Centraal Planbureau

Risicorapportage cyberveiligheid economie 2019

De risico's op **maatschappelijke schade** door cyberincidenten lijken in de toekomst toe te nemen door **verdere digitalisering.**

Het is vaak onduidelijk wat de financiële én maatschappelijke gevolgen zijn van een digitale aanval of van digitale spionage.

Dat komt doordat bedrijven:

1) niet iedere aanval opmerken;

2) niet iedere aanval publiek bekend willen maken;

3) niet altijd kunnen inschatten wat de gevolgen van een hack of diefstal zijn op de lange termijn.

Door het incomplete beeld van de kosten en baten van investeringen in cyberveiligheid kan het investeringsniveau te hoog of te laag zijn.

Het gebrek aan inzicht belemmert ook de ontwikkeling van een verzekeringsmarkt voor cyberrisico's.

CPB Notitie

Bastiaan Overvest, Marielle Non, Milena Dinkova, Ramy El-Dardiry en Rinske Windig

oktober 2019

Betere informatie cruciaal

Bekend is dat cyberaanvallen plaatsvinden bij bedrijven, huishoudens en overheden

Onbekend is hoe vaak verstoringen plaatsvinden, door wie en met welke gevolgen

Gebruikers investeren daardoor mogelijk te weinig of te veel in cyberveiligheid

Risicorapportage cyberveiligheid economie 2019

Risico's op ontwrichting

Dreiging is complex en evolueert continu

Vitale processen zijn vatbaarder geworden voor ICT-verstoringen. Dat kan leiden tot maatschappelijke ontwrichting

Niet-vitale processen zijn verweven met vitale infrastructuur waardoor de keten kwetsbaarder is

Nieuwe risico's

Kunstmatige intelligentie maakt personalisering van aanvallen mogelijk en kan sneller kwetsbaarheden in systemen vinden

5G faciliteert via hogere bandbreedte nieuwe Internet-of-Things-toepassingen. Hierdoor worden cyberdelicten zichtbaarder buiten de virtuele wereld

Uitdagingen voor bedrijven en burgers

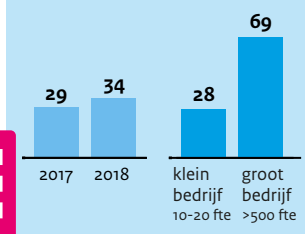
- → Hoeveel investeren in cyberveiligheid? Effecten van investeringen zijn moeilijk meetbaar
- → Hoe de informatieachterstand in te lopen als dreigingen en veiligheidsmaatregelen zich zo snel ontwikkelen?
- → Hoe veiligheid te borgen bij aaneenschakeling van ICT-toepassingen?

Uitdagingen voor overheid

- → Hoe voorlichting geven aan miljoenen gebruikers en honderdduizenden bedrijven?
- → Maatregelen tegen desinformatie overlaten aan sociale media of reguleren?
- → In hoeverre is stimuleren van samenwerking tussen organisaties effectief?

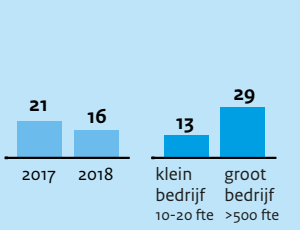
Kleine bedrijven nemen minder maatregelen dan grote bedrijven

% van bedrijven die data versleutelen



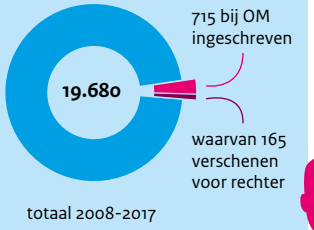
Bedrijven rapporteren **minder ICT-incidenten**

% van bedrijven die met een aanval van buiten te maken kregen



Meeste cyberdelicten komen **niet bij de rechter**

aantal geregisteerde delicten van computervredebreuk



bron: CBS

1 Inleiding

1.1 Samenvatting

1.1.1 Blijvende risico's, nieuwe risico's en onzekerheid

De risico's op ontwrichtende cyberincidenten zijn niet afgenomen. Vitale processen zijn afhankelijk van ICT. Technologische ontwikkelingen zoals 5G zullen deze afhankelijkheid van digitale processen, zowel binnen als buiten de vitale infrastructuur, alleen maar vergroten. Met de aanhoudende internationale politieke onrust blijft ook het risico bestaan dat statelijke actoren moedwillig vitale infrastructuur verstoren. Door de combinatie van blijvende geopolitieke dreigingen en toenemende digitalisering vormt digitale ontwrichting voor de samenleving een reëel risico.

De snelle ontwikkelingen op het gebied van kunstmatige intelligentie (KI) zorgen voor nieuwe risico's, maar ook voor nieuwe kansen voor cyberveiligheid. Het onderzoek naar KI zit in een bloeifase: algoritmes worden bijvoorbeeld steeds beter in patroonherkenning en in het maken van beslissingen in complexe situaties. Sommige toepassingen van KI kunnen leiden tot nieuwe of grotere risico's voor cyberveiligheid. Een voorbeeld is *deepfake*, waarbij KI-technieken gebruikt worden om foto's of video's te genereren. Deze techniek kan ingezet worden door statelijke actoren bij het verspreiden van desinformatie. Ook kunnen cybercriminelen *deepfake* inzetten als onderdeel van *spearphishing* (het sturen van gerichte en gepersonaliseerde e-mails met het heimelijke doel om informatie te verkrijgen of te hacken) of identiteitsfraude. KI kan mogelijk ook gebruikt worden voor het snel en systematisch vinden van softwarekwetsbaarheden, met het doel om deze kwetsbaarheden vervolgens te misbruiken. KI biedt aan de andere kant ook kansen voor cyberveiligheid. KI kan helpen bij het detecteren van *deepfake* en andere vormen van desinformatie, DDoS-aanvallen of malafide websites. De mogelijkheid om softwarekwetsbaarheden op te sporen kan ingezet worden door softwareontwikkelaars, waardoor voorkomen wordt dat kwetsbare software op de markt komt.

Onzekerheid en onvolledige informatie bemoeilijken beleid voor cyberveiligheid. Er circuleren meerdere adviezen en richtlijnen over het optimale niveau van investeringen in cyberveiligheid en over welke maatregelen genomen zouden moeten worden. Desondanks, of juist daardoor, is het voor individuele gebruikers en organisaties moeilijk om goed geïnformeerde maatregelen te nemen. Deels komt dit doordat bestaande adviezen en richtlijnen niet 1-op-1 van toepassing zijn op specifieke gebruikers en organisaties. Deels komt dit ook doordat informatie ontbreekt over de omvang van cyberrisico's en de financiële gevolgen. En tot slot kan een deel van de gevolgen van inadequate cyberveiligheid bij derden neerslaan. Door dit informatiegebrek kunnen gebruikers het rendement van investeringen in veiligheid niet bepalen. Dit gebrek aan informatie vormt een belemmering voor overheidsbeleid: in hoeverre is het stimuleren van private en publieke investeringen in cyberveiligheid wenselijk? Voor cyberverzekeraars betekent het gebrek aan informatie dat premies niet goed risico-gebaseerd kunnen zijn.

Het versplinterde landschap van initiatieven op het gebied van samenwerking en voorlichting kan informatievoorziening belemmeren. De overheid informeert verschillende doelgroepen over cyberrisico's via meerdere kanalen. Daarnaast stimuleert de overheid verschillende (publiek-private) samenwerkingsverbanden om deelnemers aan te moedigen om informatie en ervaringen te delen. Deze initiatieven voor samenwerking en voorlichting overlappen soms. Risico's van deze 'versplintering' zijn dat doelgroepen minder goed weten waar ze relevante informatie kunnen vinden, dat initiatieven dubbel werk doen, of juist dat belangrijke thema's blijven liggen.

1.1.2 Bedrijven hebben weerbaarheid verhoogd, huishoudens blijven achter

Nederlandse bedrijven hebben in het afgelopen jaar meer maatregelen genomen ter verhoging van weerbaarheid. Bedrijven namen in 2018 vaker maatregelen ter vergroting van de weerbaarheid tegen digitale verstoringen. Zo steeg het percentage bedrijven dat tweefactor-authenticatie toepast met negen procentpunt (34 procent in 2017) en maakten meer bedrijven logbestanden aan voor de analyse van incidenten (van 55 procent in 2017 naar 60 procent in 2018). Minder bedrijven hadden kosten na een ICT-incident door een aanval van buitenaf: 1,3 procent in 2018 tegen 2,3 procent in 2017. Een kanttekening bij deze cijfers is dat vooral bij kleinere bedrijven de adoptie van maatregelen achterblijft, waardoor zij meer vermijdbare risico's lopen.

Huishoudens blijven kwetsbaar. 8,5 procent was in 2018 slachtoffer van een digitaal misdrijf. Vooral de kennis van huishoudens over nieuwe cyberrisico's is beperkt. Minder alerte gebruikers lijken risico's te lopen als KI wordt toegepast in (*spear*)*phishing* en in het genereren van desinformatie.

1.2 Afbakening en onderzoeksverantwoording

Net als de voorgaande risicorapportages is het doel van deze notitie om inzicht te bieden in de trends, oorzaken en economische gevolgen van verschillende cyberrisico's. De focus van deze rapportage ligt vooral, maar niet uitsluitend, op Nederland en het afgelopen jaar (vanaf de verschijning van de vorige risicorapportage op 15 oktober 2018). Over wat cyberrisico's zijn, bestaan verschillende ideeën en definities. De definitie van het NCSC van cyberveiligheid 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." Uitgaande van deze definitie zijn cyberrisico's dreigingen die schade, uitval of misbruik van ICT kunnen veroorzaken. DDoS-aanvallen en *ransomware* (gijzelsoftware) vallen duidelijk onder deze definitie en worden dan ook besproken in deze rapportage.

In deze rapportage beschouwen we cyberveiligheid vanuit een breder perspectief dan alleen het klassieke op ICT-gerichte perspectief. Centraal staan in dit rapport de dreigingen en manifestaties die via digitale middelen de economie en de samenleving treffen. Het gevolg van deze bredere afbakening is dat cybercriminaliteit en de bestrijding daarvan ook binnen de scope van deze rapportage liggen. Daarbij gaat het om misdrijven die met behulp van digitale methoden worden gepleegd. *Phishing* en (aan)koopfraude kunnen weliswaar ook zonder digitale middelen worden gepleegd, maar digitale middelen (e-mail, handelsplatformen, sociale media) veranderen de schaalbaarheid en daarmee het maatschappelijke gewicht van deze delicten. Naast cybercriminaliteit zijn ook desinformatie en economische spionage belangrijke dreigingen die het vertrouwen in de digitale ruimte kunnen aantasten. Vaak zijn statelijke actoren verantwoordelijk voor deze dreigingen. Hoewel desinformatie en economische spionage ook zonder digitale middelen kunnen plaatsvinden, zorgen digitale kanalen, zoals sociale media, gebruik van softwarekwetsbaarheden en digitaal opgeslagen informatie ervoor dat de omvang ervan veel groter kan worden. De fysieke veiligheid van de Nederlandse digitale infrastructuur valt buiten de scope van deze rapportage.

De notitie is mede gefinancierd door het ministerie van Justitie en Veiligheid (J&V). Tijdens het schrijven is gebruik gemaakt van de adviezen van een klankbordgroep en inzichten uit gesprekken met diverse experts en stakeholders. We willen al deze mensen en organisaties bedanken voor hun bereidheid om te helpen en mee te denken. De verantwoordelijkheid voor de notitie ligt volledig bij het CPB.

Sinds 2016 is jaarlijks een risicorapportage cyberveiligheid economie verschenen. Deze risicorapportage is voorlopig de laatste in deze vorm. De risicorapportages hebben voor een groot aantal risico's en 'knelpunten' (zoals de arbeidsmarkt voor ICT'ers, de markt voor cyberveiligheidsdiensten, of de markt voor DDoS-mitigatie) vanuit een economisch perspectief de achterliggende oorzaken ('marktfalen') in kaart gebracht en, waar dat

mogelijk is, inzichten geboden in de kwantitatieve omvang van trends en de economische impact van risico's. Inzicht in de (economische) oorzaken en impact van verstoringen van cyberveiligheid blijft belangrijke informatie voor beleid, maar zal in de toekomst op een andere manier tot stand moeten komen. Dat kan in de vorm van gerichte empirische studies of een risicorapportage met een lagere frequentie.

1.3 Leeswijzer

Deze risicorapportage cyberveiligheid economie 2019 (RCE2019) biedt een samenhangende bespreking van de belangrijkste risico's vanuit het cyberdomein voor de economie en uiteindelijk voor de samenleving. In hoofdstuk 2 beschrijven we voor specifieke manifestaties en dreigingen de ontwikkelingen van het afgelopen jaar – hoe vaak kwam een bepaalde manifestatie bijvoorbeeld voor in Nederland en ook daarbuiten. Daarbij geven we, aan de hand van beleidsontwikkelingen of technologische ontwikkelingen, een indicatie van de toekomstige risico's. Hoofdstuk 2 is vooral beschrijvend van aard. Voor het economische perspectief van marktfalen en de bespreking van de mogelijke economische impact verwijzen we naar eerdere edities van de risicorapportage. In hoofdstuk 3 staat de impact centraal van (veelal) digitale dreigingen op de economie en de samenleving. Het gaat daarbij dus niet om het middel, zoals in hoofdstuk 2, maar om het doel of gevolg. Het afsluitende hoofdstuk gaat in op preventieve en mitigerende maatregelen.

2 Risicobeeld cyberrisico's

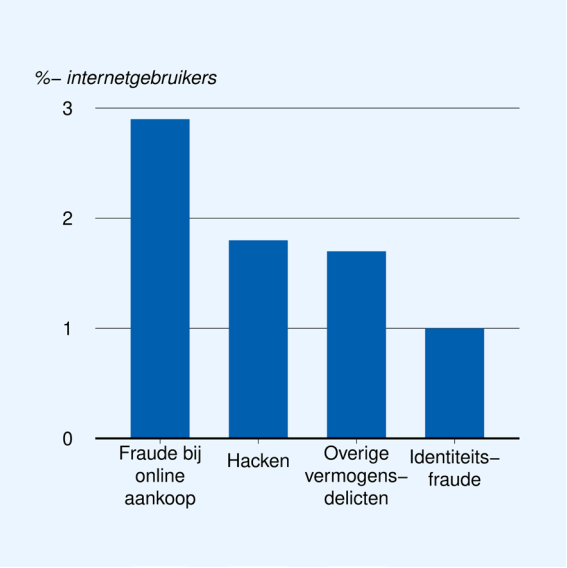
2.1 Inleiding

Op 24 juni van dit jaar was het noodnummer 112 enkele uren onbereikbaar. Hoewel deze storing volgens KPN niet werd veroorzaakt door een hack en het onderzoek naar de oorzaak nog loopt, illustreert deze uitval wel dat onze samenleving afhankelijk is van digitale systemen. Behalve de 112-storing vonden, voor zover nu bekend, in het afgelopen jaar geen grote cyberincidenten plaats in Nederland, zoals een grootschalige besmetting met malware of zeer grote DDoS-aanvallen. Dat was anders in 2017, toen met WannaCry en NonPetya besmettingen met malware plaatsvonden. En begin 2018 zagen we een aantal DDoS-aanvallen op websites van Nederlandse banken, De Belastingdienst en DigiD. Ook bleek dat in april 2018 Russische spionnen bij de OPCW in Den Haag een poging tot hacken hebben gedaan.

De risico's op ontwrichtende cyberincidenten zijn de afgelopen jaren waarschijnlijk niet kleiner geworden. De storing van het 112-noodnummer op 24 juni 2019 liet zien dat vitale processen afhankelijk zijn van digitale middelen. Door de toenemende digitalisering is de maatschappij steeds afhankelijker geworden van digitale middelen en kunnen verstoringen van cyberveiligheid, bijvoorbeeld veroorzaakt door een aanval van een kwaadwillende hacker of een buitenlandse spionagedienst, grote gevolgen hebben. Zo waarschuwde de Algemene Rekenkamer in een recent onderzoek dat de digitale veiligheid bij een aantal vitale waterwerken niet op orde is en dat de voorbereiding van Rijkswaterstaat op een cyberaanval beter kan. De komende implementatie van 5G zal de afhankelijkheid vergroten van digitale processen. Er is geen reden om aan te nemen dat de dreiging vanuit statelijke actoren of cybercriminelen in het afgelopen jaar kleiner is geworden (AIVD, 2018; NCTV, 2019).

