2014 is dit percentage gestegen tot ongeveer 0,6 procent. De cybersecurity-sector groeide daarmee veel sneller dan de ICT-sector zelf.

De benaderde ICT-bedrijven in de enquête verwachten een jaarlijkse groei van omzet uit cybersecurity-activiteiten van ongeveer 7 procent.

Conclusie is dat de Nederlandse cybersecurity-sector een relevante omvang heeft en bovendien snel groeiend is.

Een precieze meting van de waarde van cybersecurity (de uitstralingseffecten van de cybersecurity-sector) voor de economie als geheel blijkt lastig. Door te kijken naar incidenten en de omvang van de schade, kan een schatting van de waarde worden gemaakt. Voor de analyse incidenten en de omvang van de schade zijn verschillende bronnen gebruikt, namelijk studies, statistieken en een mediasearch via LexisNexis, een databank met archieven van bijna 10.000

dagbladen en tijdschriften. Echter, er gelden een aantal beperkingen bij het analyseren van incidenten en schade. Een daarvan is het reeds genoemde ontbreken van de eenduidige definitie van cybersecurity-incidenten. Daarnaast zijn meetmethoden vaak niet transparant en de data is onvolledig en niet te vergelijken. Voor nadere analyses is er een systematische verzamel- en aggregatiemethode nodig. Vanwege deze beperkingen bleek het niet mogelijk om harde conclusies te trekken over de waarde van cybersecurity. Enkele cijfers zijn wel beschikbaar.

Volgens PWC (2015) is 23 procent van bedrijven de laatste 24 maanden geconfronteerd met cybercrime. In de rest van de wereld ligt het percentage van bedrijven op negen procent. Het Nederlandse bedrijfsleven komt vooral in aanraking met phishing, virussen en hacken. In Nederland raakt cybercrime handel, financiële instellingen en de ICT-sector het meest. Betrouwbare informatie bleek beschikbaar voor de financiële sector, en dan vooral rondom online bank- en pasfraude (ECB-rapporten). De schade daar in 2014 wordt geraamd om ruim 2 duizend euro per 1000 inwoners, en is de afgelopen jaren dalend.

De Nederlandse overheid is vooral slachtoffer van informatielekkage (NCSC, 2015). Bij consumenten zijn volgens de veiligheidsmonitor van het CBS (Eurostat, 2016), de meest voorkomende cyberincidenten virussen, misbruik van persoonlijke gegevens, financiële verliezen en ongepaste websites voor kinderen. In de afgelopen jaren is het aandeel virussen flink gedaald in Nederland en het percentage ligt onder het Europese gemiddelde. Maar volgens de monitor zijn Nederlandse consumenten voorzichtiger dan het Europese gemiddelde met online winkelen, online bankieren of het zetten van hun mobiele toestellen op een wifi-netwerk.

Met behulp van de input van een 30-tal deskundigen (middels interviews en ronde tafels) uit de sector, hebben we een analyse gemaakt van de sterkten en zwakten, en kansen en bedreigingen van de Nederlandse cybersecurity-sector.

Analyse Nederlandse cybersecurity-sector	
Sterkten	***Zwakten***
• Verregaande digitalisering geeft relatief sterke/volwassen (systeem van bedrijven) in Cybersecurity-sector • Goede reputatie • Politiek, neutrale wet en regelgeving, toezicht • ISAC's: goede samenwerking binnen ISAC's en met NCSC • Goed informaticaonderwijs • Ligging, cultuur en ondernemersklimaat	• Onvoldoende specialisten/beschikbaarheid goed gekwalificeerde mensen • Investeringen en toegang tot (durf) kapitaal • Uitwisseling en samenwerking wetenschap, bedrijfsleven en overheid • Beperkt georganiseerd • Nederland vooral diensten en groothandel, minder schaalbaar

Kansen	***Bedreigingen***

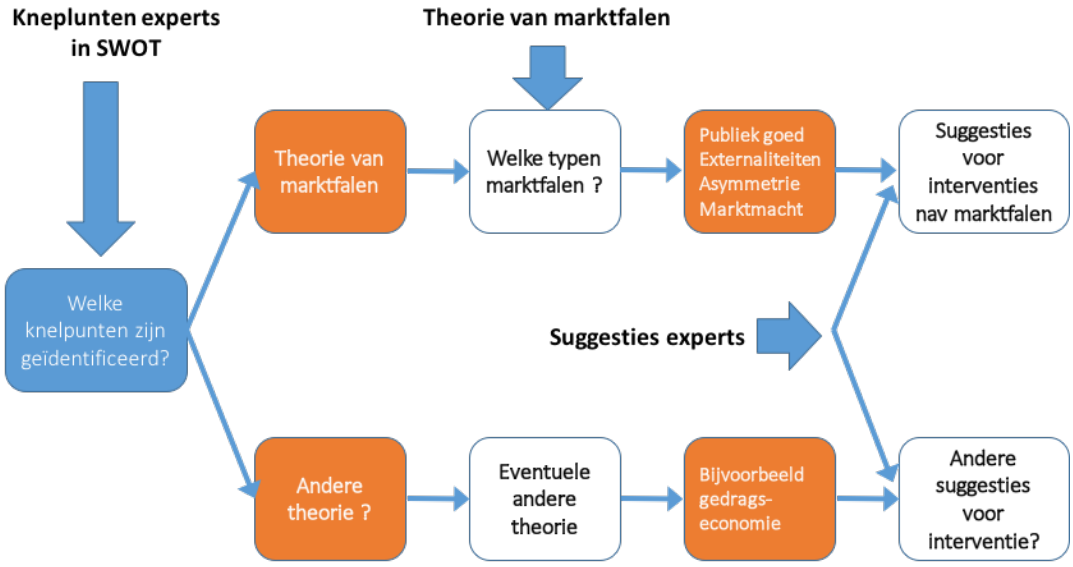
• Doorontwikkeling van de Nederlandse cybersecurity aanpak • Wetgeving • Betere uitwisseling bedrijfsleven-wetenschap • Groei awareness • Ontwikkeling domeinen	• Beschikbaarheid goed gekwalificeerde mensen • De thuismarkt is klein • Wetgeving • Kosten van beveiliging worden te hoog waardoor deze niet meer opwegen tegen de voordelen van gebruik digitale middelen. Met name voor MKB • Daling awareness • Kennis bij afnemers • Concurrentie van buitenlandse partijen en/of overnames

Doordat het niet mogelijk is om harde conclusies te trekken over de huidige waarde van cybersecurity, is het ook niet goed mogelijk om aan te geven welk potentieel gehaald kan worden, of dat er daadwerkelijk sprake is van marktfalen. Echter, bij de gesignaleerde knelpunten zijn in het onderzoek wel suggesties naar voren gebracht voor de aanpak van die knelpunten. In de volgende paragraaf analyseren vertalen we de sterkten, zwakten, kansen en bedreigingen naar maatregelen die genomen kunnen worden om de cybersecurity-sector in Nederland verder te ondersteunen.

6.2 Van knelpunten naar suggesties voor beleid

Bij het analyseren van de suggesties voor beleid is gekeken of er bij de gevonden knelpunten in de SWOT mogelijk sprake is van marktfalen (er gaat, ondanks de groei van de sector, iets mis in de markt) of andere knelpunten (bijvoorbeeld gedragsproblemen) bestaan. In onderstaand denkkader is het analyse-proces afgebeeld waarmee vanuit knelpunten, via mogelijk marktfalen, suggesties voor beleid kunnen worden gedaan.

Afbeelding 12 Denkkader voor analyse suggesties



Als markten taken niet efficiënt kunnen uitvoeren, is er sprake van marktfalen. Er kunnen vier soorten marktfalen worden onderscheiden met betrekking tot cybersecurity-producten en -diensten: [12]

1. Publieke goederen, zoals veiligheid;
2. Positieve externe effecten (externaliteiten), met name netwerkeffecten en kennis-spillovers;
3. Asymmetrie van informatie, namelijk adverse selectie in de kapitaalmarkt en onvoldoende informatie voor consumenten;
4. Marktmacht, vooral vanwege schaalgrootte, institutionele belemmeringen en padafhankelijkheid, en het hold-up probleem in de arbeidsmarkt.

In bijlage E zijn de verschillende typen marktfalen nader uitgewerkt.

Bij de volgende punten uit de analyse van sterkten, zwakten, kansen en bedreigingen zagen we aanknopingspunten voor marktfalen:

Tabel 13 Samenvatting knelpunten en marktfalen

Kenmerk	Omschrijving	Type mogelijk marktfalen
Zwakte / Bedreiging	Onvoldoende specialisten / Beschikbaarheid goed gekwalificeerde mensen	Asymmetrie van informatie/gedragsprobleem
Zwakte	Betere uitwisseling bedrijfsleven-	Positieve externaliteiten (kennis-

12 Voor een overzicht van marktfalen, zie bijvoorbeeld Baarsma & De Nooij (2006), Saline (2000).

	wetenschap (innovatie)	spillovers)
Zwakte	Betere uitwisseling bedrijfsleven-wetenschap (ecosystemen)	Marktmacht (padafhankelijkheid) Positieve externe effecten (netwerkexternaliteiten)
Zwakte	Beperkte toegang tot (durf) kapitaal	Asymmetrie van informatie (adverse selectie in de kapitaalmarkt)
Zwakte	Nederland vooral diensten en groothandel, minder schaalbaar	Marktmacht (schaalgrootte)
Kans	Doorontwikkeling van de Nederlandse cybersecurity aanpak	Asymmetrie van informatie
Bedreiging	Thuismarkt is klein	Marktmacht (schaalgrootte)
Bedreiging	Concurrentie van buitenlandse partijen en/of overnames	Marktmacht (schaalgrootte en fusies en overname)
Bedreiging	Kennis bij afnemers	Asymmetrie van informatie

Kenmerk	**Omschrijving**	**Ander type probleem**
Bedreiging	Awareness	Gedragsprobleem

Meer onderzoek is nodig om te bepalen of de hiervoor genoemde soorten marktfalen ook "hard" aantoonbaar zijn. Het identificeren ervan door de experts is een indicatie voor het bestaan.

Bij een aantal punten uit de analyse van sterkten, zwakten, kansen en bedreigingen zien we minder sterke aanknopingspunten om te spreken van marktfalen.

6.3 Suggesties voor beleid

De suggesties in deze paragraaf zijn, net als de analyse van sterkten, zwakten, kansen en bedreigingen gebaseerd op ons inzicht in de markt en de input van een 30-tal deskundigen (middels interviews en ronde tafels) uit de sector. Zie bijlage B voor een overzicht van geïnterviewden en deelnemers aan de ronde tafels. De input van de deskundigen was een lange lijst met suggesties, welke met bovenstaand kader door de onderzoekers geanalyseerd. De suggesties richten zicht direct op de cybersecurity-sector, die hierdoor (nog) sterker zou kunnen worden. Aan het eind van deze paragraaf geven we in een tabel weer hoe de gedane suggesties samenhangen met de knelpunten waarbij sprake is van mogelijk marktfalen of ander type problemen. Wanneer een bjdrage kan worden geleverd aan het oplossen/verminderen van een bepaald marktfalen, kan de bijdrage van de sector aan de economie groeien. Zoals eerder gesteld bleek het binnen de kaders van deze studie niet goed mogelijk de waarde van een sterke cybersecurity-sector voor andere economische sectoren aan te tonen.

De suggesties zijn onderverdeeld in een aantal thema's, zoals hieronder afgebeeld. Daarnaast is er een aantal suggesties die zich richten op het verkrijgen van een beter inzicht in de cybersecurity-sector, het thema "meten is weten".

Afbeelding 13 Suggesties in thema's

Hieronder lichten we de thema's toe.

EXPERTS EN EXPERTISE

In het thema *Experts en expertise*, is een aantal suggesties opgenomen die inzetten op het gesignaleerde tekort aan hoog opgeleide experts, en op welke wijze onderzoek beter benut kan worden. De cybersecurity-sector is sterk gedreven door innovatie, waarbij onderzoek en kennisuitwisseling met de wetenschap nodig is om nieuwe producten en diensten te bieden die passen bij de steeds ontwikkelende cyberdreigingen.

Mogelijk dat een onderliggende oorzaak voor het tekort aan hoog opgeleide experts ligt bij de aantrekkingskracht van het vak cybersecurity op aankomende studenten. Overigens is cybersecurity nog een relatief jong vak dat, zoals we hebben gezien in hoofdstuk 3, snel is gegroeid, waardoor er nu een tekort wordt gesignaleerd, maar dat dit de komende jaren mogelijk kan worden opgelost.

Een aantal van de gedane suggesties zouden bij uitvoering moeten worden opgepakt in samenwerking met andere partijen. De belangrijkste partij is steeds achter de aanbeveling opgenomen. Onder dit thema vallen een aantal suggesties die met het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) zouden kunnen worden opgepakt.

De volgende suggesties vallen onder dit thema:

1. Verken de meerwaarde van de inrichting van een Nationaal instituut voor Cyber Security, en hoe dit tot stand zou kunnen komen. Het instituut bundelt kennis van universiteiten waar deze nu over verschillende instellingen is verspreid (samen met OCW).

2. Verken of het stimuleren van onderzoek & onderwijs rondom cybersecurity op bestaande instellingen voor hoger en wetenschappelijk onderwijs meerwaarde op kan leveren. (samen met OCW).
3. Werk actief aan het stimuleren van ecosystemen rondom cybersecurity. Investeer in de aansluiting van onderzoek en onderwijs bij het bedrijfsleven (valorisatie), zodat de kennis ook beter kan renderen. (samen met OCW).
4. Verken op welke wijze bedrijven ondersteund kunnen worden wanneer zij investeren in (speur- en ontwikkelingswerk naar) cybersecurity.
5. Verken op welke wijze de uitstroom van studenten (middelbaar, hoger en wetenschappelijk onderwijs) in cybersecurity kan worden vergroot (vergroten aanbod en/of stimuleren van het kiezen voor een opleiding in cybersecurity. (samen met OCW).

GEEF GOEDE VOORBEELD

Bij het thema *Geef goede voorbeeld*, is een aantal suggesties opgenomen die vooral betrekking hebben op de overheid zelf. Onder dit thema vallen de volgende suggesties:

6. Heroverweeg de mogelijkheid voor een centrale overheids Security Operation Center (SOC), die als een Shared Services Center de diensten aanbiedt voor verschillende overheidsorganisaties. Primair departementen, maar mogelijk ook breder binnen de overheid. Bij deze aanbeveling past ook de suggestie om de inkoop van de overheid op het domein van cybersecurity meer te bundelen. In beide gevallen leidt bundeling tot kennisopbouw en inzicht in de laatste ontwikkelingen in de markt of zelfs het "uitdagen" van de sector. Deze uitdaging kan leiden tot innovatie aan aanbiederszijde. De overheid fungeert dan als launching customer (samen met verschillende andere departementen, of nog breder binnen de overheid).
7. Verken op welke wijze (bijvoorbeeld binnen overheidsaanbestedingen) meer ruimte kan worden gegeven aan innovatieve partijen. Het domein van cybersecurity vraag snelheid in de ontwikkeling van producten en diensten, dat betekent in de praktijk dat enerzijds de eisen aan de onderneming lager moeten kunnen liggen en anderzijds in specifieke gevallen de aanbestedingsdrempel hoger zou moeten liggen. (samen met EU).
   Doordat de overheid aan **aanbestedingsprocedures** is gehouden ontstaan mogelijk inefficiënties. Enerzijds kunnen de kosten van compliance-kosten van wetgeving en regulering hoger zijn dan de gerealiseerde efficiëntiewinsten van overheidsingrijpen (SER, 2010). Anderzijds is er mogelijk sprake van marktmacht, aangezien grotere gevestigde partijen meer middelen tot hun beschikking hebben om (slim) in te schrijven op aanbestedingen.
8. Ontwikkel een **voorlichtingscampagne** waarin de sterkten en kansen van de Nederlandse cybersecurity-sector voor ambassades en exportbevorderende instanties helder uiteen worden gezet. De Nederlandse uitgangspositie rondom onderwerpen als privacy kan op die manier nog beter worden uitgelegd. (samen met o.a RVO, ministerie van BuZa)

CONNECT, COMMIT & GO FOR IT!