Bedrijven en huishoudens ondervinden regelmatig hinder, overlast en in sommige gevallen financiële schade van cybercriminaliteit en cyberonveiligheid. Zo geeft 4,6 procent van de internetgebruikers aan in 2018 slachtoffer te zijn geweest van een digitaal vermogensdelict, zoals fraude bij onlineaankopen.[1] Ook was 1,8 procent slachtoffer van hacken, zie figuur 2.1. De gevolgen kunnen financieel zijn, zoals in het geval van fraude, maar ook niet-financieel, zoals het verlies van bestanden bij een hack. Daarnaast zijn er indirecte gevolgen; bijna 4 op de 10 slachtoffers van hacken hadden daardoor minder vertrouwen in digitale veiligheid en ruim een kwart van de internetgebruikers ziet wel eens af van internetbankieren vanwege zorgen over veiligheid. Bijna de helft van de Nederlandse bedrijven (48 procent) zag in 2018 een ICT-veiligheidsincident en in één op de vijf gevallen hadden deze incidenten financiële consequenties.[2]

Figuur 2.1 Fraude bij online aankoop meest voorkomende type cyberdelict



Bron: CBS (2019)

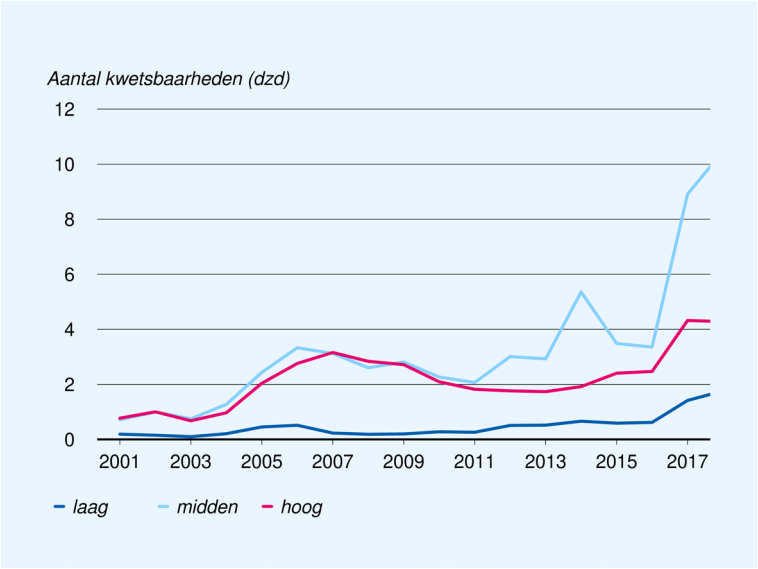
De impact van de verschillende cyberrisico's verschilt per type dreiging. De volgende paragrafen bespreken daarom voor verschillende dreigingen en kwetsbaarheden de belangrijkste ontwikkelingen en bieden een kwalitatieve risico-inschatting.

2.2 Hard- en softwarekwetsbaarheden

Een kwetsbaarheid is een zwakte in hard- of software waarvan cybercriminelen misbruik kunnen maken. Zwaktes kunnen worden veroorzaakt door fouten of lacunes in zowel het ontwerp als de implementatie van hard-of software. Cybercriminelen en statelijke actoren kunnen met behulp van specifieke software, zogenaamde *exploits*, inhaken op deze kwetsbaarheden en cyberaanvallen uitvoeren. Deze aanvallen variëren van *ransomware* tot het mijnen van cryptomunten.

[1] Fraude bij online-aankopen is één van de vormen van digitale vermogensdelicten. Andere vormen zijn bijvoorbeeld: voorschotfraude, Microsoftscams en nepboetes. (CBS, 2018).
[2] Bron: CBS Statline.

Figuur 2.2 Ontwikkeling kwetsbaarheden per risicoprofiel



Bron: National Vulnerability Database (link).

Hard- en softwarekwetsbaarheden blijven een belangrijk cyberveiligheidsrisico vormen. Het aantal bekende kwetsbaarheden in de National Vulnerability Database (NVD)[3] is in 2017 behoorlijk gestegen, maar in 2018 op een vergelijkbaar peil gebleven, zie figuur 2.2. Een alternatieve database van de private partij Risk Based Security laat eenzelfde trend zien, maar met een hogere baseline (22 duizend kwetsbaarheden in 2018 versus 16,5 duizend in de NVD) (Risk Based Security, 2018). Het verschil in absolute aantallen illustreert dat het nauwkeurig bijhouden van kwetsbaarheden een uitdaging is. Een deel van de stijging in het aantal bekende kwetsbaarheden kan waarschijnlijk worden toegeschreven aan een hogere meldingsparticipatie van organisaties.

Het Internet of Things vergroot de kans op de aanwezigheid en het misbruik van kwetsbaarheden. Het Internet of Things (IoT) heeft de potentie om het aantal verbonden apparaten drastisch te laten stijgen. IoT-apparaten zijn relatief slecht beveiligd en beveiligingsupdates worden weinig doorgevoerd.[4] Kwetsbaarheden in deze apparaten bieden daardoor kansen voor cybercriminelen. De meeste criminele activiteiten via IoT-apparaten zijn tot nog toe gericht geweest op het uitvoeren van grootschalige DDOS-aanvallen.[5] De ontwikkeling van de VPN-filter malware laat echter zien dat de mogelijke dreigingen via IoT groter zijn.[6] Deze malware, die zich nestelt in routers, maakt het mogelijk om communicatie te onderscheppen en geïnfecteerde apparaten te wissen.

Afhankelijkheden in de softwareleveranciersketen beïnvloeden de kans op misbruik van kwetsbaarheden. Organisaties maken in toenemende mate gebruik van de mogelijkheid om delen van hun digitale infrastructuur of diensten uit te besteden. Dit kan de veiligheid vergroten als de leverancier meer heeft geïnvesteerd in cyberveiligheid. Maar deze uitbestedingen in de softwareleveranciersketen kunnen ook risico's vergroten als de leverancier onvoldoende veiligheidsmaatregelen heeft genomen (Skybox Security, 2019). Misbruik van een kwetsbaarheid in de softwareleveranciersketen doet zich

[3] Deze database wordt onderhouden door het Amerikaanse National Institute of Standards and Technology.
[4] Zie bijvoorbeeld het WODC-rapport (Verkeerd) verbonden in een slimme samenleving (2017).
[5] Volgens Symantec was in 2018 bijna 80% van IoT-aanvallen te relateren aan DDOS-bedreigingen via LightAidra, Kaiten and Mirai exploits. Zie Symantec (2019).
[6] Zie nieuwsberichten over VPNfilter hier en hier.

bijvoorbeeld voor wanneer updates worden geïnfecteerd met kwaadaardige code. Symantec (2019) rapporteert een toename van dit type aanvallen in 2018 van 78 procent.

Kennis over kwetsbaarheden en code waarmee deze kwetsbaarheden kunnen worden uitgebuit (*exploits*) door criminelen of overheden, wordt op verschillende manieren verhandeld. Zo onderhouden technologiebedrijven vaak *bug bounty* programma's waarbij onderzoekers een financiële vergoeding ontvangen voor het vinden en rapporteren van kwetsbaarheden.[7] Aan de andere kant van het spectrum is er een zwarte markt waarop cybercriminelen *exploits* en kwetsbaarheden kopen en verkopen. Deze uitwisselingen vinden voor het grootste deel plaats op het *dark web* en zijn daardoor moeilijk te traceren. Daarnaast is er een grijze markt waarbij veelal overheden kennis over kwetsbaarheden kopen, bijvoorbeeld als onderdeel van hun cyberdefensieprogramma. De wenselijkheid van het gebruik van *zero-day* kwetsbaarheden door de Nederlandse overheid is onderwerp van het politieke debat.[8] De prijs die betaald wordt voor *exploits* of kennis over kwetsbaarheden, varieert van honderden dollars tot honderdduizenden dollars en is afhankelijk van de mate van vindbaarheid, hoeveel andere kwetsbaarheden er al in het product zijn gevonden en de mogelijke impact (Ablon & Bogart, 2017).

Toepassing van kunstmatige intelligentie kan het risico op misbruik van kwetsbaarheden verhogen én verlagen. Het zoeken naar kwetsbaarheden en het ontwikkelen van *exploits* is op dit moment arbeidsintensief, waardoor het aanbod mogelijk wordt beperkt.[9] Machine-learningtechnieken kunnen mogelijk helpen om kwetsbaarheden sneller op te sporen. Bij gebruik door kwaadwillenden vergroot dit risico's op misbruik[10], maar bij gebruik door softwareontwikkelaars wordt de kans kleiner dat kwetsbare software überhaupt op de markt komt.[11]

2.3 DDoS-aanvallen

Een DDoS-aanval, of Distributed Denial of Service, is een aanval waarbij een webdienst niet toegankelijk is doordat er te veel netwerkverkeer vanuit verschillende bronnen naar deze dienst gestuurd wordt.[12] Grofweg zijn er twee typen DDoS-aanvallen – volumeaanvallen (zo veel mogelijke netwerkverkeer naar een doelwit) en applicatieaanvallen (achterliggende computersystemen worden aangevallen).[13] Begin 2018 vonden serieuze DDoS-aanvallen op websites van banken en de Belastingdienst plaats, waardoor deze tijdelijk onbereikbaar waren. [14] Sindsdien zijn er geen succesvolle DDoS-aanvallen op kritieke infrastructuur gerapporteerd. Wel waren er incidenten bij kleinere websites, bijvoorbeeld meerdere geslaagde aanvallen op het schoolsysteem Magister.[15]

DDoS-aanvallen blijven veel voorkomen en variëren steeds meer in duur en grootte. Het aantal DDoS-aanvallen geobserveerd én afgeslagen door NBIP, een Nederlandse aanbieder van DDoS-mitigatiediensten, steeg met bijna vijftien procent tussen 2017 en 2018.[16] De toename van het aantal aanvallen zette zich door in

[7] Zie bijvoorbeeld dit artikel over het bug bounty programma bij Facebook.
[8] Zie bijvoorbeeld dit NOS-nieuwsbericht.
[9] Ibid.
[10] Zie bijvoorbeeld dit artikel van het World Economic Forum en dit artikel van CSO.
[11] Zie bijvoorbeeld deze blog van Bruce Schneier.
[12] Zie p.48 in NCTV (2019), voor hun definitie.
[13] In de vorige editie van de Risicorapportage (CPB, 2018) zijn meer details te vinden over DDoS-aanvallen (typen en trends) en gerelateerde risico's en beleidsopties.
[14] Zie dit nieuwsbericht van de NOS.
[15] Zie deze en deze berichtgeving.
[16] Zie deze link voor een nieuwsbericht dat de DDoS-datarapporten van de Nationale Beheersorganisatie Internet Providers (2017, 2018) samenvat.

de eerste helft van 2019.[17] Zowel in 2017 als in 2018 waren de meeste aanvallen minder dan 10 gigabit per seconde groot. Wel was de grootste aanval in 2018 bijna dubbel zo zwaar als in 2017 (68 en 36 gigabit per seconde respectievelijk), en nam in 2018 het aandeel van zeer kleine aanvallen toe. De gemiddelde duur van een aanval bleef tussen 2017 en 2018 ongeveer gelijk. Ook wereldwijd zijn er geen duidelijke signalen dat het aantal DDoS-aanvallen afneemt.[18]

Booterwebsites blijven een hardnekkig probleem. Booterwebsites zijn websites die laagdrempelig DDoS-aanvallen faciliteren, waardoor praktisch iedereen zonder bijzondere expertise een DDoS-aanval kan kopen en uitvoeren.[19] In december 2018 heeft de FBI, in samenwerking met de Nederlandse politie, vijftien booterwebsites offline gehaald.[20] Of dit tot een tijdelijk of een langduriger effect op het risico van DDoS-aanvallen zal leiden is nog onzeker. Er zijn signalen dat nieuwe booterwebsites zijn opgezet[21] en dat na een tijdelijke daling het aantal DDoS-aanvallen weer steeg in de eerste maanden van 2019.[22]

Het stijgende aantal Internet-of-Things-apparaten (IoT) in combinatie met een groeiende digitale infrastructuur kunnen in potentie leiden tot sterkere en langere DDoS-aanvallen. De uitrol van het 5G-netwerk, het vijfde generatie mobiele netwerk, kan grotere DDoS-aanvallen faciliteren doordat er meer dataverkeer mogelijk wordt en mobiele apparaten met sterkere processoren aan het mobiele netwerk aangesloten worden. Dit zou vooral effect op de impact van volumeaanvallen kunnen hebben. De voortdurende verbeteringen van de digitale infrastructuur (de uitrol van 5G bijvoorbeeld) maakt het namelijk mogelijk om steeds meer IoT-apparaten aan te sluiten[23]. Slimme koelkasten en broodroosters, Wifi-stopcontacten en stekkers, etc. zijn over het algemeen niet bijzonder goed beveiligd.[24] Dit zijn zwakke schakels die door kwaadwillenden in een *botnet* geïntegreerd kunnen worden om vervolgens krachtigere DDoS-aanvallen te kunnen uitvoeren.[25]

DDoS-aanvallen blijven een risico voor Nederland en de potentiële financiële gevolgen kunnen aanzienlijk zijn. Hoewel DDoS-aanvallen momenteel vooral naar vandalisme neigen, en vaak gericht zijn op onderwijsinstellingen en kleine webshops, is niet uit te sluiten dat statelijke actoren DDoS-aanvallen kunnen inzetten om de nationale kritieke infrastructuur te treffen.[26] Ook wanneer niet-vitale infrastructuur het doelwit is, kunnen de gevolgen van een geslaagde DDoS-aanval aanzienlijk zijn. Een gezamenlijk rapport van NBIP en SIDN (2018) doet een eerste poging om de schade van DDoS-aanvallen in kaart te brengen en schat de financiële impact per aanval op honderdduizenden euro's, afhankelijk van de sector en het seizoen.

Het oprollen van booterwebsites, voorlichting aan potentiële cybervandalen en gebruik van DDoS-mitigatiediensten blijven noodzakelijk. Hoewel een aantal booterwebsites is opgerold, is het nog steeds mogelijk om online een aanval te kopen. Met het toenemende aantal slecht beveiligde IoT-apparaten is het

[17] Zie NBIP (2019).
[18] Zie dit bericht van Kaspersky.
[19] Het vraagstuk over het aankopen van DDoS-aanvallen online werd ook in het voorjaar 2019 in de Tweede Kamer bediscussieerd. (Kamerstukken II, 2018/2019, 1853).
[20] Zie dit nieuwsbericht van tweakers.net en dit nieuwsbericht van het Department of Justice van de VS. Eerder in 2018 werd al een grote aanbieder van DDoS-diensten, webstresser.org, uit de lucht gehaald (zie dit NOS-nieuwsbericht en dit nieuwsbericht van politie.nl). Op deze platform stonden rond 135.000 klanten geregistreerd die voor vanaf 15 Euro per maand DDoS-aanvallen naar keuze konden laten uitvoeren.
[21] Zie bijvoorbeeld dit nieuwsbericht en dit rapport van Nexusguard.
[22] Aldus dit bericht van Kaspersky en NBIP (2019).
[23] Zie dit artikel van IoT-analytics bijvoorbeeld voor cijfers over het aantal IoT-apparaten van de laatste jaren en een voorspelling voor de komende jaren.
[24] Deze enquête, uitgevoerd in opdracht van het ministerie van EZK, laat bijvoorbeeld zien dat de meeste respondenten zich wel bewust zijn van de veiligheidsrisico's, maar dat minder dan de helft ook daadwerkelijk stappen onderneemt om IoT-apparaten te beveiligen.
[25] Zie bijvoorbeeld Cisco (2018). Deze risico's worden ook in het ENISA Threat Landscape rapport (ENISA, 2018) genoemd.
[26] Het NCTV (2019) gaat uitgebreid in op het risico dat statelijke actoren vormen.

daarnaast voor cybercriminelen relatief eenvoudig om een nieuwe booterdienst te starten. Blijvende inzet op het oprollen van deze websites is daarom nodig. Het afgelopen jaar is de politie een campagne gestart om scholieren er van bewust te maken dat een DDoS-aanval geen onschuldig kattenkwaad is, maar een strafbaar feit. Voorzichtige eerste cijfers suggereren dat deze campagnes succesvol zijn.[27] DDoS-aanvallen zijn goed af te slaan door gebruik te maken van een DDoS-mitigatiedienst zoals de NaWas van NBIP. In 2019 zijn er echter meerdere succesvolle aanvallen geweest. Dit suggereert dat niet alle websites of hostingproviders gebruik maken van DDoS-mitigatie. Meer aandacht hiervoor kan financiële schade voorkomen en maakt het voor vandalen minder aantrekkelijk om een aanval te kopen.