In dit cluster hebben we een aantal suggesties opgenomen die vooral betrekking hebben op het in verbinding brengen van initiatieven, hier vervolgens focus op leggen en de noodzakelijke acties uitvoeren, indien nodig voorzien van financiering. Het Amerikaanse Cybersecurity National Action Plan kan hierbij als voorbeeld dienen. Het gaat om de volgende suggesties:

9. Geef veel prioriteit (en zo mogelijk financiële ruimte) aan de doorontwikkeling van de Nederlandse cybersecurity aanpak. De doorontwikkeling kan zorgen voor een planmatige aanpak, over kabinetsperiodes heen. Op deze manier kan een brede aanpak ontstaan en is er aandacht voor zowel de bedreigingen van cybercrime als economische kansen. (samen met o.a V&J).
10. Zorg voor de toename van het bewustzijn rondom cybersecurity. Door veel aandacht te besteden aan het onderwerp zal de vraag naar producten en diensten verder toenemen, en Nederlandse thuismarkt voor cybersecurity-aanbieders doen groeien. Initiatieven zoals veiligbankieren.nl en veiliginternetten.nl helpen om ook consumenten/eindgebruikers veilig gebruik te laten maken van het internet.
11. Verken de mogelijkheid van het vormen van een zogenaamde "valley". In navolging van de beweging die bijvoorbeeld is gezien rondom biotech, biedt de clustering van cybersecurity-organisatie (zowel publiek als privaat) een plaats voor de ontwikkeling van kennis en groei. Clustering en consortiumvorming zorgt voor groei. Inspiratie kan worden gevonden bij het Institute for Information Security & Privacy zoals dat onder het Amerikaanse Georgia Tech is gevormd. Bij dit instituut werken alleen al 2.000 ambtenaren. Maar ook in Israël is een campus opgericht, waarbij in publiek-private samenwerking veel geld is geïnvesteerd. The Hague Security Delta (HSD), de Cyber Security Academy (CSA), het European Cybercrime Centre van de Europese Commissie en het European Network for Cyber Security zijn reeds in de regio Den Haag gevestigd.
12. Verken of en hoe het ter beschikking stellen van meer financiële middelen voor onderzoek en ontwikkeling en opstartfase de cybersecurity-sector kan helpen sneller te groeien. Hierbij kan gedacht worden aan directe instrumenten zoals subsidies (verruiming regels WBSO, TKI-toeslag), onderzoeksopdrachten of experimenten waarbij de nadruk op innovatie en ontwikkeling komt te liggen, of uitbreiding van bestaande instrumenten als de regeling MKB-innovatiestimulering Regio en Topsectoren (MIT) en SBIR. De inrichting van een specifiek cyber-investeringsfonds, (al dan niet in publiek-private samenwerking) kan de lastige toegang tot durfkapitaal mogelijk wegnemen.

WET & REGELGEVING

Dit cluster bevat suggesties waarbij vanuit wet- en regelgeving aan de cybersecurity-sector kan worden bijgedragen. De volgende suggesties vallen onder dit thema:

13. Houdt vast aan **wet- en regelgeving** die bijdraagt aan de privacy van internetgebruikers. Het kabinetsstandpunt rondom encryptie is daar een goed voorbeeld van. (samen met V&J)
14. Zorg voor heldere en **voorspelbare interpretatie** van wet- en regelgeving. Met name rondom de meldplicht datalekken, wordt gemist dat het niet mogelijk is om op voorhand situaties aan

de autoriteit voor te leggen, zodat duidelijk wordt of getroffen beveiligingsmaatregelen afdoende zijn. Meer duidelijkheid en een mogelijkheid om een "ruling" op voorhand te verkrijgen over een bepaalde (beveiligings)oplossing, zouden kansen kunnen betekenen voor de Nederlandse cybersecurity-sector. (samen met V&J).

15. Verken de mogelijkheden van de ontwikkeling van een accreditatie-schema voor cybersecurity-diensten en producten. In het Verenigd Koninkrijk lijkt een dergelijk schema een bijdrage aan de lokale cybersecurity-sector te leveren. In Amerika is binnen het FedRAMP-programma, een accreditatie-orgaan ingesteld dat de veiligheid van cloud-diensten beoordeeld. Ook middels convenanten of gedragscodes kan bij leveranciers aandacht voor cybersecurity worden gestimuleerd, zodat meer waarborgen ontstaan rondom *privacy by design* en *security by design*. (samen met CIO-rijk)
    De introductie van een accreditatie-schema kan een bijdrage leveren aan het oplossen van asymmetrische informatie. Immers wanneer afnemers van cybersecurity-producten of diensten niet goed in staat zijn de kwaliteit van aanbieders in te schatten, worden mogelijk minder, of kwalitatief mindere producten afgenomen.
16. Verken hoe de overheid (uiteraard passend binnen Europese aanbestedingsregels) Nederlandse producten vaker de **voorkeur** kan geven, ontstaan kansen voor de cybersecurity-sector. Een van de geïnterviewde gaf aan dat de Duitse regering in haar regeerakkoord (net na onthullingen Snowden) incentives heeft opgenomen voor de cybersecurity-wereld. Duitse bedrijven die zich bezig houden met cybersecurity genieten de voorkeur ten opzichte van buitenlandse concurrenten. Ter illustratie: Op 16 oktober 2015 heeft het Duitse Parlement een nieuwe dataretentiewet aangenomen (Privacynieuws, 2015). In de wet is opgenomen dat de data in Duitsland moet worden opgeslagen. Dit betekent dat aanbieders van telecommunicatiediensten ofwel zelf infrastructuur in Duitsland moeten opzetten, of een lokale aanbieder moeten gebruiken. Een dergelijk model zal ook de lokale aanbieder van beveiligingsproducten helpen. Daarnaast zouden centrale en decentrale overheden een forse impuls kunnen geven aan de innovatiekracht in het algemeen en die van de cybersecurity-sector in het bijzonder, door meer ruimte te bieden aan nieuwe technologieën en concepten. In een brief aan de Tweede Kamer roept StartupDelta de overheden op om aanbestedingsprocedures beter in te richten op innovatieve oplossingen (StartupDelta, 2016).
17. Ondersteun initiatieven om de **versnippering** van de Europese privacy-wetgeving te beperken.

METEN IS WETEN

Dit cluster bevat suggesties gericht op het beter in beeld krijgen van de cybersecurity-sector en de schade als gevolg van cyberincidenten.

18. Ondersteun de ontwikkeling van een heldere **definitie** van cybersecurity-incidenten.
19. Ondersteun de ontwikkeling van transparante en systematische **verzamel- en aggregatiemethodes** voor informatie over de cybersecurity-sector en cybersecurity-incidenten.

6.4 Koppeling suggesties met knelpunten

In onderstaande tabel zijn de knelpunten uit de analyse van sterkten, zwakten, kansen en bedreigingen, gekoppeld aan de hiervoor genoemde suggesties. Voor sommige knelpunten zijn meerdere suggesties gedaan, en andersom, sommige suggesties dragen mogelijk bij aan het oplossen van meerdere knelpunten.

Tabel 14 Koppeling suggesties met knelpunten en marktfalen

Kenmerk	Knelpunt	Suggesties
Zwakte / Bedreiging	Onvoldoende specialisten / Beschikbaarheid goed gekwalificeerde mensen	1, 2, 3, 5, 11
Zwakte	Betere uitwisseling bedrijfsleven-wetenschap (innovatie)	1, 2, 3, 11
Zwakte	Betere uitwisseling bedrijfsleven-wetenschap (ecosystemen)	1, 2, 3, 11
Zwakte	Beperkte toegang tot (durf) kapitaal	2, 4, 12
Kans	Doorontwikkeling van de Nederlandse cybersecurity aanpak	6, 9
Bedreiging	Thuismarkt is klein	10
Bedreiging	Concurrentie van buitenlandse partijen en/of overnames	2
Bedreiging	Kennis bij afnemers	6, 15

Kenmerk	Omschrijving	Ander type probleem
Bedreiging	Awareness	10

Uit deze tabel blijkt dat een aantal van de suggesties goed aansluiten op de geconstateerde knelpunten (met marktfalen). De overige suggesties hebben betrekking op andere knelpunten, met mogelijk verscheidene oorzaken. Deze suggesties hebben mogelijk meer betrekking op de kansen voor de ondernemers in cybersecurity-sector zelf dan dat het gaat om welvaartsverlies. In onderstaande tabel zijn die suggesties opgenomen.

Tabel 15 Koppeling suggesties met knelpunten en marktfalen

Suggestie	Omschrijving
7	Aanbestedingsprocedures en innovatie
8	Voorlichtingscampagne
13	Wet- en regelgeving
14	Voorspelbare interpretatie
16	Lokale voorkeur
17	Beperk versnippering

Suggesties 18 en 19 (definitie en verzamel- en aggregatiemethodes) hebben weer een ander karakter en zien op het beter meetbaar maken van de cybersecurity-sector en cybersecurity-incidenten.

A Bronnen

- ABI Research (2014). Global Cybersecurity Index.
- Acemoglu, D.T. (1996). A microfoundation for social increasing returns in human capital accumulation. Quarterly Journal of Economics, 61: 779–804.
- ACM (2016). Telecommonitor Q4 2015. Den Haag.
- Adviesraad voor het Wetenschaps- en Technologiebeleid (AWT) (2014) Briljante bedrijven, Effectieve ecosystemen voor ambitieuze ondernemers. Den Haag.
- Akerlof, G. (1970). The Market for “Lemons”: Quality Uncertainty and the Market Mechanism, Quarterly Journal of Economics, 83(4): 488-500.
- Anderson R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. en Savage, S. (2013). Measuring the cost of cybercrime. In Böhme, R. (ed): The Economics of Information Security and Privacy. Springer.
- Arthur, B. (1989). Competing Technologies, Increasing Returns, and Lock-In by Historical Events, Economic Journal 99: 116-131.
- Atlantic Council (2015). Risk Nexus: Overcome By Cyber Risks?
- Baarsma, B. & M. de Nooij (2006). Calculus van het publiek belang op de elektriciteitsmarkt, SEO-rapport nr. 885, Amsterdam.
- Baarsma, B., Noll, R. van der en Rougoor, W. (2013). Nieuws en markt. SEO-rapport nr. 2013-53. SEO: Amsterdam.
- Betaalvereniging Nederland (2014). Jaarverslag 2014. Amsterdam.
- Bijlsma, M., De Bijl, P. & Kocsis, V. (2009). Competition, innovation and intellectual property rights in software markets. Communications & Strategies, 74, 55-74.
- Brennenraedts et al. (2014). De impact van ICT op de Nederlandse economie. Dialogic-rapport 2014.062-1430.
- Bruyn, S. de, Korteland, M., Markowska, A., Davidson, M., Jong, F. de, Bles, M. en Sevenster, M. (2010). Handboek schaduwprijzen. CE Delft, 10 7788 25.
- Centraal Bureau Statistiek (CBS) (2015a). Korte onderzoeksbeschrijving veiligheidsmonitor (vanaf 2012). Den Haag
- Centraal Bureau Statistiek (CBS) (2015b). Slachtofferschap cybercrime en internetgebruik. Den Haag.
- Centraal Bureau Statistiek (CBS) (2015c). Veiligheidsmonitor 2014. Den Haag.
- Centraal Bureau Statistiek (CBS) (2014). Veiligheidsmonitor 2013. Den Haag.
- Centraal Bureau Statistiek (CBS) (2013). Veiligheidsmonitor 2012. Den Haag.
- Centraal Planbureau (2015). Determinanten van internetveiligheid: een empirische analyse van DDoS aanvallen. CPB Discussion Paper 306 | 29‑04‑2015
- Cyber Security Raad (CSR (2015). Advies aan de staatssecretarissen van Veiligheid en Justitie en Onderwijs, Cultuur en Wetenschap inzake cybersecurity in het onderwijs en het bedrijfsleven.
- Dcypher (2016). Persbericht: IIPVV wordt dcypher.

- De Nederlandsche Bank (DNB) (2014). Krijgt een slachtoffer van skimmen een vergoeding? DNB: Amsterdam.
- De Nederlandsche Bank (DNB) (2015). Maatschappelijk Overleg Betalingsverkeer. Rapportage aan de Minister van Financiën. DNB: Amsterdam.
- Dijk, R. van, Holt, D., Veen, F, van der, Gibcus, P. en Span, T. (2015). Financiering innovatief MKB in RIS 3-sectoren in de Noordvleugel.
- Dutch Digital Delta (2016). Nieuws. https://www.dutchdigitaldelta.nl/nieuws/barthel-blijven-investeren-in-cyber-security-r-d?utm_source=e-mailnieuwsbrief&utm_medium=email&utm_campaign=AWTI+e-mail+alert geraadpleegd februari 2016.
- E-CRIME (2015). D6.1 Report on model development and adequacy of existing models and data. Deliverable submitted on 30 November 2015 in fulfillment of the requirements of the FP7 project, E-CRIME Economic Impact of Cyber Crime.
- Ernst & Young (2011). Groeien door Veiligheid.
- European Digital Forum (EDF) (2016), The 2016 Startup Nation Scoreboard 2016
- Eurostat (2010). Security incidents and consequences.
- Eurostat (2016). 1 out of 4 internet users in the EU experienced security related problems in 2015. Eurostat Newsrelease, 9 februari 2016.
- EZ et al.; Ministerie van Economische Zaken, Centraal Bureau Statistiek, en TNO (2015). ICT, Kennis en Economie 2015. Den Haag.
- EZ (2013). Beleidsbrief Doorbraken met ICT – het benutten van de economische kansen van ICT.
- EZ (2015). Ruimte voor vernieuwing door toekomstbestendige wet- en regelgeving.
- Facebool (2015). Wassenaar rules are not the right direction.
- Fafinski, S., Dutton, W. H. en Margetts, H. (2010). Mapping and Measuring Cybercrime. Oxford Internet Institute. OII Forum Discussion Paper No 18.
- Financieel Dagblad (2015). Innovatie Nederland raakt achterop.
- Financieel Dagblad (2015-2). Haags softwarehuis in handen van Brits beursfonds.
- Financieel Dagblad (2016). Defensie als bron van innovatie.
- Florencio, D. en Herley, C. (2011). Sex, Lies and Cyber-crime Surveys. Microsoft Tech-report MSR-TR-2011-75.
- Forbes (2015). Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020.
- Frost & Sullivan (2015), The 2015 (ISC)2 Global Information Security Workforce Study
- GfK (2015). Cybersecurity 2015. Awareness, gedrag & digitaal verantwoord ondernemen. Rapport 38282.
- Go-Gulf (2013). Cyber crime statistics and trends.
- Gov.UK (2014). Cyber essentials scheme.
- Google (2015). Google, the Wassenaar Arrangement, and vulnerability research. https://security.googleblog.com/2015/07/google-wassenaar-arrangement-and.html geraadpleegd februari 2015.
- Hackmageddon (2016). March 2016 Cyber Attacks Statistics.

- Hathaway, M. (2013). Cyber Readiness Index 1.0.
- HSD (2013). Security Delta Eindrapport.
- Intel Security, Center for Strategic and International Studies (2014). Net Losses: Estimating the Global Cost of Cybercrime.
- ICT Innovatie Platform Veilig Verbonden (IIP-VV) (2013). National Cyber Security Research Agenda II (NCSRAII).
- ICT Magazine (2015). Kabinet wil toch nieuwe WBSO.
- ISACA (2016). ISACA Now Blog. http://www.isaca.org/knowledge-center/blog/Lists/Posts/Post.aspx?ID=478, geraadpleegd februari 2016.
- Kaspersky Lab (2014). IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats.
- Kocovic, P. (2008). Four laws for today and tomorrow. Journal of Applied Research and Technology Vol. 6 No. 3 December 2008.
- Kox, H. en Straathof, B. (2009). Economic aspects of Internet security. CPB Achtergronddocument.
- KPMG (2016), Competitive Alternatives 2016.
- Laing, L., Palivos, T. &. Wang. P. (1995). Learning, matching and growth. Review of Economic Studies, 62: 115–129.
- Merton, R. C. (1987), A Simple Model of Capital Market Equilibrium with Incomplete Information. The Journal of Finance, 42: 483–510.
- Moore, T. en Anderson, R. (2011). Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research. Harvard Working Paper TR-03-11.
- Motta, M. (2004). Competition Policy. Cambridge University Press, New York.
- Nationaal Cyber Security Centrum (NCSC) (2015). Cybersecuritybeeld Nederland CSBN 2015. Ministerie van Veiligheid en Justitie. Den Haag.
- Nationaal Cyber Security Centrum (NCSC) (2016). ISAC's op https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/isacs.html, geraadpleegd februari 2016.
- Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) (2016). Nederlands ICT onderzoek behoort tot de wereldtop.
- NederlandICT (2016). The Digital Gateway to Europe. http://www.nederlandict.nl/index.shtml?ch=ICT&id=13122, geraadpleegd februari 2016
- NFIA (2013). Strategisch aanvalsplan The Netherlands: Digital Gateway to Europe
- Noll, R. van der, Nooij, M. de en Tieben, B. (2010). Kwaliteitsregulering levering elektriciteit en de grootverbruiker. SEO-rapport, 2010-09. Amsterdam: SEO.
- Nu.nl (2016). Nederlands beveiligingsbedrijf Surfright verkocht voor 29 miljoen http://www.nu.nl/internet/4182615/nederlands-beveiligingsbedrijf-surfright-verkocht-29-miljoen.html geraadpleegd februari 2016.
- Obama, B (2016). FACT SHEET: Cybersecurity National Action Plan
- OECD (2015). Digital Economy Outlook 2015. Hoofdstuk 5, Trust in the Digital Economy: Security and Privacy. OECD Publishing, Paris.