2.4 Financieel gemotiveerde malware

Malware is kwaadaardige software waarmee een cybercrimineel een computer kan overnemen. De meest bekende vorm van malware is *ransomware* – software die computers, of de informatie die daarop staat, blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt. De laatste jaren zijn ook andere varianten van malware opgedoken. Bij *cryptojacking* gebruikt de crimineel de processorkracht van de besmette computer om hiermee cryptomunten (zoals bitcoin) te delven (CPB, 2018), en bij *formjacking* proberen criminelen betaalgegevens of andere vertrouwelijke informatie buit te maken door betaalformulieren op webwinkels te injecteren met malware die het formulier kan uitlezen.

***Ransomware* maakt regelmatig slachtoffers en heeft soms substantiële financiële impact.** In het afgelopen jaar kwamen meerdere organisaties in aanraking met *ransomware*. Volgens beveiligingsbedrijf Fox-IT zijn bijvoorbeeld tientallen Nederlandse bedrijven slachtoffer geworden van de *ransomware*-variant SamSam.[28] Onbekend is welke bedrijven dat zijn, of er meer Nederlandse bedrijven getroffen zijn en wat de financiële schade van SamSam was. In enkele internationale casussen is de directe financiële impact wel bekend. Meerdere Amerikaanse steden werden in het afgelopen jaar getroffen door *ransomware* en betaalden losgeld van in totaal ruim een miljoen dollar.[29] De Noorse aluminiumproducent Hydro was afgelopen maart slachtoffer van de *ransomware* LockerGoga en rapporteerde een schade van 31 tot 36 miljoen euro.[30] Naast de directe financiële impact (losgeld) zijn er ook indirecte kosten, in de vorm van verdwenen data of tijd- en productieverlies, en die zijn waarschijnlijk hoger.

Ondanks dat er nog regelmatig gevallen van *ransomware* in het nieuws komen, lijkt de dreiging van *ransomware* te zijn gedaald. De NCTV (2019) rapporteerde dit jaar dat het aantal infecties met *ransomware* in Nederland lijkt te zijn afgenomen. Ook Symantec (2019) en Microsoft (2019) zagen een afname van het aantal infecties. Voor deze daling van de dreiging kunnen meerdere verklaringen worden aangewezen. Beveiligingsbedrijven zoals Symantec stellen dat ze beter in staat zijn om *ransomware* te detecteren voordat deze de eindgebruiker bereikt. Het is ook mogelijk dat gebruikers zich meer bewust zijn geworden van de risico's, en daardoor bijvoorbeeld regelmatiger software updaten, vaker back-ups maken, of voorzichtiger omgaan met verdachte e-mails. Een derde verklaring is dat de winstgevendheid van *ransomware* onder druk is komen te staan. Via bijvoorbeeld het platform 'No More Ransom' kunnen slachtoffers van *ransomware* de versleutelde gegevens vaak kosteloos terugkrijgen. Dit ondergraaft het verdienmodel van cybercriminelen.

In 2018 is *formjacking* sterk in populariteit gestegen, terwijl *cryptojackingactiviteiten* sterk gekoppeld lijken aan de waarde van cryptomunten. Symantec (2019) rapporteert een wereldwijde toename van *formjacking* gedurende 2018, met in totaal 3,7 miljoen geblokkeerde pogingen tot *formjacking*, waarvan 1 miljoen

[27] Zie dit bericht van de politie.
[28] Zie dit bericht van Fox-IT (link).
[29] Bron: https://nos.nl/l/2290780 en hier.
[30] Bron: nieuwsbericht Hydro (link).

in november en december 2018 vielen. *Cryptojackingactiviteiten* zijn volgens hetzelfde rapport van Symantec gedurende 2018 gedaald met 52 procent. Waarschijnlijk speelt de sterke waardedaling van cryptomunten hierbij een rol. Toch blijft *cryptojacking* een interessante optie voor cybercriminelen door de anonimiteit en de lage toegangsdrempels.

Het risico van malware is blijvend, omdat cybercriminelen innoveren. Mede door de wereldwijde besmettingen van de Wannacry en nonPetya-virussen in 2017 zijn organisaties zich bewuster geworden van risico's en nemen zij voorzorgsmaatregelen, zoals het tijdig updaten van software en het maken van back-ups. Voor makers van malware betekent dit dat ze om winstgevend te blijven, hun product moeten aanpassen. Er zijn aanwijzingen dat dit ook gebeurt. De *ransomware*-variant SamSam bijvoorbeeld verwijdert of saboteert eerst back-ups voordat het bestanden vergrendelt. De eigenaar van een besmet computersysteem kan daardoor niet terugvallen op eerder gemaakte back-ups en is sneller geneigd om het losgeld te betalen. Cybercriminelen kunnen *ransomware* ook slimmer en gerichter inzetten op individuele organisaties.[31] Door zich te richten op organisaties die sterk afhankelijk zijn van IT-systemen en die snel productieverlies lijden als systemen stilliggen, kan een cybercrimineel potentieel meer verdienen dan bij een ongerichte massale verspreiding. Dit is vergelijkbaar met het onderscheid tussen gewone *phishing* en *spearphishing*, of tussen ongerichte reclame en gerichte reclame.

2.5 Social engineering

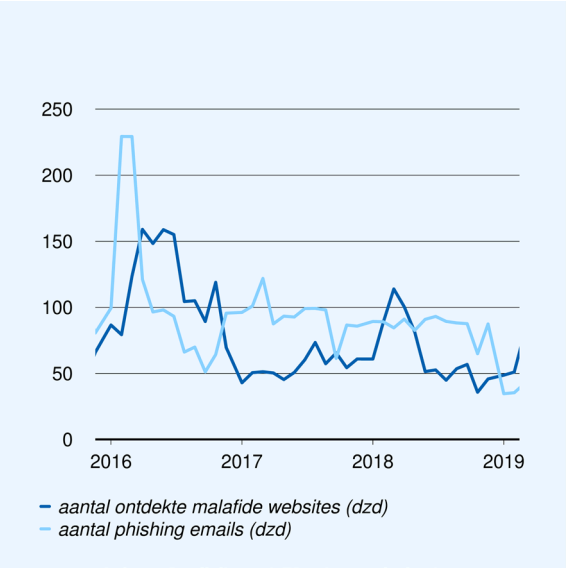
Social engineering verwijst naar technieken die een gebruiker misleiden om bepaalde informatie prijs te geven of specifieke voor hem- of haarzelf nadelige acties te ondernemen.[32] Onder deze brede definitie vallen bijvoorbeeld *phishingmails* of (aan-) en verkoopfraude, maar ook nepboetes/-facturen en zogenaamde Nigeriaanse fraude.[33] Bij *phishing* gebruiken cybercriminelen verschillende technieken om het vertrouwen van slachtoffers te winnen. Bijvoorbeeld door betrouwbare domeinen of personen te repliceren, of de slachtoffers te verwijzen naar valse loginpagina's.[34] Als *phishing* gericht is op specifieke individuen of instellingen, dan wordt gesproken van *spearphishing*. Bij aan- en verkoopfraude ontvangt het slachtoffer niet de afgesproken tegenprestatie. *Phishing* en aan- en verkoopfraude zijn cyberdelicten waar individuele gebruikers vaak mee in aanraking komen en worden daarom toegelicht in deze rapportage.

2.5.1 Phishing

***Phishing* blijft een veel gebruikte methode door cybercriminelen.** Het CBS (2018) schat dat *phishing* de oorzaak is van circa 30 procent van de digitale fraudeslachtoffers waarbij geld van de rekening is gehaald. Figuur 2.3 laat zien dat het aantal ontdekte malafide websites en *phishing* e-mailcampagnes wereldwijd sterk fluctueert in de tijd, maar sinds 2017 op een vergelijkbaar niveau is gebleven. Betaalvereniging Nederland constateert dat de totale fraudeschade in het betalingsverkeer daalt, maar dat fraude door *phishing* juist is toegenomen van 1,05 miljoen euro in 2017 naar 3,81 miljoen euro in 2018.[35] In hun jaarlijkse Security Intelligence Report laat Microsoft zien dat het aandeel *phishing* e-mails in het totale e-mailverkeer in 2018 is gestegen. Het aantal gemelde valse e-mails via de Fraudehelpdesk piekte in de eerste maanden van 2019, zie figuur 2.4. Deze piek kan worden veroorzaakt door een hogere *phishing*-activiteit ofwel een grotere bekendheid van de helpdesk zelf.

[31] Consistent hiermee is dat cybercriminelen ransomware meer lijken te richten op bedrijven. Symantec (2019) rapporteert bijvoorbeeld een toename van 12 procent bij ransomware-infecties onder bedrijven, terwijl het totale aantal infecties daalt.
[32] Zie de Glossary van de ENISA voor de definitie van social engineering.
[33] Zie hier voor uitleg van Nigeriaanse fraude.
[34] Zie bijvoorbeeld Microsoft (2019).
[35] Persbericht van Betaalvereniging Nederland, zie hier.

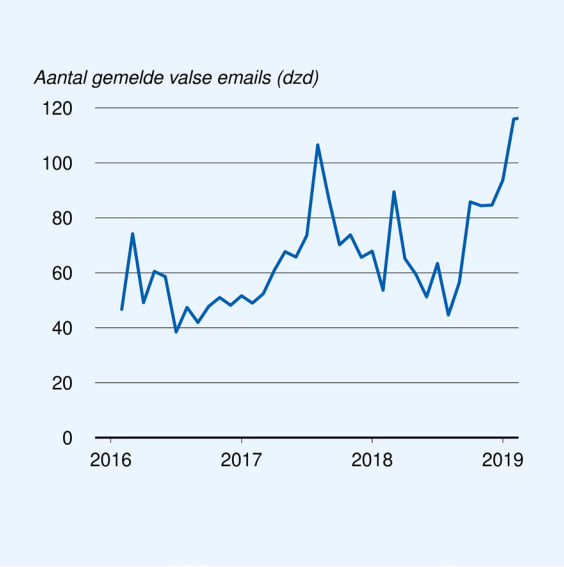
Figuur 2.3 Ontwikkeling aantal ontdekte malafide websites en phishingmails wereldwijd



Bron: Anti Phishing Working Group phishing attack trends reports, link.

***Spearphishing*vormt ook een risico in Nederland.** In het afgelopen jaar hebben zich verschillende incidenten voorgedaan die dat duidelijk maken. Zo hebben aanvallers zich voorgedaan als medewerkers van specifieke zorginstellingen om vertrouwelijk gegevens te bemachtigen.[36] De Nederlandse tak van Pathébioscopen verloor 19 miljoen euro via *spearphishing*.[37] Het NCTV (2019) waarschuwt in zijn Cybersecuritybeeld Nederland dat *spearphishing* een hoge slagingskans heeft doordat aanvallen voor slachtoffers lastig te herkennen zijn.

Figuur 2.4 Ontwikkeling aantal gemelde valse e-mails in Nederland



Bron: Fraudehelpdesk.

[36] Zie bijvoorbeeld hier en dit bericht van een ziekenhuis.
[37] Zie bijvoorbeeld dit NOS-nieuwsbericht.

Zowel de *phishing*-aanvallen als de methodes om *phishing* op te sporen worden steeds vernuftiger. Zo is het nu mogelijk om ook in het geval van tweefactor-authenticatie *phishing*-aanvallen effectief te laten zijn.[38] Cybercriminelen maken daarnaast gebruik van andere digitale communicatiemiddelen naast e-mail, zoals WhatsApp en sociale media, om de geloofwaardigheid van *phishing*-aanvallen te vergroten en spamfilters te omzeilen.[39] Een recente ontwikkeling is het gebruik van software die de stem van bijvoorbeeld een leidinggevende nabootst om daarmee geld buit te maken.[40] Deze vormen van *phishing* zijn gepersonaliseerd en daardoor tijdrovender voor criminelen. Het gebruik van Kunstmatige Intelligentie maakt het in theorie echter mogelijk om het tijdrovende aspect van *spearphishing* te automatiseren.[41] Hierdoor zouden *spearphishing*-aanvallen in omvang en frequentie kunnen toenemen. De potentieel lagere kosten voor criminelen leiden ertoe dat een grotere groep mensen interessante doelwitten kunnen vormen voor *spearphishing*-aanvallen (Herley, 2010). Kunstmatige Intelligentie wordt ook toegepast in de bescherming van consumenten en bedrijven tegen *phishing*, zowel door gevestigde partijen als door startups.[42] Hierbij wordt Machine Learning bijvoorbeeld gebruikt om verdachte berichten vroegtijdig te kunnen identificeren. Het gebruik van fysieke sleutels in een tweefactor-authenticatie blijkt daarnaast een goede manier om *phishing* tegen te gaan.[43]

2.5.2 Online (aan)koopfraude

Aankoopfraude is een veel voorkomend type cyberdelict. Bij aankoopfraude heeft een consument voor een product betaald, maar levert de tegenpartij het product niet. Van de Nederlandse huishoudens gaf 2,7 procent aan in 2018 slachtoffer te zijn geweest van aankoopfraude (CBS, 2019). Bij een groot deel van de slachtoffers verliep de fraude via een tweedehandsverkoopplatform (zoals Marktplaats.nl, Tweakers.nl of Speurders.nl). In een kwart van de gevallen werden slachtoffers bedrogen via een nepwebwinkel. Verkoopfraude, waarbij het slachtoffer wel het product levert maar de ontvanger niet betaalt, komt veel minder vaak voor. Van de Nederlandse huishoudens is in 2018 0,2 procent slachtoffer geweest van deze vorm van oplichting.

De pakkans van aankoopfraude is relatief laag, wat het aantrekkelijk maakt voor criminelen. Van de slachtoffers van aankoopfraude deed 39 procent een melding bij bijvoorbeeld de politie, bank of Marktplaats. Uiteindelijk deed 23 procent van de slachtoffers aangifte bij de politie. De voornaamste redenen voor de bevraagden om het incident niet te melden zijn dat het om een klein bedrag ging en dat melden toch niet helpt om het geld terug te krijgen (23,5 en 16,9 procent respectievelijk). Cybercriminelen kunnen via digitale middelen echter relatief eenvoudig flinke aantallen mensen oplichten, waardoor al die relatief kleine bedragen toch kunnen optellen tot een forse totale winst.

Er zijn verschillende initiatieven om aankoopfraude te bestrijden. Om aangifte te vereenvoudigen en te stimuleren, kunnen slachtoffers online aangifte doen.[44] Alle aangiftes worden verzameld bij het Landelijk Meldpunt Internet Oplichting, een speciaal onderdeel van de politie. Deze eenheid werkt samen met onder andere banken, keurmerkorganisaties, hostingbedrijven en televisieprogramma's zoals Opgelicht en Kassa om online oplichting te bestrijden. Zo kan bij meerdere meldingen de rekening van een oplichter worden geblokkeerd of een nepwebshop offline worden gehaald. Ook zoekt de politie met enige regelmaat de publiciteit om consumenten te waarschuwen en te benadrukken dat aangifte doen zinvol is, ook wanneer niet elke aangifte leidt tot vervolging.