- Oort, F. van, Eijsink, W. en Bijleveld, P. (2014). Regionale innovatie door spin-offs. ESB Jaargang 99 (4698S) 20 november 2014.
- Plato (2014). Arbeidsmarkt voor Cyber Security Professionals. Onderzoek in opdracht van het WODC.
- Ponemon Institute (2015). Cost of Cyber Crime Study 2015: Global. Gesponsord door HP Enterprise.
- Privacynews (2015). Duitsland voert bewaarplicht telecomgegevens opnieuw in.
- PWC (2014). Cybercriminaliteit tegen Nederlandse organisaties: een digitale dreiging. Economic Crime Survey Nederland 2014 - deel 2, in samenwerking met de Vrije Universiteit Amsterdam.
- PWC (2016). Paying taxes 2016.
- RAND Europe (2015). Investeren in cybersecurity. RR-1202, august 2015.
- Rijksoverheid. (2015). Meldplicht datalekken en uitbreiding boetebevoegdheid Cbp 1 januari 2016 van kracht.
- RTLZ (2015). Golf van kritiek op nieuwe 'afluisterwet'
- RVO. Valorisatieprogramma. http://www.rvo.nl/subsidies-regelingen/valorisatieprogramma geraadpleegd februari 2016.
- Saline, B. (2000). Microeconomics of Market Failures. MIT, USA.
- Security & Defence Agenda (SDA) (2012). Cyber-security: The vexed question of global rules.
- Shapiro, C. & Varian, H. (1998). Information Rules: A Strategic Guide to the Network Economy. Harvard Business Review Press.
- Shy, O. (2001). The Economics of Network Industries. Cambridge University Press.
- StartupDelta (2016). Brief Tweede Kamer: ruimte voor startups bij aanbestedingen en inkoop door overheden.
- Strategic Studies Institute, Saadawi, T., Jordan Jr., L. et al. (2011). Cyber infrastructure protection.
- Rowe, B., Wood, D. en Reeves, D. (2011). Economic Analysis of ISP Provided Cyber Security Solutions. Institute for Homeland Security Solutions. US.
- Sociaal Economische Raad (SER) (2010). Overheid én markt: Het resultaat telt!.
- TNO (2012). Cyber Security Report. Den Haag.
- TNO (2013). Cyber Security Report. Den Haag.
- TNO (2015). Cyber Security Report. Den Haag.
- UWV (2015). Technische en ICT-beroepen Samenvatting arbeidsmarktbeschrijving.
- V&J (2013). De Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam. Den Haag.
- V&J (2016). Kabinetsstandpunt encryptie. Den Haag.
- VNO NCW (2014). Bedrijven willen betere verbinding wetenschaps- en innovatiebeleid.
- Vooren, A. van der & A. Hanemaaijer (2015), De vallei des doods voor eco-innovatie in Nederland, Den Haag: PBL.
- Weda, J., Kocsis, V., Noll, R. van der, & Werff, S. van der (2014). Economic Contribution of Copyright-Relevant Industries in the Netherlands. SEO-rapport nr. 2014-08.

- Worldbank (2016), Internet users (per 100 people), http://data.worldbank.org/indicator/IT.NET.USER.P2?cid=DEC_SS_WBGDataEmail_EXT, geraadpleegd februari 2016.
- World Economic Forum (2015), The Global Competitiveness Report 2015-2016
- World Economic Forum (2016), Recommendations for Public-Private Partnership against Cybercrime.

B Geinterviewden en deelnemers ronde tafels

1. Annemarie Zielstra (TNO)
2. Bert Feskens (HSD)
3. Chris van Voorden (Innovation Quarter)
4. Elly van den Heuvel (CSR)
5. Eric van Pelt (NFIA)
6. Gijs ter Horst (Chess iX)
7. Han Schutte (Ministerie van Veiligheid en Justitie)
8. Hans van Loon (HSD)
9. Ida Haitsma (HSD)
10. Jan Piet Barthel (NWO, kwartiermaker CSRE platform)
11. Jeroen Herlaar (Mandiant)
12. Joris den Bruinen (HSD)
13. Jos de Groot (Ministerie van Economische Zaken)
14. Liesbeth Holterman (ICT Nederland)
15. Lokke Moerel (CSR / Tilburg / Morrison Foerster)
16. Marco Doeland (Betaalvereniging Nederland)
17. Mark Bressers (Ministerie van Economische Zaken)
18. Menno van der Marel (Fox-IT)
19. Michiel Steltman (DINL)
20. Patricia Zorko (Ministerie van Veiligheid en Justitie)
21. Pepijn Janssen (Red Socks)
22. Petra van Schayik (Compumatica)
23. Pieter Jansen (Cyber Sprint)
24. Rene Penning de Vries (Boegbeeld ICT)
25. Richard Borsboom (HackerOne)
26. Robyn Devine (Canadese Ambassade)
27. Ronald Prins (Fox-IT)
28. Ronald Verbeek (CIO-platform)
29. Saida van Kalsbeek (HackerOne)
30. Sandro Etalle (TUE/Security Matters)
31. Tames Rietdijk (Business Forensics)
32. Wim Hafkamp (Rabobank)
33. Wim Jagtenberg (Digital Intelligence Group)

C Onderzoeksverantwoording

Deze bijlage vormt de achtergrond voor Hoofdstuk 3 De economische omvang van de Nederlandse cybersecurity-sector

C1. Beschrijving CBS-microdata

Met behulp van microdatabestanden van het CBS is de omvang van de ICT-sector in Nederland in kaart gebracht. Er is voor de berekening van de omvang van de ICT sector gebruik gemaakt van het algemene bedrijvenregister (ABR), de Aangifte Omzetbelasting (BTW) en Banen en lonen van werknemers in Nederland (SPOLISBUS).

In het ABR systeem worden bedrijven en instellingen, met hun identificatie- en structuurgegevens, vastgesteld en geregistreerd in voor statistisch onderzoek geschikte eenheden. De statistisch eenheid die voor dit onderzoek is gebruik om een bedrijf te identificeren is het Bedrijfsidentificatienummer (BEID). Met hulp van het ABR zijn bedrijven uit verschillende ICT-sectoren geïdentificeerd, te weten bedrijven met SBI-code 26.1, 26.2, 26.3, 26.4, 26.8, 46.5, 58.29, 61, 62, 63.11 en 95.1. Omdat sector 58.29 heel weinig bedrijven omvat, zijn bedrijven met deze SBI-code omwille van vertrouwelijkheid van de data buiten beschouwing gelaten in de berekening.

Het BTW-bestand is in dit onderzoek gebruikt om de omzet en de export van bedrijven te achterhalen. In de BTW-bestanden van het CBS zijn alle statistische eenheden opgenomen waarvan informatie uit de omzetbelasting beschikbaar is. Deze informatie omvat ook de voor dit onderzoek relevante omzet en export van bedrijven. De data is afkomstig uit de registratie van de belastingdienst, zodat het databestand een integrale waarneming is van alle bedrijven in Nederland die een BTW-verplichting hebben. Alle bedrijven in dit bestand zijn voorzien van een BEID, zodat er een koppeling kan worden gemaakt met het ABR.

In het integrale bestand ‘Banen en lonen van werknemers in Nederland’ (SPOLISBUS) zijn kwantitatieve en kwalitatieve gegevens opgenomen over banen en lonen van werknemers bij Nederlandse bedrijven. Ook in dit bestand zijn alle bedrijven voorzien van een BEID, zodat de werkgelegenheid voor elk bedrijf kan worden bepaald en kan worden gekoppeld met het ABR. Hierbij wordt rekening gehouden met de deeltijdfactor en de aard van de baan (stagiairs worden hierin bijvoorbeeld niet meegenomen).

Na het combineren van deze drie databestanden resteert een analysebestand met bedrijven uit de ICT-sector zien, waarvoor het aantal bedrijven, de omzet, de export en de werkgelegenheid is bepaald. Tabel 16 en Tabel 17 laten deze statistieken voor 2010 en 2013 zien. Ook de toegevoegde waarde is opgenomen in de tabellen. Om de toegevoegde waarde te bepalen (schatten) is gebruik gemaakt van de verhouding toegevoegde waarde en omzet in de met de SBI-codes corresponderende SBI-2 codes (d.w.z. SBI-codes 26, 46, 61, 62, 63 en 95).

Tabel 16 Omvang van de ICT-sector in 2010

SBI-code	Aantal bedrijven	Omzet (mld.)	Toegevoegde waarde (mld.)**	Export (mld.)	Werkgelegenheid (fte)
ICT-goederen*	784	€ 3,5	€ 0,6	€ 2,3	9.342
Groothandel ICT	7.251	€ 27,6	€ 15,6	€ 12,1	37.700
Telecommunicatie	1.358	€ 8,7	€ 4,6	€ 1,3	16.614
Dienstverlening informatietechnologie	37.362	€ 16,8	€ 9,7	€ 2,0	93.386
Gegevensverwerking, webhosting, e.d.	3.048	€ 0,6	€ 0,4	€ 0,2	2.309
Reparatie van computers e.d.	1.392	€ 0,2	€ 0,1	€ 0,0	1.311
Totaal	**51.195**	**€ 57,5**	**€ 31,1**	**€ 17,9**	**160.662**

Bron: SEO Economisch Onderzoek o.b.v. CBS (2016)

* Deze groep slaat niet op alle bedrijven met SBI-code 26, maar omvat alleen bedrijven met SBI-code 26.1, 26.2, 26.3, 26.4 of 26.8.

** Om de toegevoegde waarde te schatten is gebruik gemaakt van de verhouding toegevoegde waarde en omzet in de met de SBI-codes corresponderende SBI-2 codes.

Tabel 17 Omvang van de ICT-sector in 2013

SBI-code	Aantal bedrijven	Omzet (mld.)	Toegevoegde waarde (mld.)**	Export (mld.)	Werkgelegenheid (fte)
ICT-goederen*	849	€ 3,4	€ 0,4	€ 2,5	8.220
Groothandel ICT	6.588	€ 35,6	€ 20,1	€ 17,5	40.240
Telecommunicatie	1.328	€ 9,1	€ 4,7	€ 1,1	12.888
Dienstverlening informatietechnologie	47.781	€ 21,3	€ 12,2	€ 4,6	97.948
Gegevensverwerking, webhosting, e.d.	4.717	x	x	x	4.350
Reparatie van computers e.d.	1.846	€ 0,2	€ 0,1	€ 0,1	1.214
Totaal	**63.109**	**x**	**x**	**x**	**164.860**

Bron: SEO Economisch Onderzoek o.b.v. CBS (2016)

* Deze groep slaat niet op alle bedrijven met SBI-code 26, maar omvat alleen bedrijven met SBI-code 26.1, 26.2, 26.3, 26.4 of 26.8.

** Om de toegevoegde waarde te schatten is gebruik gemaakt van de verhouding toegevoegde waarde en omzet in de met de SBI-codes corresponderende SBI-2 codes.

In 2013 zijn de omzet, toegevoegde waarde en export van sector 'Gegevensverwerking, webhosting, e.d.' omwille van vertrouwelijkheid niet bekend. Wel is de werkgelegenheid van de sector bekend. Om toch tot een totaal te komen in de ICT sector voor omzet en export is aangenomen dat de verhouding tussen de werkgelegenheid en de omzet en export in deze sector gelijk is aan de verhoudingen in de ICT-sector als geheel. Dit resulteert voor deze sector in een geschatte omzet van € 1,5 miljard en een export van € 0,4 miljard. De toegevoegde waarde (wederom aan de hand van SBI-2 codes) komt voor deze sector vervolgens op € 0,8 miljard.

In Tabel 18 en Tabel 19 is de internationale handel in ICT-goederen in respectievelijk 2010 en 2013 weergegeven. Data zijn uitgedraaid van de statistiek van de internationale handel in goederen (IHG). De populatie van de IHG bestaat uit alle ondernemingen in Nederland die een btw-nummer hebben en met het buitenland handelen in goederen. Bedrijven die voor de invoer uit - of de uitvoer naar - lidstaten van de EU een bedrag van 900.000, - euro per jaar overschrijden zijn verplicht maandelijks een statistiekopgave aan het CBS te verstrekken. De handel van bedrijven met minder handel wordt geschat met hulpinformatie. Bedrijven die met niet-EU landen handelen, leveren hun informatie direct aan het CBS of indirect via de douane.

De handel is uitgesplitst naar SBI-sector en gebaseerd op de productlijst zoals weergegeven in Tabel 20. Deze producten zijn zo gekozen dat deze overeenkomen met de activiteiten van bedrijven met een SBI-code binnen de ICT-sector. Een aantal sectoren bevat geen informatie over de invoer, uitvoer en/of wederuitvoer, omdat deze een bedrijf bevatten dat meer dan de helft van de totale invoer/uitvoer/wederuitvoer in de sector vertegenwoordigt. Wel zijn de totalen beschikbaar voor de hele ICT-sector.

Tabel 18 Internationale handel in ICT-goederen door Nederlandse ondernemingen in 2010

SBI-sector	Invoer	Uitvoer	Wederuitvoer	Aantal bedrijven
A	€ 0	€ 0	x	132
B	x	€ 1	€ 0	287
C	€ 2.464	€ 3.355	€ 1.957	37.050
D	€ 4	x	x	134
E	x	€ 6	€ 6	152
F	€ 74	€ 28	x	2.399
G	€ 12.568	€ 14.955	€ 13.686	106.352
H	€ 13.718	€ 1.915	€ 1.752	14.450
I	€ 1	€ 0	€ 0	277
J	€ 1.393	€ 825	€ 577	14.042
K	€ 131	€ 120	€ 112	4.608
L	x	€ 7	€ 6	641
M	€ 1.172	€ 1.943	€ 1.730	28.349
N	€ 31	€ 5	x	2.054
O	€ 103	x	x	283
P	€ 6	€ 2	x	895
Q	€ 1	x	x	449
R	€ 4	€ 0	€ 0	507
S	€ 63	x	x	1.366
T	x	x	x	87
Totaal	**€ 31.879**	**€ 23.400**	**€ 20.100**	**214.514**

Bron: SEO Economisch Onderzoek o.b.v. CBS (2016)

Tabel 19 Internationale handel in ICT-goederen door Nederlandse ondernemingen in 2013

SBI-sector		Invoer		Uitvoer		Wederuitvoer	Aantal bedrijven
A	€	0	€	1	€	0	150
B	€	1	€	3	€	0	329
C	€	1.431	€	2.273	€	1.209	36.613
D	€	12		x		x	164
E	€	3	€	12		x	124
F	€	84	€	36	€	24	3.922
G	€	15.708	€	13.876	€	12.706	114.808
H	€	6.504	€	1.892	€	1.791	13.279
I	€	2		x	€	0	277
J	€	2.665	€	1.325	€	949	16.423
K	€	66	€	82	€	75	4.785
L		x	€	5	€	5	416
M	€	410	€	455	€	282	19.112
N	€	28		x	€	5	1.684
O	€	65	€	0	€	0	686
P	€	8	€	3	€	0	1.117
Q	€	3	€	0	€	0	601
R	€	3	€	1	€	0	873
S		x	€	28	€	23	1.860
T		x		x		x	13
Totaal	**€**	**27.032**	**€**	**20.016**	**€**	**17.071**	**217.236**

Bron: SEO Economisch Onderzoek o.b.v. CBS (2016)

Tabel 20 Productcodes van ICT-goederen, overeenkomstig met de voor het onderzoek gebruikte SBI-codes van ICT-bedrijven.