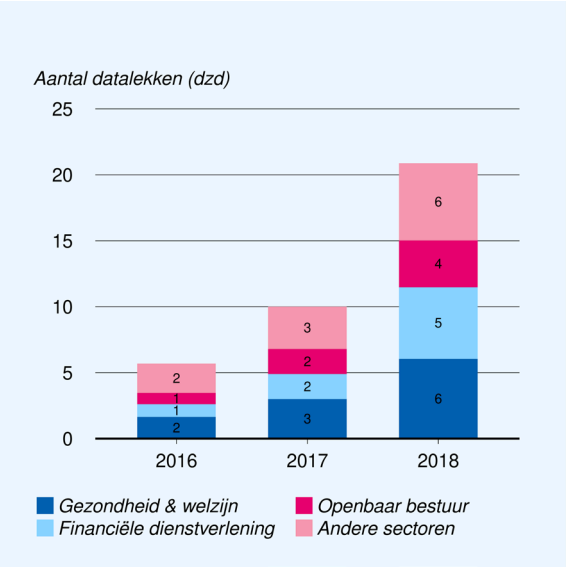
[38] Zie bijvoorbeeld dit nieuwsbericht.
[39] Zie hier voor een SMS-voorbeeld en hier voor een voorbeeld van WhatsApp. De politie spreekt van honderden meldingen over SMS-*phishing*.
[40] Zie dit bericht in het FD.
[41] Zie bijvoorbeeld Brundage et al (2018) en dit bericht van het World Economic Forum.
[42] Zie bijvoorbeeld hier (Microsoft) en hier (INKY).
[43] Google claimde in 2018 dat sinds de introductie van fysieke sleutels er geen succesvolle *phishing*-pogingen hebben plaatsgevonden bij haar werknemers. Zie dit bericht.
[44] Dit kan via de website van de politie.

De bestrijding van aankoopfraude kan versterkt worden door vaker preventief in te grijpen. De bovengenoemde initiatieven zijn over het algemeen gericht op ingrijpen nadat er slachtoffers zijn gevallen. Om de aanpak van aankoopfraude te versterken, kan meer worden ingezet op preventieve maatregelen. Zo werkt SIDN aan methoden om onbetrouwbare websites geautomatiseerd op te sporen en vroegtijdig te blokkeren, in plaats van de huidige controle na melding.[45] Mogelijk kunnen tweedehandsverkoopplatformen deze preventieve technieken ook toepassen, zodat malafide advertenties en aanbieders worden opgespoord voordat ze schade aanrichten.

2.6 Datalekken

Sinds 2016 is het aantal gemelde datalekken meer dan verdriedubbeld. Bij een datalek krijgt iemand ongeoorloofd of onbedoeld toegang tot persoonsgegevens, of worden persoonsgegevens ongewenst vernietigd, verloren, gewijzigd of verstrekt.[46] Een verloren USB-stick, per ongeluk een e-mail met vertrouwelijke informatie naar de verkeerde persoon sturen, maar ook het openbaar maken van persoonsgegevens door een hack zijn voorbeelden van datalekken. Figuur 2.5 laat het aantal gemelde datalekken zien tussen 2016 en 2018. De aantallen zijn uitgesplitst naar de sectoren waar de meldingen vandaan komen. De drie sectoren met de meeste meldingen zijn Gezondheid & welzijn, Financiële dienstverlening en Openbaar bestuur. Waar in 2016 melding werd gemaakt van bijna 6000 datalekken, was er in 2018 sprake van meer dan 20.000 meldingen. Tussen 1 januari en 1 mei 2019 zijn er al bijna 8000 meldingen bij de Autoriteit Persoonsgegevens (AP) gedaan. De verwachting is dan ook dat het totaal aantal gemelde datalekken in 2019 hoger uit zal komen dan in 2018. Twee incidenten uit de jeugdzorg in de eerste helft van 2019 (Bureau Jeugdzorg Utrecht en Stichting Kwaliteitszorg Jeugd) hebben tot Kamervragen geleid.[47]

Figuur 2.5 Stijging aantal meldingen datalekken



Bron: Autoriteit Persoonsgegevens.

[45] Zie bijvoorbeeld dit bericht van SIDN.
[46] Zie hier voor een definitie van een datalek.
[47] In april 2019 werd bekend dat 3278 dossiers van 2702 kinderen door een fout bij Bureau Jeugdzorg Utrecht werden gelekt (artikel security.nl). Bij Stichting Kwaliteitsregister Jeugd kwam ook een datalek aan het licht—de testomgeving van een kennisbank werd per ongeluk online gezet. Daardoor kwamen niet-geanonimiseerde beslissingen in SKJ-tuchtzaken vrij (artikel security.nl). Zie ook Kamerstukken II 2018/19, 31839, nr. 686 over beide incidenten.

Nederland heeft het hoogste aantal gemelde datalekken in vergelijking met andere Europese landen.[48] In Nederland werden tussen 25 mei 2018 en 28 januari 2019 15.400 datalekken gemeld. Duitsland en Groot-Brittannië volgen met respectievelijk 12.600 en 10.600 meldingen. Een mogelijke verklaring is dat de meldplicht in Nederland al eerder, in 2016, is ingevoerd, waardoor organisaties hier beter bekend zijn met de meldplicht. In de meeste andere Europese landen werd de meldplicht pas met de inwerkingtreding van de AVG in mei 2018 ingevoerd.

Bijna twee derde van de meldingen in 2018 gaat om persoonsgegevens die aan de verkeerde ontvanger zijn gestuurd. In haar jaarverslag van 2018 schrijft de AP (2018) dat 63 procent van de gemelde datalekken aan het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger te wijten is. Bij vier procent van de datalekken was het lek ontstaan door "hacken, malware en/of phishing". Dit lijkt een beperkt aandeel, maar juist bij digitale datalekken kan het aantal personen waarover gegevens lekken groot zijn. Gelekte gegevens kunnen soms direct misbruikt worden, zoals creditcardinformatie, of indirect via *phishing* of identiteitsfraude, indien een wachtwoord is gelekt.

Bescherming van persoonsgegevens kan doorschieten. In het afgelopen jaar heeft AP een dwangsom opgelegd aan het UWV[49], een boete aan Uber[50] en een boete aan het Haga Ziekenhuis in Den Haag[51]. De angst voor boetes en/of de wens om zorgvuldig aan de AVG te voldoen lijken bij verschillende organisaties tot grotere voorzichtigheid te hebben geleid.[52] Deze ontwikkeling kan de compliancekosten voor organisaties onnodig verhogen of nieuwe en maatschappelijk wenselijke toepassingen van data afschrikken. Bij de evaluatie van de AVG in 2020 kan hiernaar gekeken worden. Specifieke vragen zijn of het toezicht en de regels voldoende aansluiten bij de grootte van organisaties en of de juiste balans gevonden is tussen bescherming van persoonsgegevens en het mogelijk maken van maatschappelijk wenselijke toepassingen van data.

3 Cyberrisico's publieke belangen

3.1 Inleiding

In dit hoofdstuk staan de risico's met betrekking tot publieke belangen centraal. Verstoringen van cyberveiligheid, zoals uitval van ICT of cybercriminaliteit, kunnen soms ernstige gevolgen hebben voor getroffen bedrijven of burgers. In veel gevallen blijft dit echter beperkt tot de direct getroffenen en eventuele toeleveranciers of afnemers, en heeft de samenleving als geheel nauwelijks ongemak van de verstoring. Dit ligt anders wanneer het getroffen bedrijf behoort tot de vitale infrastructuur. Uitval van vitale processen, zoals de elektriciteitsvoorziening of het betalingsverkeer, treft de hele samenleving. Digitale middelen kunnen door kwaadwillende actoren ook op andere, minder direct zichtbare, manieren worden ingezet om publieke belangen te ondermijnen. Hierbij valt onder andere te denken aan economische cyberspionage en de verspreiding van desinformatie.

---

[48] Bron: DLA Piper (2019). Zie hier voor de link naar de survey en hier voor het gerelateerde nieuwsbericht. Internationale bedrijven met vestigingen in meerdere landen maken meldingen via het land van hun hoofdkantoor. Dit kan de ranking vertekenen voor landen als Nederland of Ierland waar meerdere hoofdkantoren van multinationals gevestigd zijn.

[49] Het UWV werd door de AP verplicht om per november 2019 een dwangsom van 150.000 euro maandelijks te betalen ingeval de gegevens niet beter beveiligd worden. Zie persbericht AP en artikel NOS. Hieraan gerelateerd is ook een nieuwsbericht van BNR dat op werk.nl CV's gelekt worden.

[50] In november 2018 heeft de AP een boete van 600.000 euro opgelegd aan Uber voor het te laat melden van gelekte gegevens van 57 miljoen Ubergebruikers (waarvan 174.000 Nederlanders). Zie nieuwsbericht AP en nieuwsbericht nu.nl.

[51] Zie dit nieuwsbericht van AP en dit artikel in de Volkskrant.

[52] Zo stopte de Fraudehelpdesk in juli 2019 met het registreren van meldingen van burgers en ondernemers van o.a. *phishing*-e-mails. Zie deze blog van Arnoud Engelfriet voor meer voorbeelden (link).

Paragraaf 3.2 gaat nader in op cyberrisico's binnen de vitale infrastructuur. Vrijwel alle vitale processen en diensten zijn afhankelijk van ICT, waardoor een cyberincident ernstige gevolgen kan hebben. Daarnaast zijn vitale processen relatief kwetsbaar voor cyberincidenten: veel systemen zijn verouderd en vervanging is een complexe operatie. Ook zijn er in sommige gevallen zorgen over de betrouwbaarheid van buitenlandse leveranciers. De cyberdreiging voor vitale processen evolueert continu en is moeilijk te voorspellen. Wel is duidelijk dat de samenleving in de toekomst alleen maar méér afhankelijk zal worden van ICT en dienen technologische ontwikkelingen zoals 5G en Kunstmatige Intelligentie nauwlettend gevolgd te worden.

Paragraaf 3.3 analyseert de risico's van economische cyberspionage. Het gaat hierbij om digitale spionage waarmee bedrijfsinformatie wordt buitgemaakt. De AIVD en NCTV benadrukken beide dat economische spionage een belangrijke dreiging is voor Nederland. Tegelijkertijd ontbreekt publieke informatie om dit te staven, omdat maar een handvol incidenten bekend is en details daarover ontbreken. Paragraaf 3.3 introduceert een denkkader dat aangeeft welke stappen een spionerende actor moet doorlopen om gestolen bedrijfsinformatie winstgevend aan te wenden. Dit kader geeft aan dat economische cyberspionage niet automatisch winstgevend is en niet altijd tot schade voor het Nederlandse bedrijfsleven leidt.

Paragraaf 3.4 bespreekt digitale beïnvloeding van de publieke opinie. Desinformatie kan het functioneren van een democratie ondermijnen en technologische ontwikkelingen, zoals Kunstmatige Intelligentie, maken het genereren en verspreiden van misleidende berichten steeds eenvoudiger. Platformbedrijven lijken zich de laatste jaren bewuster geworden van hun maatschappelijke rol en hebben, deels onder druk van de Europese Commissie en publieke ophef, stappen gezet om desinformatie tegen te gaan. De huidige zelfregulering onder bestuurlijke druk brengt echter risico's met zich mee dat platformbedrijven onder omstandigheden de vrijheid van meningsuiting ten onrechte beperken. Co-regulering, waarbij de overheid op basis van een openbaar publiek debat richtlijnen opstelt voor platformbedrijven, is een kansrijkere beleidsoptie.

3.2 Vitale processen

3.2.1 Vitale processen in toenemende mate afhankelijk van ICT

Vitale processen zijn diensten die zijn aangemerkt als essentieel voor de maatschappij. Processen worden door de NCTV aangemerkt als vitaal als uitval leidt tot ernstige maatschappelijke ontwrichting zoals vele dodelijke ongevallen of ernstige gewonden, miljarden euro's schade, of vele personen met maatschappelijke overlevingsproblemen.[53] Voorbeelden van vitale processen zijn de distributie van gas en elektriciteit, de drinkwatervoorziening, waterkeringen, het faciliteren van internet- en datadiensten en het betalingsverkeer. Bij een aantal vitale processen kan uitval een domino-effect veroorzaken. Het Nationaal Veiligheidsprofiel 2016 (Analistennetwerk Nationale Veiligheid, 2016) benoemt dat deze effecten vooral worden veroorzaakt door de energie- en telecomsectoren. Wanneer bijvoorbeeld de elektriciteit (langdurig) uitvalt, kunnen onder andere het elektronische betalingsverkeer, het openbaar vervoer en communicatiediensten uitvallen, afhankelijk van de beschikbaarheid van terugvalmogelijkheden.

Vrijwel alle vitale processen en diensten zijn afhankelijk van ICT. Dit merkte de NCTV op in het CSBN van 2019. De NCTV benadrukt daarnaast dat analoge terugvalopties vaak niet meer bestaan. Een voorbeeld hiervan, overigens bij een niet-vitaal proces, is het containerbedrijf Maersk, dat in 2018 getroffen werd door de *ransomware* NonPetya. Hierdoor vielen digitale systemen uit en ging de digitaal aangestuurde poort voor vrachtwagens niet meer open. Het bleek toen dat de poort ook niet meer handmatig geopend kon worden.[54]

[53] Deze website van de NCTV geeft een definitie van vitale processen.
[54] Op basis van een interview met hoogleraar Bibi van den Berg in het Leids Dagblad, "Digitale oorlog minstens zo destructief", 12-2-2019.

Een ander voorbeeld zijn de noodaggregaten in ziekenhuizen, die een stroomuitval moeten opvangen. Lang niet alle ziekenhuizen hebben echter de aanbevolen hoeveelheid brandstof in huis om een langdurige uitval, tot 72 uur, op te vangen. Brandstof tanken als de stroom is uitgevallen kan echter lastig zijn, omdat ook brandstofpompen op elektriciteit werken.[55]

Beveiliging van vitale processen is relatief complex. Digitale systemen die vitale processen aansturen, zijn vaak organisch gegroeid en inmiddels zeer complex, wat het moeilijker maakt om een compleet overzicht te hebben van alle risico's. Ook zijn sommige systemen al decennia oud en niet ingericht op de huidige cyberdreiging, terwijl ze in de loop der tijd wel zijn aangesloten op grotere netwerken en soms zelfs op het internet.[56] Vervanging of updaten van deze verouderde systemen is echter bijzonder kostbaar. Een onderzoek van de Algemene Rekenkamer concludeert dat de digitale veiligheid bij een aantal vitale waterwerken niet op orde is en dat de voorbereiding van Rijkswaterstaat op een cyberaanval beter kan.[57]

In het afgelopen jaar zijn er verschillende cyberincidenten geweest bij vitale processen, zowel binnen als buiten Nederland. De storing van het 112-noodnummer in juni 2019 laat zien dat ICT-afhankelijke vitale processen kunnen uitvallen.[58] In september 2018 hadden twee internationale havens, in Barcelona en San Diego, te maken met een cyberaanval.[59] Ook waren er berichten over een nieuwe hackersgroep, GreyEnergy genaamd, die digitale aanvallen heeft uitgevoerd op de energiesector in Oekraïne en Polen. Deze aanvallen hebben niet geleid tot uitval van systemen en waren mogelijk bedoeld om toekomstige cyberacties voor te bereiden.[60]

De verwachting is dat de afhankelijkheid van ICT en de kwetsbaarheid voor cyberaanvallen de komende jaren alleen maar zullen toenemen. Het NCSC brengt regelmatig beveiligingsadviezen uit om bedrijven in vitale sectoren te waarschuwen voor bekende kwetsbaarheden. Recent onderzoek van het CPB (2019) laat zien dat er de afgelopen jaren een toename is geweest van het aantal adviezen. Daarnaast is de verwachting dat het 5G-netwerk zal leiden tot een verdergaande digitalisering, waardoor steeds meer processen afhankelijk worden van ICT. Ook kunnen nieuwe toepassingen ontstaan die op termijn gaan behoren tot de vitale infrastructuur. Het kader '5G en de afhankelijkheid van ICT' gaat hier verder op in.

[55] Zie dit nieuwsbericht van de NOS.
[56] Het NCTV (2019) gaat hier verder op in.
[57] Het rapport van de Algemene Rekenkamer is hier te vinden.
[58] Overigens leek de 112-storing niet te zijn veroorzaakt door een doelbewuste aanval. Zie bijvoorbeeld de berichtgeving van de NOS.
[59] Zie dit nieuwsbericht.
[60] Meer details zijn te vinden op deze website.

5G en de afhankelijkheid van ICT

5G is een nieuwe kerntechnologie die het huidige 4G-netwerk op verschillende punten verbetert. 5G bouwt voort op bestaande netwerken, maar biedt meer capaciteit. Dataoverdracht gaat sneller en reactietijden zijn korter. Daarnaast kunnen meer gebruikers en/of apparaten tegelijk gebruik maken van het netwerk.

De verwachting is dat 5G tot veel nieuwe toepassingen gaat leiden. Door de korte reactietijden maakt 5G real-time interacties mogelijk tussen bv. machines of auto's. Dit is een belangrijke bouwsteen bij de ontwikkeling van zelfrijdende voertuigen. Ook over toepassingen in de medische wereld wordt veel gesproken. Voorbeelden als opereren op afstand spreken tot de verbeelding. Bestaande toepassingen, die nu nog op beperkte schaal worden gebruikt, zullen waarschijnlijk veel meer worden toegepast als het netwerk duizenden apparaten dicht op elkaar kan bedienen. Hierbij valt onder andere te denken aan *smart homes* vol aan elkaar gekoppelde IoT-apparaten en aan het gebruik van een veelheid aan sensoren in de industrie.

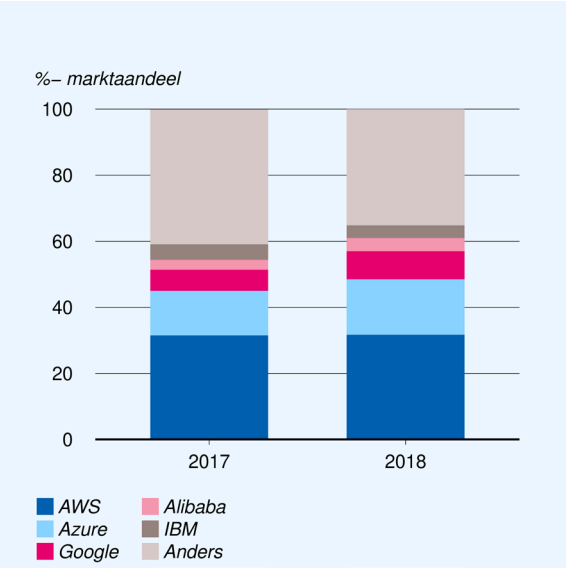
Een aantal nieuwe toepassingen kunnen essentieel worden voor het functioneren van de maatschappij. De verwachting is dat de samenleving door 5G meer dan nu afhankelijk gaat worden van allerlei digitale processen. Deze digitale processen kunnen daardoor deel gaan uitmaken van de vitale infrastructuur. Een voorbeeld hiervan is het wegverkeer. Op dit moment is dit niet aangemerkt als vitaal proces. Maar wanneer een groot deel van het verkeer gaat bestaan uit zelfrijdende voertuigen, die communiceren met elkaar en met wegsensoren, 'slimme' stoplichten en verkeersborden, kan uitval van systemen grote gevolgen hebben voor de verkeersveiligheid. Ook uitval of verstoring van medische toepassingen zou in potentie grootschalig mensen in gevaar kunnen brengen.

3.2.2 Afhankelijkheid van één of enkele (buitenlandse) aanbieders

Nederland is sterk afhankelijk van buitenlandse leveranciers en heeft weinig uitwijkopties. Bij sommige digitale diensten hebben één of enkele aanbieders een dermate hoog (gezamenlijk) marktaandeel dat de maatschappelijke cyberveiligheid sterk afhankelijk is van een handvol partijen. Figuur 3.1 illustreert dit voor clouddiensten. De vijf grootste aanbieders hebben wereldwijd gezamenlijk een marktaandeel van rond de 60 procent, en dit marktaandeel is groeiende. Door het grote marktaandeel hebben deze aanbieders waarschijnlijk meer mogelijkheden om zich te wapenen tegen cyberaanvallen, maar wanneer het mis gaat, worden zeer veel systemen tegelijk getroffen. DDoS-mitigatiediensten zijn hiervan een voorbeeld. Door een recente softwarestoring bij DDoS-mitigatiedienst Cloudflare lag een deel van het internet kortstondig plat.[61] Ook sommige markten voor hard- en software zijn sterk geconcentreerd en kunnen daarmee indirect risico's opleveren voor de maatschappelijke cyberveiligheid. Voor individuele klanten kunnen deze grote aanbieders echter juist aantrekkelijk zijn, omdat ze door hun omvang een betere prijs-kwaliteitverhouding kunnen bieden. Grote aanbieders kunnen over het algemeen meer investeren in innovatie en beveiliging en daardoor aantrekkelijkere producten bieden. Ook dataverzameling speelt een rol. Grote DDoS-mitigatiediensten hebben bijvoorbeeld meer data over DDoS-aanvallen en kunnen daardoor betere bescherming bieden.

[61] Zie dit nieuwsbericht.

Figuur 3.1 Helft van de cloudmarkt voor de top-3 aanbieders



Bron: Canalys.

Als een grote aanbieder in het buitenland is gevestigd, kunnen zorgen ontstaan over de betrouwbaarheid van die partij. Meerdere staten hebben een 'offensief cyberprogramma', gericht tegen Nederland (AIVD, 2019). Het Russische cyberprogramma, in combinatie met wetgeving die vereist dat Russische bedrijven de inlichtingendiensten desgevraagd ondersteunen, heeft het kabinet doen besluiten om het gebruik van antivirussoftware van Kaspersky uit te faseren.[62] Recentelijk zijn er zorgen ontstaan over de betrouwbaarheid van sommige buitenlandse leveranciers van 5G-technologie.[63] Ook opslag van persoonsgegevens in het buitenland ligt gevoelig.[64]

Er zijn daarnaast zorgen over de mogelijke gevolgen van overnames door buitenlandse partijen van bedrijven die van vitaal belang zijn voor Nederland. In september 2013 deed América Móvil een poging om KPN over te nemen, wat de vraag opriep welke gevolgen dit zou kunnen hebben voor de nationale veiligheid. De overnamepoging van América Móvil leek ingegeven door bedrijfseconomische belangen, maar andere buitenlandse spelers zouden kunnen handelen uit geopolitieke of ideologische motieven en hun toegang tot Nederlandse communicatienetwerken misbruiken. Op het moment van schrijven ligt er een wetsvoorstel bij de Tweede Kamer dat de minister van Economische Zaken en Klimaat de bevoegdheid heeft om overnames in de telecomsector te verbieden als deze leiden tot een bedreiging van het publiek belang.[65] Daarnaast is er ongerustheid over de toenemende rol van China op het wereldtoneel. Deze zorgen betreffen oneerlijke handelspraktijken, waarbij Chinese bedrijven opereren met staatssteun terwijl de Chinese markt is afgeschermd voor buitenlandse bedrijven, maar ook ontwikkelingen op het gebied van veiligheid en (politieke) beïnvloeding roepen bezorgdheid op. In de China-strategie geeft het kabinet onder andere aan voor bepaalde sleuteltechnologieën niet afhankelijk te willen worden van China.[66]

[62] Voor meer informatie, zie Kamerstukken II 2017/18, 30821, nr. 46.
[63] Zie Kamerstukken II, 2019.
[64] Dit artikel gaat verder in op de gevolgen van de AVG voor dataopslag buiten de EU.
[65] Zie dit nieuwsbericht.
[66] De China-strategie is hier te vinden.

3.2.3 Cyberdreigingen omgeven met veel onzekerheid

De cyberdreiging voor vitale processen evolueert continu en is moeilijk te voorspellen. De grootste dreiging lijkt uit te gaan van statelijke actoren. Het CSBN benoemt dat het uitvoeren van cyberspionage of een cyberaanval weinig riskant is. Inbraak in elektronische systemen wordt lang niet altijd direct opgemerkt en aanvalsmiddelen zijn makkelijk en tegen relatief lage investeringen te verkrijgen. De attributie aan statelijke actoren is daarentegen zeer complex en wanneer dit wél gebeurt, blijft dit in veel gevallen zonder consequenties. De dreiging die uitgaat van statelijke actoren, is sterk verbonden met actuele geopolitieke ontwikkelingen en daarmee moeilijk voorspelbaar.

De vitale infrastructuur is verweven geraakt met andere, niet als vitaal aangemerkte, processen. Het NCSC maakt een 'binair' wel/niet-onderscheid tussen vitale en niet-vitale processen. In de praktijk is dit onderscheid echter niet altijd zo duidelijk. Vitale processen zijn steeds meer onderdeel geworden van een netwerk, waardoor een incident bij een niet-vitale aanbieder ook een vitaal proces kan beïnvloeden. Een focus op de huidige lijst vitale processen brengt het gevaar met zich mee dat belangrijke ondersteunende processen buiten beeld blijven. Hier valt bijvoorbeeld te denken aan leveranciers van cruciale software, digitale systemen voor de levering van zonne-energie, hostingbedrijven en anti-DDoS aanbieders die de Nederlandse banken beschermen. Daar komt bij dat deze ondersteunende processen in private, soms buitenlandse, handen kunnen zijn, bij soms zeer grote machtige aanbieders. De WRR (2019) pleit tegen deze achtergrond voor een Cyberafhankelijkheidsbeeld, dat inzichtelijk maakt van welke partijen, digitale processen en diensten het functioneren van vitale processen afhankelijk is.

Technologische ontwikkelingen veranderen het cyberveiligheidslandschap en dienen nauwlettend gevolgd te worden. Een van de belangrijkste toekomstige ontwikkelingen is de aanleg van een 5G-netwerk, met de bijbehorende nieuwe toepassingen. De veiligheid van het 5G-netwerk is momenteel omgeven door onzekerheid en wordt door de overheid kritisch gevolgd. Hier speelt deels ook een economische afweging. Uitsluiting van leveranciers van 5G-technologie, of uitstellen van aanleg van het netwerk in afwachting van meer informatie over de veiligheid kan in potentie leiden tot economische schade. Wanneer nieuwe toepassingen zoals zelfrijdende voertuigen en zorg op afstand concrete vorm krijgen, is onderzoek nodig of deze processen moeten worden aangemerkt als vitaal. Ook andere ontwikkelingen, zoals op het gebied van Kunstmatige Intelligentie, kunnen tot nieuwe veiligheidsvraagstukken leiden. Wanneer KI gebruikt gaat worden bij de aansturing van vitale processen, zouden criminelen of vijandige statelijke actoren deze systemen bijvoorbeeld kunnen beïnvloeden door de trainingsdata te manipuleren. Tegelijk zou KI ook behulpzaam kunnen zijn om vitale processen beter te beveiligen.

Verschillende beleidsmaatregelen zijn gericht op het vergroten van de weerbaarheid van vitale infrastructuur. De Wet beveiliging netwerk- en informatiesystemen (Wbni), die per 9 november 2018 in werking is getreden, verplicht aanbieders van essentiële diensten en digitale dienstverleners maatregelen te nemen om hun ICT-systemen te beveiligen en stelt een meldplicht in bij ernstige incidenten.[67] Opvallend is hierbij dat niet alle processen die door de NCTV worden aangemerkt als vitaal onder de beveiligingsverplichting vallen.[68] De Wbni is een implementatie van de NIB-richtlijn van de EU, waar onder andere nucleaire energie en waterwerken buiten vallen. Voor deze processen bevat de Wbni alleen een meldplicht. Naast ontwikkelingen op het gebied van wetgeving wordt voor de derde keer een grootschalige cyberoefening georganiseerd met vitale partijen uit de publieke en private sector (ISIDOOR III).

[67] Meer informatie is te vinden op de website van de NCTV.
[68] Overigens kunnen bedrijven op grond van andere wettelijke regimes wel weer beveiligingsverplichtingen hebben.

3.3 Economische cyberspionage

3.3.1 Inleiding

Verschillende organisaties waarschuwen voor economische cyberspionage door statelijke actoren. In zijn jaarverslag schrijft de AIVD (2018) dat meerdere landen, waaronder China, Iran en Rusland, digitale middelen inzetten om economische doelen te bereiken, ten koste van onder andere Nederlandse belangen. Ook de NCTV (2019) ziet economische spionage als een actuele dreiging voor Nederland en noemt China als grootste dreigingsbron. Economische cyberspionage is het illegaal verkrijgen van kennis en economisch waardevolle informatie via digitale kanalen.[69] Buitenlandse inlichtingendiensten of andere statelijke actoren hebben verschillende digitale middelen hiervoor. Spionnen kunnen malware inzetten, digitale 'achterdeurtjes' in netwerken plaatsen of via digitale dienstverleners, zoals softwareleveranciers of clouddiensten toegang proberen te krijgen tot vertrouwelijke informatie (AIVD, 2019). Daarnaast kunnen in verschillende landen ook producenten en dienstverleners verplicht worden om samen te werken met inlichtingendiensten.[70] Inlichtingendiensten kunnen ook *phishing* of *spearphishing* inzetten om in organisaties door te dringen.[71] Organisaties kunnen ook door concurrenten bespioneerd worden.[72] Toch is er een belangrijk verschil tussen bedrijfsspionage door concurrenten en economische spionage door statelijke actoren. Statelijke actoren, uit landen met een offensief cyberprogramma, hebben veel meer capaciteit en technische mogelijkheden om te spioneren. Ook is in het geval van spionage door een land attributie complexer en zijn er minder mogelijkheden om schade te verhalen. Dit suggereert dat statelijke economische spionage een groter risico vormt dan bedrijfsspionage.

Publieke informatie ontbreekt over de omvang en impact van de dreiging. Er zijn geen betrouwbare cijfers over hoe vaak Nederlandse bedrijven bespioneerd worden en wat de financiële schade daarvan was. Ondanks de grote dreiging van economische cyberspionage zijn geen Nederlandse bedrijven met winstwaarschuwingen[73] gekomen nadat ze slachtoffer werden van een hack. Wel hebben (ex-)werknemers van AMSL bijvoorbeeld technologische kennis gestolen en hiermee een eigen onderneming opgestart, maar het is onbekend of deze personen hebben gehandeld namens een staat.[74] In het buitenland lijken meer gevallen bekend. Zo heeft de FBI twee Chinezen aangeklaagd vanwege het hacken van meer dan 45 organisaties en de diefstal van gevoelige data.[75] Ook internationaal ontbreken vooralsnog gegevens om de financiële schade voor getroffen bedrijven te kwantificeren.[76]

Informatie ontbreekt om het risico van economische cyberspionage goed te duiden. Terwijl de gerapporteerde dreiging van economische cyberspionage hoog is, is slechts een beperkt aantal incidenten bekend en ontbreekt informatie over (aantoonbare) economische schade. Dit is een paradoxale situatie. Deze paragraaf biedt een denkkader om de paradox te verklaren. Dit kader helpt om ook in te schatten in welke gevallen economische spionage een groot risico vormt en wanneer dat minder aannemelijk is. Het onderwerp van economische cyberspionage past in het thema economische veiligheid. Economische veiligheid is "het ongestoord functioneren van Nederland als een effectieve en efficiënte economie" (NCTV, 2019b).

---

[69] Deze definitie sluit aan bij de algemene definitie van digitale spionage van de AIVD ("het met digitale middelen verwerven van gevoelige of vertrouwelijke informatie van een andere staat voor het behalen van eigen strategische doelen.")
[70] Zie bijvoorbeeld AIVD, 'Offensief cyberprogramma. Een ideaal businessmodel voor staten' en de Kamerbrief van 16 juli 2019 van de minister van JenV 'Reactie Kaspersky Lab inzake rol van de overheid en IT-branche in cybersecurity'.
[71] Zoals dit artikel suggereert.
[72] Een casus is de zaak Waymo vs. Uber (link).
[73] Beursgenoteerde bedrijven zijn op grond van de Wet financieel toezicht verplicht om koersgevoelige informatie zo spoedig mogelijk bekend te maken via een persbericht.
[74] Bron: FD (link).
[75] Zie dit nieuwsbericht van de FBI: link.
[76] Zie bijvoorbeeld Anderson et.al. (2019). Zij schrijven o.a.: "While we do not dispute the occurrence of IP infringement, we failed to find any case with quantifiable losses".

3.3.2 De schakels van economische spionage

Wanneer is economische cyberspionage winstgevend voor statelijke actoren? Nieuwsberichten en onderzoeksrapporten over economische cyberspionage richten zich vaak op diefstal van bedrijfsgeheimen en lijken te veronderstellen dat het bemachtigen daarvan automatisch tot schade leidt voor het lijdende voorwerp en winst voor de statelijke actor. Diefstal van bedrijfsgeheimen is echter pas de eerste stap in de 'waardeketen' van economische cyberspionage. Deze waardeketen bestaat uit verschillende schakels. Een spionerend land moet deze schakels doorlopen voordat de spionage winstgevend kan zijn, zie figuur 3.2.