Productgroep	Productcodes (6-cijferig)										
8443	.31	.32									
8470	.50										
8471	.41	.49	.50	.60	.70	.80	.90				
8472	.90										
8473	.29	.30	.40	.50							
8511	.90										
8512	.90										
8517	.11	.12	.18	.61	.62	.69	.70				
8518	.10	.21	.22	.29	.30	.40	.50	.90			
8519	.20	.30	.50	.81	.89						
8521	.10	.90									
8522	.10	.90									
8523	.21	.29	.41	.49	.51	.52					
8525	.50	.60	.80								
8527	.12	.13	.19	.21	.29	.91	.92	.99			
8528	.41	.49	.51	.59	.61	.69	.71	.72	.73		
8529	.10	.90									
8530	.90										
8531	.10	.90									
8532	.10	.21	.22	.23	.24	.25	.29	.30	.90		
8533	.10	.21	.29	.31	.39	.40	.90				
8534	.00										
8536	.70										
8540	.11	.12	.20	.40	.60	.71	.79	.81	.89	.91	.99
8541	.10	.21	.29	.30	.40	.50	.60	.90			
8542	.31	.32	.33	.39	.90						
8543	.90										
8548	.90										
9013	.10	.20	.80	.90							
9504	.50										

Bron: SEO Economisch Onderzoek o.b.v. Eurostat (2016)

C2. Vragenlijst

1. Op welke activiteit(en) is uw organisatie gericht? *Graag alle activiteiten aanvinken die op uw organisatie van toepassing zijn.*
   a. Vervaardiging van elektronische componenten, printplaten, computers en randapparatuur, communicatieapparatuur, consumentenelektronica of informatiedragers
   b. Groothandel in ICT-apparatuur
   c. Uitgeven van software
   d. Draadgebonden telecommunicatie
   e. Draadloze telecommunicatie
   f. Telecommunicatie via satelliet
   g. Overige telecommunicatie
   h. Dienstverlenende activiteiten op het gebied van informatietechnologie
   i. Reparatie van computers en communicatieapparatuur
   j. Overige, namelijk...{*open antwoordveld*}
   k. Geen ICT-activiteiten
2. Houdt uw organisatie zich bezig met het leveren van producten en/of diensten gericht op het verhogen van het niveau van cybersecurity? { *Ja, Nee, Weet niet*}
3. U geeft aan dat uw organisatie zich bezighoudt met activiteiten gericht op het verhogen van cybersecurity. Welke onderstaande cybersecuritydiensten en -producten levert uw organisatie? *Graag alle mogelijkheden aanvinken die op uw organisatie van toepassing zijn.*

Identity, privacy and trust management	**Producten en diensten rondom veilige digitale toegang (verlening) tot en uitwisseling van informatie**	**Certificaten (incl. leveranciers, CA, etc.)** **Advies (incl. privacy & legal)** **Elektronische identiteiten** **Biometrie** **Secure communication (bv. VPN, Encryptie van communicatie)**
Malware and malicious infrastructures	Verzamelen en verspreiden van informatie over dreigingen en kwetsbaarheden, en de organisaties daarachter.	Intelligence Honeypots Media (vakbladen, nieuwsbrieven, etc.) Secure Intelligent Sharing (platformen)
Attack detection, attack prevention and monitoring	Producten en diensten rondom preventie, detecteren en monitoren van digitale aanvallen.	Detectie- / Monitoringdiensten / SIEM Detectieproducten (virusscanners / IDS) Preventiediensten (PEN-Testen / ethical hacking) Preventieproducten (IPS / Firewalls)
Forensics and incident management	Producten en diensten rondom het vaststellen van sporen van aanvallen en/of fraude. Inclusief (crisis)beheersing en herstel na afloop.	Sporenonderzoek & analyse Fraudeonderzoek Opsporing CERT / Incident & Response Management Recovery
Data, Policy & Access Management	Producten en diensten rondom opslag en gebruik van data (inclusief regels/beleid), zo dat kan worden voldaan aan toepasselijke wet- en regelgeving en risicobeleid (compliance) en de beheersing daarvan.	Cybersecurity binnen hostingdiensten (cloud) Governance, Risk & Compliance diensten Secure Document Management Data-encryptie Juridisch advies rondom data-opslag Authenticatie/ autorisatie-producten (DC-kant) 'Outsourced' Security Management (SOC/ Updates & Patching /Professional Services) Awareness / Opleiden, trainen & oefenen
Risk Management, Economics & Regulation	Producten en diensten rondom gebruik van ICT-voorzieningen (inclusief regels/beleid), zo dat kan worden voldaan aan toepasselijke wet- en regelgeving en risicobeleid. Inclusief afhandeling excepties en bedrijfseconomische aspecten (aansprakelijkheid, risico vs. schade).	Certificeringen (ISO, Common Criteria, Privacy) Cyberverzekeringen Legal (aansprakelijkheid, corporate liability) Risk Management & Compliance BCM-/ en weerbaarheidsadvies Mobile Device Management
Secure Design and Engineering	Producten en diensten rondom het veilig (laten) ontwerpen en bouwen van ICT-voorzieningen (hard- en software).	Secure Software ontwerp en bouw Secure Hardware ontwerp en bouw Secure Operating Systems Beveiliging rondom SCADA/ PCS Internet of Things Security
Offensive Cyber capabilities	Producten en diensten rondom het pen-testen en aanvallen van ICT-voorzieningen (hard- en software)	Producten/diensten tbv Defensie-/Politie-/ Inlichtingen- en veiligheidsdiensten Spyshops
Overig		Namelijk…..{open antwoordveld}

4. U geeft aan dat uw organisatie zich bezig houdt met activiteiten voor het verhogen van cybersecurity bij afnemers. Ongeveer welke gedeelte (in percentage) van de netto omzet van uw organisatie in 2014 heeft uw organisatie verkregen door de hierboven aangevinkte activiteiten?
5. Ongeveer welke gedeelte (in percentage) van de netto omzet van uw organisatie in 2010 heeft uw organisatie verkregen door de hierboven aangevinkte activiteiten?

6. Voor het onderzoek willen we een inzicht krijgen in de ontwikkeling van cybersecurity in de komende 3 tot 5 jaar. Met hoeveel procent verwacht u dat de netto omzet van uw organisatie door activiteiten rondom cybersecurity jaarlijks zal veranderen?
7. Bij welke van onderstaande cybersecuritydiensten en -producten verwacht u de komende 3 tot 5 jaar de meeste groei? *Zie dezelfde lijst zoals bij vraag 3.*
8. In hoeverre verwacht u dat de volgende ontwikkelingen een negatief effect zullen hebben op de omzet van activiteiten rondom cybersecurity? *{'Helemaal niet', 'Nauwelijks', 'In redelijke mate', 'In hoge mate', 'In zeer hoge mate'; en 'weet niet/ geen mening'*}
    a. Tekort aan gekwalificeerd personeel
    b. Concurrentie van buitenlandse partijen
    c. Afname gebruik internet
    d. Overige {...}
9. Hoeveel personeelsleden, uitgedrukt in voltijdbanen (fte), zijn actief in de Nederlandse vestiging(en) van uw organisatie?
10. Wat was de netto omzet, uitgedrukt in miljoenen euro, van de Nederlandse vestiging(en) van uw organisatie in 2014?
11. Wat is uw functie binnen uw organisatie?
    a. Directeur
    b. Adjunct-directeur
    c. Hoofd financiële zaken
    d. Hoofd ICT-afdeling
    e. Hoofd facilitaire dienst
    f. Sales manager
    g. Product manager
    h. Overige, namelijk...{*open antwoordveld*}

D Onderzoeksverantwoording waarde van cybersecurity

Deze bijlage vormt de achtergrond voor hoofdstuk 4 Uitstraling en vestigingsklimaat.

D1. Methoden om de waarde van cybersecurity te schatten

Er is een aantal methoden voor het meten van de waarde van cybersecurity geformuleerd, zoals (1) de betalingsbereidheid van de afnemers van cyberproducten en -diensten, een soort verzekeringspremie, (2) de investeringen in cybersecurity en (3) het aantal cyberincidenten en -schade.

Een eerste methode waarmee de waarde van cybersecurity kan worden bepaald is de betalingsbereidheid (*willingness to pay*, WTP) voor maatregelen die de cybersecurity verhogen (zie voor een overzicht van waarderingsmethoden in de context van leveringszekerheid Van der Noll *et al*., 2010). Er zijn verschillende methoden om de betalingsbereidheid voor een hoger niveau van veiligheid te bepalen. De betalingsbereidheid kan door een “uitgesproken voorkeur” gemeten worden (Moore & Anderson, 2011). Tijdens een enquête geven afnemers van producten en diensten aan wat hun betalingsbereidheid is voor een veilig netwerk of veiligere ICT-producten. Uitgesproken voorkeuren kennen echter methodologische bezwaren. Daarnaast kan betalingsbereidheid gezien worden ook als een vorm van preventie om cyberschade door cyberonveiligheid te voorkomen. Dit is een soort verzekeringspremie.

Een tweede methode is om te kijken naar investeringen in cybersecurity door het bedrijfsleven en de overheid. Deze investeringen zijn ook een proxy voor de waarde van de vermindering van het cyberrisico. Daarnaast signaleren deze investeringen de verantwoordelijkheid die de economie neemt voor de vermindering van de kansen op cyberincidenten.

Een derde methode is gebaseerd op daadwerkelijke incidenten en schadekosten door onvoldoende cybersecurity.[13] Deze benadering dekt de waarde van cybersecurity slechts gedeeltelijk. Maar voor deze studie lijkt deze methode een haalbare proxy te geven voor de waarde van cybersecurity. In de volgende paragrafen worden deze methoden nader toegelicht.

D.1.1 Meten van betalingsbereidheid door uitgesproken voorkeuren

De meest vanzelfsprekende methode zou kunnen zijn als de afnemers van cybersecuritydiensten en -producten zouden kunnen aangeven hoeveel zijn bereid zijn om voor een hoger niveau van veiligheid te betalen. Met andere woorden als de afnemers hun voorkeur zouden kunnen uitspreken. Er is slechts één studie bekend die de uitgesproken voorkeuren van afnemers meet. Rowe et al. (2011) laat zien dat Amerikaanse consumenten bereid zijn om voor internettoegang

[13] Het is gebruikelijk om preventiekosten en schadekosten als maatstaf te gebruiken voor het kwantificeren van uitstralingseffecten. Het milieubeleid is hiervan een voorbeeld. Zie bijvoorbeeld CE Delft (2010), Handboek schaduwprijzen.

met een hoger niveau van cybersecurity extra te betalen. Via een vignettenanalyse[14] werden consumenten gevraagd hoeveel ze zouden betalen voor verbeteringen in het ISP-veiligheidsbeleid, of, als alternatief, met hoeveel ze zouden moeten worden gecompenseerd om ongunstige wijzigingen in het ISP-beleid te accepteren. Zoals Tabel 21 geeft, zijn mensen bereid om tussen 2,94 en 6,51 dollar per maand te betalen, afhankelijk van de type veiligheidsverbetering.

Tabel 21 Amerikanen zijn bereid om voor veiliger internettoegang te betalen

	Estimated WTP ($/month)	95% Confidence Interval
Time Spent Complying with ISP Security Requirements: WTP to avoid 1 hour of time complying with security requirements	0.73	[0.57 to 0.92]
Limiting Internet Access: WTP to move from ISP being able to entirely restrict access to not restrict access at all	4.32	[3.72 to 4.92]
Risk of Computer Shutting Down or Crashing: WTP to move from not reduced to greatly reduced	4.40	[3.83 to 4.97]
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	6.51	[5.86 to 7.16]
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	2.94	[2.44 to 3.45]

Note: 95% confidence interval was estimated using Krinsky-Robb parametric bootstrapping technique.

Bron: Rowe et al. (2011).

Deze onderzoeksresultaten vormen een te beperkte basis voor toepassing in dit onderzoek.

D.1.2 Relatie tussen schade en waarde: een verzekeringspremie

Voor het meten van betalingsbereidheid kan er gekeken worden naar de preventieve uitgaven. In welk geval zijn huishoudens of bedrijven bereid om preventief geld uit te geven? Ze zullen alleen preventieve uitgaven willen doen zolang het verwachte nut van deze uitgaven groter is dan de kosten. De betalingsbereidheid om dergelijke uitgaven te doen geeft dan een indicatie van de minimale kosten van het schadelijke effect en dus van de waarde van de mitigatie van het schadelijke effect. Als een huishouden € 100 per jaar uitgeeft om de cybersecurity te verhogen van niveau 1 naar niveau 2, dan is de waarde van deze veiligheid € 100 of meer. De waarde kan ook bijvoorbeeld € 120 zijn (in dat geval behaalt het huishouden een surplus); als de waarde van de veiligheid € 80 zou zijn, zou het huishouden geen € 100 betalen.

Wat is de relatie tussen de betalingsbereidheid om cyberschade te voorkomen en cyberschade die zich daadwerkelijk heeft voorgedaan? Voor dit vraagstuk is het niet mogelijk om, zoals in de milieukunde wel het geval is, een schaduwprijs te berekenen (zie Bruyn et al., 2010). De

[14] Door middel van vignettenanalyse (ook wel een *conjoint analysis* genoemd) worden mensen ondervraagd over hun voorkeuren. De analyse is gebaseerd op een enquête. Vaak kunnen die voorkeuren op de markt geobserveerd worden uit aankoopgedrag. Als marktgedrag echter niet gemeten kan worden omdat er (nog) geen markt is, kan een vignettenanalyse uitkomst bieden. Tijdens het onderzoek bestaat de kans op strategisch of sociaal wenselijk antwoordgedrag. Met een vignettenanalyse wordt die kans sterk verkleind.

schaduwprijs wordt daar berekend per eenheid effect (bijvoorbeeld uitstoot van een kilogram schadelijke stof). In de context van cybersecurity zijn er echter nog geen eenheden vastgesteld om mee te rekenen.

Om de vertaalslag te maken van de schade door incidenten naar betalingsbereidheid voor cybersecurity, zijn kansen en risicovoorkeuren nodig. Een voorbeeld maakt dit helder. Stel dat een onderneming in jaar *t* is getroffen door een cyberincident dat €100.000 heeft gekost (directe uitgaven maar ook indirecte kosten, bijvoorbeeld reputatieschade). Als de onderneming bij aanvang van het jaar er volledig zeker van zou zijn dat het incident zou plaatsvinden (en ook de kosten ervan goed zou kunnen inschatten), zou de onderneming tot € 100.000 willen betalen om het incident te voorkomen. De betalingsbereidheid is in dat geval dus € 100.000 en de waarde van het verhogen van de veiligheid (het voorkomen van het incident) kan op basis van die betalingsbereidheid vastgesteld worden. De kans van een incident is echter kleiner dan 1 en de betalingsbereidheid dus ook lager dan € 100.000. Wanneer de kans op het incident 0,5 zou zijn en de ondernemer risiconeutraal, zou de verwachte waarde van de schade € 50.000 zijn. De ondernemer zou in dat geval tot € 50.000 willen betalen om het risico weg te nemen.

De waarschijnlijkheid van incidenten en risicovoorkeuren zijn echter onbekend. We weten wel welk percentage van de bevolking te maken heeft gehad met een bepaald type incident (zie enkele tabellen in de volgende sectie). Een rekenvoorbeeld uitgaande van risiconeutrale preferenties kan dan gemaakt worden. Neem aan dat er per periode één incident plaatsvindt in een populatie met 100 huishoudens. Het vermogen van het getroffen huishouden daalt met € 1.000 wanneer het incident zich voordoet. Een verzekeringsproduct met een premie van € 10 per huishouden die € 1.000 uitkeert wanneer het incident plaatsvindt, zou dan door alle huishoudens worden aangeschaft. De opgetelde preventieve uitgaven zijn in dat geval dus € 1.000. De waarde van het voorkomen van het incident is in dit rekenvoorbeeld gelijk aan de vermogensschade die het incident veroorzaakt.

In de praktijk kunnen er echter ook 2 of meer incidenten in de periode voorkomen. In dit geval maakt de verzekeraar naar verwachting verlies. Wanneer de kansverdeling ook de mogelijkheid toestaat dat het incident helemaal niet plaatsvindt, dan maakt de verzekeraar winst. De kosten van een incident overschatten in dat geval de waarde van veiligheid. De kosten van een incident dat plaatsvindt in periode *t* kunnen dus niet zonder meer worden geïnterpreteerd als de waarde van veiligheid in periode *t*. De periode waarbinnen de incidenten worden geregistreerd moet lang genoeg gekozen worden zodat de waargenomen frequentie de kansverdeling beter benadert.

Cyberverzekering bestaat al langer (OECD, 2015, Anderson et al. 2013, RAND Europe, 2015). Een vorm van verzekering is dat bedrijven het risico, gekoppeld aan technologische ontwikkeling, een onderdeel maken van hun risicomanagementstrategieën. De verzekeringsmarkt ontwikkelt zich in deze richting.[15] [16] Dit gebeurt ook als respons op de kosten die een meldplicht veroorzaken

[15] Bijvoorbeeld: http://www.aon.com/netherlands/cyberrisico/verzekering/#; http://www.nu.nl/mkb/3800345/mkb-kan-zich-verzekeren-cybercrime.html of

(bijvoorbeeld om consumenten te informeren over een incident of reputatieschade en juridische kosten ten gevolg van aansprakelijkheid te voorkomen).

D.1.3 Investeringen in cybersecurity

Een recente studie van RAND Europe (2015) kijkt naar investeringen in cybersecurity door het bedrijfsleven. Privé investeringen signaleren namelijk de verantwoordelijkheid die de economie neemt voor de vermindering van de cyberrisico's. Verantwoordelijkheid betreft de moeite die bedrijven nemen om verschillende type marktfalen (zoals informatieasymmetrie en externaliteiten; Moore & Anderson, 2011, Kox & Straathof, 2009) te internaliseren. De RAND-studie analyseert investeringsprikkels en de mate van investeringen in 12 vitale sectoren, zoals energie, telecommunicatie en ICT, drinkwater, voedsel, gezondheid, financieel, keren en beheren oppervlakwater, rechtsorde, openbaar bestuur, transport en chemische en nucleaire industrie.

Uit de interviews die in die studie zijn uitgevoerd, blijkt dat de belangrijkste reden voor investeringen de angst is voor reputatieschade. Die wordt mogelijk groter door de meldplicht vanaf 2016. Ook zijn bedrijven bang voor mogelijke rechtszaken vanwege aansprakelijkheid (NB: dit is een reden waarom de eerder genoemde verzekering een grotere rol zou kunnen spelen binnen het risicomanagement van organisaties). Daarnaast investeren bedrijven in cybersecurity om de kans op een cyberaanval en schade daarvan te verminderen. Het meten van de hoogte van de investeringen blijkt echter moeilijk om vier reden. Ten eerste, er is geen ultieme definitie van cybersecurity. Ten tweede, er is geen duidelijk kostenmodel. Ten derde, cybersecurity heeft betrekking op preventie, detectie en herstel en dus op een diversiteit van organisaties met verschillende producten en diensten. Ten vierde, cybersecurity vormt een integraal onderdeel van de bedrijfsvoering. Daardoor is het moeilijk om cyberuitgaven te isoleren van andere projecten, processen en producten. Om deze redenen heeft de RAND-studie geen bedrag voor investeringen in cybersecurity kunnen berekenen.

D.1.4 Cyberincidenten en -schade

De economische impact van een sterke cybersecuritysector op Nederlandse bedrijven kan gemeten worden door de daadwerkelijke incidenten en schadekosten door onvoldoende cybersecurity te berekenen. Dit is een simpele methode om de waarde van cybersecurity te meten. Denk hierbij aan de schade die sectoren hebben ten gevolge van cyberincidenten en andere vormen van digitale onveiligheid. Deze kosten zijn de opportuniteitskosten van onvoldoende veiligheid (voor een uitgebreid kader om cyberkosten te meten zie Anderson et al., 2013; exercitie uitgevoerd voor Engeland en de VS). Men moet hierbij opletten met de

---

https://www.cyberrisicoverzekering.nl/pdf/Virtuele_risico_echte_schade_over_het_verzekeren_van_cyberrisico.pdf

[16] NB: De cybersecuritysector kan ook het functioneren van de verzekeringsmarkt beïnvloeden, bijvoorbeeld hoe hoog de marge is in deze markt. De analyse van de verzekeringspremie valt echter buiten de scope van deze studie.

interpretatie van schade. Schade voor het ene bedrijf kan namelijk winst zijn voor bijvoorbeeld een concurrent (denk aan uitval van een e-commerce website). Daarnaast is de schade niet direct vertaalbaar naar de betalingsbereidheid van consumenten en bedrijven (zie eerdere paragraaf). Uiteindelijk is de meting sterk afhankelijk van de verschillende definities en beschikbare informatie. Met deze bezwaren mikt deze notitie de omvang van schade van cybercrime in Nederland in kaart te brengen.

D2. Cyberincidenten en -schade als proxy

Om in kaart te brengen hoeveel cyberincidenten hebben plaatsgevonden in Nederland in de afgelopen 5 jaar en wat de mogelijke schade ervan is, wordt gebruik gemaakt van verschillende bronnen. Ten eerste is een overzicht van studies gemaakt over schade ten gevolge van cybercriminaliteit. Ten tweede zijn statistieken over cyberincidenten geanalyseerd. Het CBS, de DNB en ECB, consultancy- en ICT-bedrijven hebben er statistieken over beschikbaar. Deze statistieken zijn echter onvolledig. Namelijk zijn er een verschillende definities en methoden betreffend het meten van incidenten en schade. Deze tekortkomingen staan apart genoemd in een paragraaf. Uiteindelijk richt deze studie zich op Nederland met een mediasearch. Met een mediasearch in LexisNexis, de belangrijkste mediamonitor, is een lijst van alle incidenten en een beeld van de cyberschade opgesteld. Aan het eind van deze paragraaf trekken we conclusies.

D.2.1 Definities en categorisaties

Volgens de definitie van de Nationale Cybersecurity Strategie (V&J, 2013) betreft cybersecurity het voorkomen van incidenten door verstoring, uitval of misbruik van ICT. Incidenten worden veroorzaakt door cybercriminelen maar ook zonder een moedwillige dader. In deze notitie wordt voornamelijk naar incidenten via cybercrime gekeken.

Wat is cybercrime? Een aantal studies wijst uit dat hier geen eenduidig antwoord op te geven is. Ten eerste er is onduidelijkheid over de afbakening van cybercrime versus non-cybercrime (Fafinski et al., 2010, RAND Europe, 2015, Anderson et al., 2013). Wellicht zijn deze vormen van elkaar afhankelijk. Ook kan er een overlap ontstaan, wat tot een overschatting leidt van de kosten van criminaliteit. Neem hierbij als voorbeeld de definitie van de Council of Europe Convention on Cybercrime (CECC; Fafinski et al., 2010), waarbij het stelen van een computer onvermijdelijk én bij non-cybercrime én bij cybercrime geteld kan worden. Het CECC typeert cybercrime als:

- overtredingen tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computer data en systemen;
- computer-gerelateerde overtredingen;
- content-gerelateerde overtredingen.

Om een overschatting te voorkomen waar ook veel normale misdaad onder valt, kiest deze studie voor een conservatieve aanpak wat betreft de afbakening van cybercrime. Conservatief houdt in dat in de afbakening slechts de meest voorkomende digitale vormen van criminaliteit de lading zullen dekken, conform de aanpak van het NCSC (2015). Dit in tegenstelling tot een afbakening waar koste wat kost alle vormen van cybercrime in moeten vallen.

Ten tweede er is onduidelijkheid over de verschillende categorieën binnen cybercrime (Fafinski et al., 2010). Er kan een onderscheid worden gemaakt tussen zogenoemde manifestaties en middelen (NCSC, 2015). Manifestaties zijn bijvoorbeeld: verstoring van ICT, digitale spionage, diefstal van informatie en diefstal van financiële middelen. De middelen zijn de manieren waarop een manifestatie is bereikt, bijvoorbeeld ransomware, spam, spyware, defacing, Distributed Denial of Service (DDoS), phishing, hacking of fraude (zie Tabel 26 voor een long-list van middelen). Het is niet duidelijk of een incident altijd in één manifestatie past of door één middel veroorzaakt wordt. Dit is zeer afhankelijk van de specifieke definities die gebruikt worden. Zo kan zonder verdere specificatie digitale spionage ook gelden als diefstal van informatie en kan ransomware verspreidt worden door spam.

In deze studie kiezen we daarom voor een aanpak waarbij wordt gekeken alleen naar de frequentie of omvang van bepaalde cybercrime middelen, zonder iets te kunnen zeggen over een totaal van de categorieën bij elkaar, conform de aanpak van het CBS (2015c).

Uiteindelijk verschillen de categorisaties van bijna alle publicaties en statistieken omdat ze worden gebruikt voor verschillende doeleinden. De meeste bronnen focussen slechts op één (eigen) categorisatie op basis van middelen (zie Tabel 26 voor een long-list van definities en Tabel 27 t/m Tabel 30 voor de definities van organisaties die de informatiebronnen zijn van deze studie).

D.2.2 Informatiebronnen

Naast de definities verschillen ook de informatiebronnen. Beschikbare data over de cyberschade is gefragmenteerd en moeilijk te vergelijken. Daarnaast is er geen manier om de data op te tellen. Daarom vergelijkt deze studie een aantal Nederlandse en internationale bronnen zonder te streven naar volledigheid.

STUDIES

De studies zijn afkomstig van statistische bureaus, bedrijven, overheden, verenigingen en wetenschappelijke tijdschriften.

STATISTIEKEN

De statistieken zijn afkomstig van de Betaalvereniging Nederland, de DNB en ECB, het CBS en Eurostat,[17] TNO, het NCSC, PWC, het Ponemon Institute en een aantal ICT-bedrijven, zoals Kaspersky Lab (2014)[18] en Intel Security (2014). Tussen de verschillende bronnen is een verschil in categorisatie en de methodologie van cybercrime die de statistieken hanteren. Voor een aantal

[17] De statistieken van Eurostat over het bedrijfsleven is minder volledig dan die van ICT- en onderzoekbureaus. Daarom staan de Eurostat-cijfers alleen in de bijlage.

[18] Kaspersky Lab heeft ook een real-time aanvallenkaart: https://cybermap.kaspersky.com/. In deze kaart worden aanvallen aangetoond die gemeten zijn door detectieproducten, zoals virusscanners. Zo'n meting onthoudt dat niet alle genoemde aanvallen tot een incident en schade leiden. Een vergelijkbare kaart is die van Google en Arbor Networks: http://www.digitalattackmap.com.

bronnen staat de beschrijving van de methodologie in de tekst. Voor de rest van de bronnen is de beschrijving geplaats in de bijlage (Tabel 27 t/m Tabel 30).

MEDIASEARCH VAN NIEUWSARTIKELEN

Naast de studies en statistieken wordt gekeken naar het aantal cyberincidenten in het nieuws. De nieuwsartikelen zijn afkomstig uit 60 Nederlandse kranten uit de LexisNexis academische bibliotheek.[19] De zoekwoorden uit Tabel 31 in de Bijlage zijn gebruikt om artikelen te vinden in de periode 1-1-2010 tot 1-12-2015 (zie Bijlage C voor een uitgebreide beschrijving van de mediasearch).

In sommige gevallen kan het onduidelijk zijn wie de eigenaar van de schade (slachtoffer) is. De economie is zo verweven dat de schade altijd zijn weg zal vinden naar zowel consumenten, bedrijven en de overheid. Ook als puur wordt gekeken naar de eigenaar van de schade kan een probleem ontstaan. Bijvoorbeeld, als een rekening wordt leeggeroofd kunnen mensen in de meeste gevallen hun geld terugkrijgen van de bank. Maar dit zou in gevallen buiten de bancaire sector meestal niet gebeuren. Bij de resultaten is voor elk type incident kort toegelicht op welke doelgroep de grootste impact valt.

De categorisatie binnen de mediasearch is gefocust op verschillende middelen van cybercrime en is grotendeels overgenomen van de EuroBarometer van TNO. Deze lijst is uitgebreid tot elf verschillende categorieën om een zo compleet mogelijk beeld te geven van verschillende soorten middelen. De definities zijn aangepast om naast cybercrime voor consumenten ook de gevolgen voor bedrijven en de overheid in beeld te krijgen. De meeste incidenten behoren tot één categorie. Twee categorieën die vaak samenvallen zijn 'geïnfecteerd apparaat' en 'informatiehack'.

Eén categorie is niet in de lijst opgenomen omdat deze een grote overlap heeft met andere categorieën, en dit is *Identiteitsfraude*. Zo wordt deze categorie door het CBS getypeerd als *skimming* en *phishing*. Er is besloten om *phishing* als aparte categorie te vermelden, en *skimming* onderdeel te laten zijn van *online bankier- of pasfraude*, naar het voorbeeld van de EuroBarometer.

Vier categorieën zijn wel in de lijst opgenomen, maar niet apart vermeld in de resultaten, vanwege een gebrek aan significante informatie uit de mediasearch. Dit zijn: *koop- en verkoop fraude, racistische/extremistische/kinder-pornografische content; online illegale handel en illegaal downloaden*; en *datalekken door werknemers*.

MEETFOUTEN

Er zijn mogelijke meetfouten die kunnen ontstaan tijdens het meten van cybercrime, vooral omdat cijfers gebaseerd zijn op meldingen en enquêtes (zie Tabel 22). Voor de conclusies gelden deze beperkingen. Meetfouten kunnen worden onderverdeeld in drie verschillende groepen, afhankelijk van of ze tot onder- of over-rapportage leiden, en of ze worden veroorzaakt door prikkels, externaliteiten of door onwetendheid.

---

19 www.lexisnexis.nl

Tabel 22 Type meetfouten betreffend meldingen

Oorzaak \ Gevolg	Onder-rapportage	Over-rapportage
Prikkels	Slachtoffers	Security bedrijven
Externaliteiten	Iedereen	Iedereen
Onwetendheid	Iedereen	Iedereen

Slachtoffers en andere verantwoordelijken hebben prikkels om minder schade te rapporteren, aangezien het voor hun kan leiden tot minder vertrouwen en minder productie (Moore & Anderson, 2011). Daarnaast hebben cybersecurity bedrijven en andere belanghebbenden prikkels om meer schade te rapporteren omdat het voor hun business kan leveren (Moore & Anderson, 2011).

Een andere reden voor onjuiste rapportering van schade is externaliteiten. Schade bij één partij kan zorgen voor meer schade bij andere partijen, vanwege een vermindering van productie of consumptie. Dit leidt tot minder schade rapportering dan de daadwerkelijke schade. Daarnaast kan schade bij één partij zorgen voor meer winst bij een andere partij, vanwege een verplaatsing van productie of consumptie. Dit leidt tot meer schade rapportering dan de daadwerkelijke schade (Moore & Anderson, 2011).

Daarnaast weten slachtoffers vaak niet wat de schade is. Bedrijven zijn geïnformeerd dat consumenten ontevreden zijn vanwege een cyberincidenten maar het is ingewikkeld om ontevredenheid te kwantificeren. Prikkels, externaliteiten en onwetendheid kunnen leiden tot een scheef beeld van de echte omvang van schade.

Een laatst type meetfout komt voor door beperkingen van enquêtes (Florencio & Herley, 2011). Het grootste knelpunt betreft de beperkingen van een steekproef. Schade kan namelijk geconcentreerd zijn (niet voor iedereen gelden in de populatie) en kan in een steekproef worden 'gemist' of niet representatief worden gemeten. Daarnaast als een extreem grote schade - een *outlier* - gerapporteerd wordt, wordt deze schade extrapoleerd naar de hele populatie. Zo'n extrapolatie leidt tot een overschatting van de schade. Uiteindelijk zijn veel mensen zich niet bewust dat de schade die ze ondervinden het gevolg is van cybercrime. Voor een uitgebreide analyse over meetfouten zie E-CRIME (2015).

D3. Resultaten

Zoals eerder is genoemd kennen statistieken van cyberincidenten methodologische beperkingen, namelijk de afwezigheid van een eenduidige definitie van cybercriminaliteit, de onvolledigheid van de data en methodologische beperkingen betreffende het meten van de schade. Om deze reden is de optelling van het aantal cyberincidenten en -schade niet mogelijk. Wat hieronder staat is de conclusie van studies, statistieken over enkele middelen die gebruikt zijn in cyberincidenten en een samenvatting van de resultaten van de mediasearch. Waar mogelijk is een internationale vergelijking weergeven.

D.3.1 Totaalbeeld

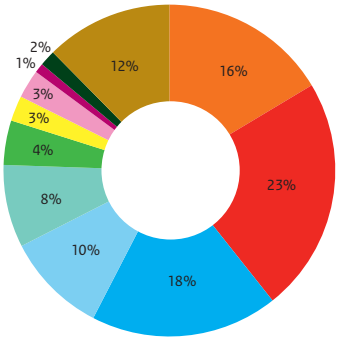
In de meest recente studie van PWC (2014) over criminaliteit in Nederland is cybercriminaliteit voor het eerst meegenomen als een aparte vorm van criminaliteit. Tijdens het onderzoek geven 875 respondenten hun mening over cybercriminaliteit binnen de BV Nederland. Volgens PWC is 23 procent van bedrijven de laatste 24 maanden geconfronteerd met cybercrime. Op het wereldniveau is dit percentage 9 procent. Deze vorm van criminaliteit volgt na diefstal van geld, goederen en fraude (bij 65 procent van bedrijven) en diefstal van informatie (27 procent) en komt vaker voor dan corruptie en concurrentievervalsing. 14 procent van bedrijven heeft 1 à 5 incidenten ervaren, 4 procent 6 à 10 incidenten en 5 procent meer dan 10 incidenten.

D.3.2 Schade per middel en type slachtoffers

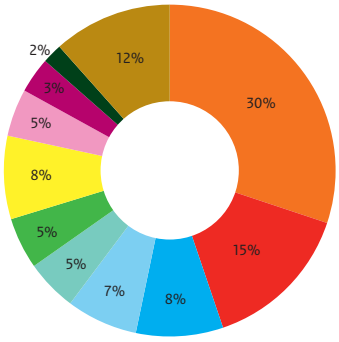
Op het niveau van type slachtoffers is de informatie over cyberincidenten sporadisch. Het Nationaal Cyber Security Centrum (2015) rapporteert de verdeling van incidenten tussen middelen. Zoals de afbeelding aantoont is de Nederlandse overheid vooral geraakt door informatielekkage (23 procent) en injectie-aanvallen (18 procent).