Figuur 3.2 De waardeketen van economische cyberspionage

Diefstal data: door toenemende digitalisering is deze eerste stap eenvoudiger geworden. Bij bedrijven wordt informatie steeds meer digitaal opgeslagen en gedeeld. Spionerende landen spelen hierop in door inzet van *exploits*, toegang via achterdeurtjes in software of slim ontworpen *phishing*-mails. Ook kunnen insiders makkelijk digitale informatie naar buiten smokkelen.[77] Deze fase in de waardeketen wordt gekenmerkt door schaalvoordelen: met een relatief klein aantal medewerkers kan een land proberen om bij een groot aantal bedrijven te spioneren.

Vinden van potentieel waardevolle informatie: dit is een arbeidsintensieve fase met hoge kosten. Wanneer een statelijke actor erin is geslaagd om data te bemachtigen via spionage is de volgende stap om uit deze data potentieel waardevolle informatie te destilleren. Deze stap vraagt om marktkennis en/of technologische expertise en is daardoor veel minder goed schaalbaar dan de eerste fase.

Overdracht informatie aan bedrijf: naarmate bedrijfsleven en overheden meer met elkaar vervlochten zijn, is deze stap eenvoudiger. Informatie moet op de juiste plek terechtkomen om waardevol te kunnen zijn. Dit kan een lastig allocatievraagstuk zijn voor statelijke actoren, want de organisatie die de informatie mag ontvangen, moet zowel politiek betrouwbaar zijn als in staat zijn om snel de informatie te benutten. Er kan een prikkel zijn om de gestolen informatie te delen met grote bedrijven die goede politieke connecties hebben, maar dat zijn niet noodzakelijk de bedrijven met de flexibiliteit om nieuwe producten te ontwikkelen. Een risico voor statelijke actoren in deze fase is dat de kennis gedeeld wordt met grote logge bedrijven die er vervolgens weinig mee kunnen of willen doen. In hoeverre deze fase een knelpunt is, hangt ook af van de nationale context: in welke mate zijn overheden en bedrijven met elkaar verweven?

Doorontwikkeling: data of informatie zijn zelden direct waardevol. Om uiteindelijk tot een winstgevend product of procesverbetering te leiden zal het bevoordeelde bedrijf de gestolen informatie moeten verrijken. Dit verloopt net als bij een regulier R&D-proces en kent in grote lijnen dezelfde onzekerheden. Een verschil met een regulier R&D-proces is dat het bevoordeelde bedrijf minder mogelijkheden heeft voor 'open innovatie': omdat het bedrijf werkt met gestolen informatie kan het moeilijker samenwerken met experts van buiten het bedrijf. Zo is het niet verstandig om gestolen broncode extern te delen, of is het lastig om nieuwe R&D-medewerkers aan te trekken – zeker als die afkomstig zijn van het bespioneerde bedrijf.

Marktfase: afhankelijk van snelheid waardeketen en bescherming intellectuele eigendom. In de laatste fase van de waardeketen gaat het om het economisch benutten van de gestolen informatie. Ook deze fase verschilt weinig van een regulier R&D- en innovatieproces. Risico's voor benutting zijn dat het bevoordeelde

[77] Een mogelijkheid voorbeeld hiervan is de casus van een Chinese medewerker van Apple (link).

bedrijf ondanks de gestolen informatie later op de markt komt dan het bespioneerde bedrijf, of dat de gestolen kennis beschermd is met een octrooi. Gestolen informatie kan in bepaalde gevallen zonder veel extra kosten waardevol zijn, bijvoorbeeld concurrentiegevoelige informatie over overnames of broncode voor softwaretoepassingen. Ook kan gestolen informatie een bedrijf helpen om dichter bij de technologische frontier te komen.

3.3.3 Conclusie

Voorlopig is het nog onzeker hoe winstgevend economische cyberspionage werkelijk is. De waardeketen van economische cyberspionage bevat meerdere knelpunten en risico's. Dit suggereert dat cyberspionage niet automatisch zal leiden tot financiële schade voor het getroffen bedrijf. In bepaalde situaties kunnen deze knelpunten veel minder spelen en is het risico op schade voor Nederlandse bedrijven groter. Dit is het geval wanneer gestolen informatie nauwelijks doorontwikkeld hoeft te worden en snel toegepast kan worden. Dit kan bijvoorbeeld spelen bij diefstal van biedstrategieën bij een aanbesteding, contracten met afnemers, of diefstal van broncode. Ook lijkt het risico op schade groter als de kennisoverdracht tussen inlichtingendiensten en bedrijven laagdrempelig is. Of economische cyberspionage nu wel of niet tot financiële schade zal leiden, het is aannemelijk dat vanwege de digitalisering van informatie en producten het risico op diefstal groot zal blijven.

3.4 Digitale beïnvloeding

3.4.1 Risico's voor goed functionerende democratie

Desinformatie gaat over het bewust creëren en verspreiden van onware, inaccurate of misleidende informatie.[78] Het bestaan van desinformatie is op zichzelf niet nieuw. Digitalisering heeft de productie, verspreiding en consumptie van informatie in onze samenleving echter veranderd en daarmee zijn ook nieuwe risico's voor desinformatie geïntroduceerd. Inmiddels wordt nieuws door Nederlanders het meest via online kanalen geconsumeerd.[79] Wardle en Derakhshan (2017) onderscheiden vier dimensies waarlangs digitalisering de informatie-waardeketen heeft veranderd: 1) het is makkelijker geworden om informatie te creëren en te publiceren, 2) informatieconsumptie vindt door sociale media deels in het openbaar plaats, 3) de verspreiding van nieuws verloopt sneller door mobiele communicatie en online publicatie, en 4) informatie wordt actiever gedeeld tussen gelijkgestemden die elkaar vertrouwen.

Personen, organisaties of staten kunnen verschillende redenen hebben om desinformatie in te zetten.[80] Sommige actoren gebruiken desinformatie voor financieel gewin. Zogenaamde *clickbait*-websites kunnen bijvoorbeeld winst maken via advertenties door consumenten met sensationele, maar onware, informatie te lokken. Daarnaast kunnen actoren tot doel hebben de publieke opinie te beïnvloeden of te polariseren. Het gaat dan onder andere om pogingen verkiezingen met desinformatie te manipuleren, maar het kan ook gaan om beïnvloeding van het maatschappelijke debat of gedrag zoals in het geval van desinformatie over vaccinatie.[81] Tot slot kan desinformatie voortkomen uit een behoefte tot vermaak, vaak gaat dit gepaard met online pesten. In deze paragraaf beperken we ons tot desinformatie gericht op het manipuleren van de publieke opinie. Deze vorm van desinformatie kan in potentie het publieke belang van een goed functionerende democratie ondermijnen.

[78] Zie van Keulen, Korthagen, Diederen en van Boheemen (2018)
[79] Reuters Institute, Digital News Report 2019.
[80] Zie bijvoorbeeld ook het white paper van Google (2019).
[81] Zie bijvoorbeeld Wellcome (2018).

Zorgen over de impact van digitale desinformatie op de publieke opinie zijn in de afgelopen jaren toegenomen. Zo beschouwt de Europese Commissie de blootstelling van haar burgers aan desinformatie als een majeure uitdaging.[82] Buitenlandse mogendheden hebben verkiezingen en publieke beeldvorming in andere landen actief getracht te beïnvloeden. Het bekendste voorbeeld is de afgelopen Amerikaanse presidentsverkiezing. De inzet van Russische *trolls* via Twitter na het neerschieten van de MH17 is een voorbeeld van hoe ook in Nederland desinformatie wordt ingezet om de publieke beeldvorming te manipuleren.[83]

Nederlandse burgers zijn zelf minder bezorgd over de impact van desinformatie in vergelijking met andere landen. Uit een enquête van Reuters blijkt dat 53 procent van de Nederlanders het meeste nieuws vertrouwt en slechts 31 procent van de Nederlanders zich zorgen maakt over wat waar en onwaar is met betrekking tot online nieuws. Ter vergelijking, in Frankrijk en de VS maakt 67 procent van de mensen zich hier zorgen over (Reuters Institute, 2019). De relatief hoge score voor mediageletterdheid op de index van het Open Society Institute (2018) suggereert dat de Nederlandse samenleving weerbaarder is tegen desinformatie. Het feit dat Nederlanders zich relatief weinig zorgen maken, kan echter ook een risico zijn als het vertrouwen ongegrond blijkt te zijn.

3.4.2 Digitalisering en marktfalen maken misleiding mogelijk

Kunstmatige intelligentie vergroot de risico's doordat het produceren van geloofwaardige desinformatie eenvoudiger wordt.[84] Kunstmatige intelligentie (KI) maakt het mogelijk om de manipulatie van geluid en videobeelden te vereenvoudigen en geloofwaardiger te maken (ook bekend onder de term *deep fake news*). Daarnaast kan KI worden ingezet voor de automatische generatie van valse berichtgeving. De inzet van menselijke *trolls* wordt hierdoor overbodig en deze automatisering kan tot schaalvergroting leiden in de productie van desinformatie (Brundage et al., 2018). De verspreiding van desinformatie vindt veelal plaats door de inzet van *bots* op sociale media. Een wetenschappelijke studie uit 2017 schat dat tussen de 9 procent en 15 procent van de accounts op Twitter *bots* zijn (Varol et al. 2017). De verwachting is dat deze *bots* in de toekomst slimmer zullen worden ingezet. Bijvoorbeeld door specifiek doelgroepen te selecteren die vatbaar zijn voor desinformatie. KI kan tegelijkertijd ook worden ingezet bij de bestrijding van desinformatie. Platformbedrijven gebruiken bijvoorbeeld *machine learning* om namaakaccounts en verspreiding via bots sneller te herkennen.

In 2017 constateerde het CPB (2017) twee marktfalens die de disseminatie van misleidende informatie via platformen kunnen versterken. In de eerste plaats hebben platformen meer informatie dan hun gebruikers en kunnen ze deze informatieasymmetrie benutten. Dit kan er bijvoorbeeld toe leiden dat nieuws voor consumenten door platformen wordt gefilterd om de aantrekkelijkheid van het platform voor de consument te vergroten. Daarnaast ondervinden platformen mogelijk onvoldoende prikkels om ongewenst gedrag van hun gebruikers tegen te gaan, zoals bij de verspreiding van desinformatie door nepaccounts.

De Nederlandse taal en de inrichting van het kiesstelsel maken het voor buitenlandse actoren relatief minder aantrekkelijk om desinformatie in Nederland te verspreiden. De beperkte kennis van de Nederlandse taal in het buitenland zorgt ervoor dat verspreiders van desinformatie relatief veel investeringen moeten doen om geloofwaardige desinformatie op te stellen. De opbrengsten voor kwaadwillende actoren bij verkiezingen zijn daarnaast minder hoog doordat het systeem van evenredige vertegenwoordiging ervoor zorgt dat elke stem evenveel invloed heeft op de verkiezingsuitslag. Daarnaast zorgt het meerpartijenstelsel in Nederland voor meer variatie in het publieke debat, waardoor het voor kwaadwillende actoren moeilijker is om te polariseren en burgers te 'sturen' richting één bepaalde partij.

---

[82] Zie website van Europese Commissie hier.
[83] Zie berichtgeving in o.a. de Groene Amsterdammer (hier) en het NRC Handelsblad (hier).
[84] Zo heeft het OM tegenover de NOS recent zorgen uitgesproken over de opkomst van deep-fakefilmpjes die steeds beter worden.

3.4.3 Maatregelen tegen desinformatie zijn nog niet toekomstbestendig

Platformbedrijven lijken zich bewuster te zijn geworden van hun maatschappelijke rol. Deels onder druk van de Europese Commissie en publieke ophef, hebben digitale platformen in de afgelopen jaren stappen gezet om de bovengenoemde risico's te verkleinen. Wereldwijde marktleiders (o.a. Google, Facebook, Twitter) hebben zich in september 2018 gecommitteerd aan een EU-brede praktijkcode voor het voorkomen van desinformatie. Deze marktpartijen rapporteren inmiddels maandelijks over maatregelen die zij nemen om desinformatie tegen te gaan. Zo geven platformen inzage in politieke advertenties (zie Facebooks *Ad Library Report* en Twitters *Ads Transparency Center*) en zijn in sommige gevallen de geografische reikwijdte van politieke advertenties ingeperkt[85]. Daarnaast informeren grote platformen gebruikers actief over de herkomst van advertenties en de betrouwbaarheid van berichtgeving. Hierdoor wordt de informatieasymmetrie tussen gebruiker en platform kleiner gemaakt. De verspreiding van onjuiste berichtgeving wordt tot slot tegengegaan door botaccounts te verwijderen en in *ranking* algoritmes de betrouwbaarheid van berichten mee te nemen.

De huidige Europese aanpak van desinformatie via zelfregulering onder bestuurlijke druk brengt risico's met zich mee voor de vrijheid van meningsuiting en de continuïteit van beleid. Socialemediabedrijven maken afwegingen welke type berichten op hun platformen zijn toegestaan. Wanneer berichten niet voldoen aan hun richtlijnen, kunnen deze worden verwijderd. De Europese Commissie spoort platformbedrijven aan om meer te doen om desinformatie te voorkomen. Er is daarmee een tendens ontstaan om de verantwoordelijkheid voor de verwijdering van misleidende berichten bij de platformen te leggen. In Duitsland is dit zelfs recentelijk in de wet verankerd via de *Netzwerkdurchsetzungsgesetz* die platformen verplicht illegale haatzaaiende berichten binnen een bepaalde tijdsperiode te verwijderen. Human Rights Watch waarschuwt dat deze wet leidt tot onnodige censuur en daarmee de vrijheid van meningsuiting aantast[86]. Het is voor platformbedrijven op dit moment onduidelijk wat de gevolgen zijn als er niet aan publieke druk gehoor wordt gegeven. Door de huidige focus op zelfregulering bestaat een reëel risico op zelfcensuur van platformbedrijven, die verder kan gaan dan maatschappelijk wenselijk is[87]. Daarnaast is er een risico dat zelfregulering vooral een reflex is op de hevigheid van het publieke debat. Platformbedrijven zullen geneigd zijn maatregelen te nemen in tijden van commotie. De bestendigheid van de maatregelen is daarbij niet geborgd[88].

Co-regulering is een kansrijkere beleidsoptie. Overheden kunnen, op basis van een openbaar debat, richtlijnen geven aan platformbedrijven over hoe om te gaan met desinformatie en andere maatschappelijk ongewenste vormen van beïnvloeding. Het is hierbij wenselijk dat de richtlijnen recht doen aan de diversiteit en de dynamiek van platformen. Een belangrijke vraag waarop een dergelijke richtlijn uitsluitsel kan geven, is of gepersonaliseerde politieke advertenties acceptabel zijn. Een uitgangspunt voor richtlijnen moet daarnaast zijn dat de markt toegankelijk blijft voor kleine nieuwe partijen, zodat toetreding van nieuwe platformbedrijven mogelijk blijft.

Het belang van onderwijs gericht op mediawijsheid wordt vergroot door de uitgebreidere rol van consumenten in de nieuwswaardeketen. Sociale media zorgen ervoor dat consumenten niet alleen passief nieuws tot zich nemen, maar ook een rol hebben in de verspreiding van nieuws. Hun rol is daarmee groter geworden. Het opleiden van media-kritische burgers kan er daardoor voor zorgen dat de impact van desinformatie op twee manieren wordt verkleind: de kans op viraal gaan van onjuiste informatie wordt kleiner doordat burgers minder snel geneigd zijn onjuist nieuws te delen, en het wordt minder waarschijnlijk dat

[85] Bijvoorbeeld tijdens het Ierse referendum over abortuswetgeving, zie berichtgeving hier.
[86] Zie dit bericht op de website van Human Rights Watch.
[87] Zie bijvoorbeeld ook Van Til (2019)
[88] Zie bijvoorbeeld ook Desmaris, Dubreuil, en Loutrel (2019)

desinformatie erin slaagt iemands mening zelf te beïnvloeden. In Finland is mediatraining al enige tijd onderdeel van het curriculum op basis- en middelbare scholen, en dit lijkt effectief.[89]

4 Preventie en bestrijding

4.1 Inleiding

De preventie en bestrijding van verstoringen van cyberveiligheid omvatten verschillende aspecten. NIST, het National Institute of Standards and Technology, vat deze samen in vijf stappen: het identificeren van risico's, beschermen tegen deze risico's, aanvallen detecteren, aanvallen mitigeren en schade herstellen.[90] Deze stappen zijn algemeen toepasbaar voor zowel bedrijven en burgers als voor de overheid.