Afbeelding 14 De overheid is slachtoffer van informatielekkage, private partijen van phishing

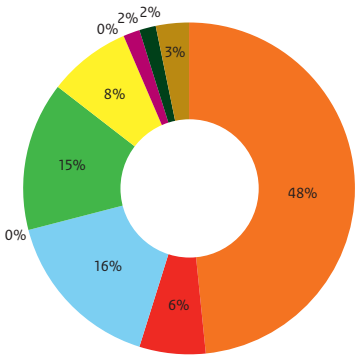
Figuur 19 **Type incidenten waarbij een overheidspartij betrokken was**



Figuur 20 **Type incidenten waarbij een private partij betrokken was**



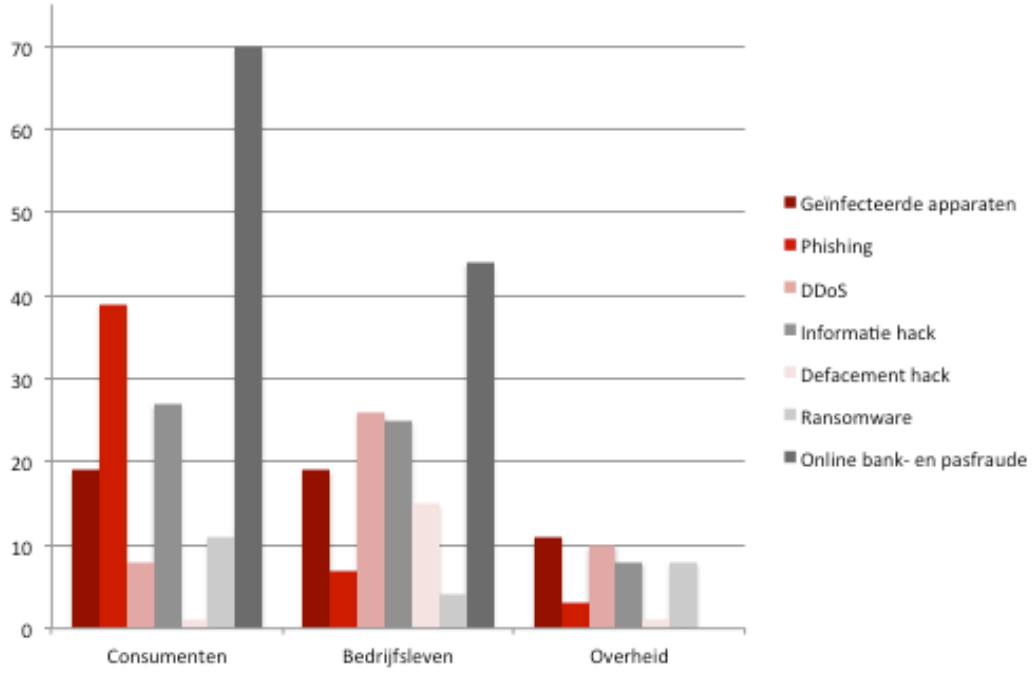
Figuur 21 **Type incidenten waarvoor het NCSC een internationaal hulpverzoek ontving**



Bron: NCSC (2015).

Door te zoeken in LexisNexis op zoektermen in Tabel 31 in de Bijlage kwamen enkele tienduizenden nieuwsartikelen naar voren. Hier zijn 269 incidenten uit overgebleven door te selecteren op unieke cybercrime incidenten. Exacte conclusies kunnen niet worden getrokken uit kwantitatieve opsommingen. Enkele nieuwsartikelen benoemen één incident bij één persoon terwijl andere nieuwsartikelen een golf van incidenten bij meerdere personen benoemen. De data kunnen daarentegen wel een samenvatting per categorie ondersteunen (zie Afbeelding 15). In deze samenvatting zijn de aantallen en de slachtoffers van incidenten opgenomen. In de afbeelding zijn alleen de totalen voor de periode 2010 en 2015 weergegeven. De jaarlijkse uitsplitsing staat in Tabel 40 t/m Tabel 46 maar op basis ervan kan er geen conclusie over een trend getrokken worden. Bron: SEO Economisch Onderzoek

Afbeelding 15 Online bank- en pasfraude, informatie hack en phishing zijn vaker gerapporteerd in de media



Bron: SEO Economisch Onderzoek via mediasearch in de periode 01-01-2010 en 01-12-2015; Aantal incidenten per middelen en type slachtoffer

D.3.3 Consumenten

Het CBS, TNO en GfK kijken naar de consumenten als slachtoffers. In Tabel 23 is te zien welk deel van de consumenten jaarlijks in aanraking komt met verschillende vormen van cybercrime (CBS, 2015b). Volgens het CBS neemt het aantal incidenten af wat identiteitsfraude (skimming en phishing), koop- en verkoopfraude en hacken betreft.

Tabel 23 Minder Nederlandse consumenten komen in aanraking met cyberincidenten

	2012	2013	2014
Identiteitsfraude (skimming en phishing)	1,5	1,3	0,8
Koop- en verkoopfraude	3,0	3,3	3,5
Hacken	6,0	6,2	3,5

Bron: CBS (2015b); Jaarlijkse aangifte van verschillende typen cybercrime door consumenten, in percentage van de bevolking

TNO analyseert ook andere type cyberincidenten. Volgens de Eurobarometer komt een grotere gedeelte van de Nederlandse populatie in aanraking met DOS, racistisch of extremistische content en online bankier fraude (zie Tabel 24). Maar we moeten opletten met de vergelijking tussen verschillende databronnen. Met name hanteren onderzoeksinstituten verschillende definities en methoden.

Tabel 24 Meer Nederlandse consumenten komen in aanraking met cyberaanvallen

	2012	2013	2014
Identiteitsdiefstal	7	5	3
Phishing	54	61	59
Koop- of verkoop fraude	9	14	16
Hacken	n.a.	16	16
DoS	28	43	43
Racistisch of extremistische content	11	15	20
Online bankier fraude	n.a.	7	8
Geïnfecteerd apparaat	n.a.	n.a.	62
Ransomware	n.a.	n.a.	10
Kinderporno content	n.a.	n.a.	6

Bron: TNO EuroBarometer (2012, 2013, 2015); Jaarlijkse aangifte van verschillende typen cybercrime door consumenten, in percentage van de bevolking

GfK (2015) brengt slachtofferschap en het voorgenomen gedrag van consumenten in kaart via een enquête. Ook volgens GfK zijn ongewenste e-mail, phising en virussen de meest voorkomende vormen van cyberincidenten. Identiteitsdiefstal en ongeoorloofde afschrijving via internetbankieren komen bijna nooit voor tussen consumenten.

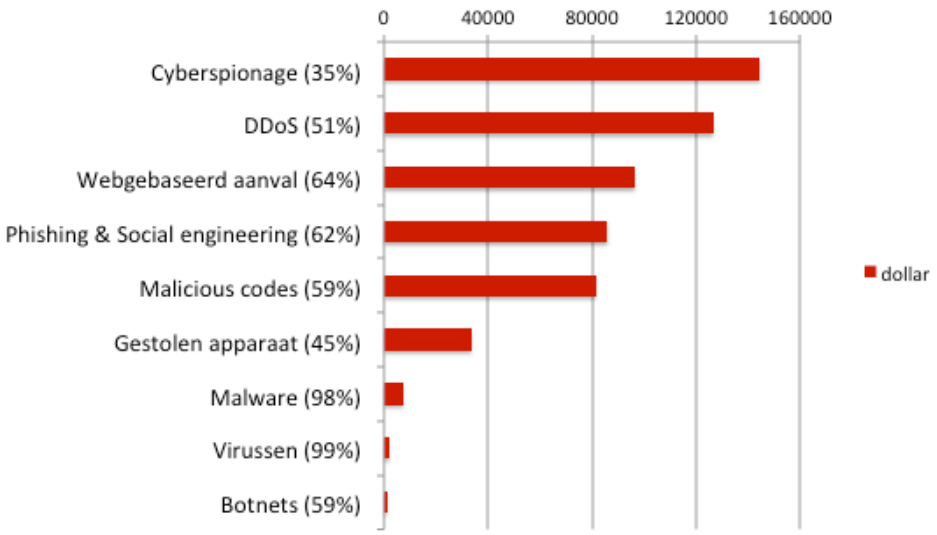
Een recente studie van Eurostat (zie Eurostat, 2016) analyseert in hoeverre internetgebruiker cyberincidenten ervaren. In 2015 heeft 25 procent van Europese internetgebruiker problemen ervaren die gerelateerd zijn aan cyberincidenten. In Nederland is dit aandeel slechts 11 procent, de tweede laagste binnen de EU. De meest voorkomende incidenten zijn virussen, misbruik van persoonlijke gegevens, financiële verliezen en ongepaste websites voor kinderen. In de afgelopen jaren is het aandeel virussen flink gedaald in Nederland: van 23 procent in 2010 naar 6 procent in 2015. Dit percentage ligt onder het Europese gemiddelde (respectievelijk 31 procent in 2010 en 21 procent in 2015). Maar ten minste 20 procent van de Nederlandse internetgebruiker doen geen online winkelen, online bankieren of zetten hun mobiele toestellen niet op een wifi-netwerk

vanwege bezorgdheid over de veiligheid. Dit betekent dat Nederlandse mensen voorzichtiger zijn dan het Europese gemiddelde.

D.3.4 Bedrijfsleven

Recentelijk heeft het Ponemon Institute (2015) 2.128 mensen binnen 252 bedrijven in zeven landen[20] gevraagd over het aantal cyberincidenten en de schade daarvan. Bijna alle gevraagde bedrijven zijn geraakt door virussen en malware. De meest genoemde middelen veroorzaken echter niet de grootste schade voor een organisatie. Een virus kostte 1.900 dollar en een malware kostte 7.400 dollar voor een organisatie (zie Afbeelding 16). Het duurste incident is cyberspionage dat bijna 145.000 dollar schade heeft veroorzaakt voor organisaties. Maar cyberspionage komt substantieel minder vaak voor dan virussen en malware.

Afbeelding 16 Cyberspionage veroorzaakt de grootste schade maar het komt minder vaak voor dan ander middelen

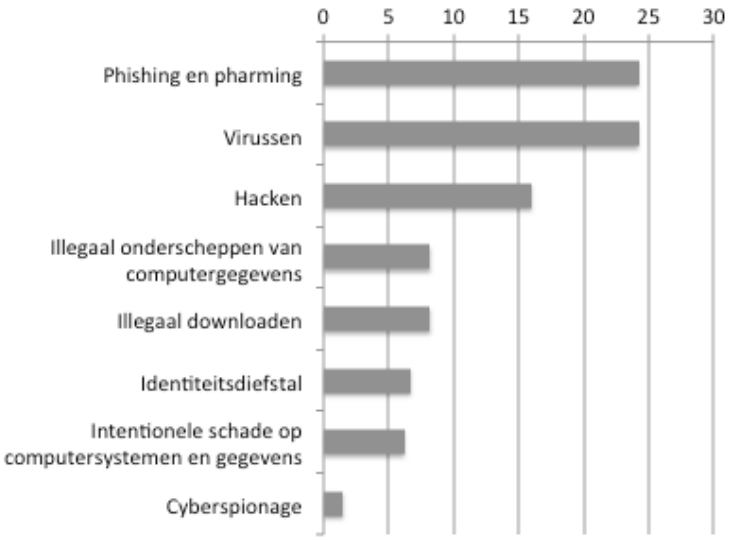


Bron: Ponemon Institute (2015). Schade in dollar gewogen door aanvallenfrequentie. In haakjes hoeveel percentage van gevraagde bedrijven het type aanval hebben ervaren.

In Nederland zijn ook phishing, virussen en hacken de meest frequent voorkomende vormen van cybercrime binnen het bedrijfsleven. Zoals Afbeelding 17 aantoont komen ongeveer 25 procent van bedrijven in aanraking met phishing en virussen en 16 procent met hacken.

[20] De zeven landen: VS, Duitsland, Japan, Engeland, Brazilië, Australië en Rusland.

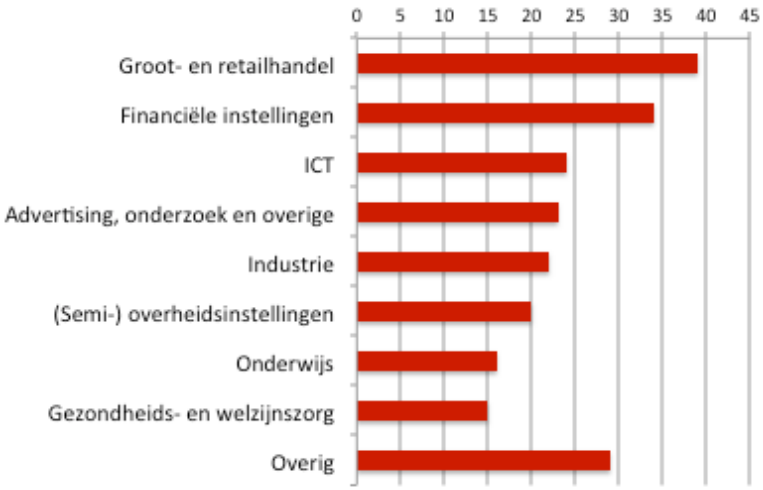
Afbeelding 17 Phishing en virussen zijn de meest genoemde vormen van cybercrime tussen Nederlandse bedrijven



Bron: PWC (2014). Data in %.

In tegenstelling tot de internationale trend ervaren voornamelijk handel, financiële instellingen en de ICT-sector de meest incidenten in Nederland (zie Afbeelding 18).

Afbeelding 18 In Nederland raakt cybercrime handel en financiële instellingen het meest



Bron: PWC (2014). Data in %.

Banksector: online bank- en pasfraude

In details is online bank- en pasfraude het meest gerapporteerd. Dit is vanwege de meldplicht naar de Europese centrale banken. In Tabel 25 is te zien hoeveel financiële schade er de afgelopen jaren is veroorzaakt door verschillende vormen van online bank- of pasfraude. Phishing, malware en skimming zijn de meest voorkomende vormen van criminaliteit die tot fraude leiden.

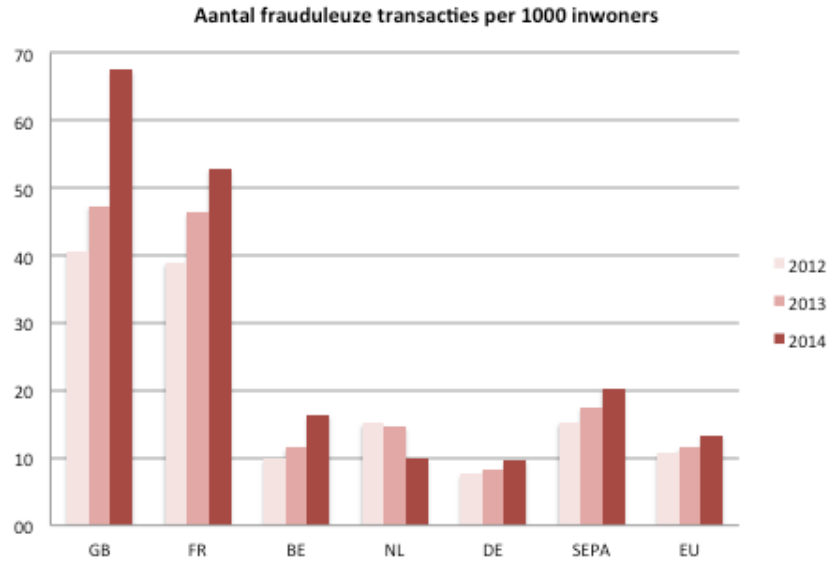
Tabel 25 Financiële schade daalt substantieel in Nederland

	2011	2012	2013	2014
Phishing	n.a.	11,5	4,7	3,9
Malware	n.a.	22,0	4,1	0,4
Overige	n.a.	1,3	0,8	0,4
Totaal Internet bankieren	*34,9*	*34,8*	*9,6*	*4,7*
Skimming	39,0	29,0	6,8	1,3

Bron: Jaarlijkse financiële schade door phishing, malware en skimming, in miljoenen euro's; Betaalvereniging Nederland (2014), DNB (2014)

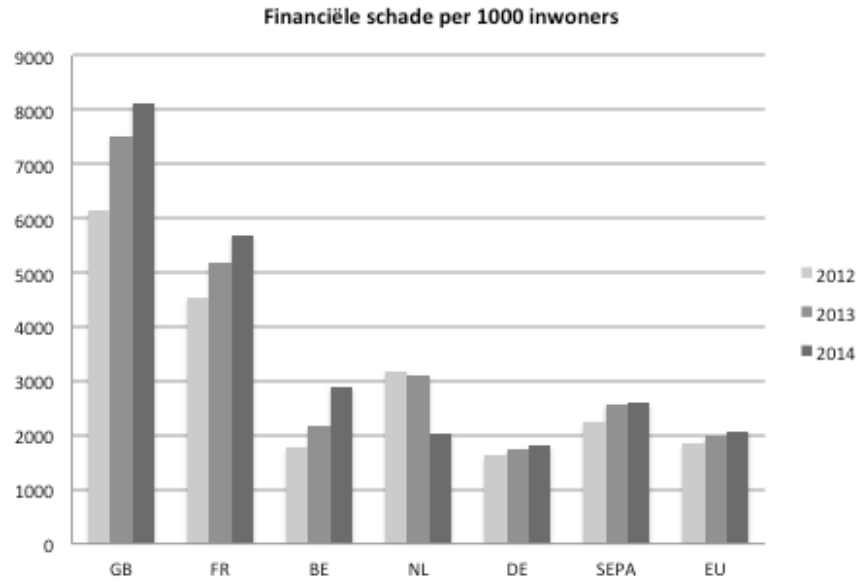
Zoals de tabel laat zien is de schade in de banksector afgenomen in de periode 2011 en 2014. Dit gebeurt desondanks de toenemende tendentie in Europa (Afbeelding 19 en Afbeelding 20). Het aantal incidenten ligt inmiddels onder het Europese gemiddelde en ook het schadebedrag ligt onder het EU-gemiddelde.

Afbeelding 19 Ondanks de stijging in Europa neemt het aantal frauduleuze transacties af in Nederland



Bron: ECB (2013, 2014, 2015)

Afbeelding 20 De financiële cyberschade in Nederland daalt en komt dichterbij het Europese gemiddelde



Bron: ECB (2013, 2014, 2015)

In de categorie online bank- en pasfraude waren er in totaal 88 incidenten in het nieuws. Dit waren grotendeels kleine incidenten waarbij individuen geskimd werden voor honderden tot duizenden euro's. Er waren enkele meldingen van groeperingen die voor honderdduizend tot 2 miljoen euro hebben weten buit te maken bij grote groepen slachtoffers. Tot slot waren er ook incidenten waarbij de online bankomgeving direct werd gemanipuleerd. Bij één incident in 2011 is er op deze wijze 45 miljoen verduisterd van twee banken. Door gebrek aan informatie in de nieuwsartikelen over de exacte impact van veel skim incidenten is er besloten om skimmen te classificeren als schade voor consumenten én bedrijven. Banken vergoeden immers onder normale omstandigheden de schade als er geskimd is, en kunnen reputatieschade oplopen (DNB, 2015). Het aantal incidenten dat verschijnt in nieuwsartikelen is veel lager dan het aantal gerapporteerd door DBN en ECB.

D4. Categorisatie en definities

Tabel 26 Long-list van definities van middelen die gebruikt is voor de mediasearch

Categorieën	Definities
Geïnfecteerd apparaat (Spyware/Sniffing/Datalek/Virus)	Cybercrime door middel van malafide software (virussen, etc.) op de computer/account/netwerk/website, behalve ransomware
Phishing (Pharming/Malvertising/Spoofing)	Cybercrime door middel van frauduleuze berichten, met als doel om informatie of geld uit een computer/account/netwerk/website te verkrijgen
Distributed Denial of Service (DDoS)	Cybercrime door middel van DDoS aanvallen met als doel om een computer/account/netwerk/website te laten crashen
Informatiehack	Cybercrime door middel van hacken, met als doel om informatie uit een computer/account/netwerk/website te verkrijgen
Defacement hack	Cybercrime door middel van hacken met als doel om een computer/account/netwerk/website te transformeren of uit te schakelen
Ransomware	Cybercrime door middel van ransomware (een type malware), met als doel om geld te verkrijgen in ruil voor toegang tot een computer/account/netwerk/website
Online bank- of pasfraude (Skimming)	Cybercrime door middel van betaalpas of online bankfraude
Koop- en verkoopfraude	Online fraude waar gekochte goederen niet geleverd of vervalst zijn, in vergelijking met hoe ze zijn aangeboden
Racistische/extremistische/kinderpornografische content	Cybercrime door bestaan van illegale aanstootgevende content op een computer/account/netwerk/website
Online illegale handel en illegaal downloaden	Cybercrime door middel van illegale handel van goederen of digitale piraterij om auteursrechtelijke informatie te verkrijgen via een computer/account/netwerk/website
Datalek door werknemers	Cybercrime door middel van verspreiding van vertrouwelijke informatie door een werknemer

Tabel 27 Categorisaties, definities en methodologie CBS (2013, 2014, 2015c)

Categorieën	Definities
Identiteitsfraude	Zonder toestemming via internet gebruik maken van iemands persoonlijke gegevens voor financieel gewin, bijv. voor het opnemen of overmaken van geld, het afsluiten van leningen of het opvragen van officiële documenten.
Koop- en verkoopfraude	Oplichting via internet bij het kopen of verkopen van goederen, bijv. doordat gekochte goederen niet geleverd werden of niet betaald werd voor geleverde diensten.
Hacken	Bij hacken wordt er met kwade bedoelingen ingebroken of ingelogd op een computer, emailaccount, website of profielsite (bijvoorbeeld facebook of twitter).
Methodologie	Jaarlijkse steekproef van de veiligheidsmonitor onder personen van boven de 15 jaar oud in Nederlandse particuliere huishoudens. door middel van een vragenlijst. De respons was in 2012 en 2013, ongeveer 30.000 en 60.000 personen (CBS, 2015a).

Tabel 28 Categorisaties, definities en methodologie van de Betaalvereniging (2014) en de DNB (2015)

Categorieën	Definities
Online bankfraude door malware	Door middel van deze schadelijke software worden normale online betalingsprocessen beïnvloed of wordt informatie gestolen. Ook komt het tegenwoordig voor dat via trojans een vervangende pas wordt aangevraagd.
Online bankfraude door phishing	Phishing is het ontfutselen van persoonlijke informatie, waaronder inlogcodes.
Overige	nog uit te vinden
Methodologie	nog uit te vinden

Tabel 29 Categorisaties, definities en methodologie TNO EuroBarometer (2012, 2013, 2015)

Categorieën	Definities
Geïnfecteerd apparaat	Ontdekking van malafide software (virussen, etc.) op een apparaat
Phishing	Frauduleuze e-mails of telefoontjes ontvangen die vragen naar toegang tot de computer, logins of persoonlijke details (inclusief bankier of betaal informatie)
Denial Of Service	Niet in staat zijn om toegang te verkrijgen tot online diensten (bijvoorbeeld bancaire of publieke diensten) vanwege cyberaanvallen
Slecht materiaal	Per ongeluk racistisch of extremistisch materiaal online tegenkomen
Hacking	Social media of emailaccount wordt gehackt
Koop- verkoop fraude	Online fraude waar gekochte goederen niet geleverd of vervalst zijn, in vergelijking met hoe ze zijn aangeboden
Ransomware	Gevraagd worden voor een betaling in ruil voor de teruggave van controle van het apparaat
Online bankier fraude	Slachtoffer zijn van betaalpas of online bankfraude
Identiteitsfraude	Persoonlijke data te stelen en iemand te imiteren door bijvoorbeeld te winkelen onder iemands naam
Kinderporno	Per ongeluk kinderporno online tegenkomen
Methodologie	Jaarlijkse steekproef van de Cyber Security EuroBarometer onder personen van boven de 15 jaar oud in Nederlandse particuliere huishoudens, door middel van een vragenlijst. De respons was elk jaar ongeveer 1.000 personen.

Tabel 30 Categorisaties, definities en methodologie Eurostat (2010)

Geïnfecteerd apparaat (E_SECIANY)	ICT related security incidents excluding disclosure of confidential data in electronic form by employees
Phishing (E_SECICNFA)	ICT related security incidents that resulted in disclosure of confidential data due to intrusion, pharming, phishing attacks
Datalek (E_SECICNFA)	ICT related security incidents resulting in disclosure of confidential data in electronic form by employees whether on intention or unintentionally
Malware (E_SECIDD)	ICT related security incidents that resulted in destruction or corruption of data due to infection or malicious software or unauthorised access
DDoS (E_SECIUSA)	ICT related security incidents that resulted in unavailability of ICT services due to attacks from outside, e.g. Denial of Service attack
Methodologie	Eenmalige steekproef in 2010 van 9.871 bedrijven in Nederland, door middel van een vragenlijst. De steekproef is gekozen door middel van een 'Neyman' allocatie, en bevat bedrijven met meer dan tien werknemers, met NACE codes C, D, E, F, G, H, I, J, L en N. De steekproef is uitgevoerd door het CBS.

Tabel 31 Zoekwoorden gebruikt in mediasearch via LexisNexis

* Aanval/dreiging/slachtoffer	Hacken/hacking/cyberhack
* Bank fraude	Hacktivisten
* Crime	Illegale online handel
* Criminaliteit	Inbreuk persoonlijke informatie
* Diefstal	Internet crime
* Fraude	IP/vertrouwelijke gegevens diefstal
* Illegaal bezit	Licentie protectie
* Inbraak	Malvertising/online advertising fraud
* Misbruik	Malware
* Misbruik/criminaliteit	Man-in-the-middle-aanval
* Schade	Morris-worm/Mydoom
* Verstoring/uitval	Netwerk aanval/dreiging/slachtoffer/criminaliteit
Anti-virus	Online Kinderporno
Applicatie aanval/dreiging/slachtoffer/criminaliteit	Online zwarte markten/Illegaal downloaden
Authenticatie probleem	Open SSL: heartbleed/poodle/freak/bar mitzvah
Bitcoin/digitale munt/cryptocurrency diefstal	Programmable logic controller/Blastervirus/Dorifel/Sasfis
CAPTCHA solving services	Ransomware/cryptoware/gijzelvirussen
Computer aanval/dreiging/slachtoffer/crime/criminaliteit	Scriptkiddies
Computer network security	Server aanval/dreiging/slachtoffer/criminaliteit
Computer virus	Skimming/skimmen/pasfraude/betalingsfraude
Computer Worm	(Spear-)Phishing/Pharming/social engineering
Criminele *dienst	Spoofing/identiteitsvervalsing
Datalek/data breach	Spyware/sniffing
DDoS	SQL-injectie/Logic bomb
Defacen/defacing/*vandalisme/*beschadigen	Trojan/trojaans/banking trojan
Diginotar	XSS/Cross Site Scripting

Deze lijst van woorden die cybercrime kunnen impliceren is tot stand gekomen na evaluatie van onze bronnen en de LexisNexis indextermen. Elk woord met een * is driemaal opgezocht, met de volgende voorvoegsels: cyber, online en digitale. Ook zijn een aantal woorden in het Engels opgezocht, waar gebruikelijk om Engelse verbasteringen te gebruiken.

Tabel 32 Categorieën cybercrime per middelen en manifestaties per beschikbare databron

	NCSC	Mediasearch	CBS	TNO EuroBarometer	Betaalvereniging / DNB / ECB	PwC	Eurostat
Middelen							
Geïnfecteerd apparaat (spyware of virus)	n.a.	T	n.a.	C	n.a.	B	C
Phishing	T	T	(als deel van identiteitsfraude)	C	n.a.	B	n.a.
Denial Of Service	T	T	n.a.	C	n.a.	n.a.	B
Hacking	T	T (defacement/informatie hack)	C	C	n.a.	B	n.a.
Koop- verkoop fraude	n.a.	n.a.	C	C	n.a.	n.a.	C
Ransomware	T	T	n.a.	C	n.a.	n.a.	n.a.
Online bankier- of Pasfraude	n.a.	T	(als deel van online bankierfraude)	C	C + B	n.a.	C
Identiteitsfraude	n.a.	Zie phishing en skimming	C (phishing / skimming)	C	n.a.	B	C
Racistisch/Extremistische en Kinderpornografische content	n.a.	**n.a.**	n.a.	C	n.a.	n.a.	C
Illegaal donwloaden	n.a.	**n.a.**	n.a.	n.a.	n.a.	B	n.a.
Datalek door eigen werknemers	T	**n.a.**	n.a.	n.a.	n.a.	n.a.	B

Bron:SEO Economisch Onderzoek; C: consumenten, B: bedrijfsleven; O: overheid; T: totale economie; n.a.: niet beschikbaar

Tabel 33 Informatiebronnen betreffend cyberstatistieken

Naam organisatie	Type organisatie
Accenture	Consultancy
AIVD (Algemene Inlichtingen- en Veiligheidsdienst)	Overheid
Akamai / State of the Internet	ICT
Arbor Networks (Digital Attack Map)	ICT
AV-Test Institute	ICT
Betaalvereniging	Vereniging
BREIN	ICT
Capgemini	Consultancy
CBS (Central Bureau voor Statistiek)	Overheid
Deloitte	Consultancy
DNB (De Nederlandsche Bank)	Overheid
ECB (European Central Bank)	Overheid
Eurostat	Overheid
E&Y	Consultancy
Electronic Crimes Taskforce	Overheid
EMC2	ICT
ENCS (European Network for Cyber Security)	Vereniging
Fox-IT	ICT
Fraudehelpdesk	Overheid
F-Secure	ICT
Google (Digital Attack MaP)	ICT
Intel Security / McAfee	ICT
Kaspersky Lab	ICT
KPN	ICT
NCSC (Nationaal Cybersecurity Centrum; Ministerie van V&J; NCTV)	Overheid
NederlandICT	Vereniging
NVB (Nederlandse Vereniging van Banken)	Vereniging
Politie	Overheid
PwC	Consultancy
Security Delta	Overheid
Security Matters	ICT
Thuiswinkel.org	Anders
Vasco Authentication	ICT
Vereniging Abuse Information Exchange	Vereniging
WikiLeaks	Anders

D5. Uitgebreide data

Tabel 34 Aantal incidenten, schade en stilstaande dagen tussen vormen van cybercrime in de wereld

	Incidenten	Schade	Stilstaande periode
	%	Dollar	Dagen
Cyberspionage	35	144.542	54,4
DDoS	51	126.545	19,3
Webgebaseerd aanval	64	96.424	27,7
Phishing & Social engineering	62	85.959	21,9
Malicious codes	59	81.500	47,5
Gestolen apparaat	45	33.565	12,3
Malware	98	7.378	5,8
Virussen	99	1.900	2,4
Botnets	59	1.075	2,2

Bron: Ponemon Institute (2015). n = 252 bedrijven in 7 landen

Tabel 35 Cybercrime in Nederland per sector

	%
Groot- en retailhandel	39
Financiële instellingen	34
ICT	24
Advertising, onderzoek en overige specialistische dienstverlening	23
Industrie	22
(Semi-) overheidsinstellingen	20
Onderwijs	16
Gezondheids- en welzijnszorg	15
Overig	29

Bron: PWC (2014)

Tabel 36 Vormen van cybercrime in Nederland

	%
Phishing en pharming	24,2
Virussen	24,2
Hacken	16
Illegaal onderscheppen van computergegevens	8,2
Illegaal downloaden	8,2
Identiteitsdiefstal	6,7
Intentionele schade op computersystemen en gegevens	6,2
Cyberspionage	1,5

Bron: PWC (2014)

Tabel 37 Aantal frauduleuze transacties en financiële schade in miljoenen euro's per 1000 inwoners in EU-landen

	Aantal frauduleuze transacties per 1000 inwoners			Financiële schade in miljoenen euro's per 1000 inwoners		
	2012	2013	2014	2012	2013	2014
GB	40,5	47,4	67,5	6.132	7.506	8.132
LU	36,6	34,1	37,7	7.821	7.602	7.990
IE	22,3	22,2	38,4	5.481	4.896	6.581
DK	20,3	26,7	33,4	3.276	4.830	5.721
FR	39	46,4	52,9	4.525	5.177	5.695
BE	9,9	11,5	16,4	1.780	2.158	2.901
SE	12,5	14,6	15,6	1.900	2.330	2.565
MT	15,8	13,2	13,5	2.750	2.738	2.501
AT	8,8	10	12,8	1.921	2.182	2.306
NL	***15,1***	***14,6***	***9,8***	***3.183***	***3.090***	***2.046***
DE	7,6	8,2	9,7	1.618	1.743	1.813
FI	7,4	8	8,6	1.276	1.538	1.684
IT	4,2	4,2	7	899	898	1.298
CY	10,4	10,3	8	2.213	1.660	1.297
ES	14,2	14,4	14,3	959	1.046	1.004
EE	3,7	4	4,7	653	651	711
PT	3,9	5,1	4,5	714	1.002	682
LV	3,1	3,4	3,6	487	551	512
SI	3,1	2,8	3,1	482	378	404
CZ	1,6	2,2	2,8	491	304	305
GR	3	2,5	2,3	668	362	249
HR	0	0	1,5			185
SK	0,9	1,3	1,6	123	158	161
LT	1	1	1,1	154	165	150
BG	0,7	1	1,2	92	126	144
PL	0,6	0,9	1,1	94	128	125
HU	0,8	0,9	1	120	119	101
RO	0,4	0,5	0,6	48	53	73
SEPA	*15,3*	*17,4*	*20,3*	*2.253*	*2.580*	*2.599*
EU	*10,6*	*11,5*	*13,4*	*1.847*	*1.977*	*2.077*

Bron: ECB (2013, 2014, 2015)

Tabel 38 Aandeel bedrijven dat in aanraking is gekomen met bepaalde vormen van cybercrime, in percentage van de gevraagde bedrijven

	2010
Denial of Service	7
Alle vormen (excl. Lek van personeel)	22
Geen vormen	78
Lek van personeel	4

Bron: Eurostat (2011)

D6. Data uit mediasearch

De LexisNexis academische bibliotheek kan naar deze woorden zoeken in een krantenartikel, maar ook in zogeheten *indextermen* die elk artikel typeren. Booleaanse operatoren zijn, waar nodig, gebruikt om dubbele zoek resultaten te voorkomen. Drie veelgebruikte operatoren zijn AND, OR en NOT. Door bijvoorbeeld te zoeken op "cybercrime AND fraude NOT skimming" worden artikelen uitgezocht die de woorden cybercrime en fraude in het document of de indextermen bevat, maar niet het woord skimming in het document of in de indextermen bevat.

Voor elk geselecteerd nieuwsartikel is het volgende vastgelegd: *De titel; bron; datum; omvang schade; de eigenaar van de schade (slachtoffer): consumenten/bedrijven/overheden; de categorie* waartoe het middel voor de schade behoort uit Tabel 26 in de Bijlage. Een artikel kan meerdere slachtoffers en categorieën raken. Artikelen die gaan over hetzelfde incident zónder nieuwe informatie te bieden over de omvang schade, doelgroep schade, of de categorie, zijn niet apart vastgelegd.