Voor de eerste twee stappen, identificatie van cyberrisico's en bescherming daartegen, is veel aandacht. Bewustwordingscampagnes zoals Alert Online en platformen zoals het Digital Trust Center proberen het risicobewustzijn onder burgers en bedrijven te verhogen en gebruikers te stimuleren tot het nemen van voorzorgsmaatregelen. Het NCSC brengt met enige regelmaat beveiligingsadviezen uit, overheidsorganisaties zijn verplicht om standaarden voor veilige gegevensuitwisseling toe te passen, technische beschermingsmethodes worden continu verbeterd, en zo zijn er nog veel meer initiatieven te noemen. Paragraaf 4.2 gaat verder in op een aantal van deze onderwerpen, met speciale focus op de onderwerpen waarvoor statistische gegevens bekend zijn.

Over de derde en vierde stap, aanvallen detecteren en mitigeren, is veel minder bekend. Het is niet onmogelijk dat aanvallen lange tijd onopgemerkt kunnen blijven, of zelfs nooit ontdekt worden. Sommige typen aanvallen, zoals DDoS en *ransomware*, leggen systemen plat en worden daardoor snel opgemerkt. Maar bijvoorbeeld inbraak in systemen, cyberspionage of inzet van apparaten in een *botnet* wordt vaak pas laat gedetecteerd. Een rapport van cyberveiligheidsbedrijf FireEye (2019) schat dat in 2018 de mediane tijd voordat een cyberinbraak door bedrijven werd gedetecteerd, 78 dagen was. Volgens onderzoek van Accenture blijft bij bedrijven in de financiële sector 42 procent van de cyberaanvallen minstens een week onopgemerkt.[91] En rapporten van het RAND Europe en WODC (2015) en de WRR (2019) concluderen beide dat de focus bij cybersecurity vooral uitgaat naar preventie en dat detectie en mitigatie meer aandacht verdienen, juist omdat volledige preventie onmogelijk is. Vanwege het gebrek aan verdere inzichten in detectie en mitigatie door bedrijven en consumenten bespreken we dit niet verder in deze rapportage. Wel besteden we in paragraaf 4.3 aandacht aan de opsporing en berechting van cybercriminelen. Niet alleen mitigeert politie en het OM hiermee de activiteiten van deze criminelen, er kan ook een afschrikkende werking van uitgaan.

Ook over de vijfde stap, schadeherstel na een cyberaanval, is weinig bekend. Voor een aantal specifieke incidenten zijn inzichten over schade beschikbaar, maar schattingen van de schade van cyberaanvallen in het algemeen lopen sterk uiteen.[92] De laatste jaren groeit echter de aandacht voor cyberverzekeringen die de (financiële) gevolgen van een cyberaanval afdekken. Op dit moment is de markt voor deze verzekeringen nog zeer bescheiden, maar als de markt volwassen wordt, kan dit leiden tot betere inzichten in de schade door een cyberaanval. Daarnaast hebben cyberverzekeringen ook invloed op de preventieve maatregelen die verzekerde

[89] Zie bijvoorbeeld de berichtgeving van het World Economic Forum en CNN.
[90] Zie het NIST cybersecurity raamwerk.
[91] Zie dit bericht.
[92] Hiscox (2019) rapporteert bijvoorbeeld een gemiddelde schade van 369.000 dollar per incident terwijl Radware (2018) de gemiddelde schade per incident schat op 1.1 miljoen dollar en Accenture (2019) spreekt van 13 miljoen dollar schade per organisatie per jaar.

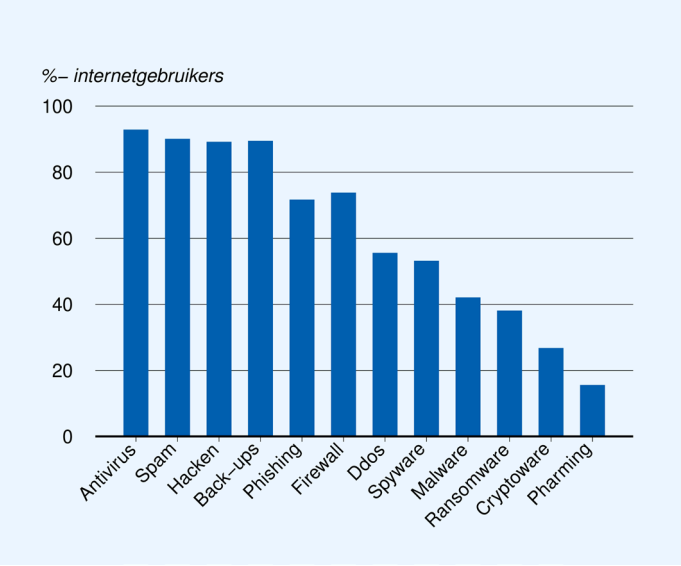
bedrijven treffen en kan de informatie die verzekeraars verzamelen, behulpzaam zijn bij het identificeren van risico's en het detecteren en mitigeren van aanvallen. Paragraaf 4.4 analyseert de markt voor cyberverzekeringen.

De overheid ziet kennisdeling rondom deze vijf stappen als een belangrijk instrument om cybercriminaliteit te voorkomen en te bestrijden. Zij zet dan ook sterk in op voorlichting en publiek-private samenwerking. Er is echter nog weinig bekend over de mate waarin dit beleid efficiënt wordt vormgegeven. De effecten zijn vaak moeilijk meetbaar waardoor een evaluatie lastig is. Paragraaf 4.5 gaat hier verder op in.

4.2 Identificatie van en bescherming tegen cyberrisico's

De meeste internetgebruikers zijn op de hoogte van veel voorkomende onlinegevaren, maar de kennis over nieuwe dreigingen is beperkt. Figuur 4.1 geeft een aantal kerncijfers uit een CBS-enquête uit (CBS, 2018) die vraagt naar de kennis van internetgebruikers. Veel respondenten weten wat (ongeveer) wordt bedoeld met een antivirusprogramma, back-ups maken, hacken of spam. De kennis over minder voorkomende en/of nieuwere vormen van cybercrime is echter beperkt. Zo geeft slechts 27 procent aan te weten wat er wordt bedoeld met *cryptoware* (een vorm van *ransomware*) en is 16 procent op de hoogte van *pharming* (het omleiden van internetverkeer naar een valse website). Uit dezelfde CBS-enquête blijkt dat veel internetgebruikers bezorgd zijn over hun online veiligheid, vooral als het gaat om potentieel misbruik van bank- of persoonsgegevens.

Figuur 4.1 Nieuwe cyberrisico's veelal onbekend bij internetters



Bron: CBS (2019)

Wat betreft veiligheidsmaatregelen zijn niet alle internetgebruikers proactief, zeker als het gaat om minder bekende maatregelen. Ongeveer 45 procent houdt computerprogramma's (bv. besturingssysteem, virusscanner, internetbrowser) vaak up-to-date, 29 procent geeft aan dit soms te doen. Toegang tot apparaten beschermen met een wachtwoord, vingerafdruk, etc. is gebruikelijk; 64 procent van de internetgebruikers doet dit vaak en 17 procent soms. Deze percentages lopen echter sterk terug wanneer het gaat om minder bekende maatregelen. Een wachtwoordmanager wordt bijvoorbeeld weinig gebruikt, 9 procent van de respondenten gebruikt deze.

De wereldwijde uitgaven van bedrijven aan cyberveiligheid groeien sterk en gaan vooral naar security-as-a-service. Schattingen van de wereldwijde uitgaven aan cyberveiligheid lopen enigszins uiteen. Gartner gaat uit van een markt ter grootte van 114 miljard dollar in 2018 en een jaarlijkse groei van de uitgaven van 8,7 procent.[93] IDC schat de markt in 2018 op 92 miljard dollar, met een gemiddelde jaarlijkse groei van 9,9 procent tot 2022.[94] Zowel Gartner als IDC noemen dat security-as-a-service, waarbij (een deel van) de beveiliging wordt uitbesteed, als de grootste en sterkst groeiende uitgavencategorie. Voor Nederland zijn geen betrouwbare schattingen van de uitgaven aan cyberveiligheid beschikbaar. Wel geeft een CBS-enquête uit 2018 aan dat 44 procent van de geënquêteerde bedrijven hun ICT-beveiliging voornamelijk laten uitvoeren door externe leveranciers. Dit percentage loopt op tot 69 procent bij bedrijven met 20 tot 50 werkzame personen, en ligt lager bij heel kleine of heel grote bedrijven.[95]

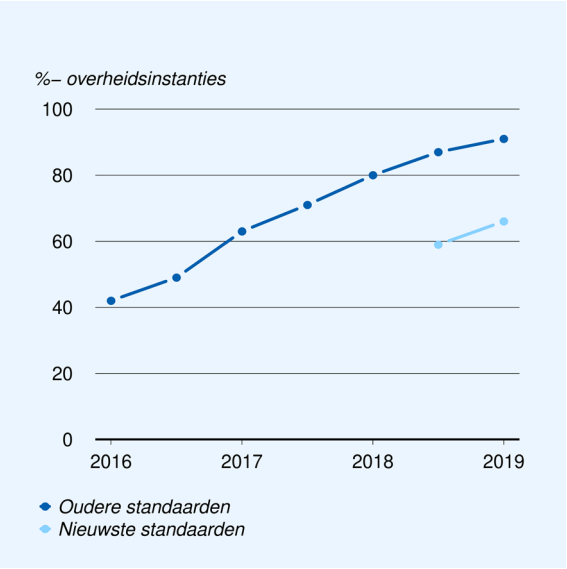
Net als bij consumenten treffen niet alle bedrijven voorzorgsmaatregelen en worden meer geavanceerde maatregelen vooral door grote bedrijven genomen. De eerder genoemde CBS-enquête geeft aan dat 87 procent van alle ondervraagde bedrijven antivirussoftware gebruikt, 68 procent bewaart een back-up op een andere fysieke locatie of in de cloud. Deze basismaatregelen worden ook door kleine bedrijven regelmatig genomen. Verdergaande maatregelen, zoals encryptie bij het opslaan en versturen van data, worden vooral genomen bij grote bedrijven.

Technische standaarden voor veilig onlineverkeer blijven zich doorontwikkelen. Het NCSC publiceerde in april 2019 een vernieuwde TLS-richtlijn, voor het beveiligen van verbindingen op internet.[96] TLS versleutelt de data die verstuurd worden tussen de gebruiker en de website; wanneer een website is beveiligd met TLS, verschijnt 'https' in het adres en is er een slotje zichtbaar. Ook verouderde DNS -toepassingen worden uitgefaseerd.[97] Verouderde DNS-protocollen kunnen misbruikt worden om internetgebruikers om te leiden naar een malafide website.

Het gebruik van technische standaarden groeit, maar is nog niet honderd procent. Forum Standaardisatie meet met enige regelmaat in welke mate overheidswebsites en e-mail beveiligd zijn.[98] Oudere standaarden voor het beveiligen van websites (DNSSEC en TLS/HTPPS) en om *phishing* via e-mail tegen te gaan (DKIM, DMARC en SPF) worden breed gebruikt door overheidsorganisaties. De bovenste lijn in figuur 4.2 geeft de adoptiegraad van deze oudere standaarden weer. Begin 2019 lag die rond de 90 procent, met een gestage groei sinds medio 2015, toen de adoptiegraad op 35 procent lag. Nieuwere standaarden zoals DANE voor encryptie van e-mailverkeer en SPF en DMARC met strikte toepassing worden minder vaak gebruikt. De toepassing hiervan groeit wel, van 59 procent medio 2018 naar 66 procent begin 2019. De adoptiegraad van standaarden onder alle .nl-domeinnamen ligt een stuk lager. In juli 2019 was bijvoorbeeld 54 procent van deze domeinnamen beveiligd met DNSSEC.[99]

[93] Zie dit nieuwsbericht van Gartner.
[94] Zie dit bericht.
[95] Deze data zijn terug te vinden op CBS Statline onder ICT-gebruik bij bedrijven.
[96] Zie dit bericht van NCSC.
[97] Zie dit nieuwsbericht van SIDN.
[98] Zie dit verslag van Forum Standaardisatie.
[99] Zie deze grafiek van SIDN.

Figuur 4.2 Gestage adoptie van standaarden in overheidsdomein



Bron: Forum Standaardisatie.

Bij authenticatie is een verschuiving zichtbaar naar steeds geavanceerdere methoden die steeds vaker gebruik maken van fysieke sleutels of van biometrische gegevens. Authenticatie is het proces waarmee een mens of een machine zijn identiteit kan bevestigen. Bekende authenticatiemethoden zijn het gebruik van een wachtwoord, of een vorm van twee-factor-authenticatie waarbij de gebruiker zowel een wachtwoord als een sms-code moet invullen. Cybercriminelen worden er steeds handiger in om deze methoden te omzeilen.[100] Om deze reden is er een verschuiving gaande naar alternatieve authenticatiemethodes. In plaats van onversleutelde SMS-authenticatie gebruiken bedrijven steeds vaker apps die data versleuteld verzenden.[101] Daarnaast maken sommige bedrijven gebruik van een fysieke sleutel.[102] Ook biometrie wint aan populariteit. Een van de meest bekende toepassingen van biometrie is de vingerafdrukscanner, die al een aantal jaren in opkomst is. In 2018 was 60 procent van de wereldwijd verscheepte smartphones voorzien van een vingerafdrukscanner.[103] Ontwikkelingen op het gebied van kunstmatige intelligentie maken ook andere vormen van authenticatie op basis van biometrische gegevens mogelijk, zoals stemherkenning of gezichtsherkenning; een techniek die in de nieuwste generatie smartphones al wordt aangeboden.

De continue ontwikkeling van nieuwe preventie- en mitigatiemethoden helpt om cybercriminaliteit te bestrijden, maar er bestaat een risico dat gebruikers achterblijven. Nieuwe technieken om internetgebruikers te beschermen, zoals verbeterde standaarden voor veilig online dataverkeer en veiligere authenticatiemethoden, dragen bij aan de bestrijding van cybercrime. Bij veel van de hiervoor beschreven ontwikkelingen zien we echter dat de adoptie van nieuwe technieken achterloopt. De nieuwste technische standaarden worden nog lang niet bij alle websites toegepast, consumenten beperken zich tot de basale beveiliging en zelfs daarbij is de adoptiegraad niet volledig. Ook in het bedrijfsleven worden meer geavanceerde technieken minder vaak toegepast.

Het is onduidelijk welk niveau van investeringen in cyberveiligheid afdoende is. Het verband tussen investeringen in veiligheid en incidenten of bedrijfsresultaten is gecompliceerd, omdat oorzaak en gevolg door elkaar heen lopen. Aan de ene kant is het te verwachten dat investeringen in cyberveiligheid de kans op

[100] Onder andere Fox-IT benoemt dat SMS-authenticatie niet volledig waterdicht is.
[101] ING is bijvoorbeeld bezig om inloggen via SMS uit te faseren en zoveel mogelijk klanten betalingen te laten bevestigen via een app.
[102] Google is hier een voorbeeld van.
[103] Zie deze statistieken.

een incident verkleinen, hoewel waarschijnlijk na een bepaald punt de toegevoegde waarde van extra investeringen af zal nemen. Tegelijkertijd zullen bedrijven die een groter risico lopen op een incident, bijvoorbeeld grote bedrijven of bedrijven die sterk afhankelijk zijn van ICT, meer maatregelen nemen. Ook zijn bedrijven die veel maatregelen nemen, zich waarschijnlijk meer bewust van de cyberdreiging, waardoor ze een incident eerder zullen detecteren en rapporteren.

Het nut van een financiële benchmark voor investeringen in cyberveiligheid is zeer beperkt. Verschillende onderzoeken geven een benchmark voor de optimale investering door bedrijven in cyberveiligheid. Deze benchmarks variëren sterk, tussen 3,7 en 10 procent van het totale ICT-budget.[104] Een WODC-rapport (RAND Europe en WODC, 2015) geeft op basis van interviews met experts echter aan dat het heel moeilijk is om vast te stellen hoeveel een bedrijf uitgeeft aan cyberveiligheid, onder andere omdat deze kosten vaak integraal onderdeel zijn van (ICT-) projecten. Dit maakt het vaststellen en hanteren van een benchmark lastig. Daarnaast zijn het niet zozeer de uitgaven in kwantitatieve zin die bescherming bieden, maar de maatregelen in kwalitatieve zin. Een financiële benchmark heeft daarom weinig nut.