Tabel 39 Aantal incidenten per middelen en type slachtoffer

	Consumenten	Bedrijfsleven	Overheid
Geïnfecteerde apparaten	19	19	11
Phishing	39	7	3
DDoS	8	26	10
Informatiehack	27	25	8
Defacement hack	1	15	1
Ransomware	11	4	8
Online bank- en pasfraude	70	44	0

Bron:SEO Economisch Onderzoek via mediasearch in de periode 01-01-2010 en 01-12-2015

Informatie over andere middelen via mediasearch

In de categorie geïnfecteerde apparaten waren er 34 incidenten in het nieuws. De in het nieuws bekende virusinfecties hebben voor systeemuitvallen gezorgd, ter preventie van informatielekken. Hierdoor waren belangrijke diensten als DigiD of CT-scans in ziekenhuizen niet beschikbaar. Daarnaast meldt één nieuwsbericht dat er met sommige spyware voor één miljoen euro is gestolen van consumenten, door middel van diefstal van de financiële informatie.

Er was één type spyware dat in het oog springt: het Dorifel virus. In 2013 werden meer dan 30 grote instellingen geïnfecteerd, waaronder veel gemeentes en universiteiten. Data werd gestolen, vele netwerken zijn dagenlang uit de lucht geweest, en productiviteit werd gehinderd. Virusinfecties hebben alle typen slachtoffers getroffen.

In de categorie *phishing* zijn er 44 incidenten in het nieuws gemeld. De incidenten lopen zeer uiteen wat betreft omvang, van hele kleine bedragen tot 70.000 euro. Niet alleen banken, maar ook organisaties als webshops, scholen, het Centraal Justitieel Incassobureau en PostNL zijn

gebruikt als dekmantel. Phishing aanvallen kwamen vooral voor bij consumenten. Er is een stijgende trend waarneembaar.

In de categorie Distributed Denial of Service (DDoS) waren er in totaal 35 incidenten in het nieuws. DDoS-aanvallen hebben er in ten minste drie incidenten voor gezorgd dat grote netwerken zijn platgelegd van Internet Service Providers (ISPs), waardoor honderdduizenden mensen beïnvloed werden. In verreweg de meest incidenten was er sprake van aanvallen op netwerken van individuele bedrijven of overheidsinstanties. Deze aanvallen zorgden ervoor dat vele online diensten niet meer beschikbaar waren, waaronder die van scholen, banken, nieuws instanties, gemeentes en telefonie providers. Alleen de DDoS incidenten die schoolnetwerken of ISPs hebben platgelegd zijn geclassificeerd als directe schade voor consumenten. De exacte schade is onbekend.

Betreffend *informatiehacks* zijn er 43 incidenten in het nieuws gemeld. Informatiehacks hebben in 27 incidenten ervoor gezorgd dat enkele individuele gegevens of netwerken zijn gekraakt. In 16 incidenten was er daarentegen sprake van grootschalige hacks bij bedrijven, waarbij tussen de 1.000 en 1,3 miljoen accounts zijn verkregen. Zowel grote multinationals als individuele partijen zijn slachtoffer geworden. Een aantal grote hacks is geclassificeerd als schade voor consumenten én bedrijven, omdat persoonsgegevens werden gestolen uit de databases van bedrijven. De exacte schade is onbekend.

In de categorie *defacement hack* waren er 16 incidenten in het nieuws in totaal. Wanneer het netwerk of een aantal computers van een kleine instelling geraakt worden kunnen er tienduizenden euro's schade ontstaan vanwege verlies aan productiviteit en herstelkosten. In 2010 was er eenmalig een golf waarneembaar waarbij honderden websites zijn gewist of gewijzigd. In negen incidenten ging het om een gesubsidieerde instellingen of vereniging.

19 ransomware-incidenten zijn in het nieuws gemeld. In alle 11 incidenten bij consumenten zijn grote groepen mensen opgelicht voor honderden euro's per keer. Bij elkaar zijn er vele duizenden computers besmet. Wanneer het netwerk of een aantal computers van een kleine instelling geraakt worden kunnen er tienduizenden euro's schade ontstaan vanwege verlies aan productiviteit en herstelkosten. De meeste ransomware was gericht op consumenten, maar enkele grotere infectiegolven raakten alle doelgroepen.

Tabel 40 Aantal incidenten geïnfecteerde apparaten (Spyware virussen)

	Consumenten	Bedrijfsleven	Overheid
2010	2	4	1
2011	5	3	4
2012	3	4	4
2013	4	2	1
2014	3	3	1
2015	2	3	0
Totaal	**19**	**19**	**11**

Bron: SEO Economisch Onderzoek

Tabel 41 Aantal incidenten Phishing

	Consumenten	Bedrijfsleven	Overheid
2010	5	0	0
2011	10	1	0
2012	6	1	1
2013	4	3	0
2014	7	1	0
2015	7	1	2
Totaal	**39**	**7**	**3**

Bron: SEO Economisch Onderzoek

Tabel 42 Aantal incidenten Distributed Denial of Service (DDoS)

	Consumenten	Bedrijfsleven	Overheid
2010	0	1	1
2011	0	2	1
2012	1	1	0
2013	1	6	4
2014	1	2	1
2015	5	14	3
Totaal	**8**	**26**	**10**

Bron: SEO Economisch Onderzoek

Tabel 43 Aantal incidenten Informatiehack

	Consumenten	Bedrijfsleven	Overheid
2010	0	0	0
2011	8	6	4
2012	7	9	2
2013	3	1	0
2014	8	7	0
2015	1	2	2
Totaal	**27**	**25**	**8**

Bron: SEO Economisch Onderzoek

Tabel 44 Aantal incidenten Defacement hack

	Consumenten	Bedrijfsleven	Overheid
2010	0	4	0
2011	0	1	1
2012	0	4	0
2013	0	3	0
2014	1	1	0
2015	0	1	0
Totaal	**1**	**15**	**1**

Bron: SEO Economisch Onderzoek

Tabel 45 Aantal incidenten Ransomware

	Consumenten	Bedrijfsleven	Overheid
2010	0	0	0
2011	1	0	0
2012	1	0	1
2013	3	0	0
2014	5	3	3
2015	1	1	4
Totaal	**11**	**4**	**8**

Bron: SEO Economisch Onderzoek

Tabel 46 Aantal incidenten Online bank- of pasfraude

	Consumenten	Bedrijfsleven	Overheid
2010	22	24	0
2011	18	18	0
2012	22	22	0
2013	9	7	0
2014	10	5	0
2015	4	3	0
Totaal	**70**	**44**	**0**

Bron: SEO Economisch Onderzoek

E Marktfalen

Deze bijlage vormt de achtergrond bij het analysekader uit paragraaf 6.2.

Als markten taken niet efficiënt kunnen uitvoeren, is er sprake van marktfalen. Er kunnen vier soorten marktfalen worden onderscheiden met betrekking tot cybersecurity-producten en -diensten:[21]

1. Publieke goederen
2. Positieve externe effecten
3. Asymmetrie van informatie
4. Marktmacht

Ad 1) **Publieke goederen** zijn producten of diensten die niet-uitsluitbaar en niet-rivaliserend zijn. Dit betekent dat het produceren van publieke goederen door de markt niet mogelijk is, omdat geen partij mag worden uitgesloten van de voordelen en het gebruik van deze goederen (niet-uitsluitbaarheid) en dat het gebruik door een consument niet ten koste mag gaan van het gebruik door andere consumenten (niet-rivaliserend). Hierdoor zijn publieke goederen vaak gekoppeld aan willekeurig gedrag: consumenten kunnen gebruikmaken van publieke goederen zonder eraan bij te dragen (ervoor te betalen). Voorbeelden van publieke goederen zijn defensie en dijken.
Deze voorbeelden geven aan dat cybersecurity ook kenmerken heeft van een publiek goed. In algemeen zin kan geen enkele gebruiker van een veilig internet worden uitgesloten. Daarnaast is veiligheid ook niet-rivaliserend: de veiligheid van gebruiker A gaat niet ten koste van gebruiker B.

Ad 2) **Positieve externe effecten**. Het kan gebeuren dat de productie van goederen en diensten gevolgen heeft buiten de desbetreffende markt (bijvoorbeeld op andere markten) en dat marktspelers die gevolgen niet meenemen in de kosten en baten bij het nemen van marktbeslissingen. Deze effecten worden externe effecten of externaliteiten genoemd. Externe effecten hebben geen markt en dus ook geen prijs. De maatschappelijke kosten of baten die rekening houden met deze externe effecten zijn hoger dan, respectievelijk, de particuliere kosten of baten. Externe effecten kunnen negatief of positief zijn. In de markt van cybersecurity-producten en -diensten is er sprake van positieve externaliteiten. Externe effecten zijn positief als de sociale baten van een activiteit hoger zijn dan de particuliere baten en de markt deze baten niet kan internaliseren. In de cybersecuritysector kan er sprake zijn van twee soort positieve externaliteiten: kennis-spillovers en netwerkexternaliteiten:

- *Kennis-spillovers*:[22] Kennis-spillovers vinden plaats in het innovatieproces. Als kennis-spillovers niet geïnternaliseerd is, vindt er wellicht minder innovatie plaats dan sociaal wenselijk is. Kennis-spillovers leiden tot externaliteiten als bedrijven niet alle vruchten

---

21 Voor een overzicht van marktfalen, zie bijvoorbeeld Baarsma & De Nooij (2006), Saline (2000).

22 Bijlsma et al. (2009).

van hun investeringen in kennis en innovatie kunnen plukken omdat andere bedrijven die kennis gebruiken zonder daarvoor het volle pond te betalen. De tekortkomingen van het systeem van intellectuele eigendomsrechten (IER) zijn hier mede schuldig aan: het is niet altijd mogelijk IER aan te vragen. En als het wel mogelijk is, kan dit hoge kosten met zich meebrengen. Ook de periode en de omvang van ideeën waarover innovators worden beschermd door middel van IER, zijn beperkt. De stimuli om te innoveren nemen dus af. Hierdoor ontstaat een lager dan sociaal optimaal innovatieniveau en vermindert de welvaart op de lange termijn.

- *Netwerkexternaliteiten*:[23] Netwerkexternaliteiten vinden plaats in de vraagkant van de markt. Netwerkeffect betekent dat de waarde van een product of dienst voor een consument hoger is als er meer consumenten ook gebruik maken van hetzelfde product of dienst. ICT-producten zijn typisch gekenmerkt met netwerkexternaliteiten. Hier kan DNSSEC als voorbeeld gelden. Invoering van deze standaard kent aanvankelijk een 'hobbel' omdat niemand er gebruikt van maakt, maar naarmate de standaard ingeburgerd raakt neemt de toepassing meer dan proportioneel toe.

Ad 3) **Asymmetrie van informatie**:[24] Als een partij in de markt beschikt over meer of betere informatie dan een andere partij, bestaat de kans op een suboptimale prijs, hoeveelheid of kwaliteit. Onvolledige informatie kan van invloed zijn op de prijzen (of vraag), kosten, risico's en kwaliteit. In de cybersecurity-sector kan er sprake zijn van adverse selectie. Dat wil zeggen dat een belangrijk kenmerk van een product of het bedrijf alleen van tevoren bekend is bij het bedrijf, voordat de afnemer ze afneemt. Dit kenmerk kan bijvoorbeeld de kwaliteit van een product of dienst zijn. Consumenten zijn bereid meer te betalen voor een betere kwaliteit, maar kunnen die kwaliteit niet van tevoren controleren. Producenten van een product met een mindere kwaliteit zullen een lagere prijs hanteren. Producenten van een product met een hogere kwaliteit zouden graag een hogere prijs berekenen, maar consumenten willen geen meerprijs betalen als de hogere kwaliteit van het product niet kan worden geverifieerd. Dit probleem is adverse selectie genoemd. Met betrekking van de cybersecurity-sector kan er sprake zijn van adverse selectie in de kapitaalmarkt.[25] Meer innovatieve bedrijven hebben hierdoor moeite financiering te krijgen en komen uiteindelijk niet tot bloei.

Ad. 4) Door **marktmacht** vermindert de concurrentiedruk.[26] Naarmate de marktmacht toeneemt, stijgen de prijzen, dalen de productie- en verkoopcijfers en investeren bedrijven minder in innovatie, kwaliteit en capaciteit. Het eindresultaat van marktmacht is een afname in economische welvaart. Dit is de som van het verlies aan consumentenwelvaart dat ontstaat ten gevolge van marktmacht en de mogelijke extra winst van de producent door marktmacht

---

23 Shapiro & Varian (1998), Shy (2001).

24 Akerlof (1970).

25 Merton (1987).

26 Zie bijvoorbeeld Motta (2004).

(producentensurplus). Concurrentie wordt minder hevig als er toetredingsbelemmeringen zijn. Bij toetredingsbelemmeringen verhogen bedrijven de prijzen tot boven het efficiënte niveau. Er zijn diverse vormen van toetredingsbelemmeringen die relevant kunnen zijn voor de cybersecuritymarkt:

Schaalvergroting: Schaalvergroting verwijst naar de afname van de kosten per eenheid naarmate de capaciteit of de productie van een bedrijf toeneemt. In deze markten zijn investeringen vaak kapitaalintensief met een grote vast component, die net gevoelig is voor de omvang van de productie. Schaalvergroting biedt grote bedrijven dan een kostenvoordelen waardoor de markt gedomineerd zal worden door een beperkt aantal bedrijven. Maatschappelijk gezien is dit ook de wenselijke situatie. Maar als schaalvergroting leidt tot marktmacht, kunnen bedrijven een hogere prijs berekenen dan het efficiënte niveau of minder investeren dan maatschappelijk gezien wenselijk is. De welvaartswinst slaat dan alleen bij producenten neer en komt niet ten goede aan de consument. In de ICT-sector is er sprake van schaaleffecten. Een geconcentreerde markt is dan de logische uitkomst van het marktproces met alle problemen van dien voor de concurrentieverhoudingen en de prijsvorming.

Fusies en overnames: Een overname van of fusie met een concurrerend bedrijf of een ander bedrijf in de verticale keten kan winst aan efficiency opleveren voor de overnemende of fuserende bedrijven. Een negatief gevolg hiervan is echter dat de horizontale markt meer geconcentreerd raakt en de prijzen stijgen. In plaats daarvan kunnen deze bedrijven eerst ook een lagere prijs berekenen, waarmee ze concurrerende bedrijven van de markt kunnen uitsluiten, waardoor de concentratie nog hoger wordt.

Padafhankelijkheid:[27] Sommige markten worden gekenmerkt door padafhankelijkheid en technologische superioriteit. Ten gevolge van een historische ontwikkeling die is beïnvloed door de accumulatie van kennis in R&D, verloopt technologische ontwikkeling vaak volgens een bepaald patroon. Dit noemen we padafhankelijkheid. Voorbeelden hiervan zijn innovaties in de software-industrie. De markt zit daardoor vast aan bestaande technologieën of platforms en nieuwe, potentieel betere producten of technologieën worden niet uitgevonden. Padafhankelijkheid is van invloed op kennis-spillovers en netwerkexternaliteiten, maar vooral op marktmacht: het belemmert concurrerende technologieën en leveranciers namelijk toe te treden tot de markt.

Institutionele belemmeringen – intellectueel eigendomsrechten:[28] Het systeem van intellectueel eigendomsrechten heeft als doel innovaties van bedrijven te beschermen en biedt innovators de mogelijkheid hun kosten voor onderzoek en ontwikkeling terug te verdienen via licentiekosten. De licentiekosten vormen een kostenelement voor volgende innovators. Licentiekosten werken

---

27 Zie bijvoorbeeld Arthur (1989).

28 Bijlsma et al. (2009).

marktmacht in de hand, om twee redenen: de hoogte van licentiekosten en voordeel van de koploper (‘first mover’).

Onvolledige contracten en het hold-up probleem:[29] Volgens de contracttheorie kunnen inefficiënties ontstaan vanwege de moeilijkheden om volledige contracten te schrijven. Een van de meest voorkomende problemen is het hold-up probleem. Het hold-up probleem is een situatie waar beide gecontracteerde partijen in staat zijn om zo efficiënt mogelijk samen te werken (bv. een arbeidscontract te schrijven), maar de contract kan niet tot stand komen: partij A heeft bezorgdheid dat partij B niet gaat committeren aan hun afspraak omdat na het contracteren B ook een andere mogelijkheid krijgt met een hogere waarde (met andere woorden heeft partij B onderhandelingsmacht). Vanwege deze hogere waarde gaat B de eerdere contractwaarde niet meer accepteren ('hold-up') en een hogere contractwaarde vragen. Partij A weet dit van tevoren en gaat het contract niet aanbieden. De samenwerking komt dus niet tot stand. Het hold-up probleem kan leiden tot hoge economische kosten en onderinvestering. Bijvoorbeeld kan een cybersecurity-bedrijf een gecombineerd arbeids- en opleidingscontract schrijven met een student dat hij na de periode bij het bedrijf gaat werken. Maar door de opleiding wordt de waarde van de student hoger in de arbeidsmarkt en kan hij waarschijnlijk meer verdienen bij een ander bedrijf. Dit wetend gaat de student na de opleiding een hoger salaris vragen en om het verlies te voorkomen gaat het bedrijf het opleidingscontract niet aanbieden.

[29] Laing et al. (1995), Acemoglu (1996).