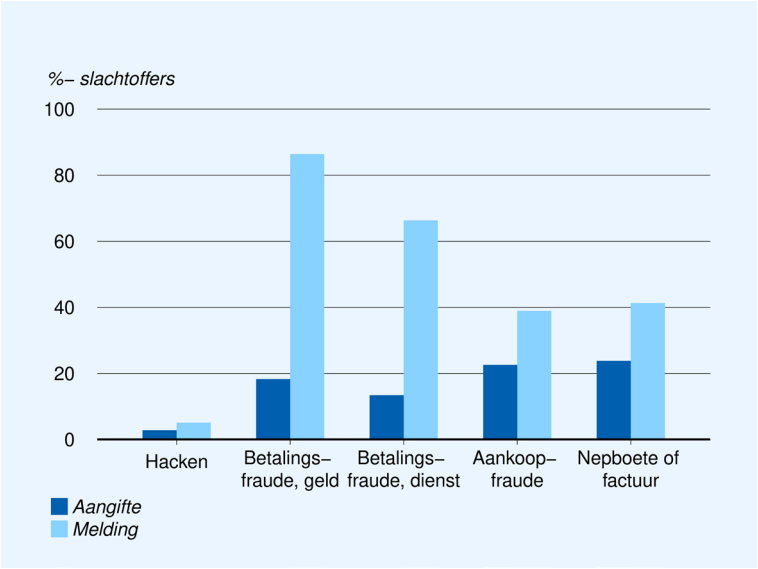
4.3 Opsporing en berechting cybercriminelen

Het afgelopen jaar heeft de politie verschillende successen geboekt bij het offline halen van criminele websites. Eind december 2018 werd bekendgemaakt dat de FBI samen met onder andere de Nederlandse politie 15 DDoS-as-a-service-websites offline heeft gehaald.[105] Ook nam de politie in samenwerking met Europese partners Wall Street Market over, een grote marktplaats op het *darkweb* waar onder andere *ransomware* werd verhandeld.[106] Of deze acties een blijvend effect hebben, is nog niet duidelijk. Digitale veiligheid blijft ook in 2019 een kernpunt voor het ministerie van Justitie en Veiligheid.[107] Met de Wet Computercriminaliteit III, die op 1 maart 2019 in werking is getreden, heeft de politie nieuwe bevoegdheden gekregen om computercriminaliteit te bestrijden.[108]

Ondanks de successen bij de aanpak van grensoverschrijdende cybercrime, blijft de aangiftebereidheid onder slachtoffers laag. Een recente CBS-enquête (CBS, 2018) vraagt slachtoffers van digitale criminaliteit in 2018 of ze de misdaad hebben gemeld en of ze aangifte hebben gedaan. Figuur 4.3 geeft de resultaten voor een aantal categorieën van cybercrime. Opvallend is dat fraude via het betalingsverkeer, waarbij geld van de rekening is gehaald, vaak wordt gemeld en dan met name bij de bank of financiële instelling. Dit is waarschijnlijk nodig om de financiële schade vergoed te krijgen. Andere vormen van fraude worden minder vaak gemeld. Belangrijke redenen om fraude niet te melden is dat het ging om een klein bedrag, of dat het slachtoffer denkt dat melden toch niet helpt om een vergoeding te krijgen of de dader te pakken. Hacken wordt bijzonder weinig gemeld. Redenen die slachtoffers hiervoor geven, zijn dat melding niet mogelijk is, te veel moeite is, of dat de dader toch niet wordt gepakt. De bereidheid om aangifte te doen bij de politie is bij alle vormen van cybercrime laag. Naast bovengenoemde redenen noemen slachtoffers ook relatief vaak dat de bank of financiële instelling het verder zou afhandelen. De resultaten van deze CBS-enquête zijn om statistische redenen niet direct te vergelijken met eerdere enquêtes. De genoemde resultaten sluiten desondanks redelijk aan bij de Veiligheidsmonitor 2017, die concludeerde dat 3,7 procent van de slachtoffers van hacken en 19,8 procent van de slachtoffers van koop- en verkoopfraude aangifte doen.[109] Dit suggereert dat de aangiftebereidheid redelijk constant is gebleven over tijd.

[104] Dit overzichtsartikel gaat hier verder op in.
[105] Zie bijvoorbeeld dit nieuwsbericht.
[106] Zie hier.
[107] Zie dit nieuwsbericht.
[108] Dit bericht gaat verder in op de nieuwe bevoegdheden van de politie.
[109] Bron: CBS Statline.

Figuur 4.3 Aangiftebereidheid hoog bij financiële delicten, laag bij hacken



Bron: CBS (2019)

Aangifte van cybermisdrijven leidt slechts in een klein aantal gevallen tot vervolging en schuldigverklaring. Niet alle cybermisdrijven worden apart geregistreerd. Online fraude wordt bijvoorbeeld samen met niet-digitale vormen van fraude geregistreerd in de categorie 'bedrog'. Alleen computervredebreuk, ofwel inbreken in een computersysteem, vormt een aparte categorie. De gegevens in tabel 4.1 laten zien dat zowel in 2017 als in voorgaande jaren van de geregistreerde gevallen van computervredebreuk slechts een zeer klein deel uitmondt in strafrechtelijke vervolging en dat een nog kleiner deel uiteindelijk resulteert in een schuldigverklaring. Bij bedrog, waarvan alleen het totaal van onlinefraude en niet-digitale vormen van bedrog bekend is, is het aandeel vervolgingen en schuldigverklaringen vergelijkbaar. Opvallend is dat bij diefstal/verduistering en inbraak relatief veel vaker een strafzaak met schuldigverklaring volgt. Waarschijnlijk zijn bij deze zaken vaker concrete sporen of getuigenverklaringen beschikbaar.

Een hoger percentage vervolgingen en veroordelingen bij cybercrime kan slachtoffers stimuleren om aangifte te doen. De perceptie dat aangifte doen 'toch niet helpt' kan verschuiven als het aandeel vervolgingen en veroordelingen stijgt. In dit verband is het goed dat successen, bijvoorbeeld het oppakken van fraudeurs op Marktplaats, zoveel mogelijk worden gedeeld en aandacht krijgen in de media. De politie probeert aangiftes verder te stimuleren door online aangifte mogelijk te maken.[110]

[110] Zie onder andere dit nieuwsbericht.

Tabel 4.1 Computervredebreuk in perspectief

Delict	Computervredebreuk		Bedrog (totaal)	Diefstal/ verduistering en inbraak
Periode	2008-2017	2017	2017	2017
Geregistreerde misdrijven	19.680	2.300	39.760	428.280
Ingeschreven bij OM	715	90	1.925	47.965
Schikking met OM	140	5	95	2.460
Strafbeschikking OM	30	0	145	6.600
Geseponeerd door OM	95	15	200	2.185
Rechtsgang	165	10	820	29.215
Uitspraak schuldig	125	10	670	26.780
Vrijspraak	35	0	140	2.320

Bron: CBS, WODC en Raad voor de Rechtspraak (2017).

4.4 Cyberverzekeringen

4.4.1 Nederlandse markt voor cyberverzekeringen is klein maar groeiende

Cyberverzekeringen dekken de (financiële) schade die ontstaat bij een cyberincident. De meeste cyberverzekeringen richten zich op bedrijven.[111] De eerste toetreders op de markt waren grote internationale verzekeraars, die zich vooral richtten op het grootbedrijf. Inmiddels zijn er ook verschillende Nederlandse aanbieders die zich meer richten op het mkb.[112] Onder de noemer cyberincident vallen zowel aanvallen van buitenaf, zoals hackers die bedrijfsgegevens buitmaken, als interne incidenten, zoals een datalek door een verloren laptop. De dekking wisselt per verzekering, maar omvat ruwweg de kosten van bedrijfsstilstand, crisismanagement, herstelkosten en aansprakelijkheidskosten.

De Nederlandse markt voor cyberverzekeringen groeit snel, maar is vergeleken met andere verzekeringen nog bescheiden. Volgens een enquête van het Verbond van Verzekeraars bedroeg het premie-inkomen in 2015 maximaal 10 miljoen euro, en was dit in 2017 minimaal 20 miljoen euro.[113] Deze groei wordt zowel veroorzaakt door toetreding van nieuwe aanbieders als door groei van bestaande aanbieders. Het premie-inkomen is echter in relatieve termen nog bescheiden. In 2017 was het premie-inkomen van aansprakelijkheidsverzekeringen voor bedrijven 800 miljoen euro en van schadeverzekeringen voor bedrijven 1,4 miljard euro.[114]

Wereldwijd is de markt het meest ontwikkeld in de VS. De totale premie-inkomsten voor cyberverzekeringen wereldwijd werden in 2016 geschat op 2,5 tot 3,5 miljard dollar.[115] 85 tot 90 procent van de markt bevond zich in de VS en 5 tot 9 procent in Europa. Een jaar later, in 2017, werden de premie-inkomsten in de VS geschat op ongeveer 3 miljard dollar (EU-U.S. Insurance Dialogue Project, 2018). Om dit in perspectief te plaatsen, deze premie-inkomsten zijn een factor 150 hoger dan in Nederland, terwijl de Amerikaanse

[111] Cyberverzekeringen voor particulieren zijn (vrijwel) niet verkrijgbaar in Nederland. Een reden hiervoor kan zijn dat de schade bij een cyberincident voor particulieren in financiële termen vaak beperkt is en veelal al is gedekt in andere verzekeringen. Tegelijkertijd groeit de aandacht voor de mogelijke gevolgen van identiteitsfraude. Hierdoor zou in de toekomst wel een particuliere markt kunnen ontstaan.
[112] De verzekeringen van Centraal Beheer en de Goudse zijn bijvoorbeeld expliciet bedoeld voor mkb-bedrijven met maximaal 10 miljoen euro omzet.
[113] Zie dit persbericht.
[114] Op basis van deze gegevens van het Centrum voor Verzekeringsstatistiek.
[115] Zie OECD (2017) p. 60.

economie ruim 23 keer zo groot is als die van Nederland.[116] Dus ook gecorrigeerd voor de omvang van de economie is de markt voor cyberverzekeringen in de VS duidelijk groter. Hierbij zal deels meespelen dat de VS een sterkere verzekeringscultuur kent.[117] Daarnaast was er in de VS al eerder dan in Europa een meldplicht van datalekken, wat de markt gestimuleerd kan hebben (RAND Europe en WODC, 2015).

4.4.2 Nog veel onzekerheden op de markt voor cyberverzekeringen

Verzekeraars hebben moeite om een risico-inschatting te maken en een dekking met bijbehorende realistische risicopremie te formuleren. Er zijn maar weinig harde gegevens beschikbaar over hoe vaak cyberaanvallen voorkomen en wat de directe en indirecte (financiële) gevolgen kunnen zijn.[118] Cyberrisico's zijn daarnaast dynamisch, waarbij dreigingen voortdurend evolueren. Dit maakt het voor verzekeraars moeilijk om een specifieke dekking te bepalen met een daarbij behorende realistische prijs. In het huidige verzekeringsaanbod is dit terug te zien. Er is een behoorlijke variatie in voorwaarden en gedekte schade, en de formuleringen zijn vanuit juridisch oogpunt niet altijd duidelijk. Deze onduidelijkheid wordt versterkt door een gebrek aan jurisprudentie. Een illustratie hiervan is een grote rechtszaak die momenteel loopt in de VS. Voedselproducent Mondelez leed miljoenen dollars schade door de NonPetya-*ransomware* en verhaalde deze op hun cyberverzekering. Verzekeraar Zurich weigert echter uit te keren op grond dat NonPetya een oorlogshandeling is, die is uitgesloten in de polis.[119]

Voor potentiële afnemers is het moeilijk om te bepalen of een cyberverzekering verstandig is. Veel bedrijven hebben moeite om in te schatten welke cyberrisico's ze lopen en wat de mogelijke gevolgen van een cyberincident kunnen zijn. Daarnaast kan de bovengenoemde onduidelijkheid over de dekking van een cyberverzekering een drempel vormen voor potentiële afnemers.[120] Ook is het niet altijd duidelijk in hoeverre andere bedrijfsverzekeringen, zoals een bedrijfsschadeverzekering of rechtsbijstandverzekering, de gevolgen van een cyberaanval deels al dekken. Vaak sluiten deze verzekeringen cyberincidenten niet expliciet uit van hun dekking.

Sommige cyberaanvallen kunnen snel veel slachtoffers maken en zijn daardoor complex om te verzekeren. Het basisprincipe achter schadeverzekeringen, zoals brand- en autoverzekeringen, is dat de risico's niet of nauwelijks gecorreleerd zijn. Schade bij één verzekerde heeft geen gevolgen voor het risico op schade bij een andere verzekerde. Hierdoor is de schadelast, gemiddeld over alle verzekerden, te overzien. Bij schade veroorzaakt door natuurfenomenen, zoals storm of hagel, worden wel veel mensen tegelijk getroffen, maar blijft de schade meestal beperkt tot een bepaald land of regio. Door herverzekering bij een internationale partij kan dit risico beperkt gespreid worden. Bij cyberdreigingen is dit ingewikkelder. *Ransomware* kan bijvoorbeeld snel en wereldwijd veel slachtoffers maken. Experts zijn het er niet over eens in hoeverre zulke extreme gebeurtenissen te verzekeren zijn. Sommigen zien het als onoplosbaar probleem, omdat herverzekering en spreiding van de risico's, bijvoorbeeld over bedrijfstakken of geografische regio's, op het eerste gezicht geen oplossing bieden. Anderen denken dat er wel een uitweg uit dit probleem te vinden is en trekken een analogie met terrorismeverzekeringen. Bij terrorisme is de potentiële schadelast ook extreem groot en in een aantal landen fungeert de overheid daarom als achtervang mochten verzekeraars hierdoor in de problemen komen.[121]

---

[116] Zie bijvoorbeeld deze gegevens van het CBS.
[117] De markt voor bedrijfsaansprakelijkheidsverzekeringen, gecorrigeerd voor GDP, is in de VS duidelijk groter dan in Europa. Zie bijvoorbeeld Swiss Re Group (2014).
[118] Onder andere EIOPA (2018) gaat hier verder op in.
[119] Zie bijvoorbeeld dit artikel uit de New York Times.
[120] Hoofdstuk 4 van OECD (2018) gaat hier verder op in.
[121] Zowel EIOPA (2018) als het OECD (2018) bespreken het probleem van gecorreleerde risico's in meer detail.

Er is nog geen consensus hoe moreel gevaar bij een cyberverzekering beperkt kan worden. Een schadeverzekering beperkt, in het algemeen, de prikkel om te investeren in preventieve maatregelen en kan leiden tot roekeloos gedrag. In de economische literatuur staat dit fenomeen bekend als 'moreel gevaar'. Niet-cyberverzekeringen ondervangen dit door voorwaarden te stellen aan de verzekerde en niet uit te keren wanneer sprake is van roekeloosheid. Bij het afsluiten van een gebouwverzekering kan de verzekeraar bijvoorbeeld eisen dat er voldoende rookmelders en brandblussers aanwezig zijn en wanneer een automobilist bewust roekeloos rijdt en daardoor een ongeluk veroorzaakt, kan de verzekeraar weigeren uit te keren. Bij cyberverzekeringen is dit momenteel nog minder ontwikkeld. Het is niet altijd eenvoudig om te bepalen wat passende voorzorgsmaatregelen zijn op cyberveiligheidsgebied, en preventieve maatregelen vragen daarnaast regelmatig onderhoud. Ook is er nog geen jurisprudentie over wat 'roekeloosheid' inhoudt in het kader van cyberveiligheid. In de huidige markt zijn er dan ook grote verschillen tussen verzekeraars. Er zijn pakketten op de markt die een cybersecurity-abonnement bij een specifiek beveiligingsbedrijf combineren met een verzekering voor het restrisico. Andere verzekeraars adviseren een bepaald merk beveiligingssoftware en bieden (met korting) een cybersecurity-abonnement, zonder dit te verplichten. Weer andere verzekeraars laten de uitvoering van de cyberbescherming volledig aan het verzekerde bedrijf en stellen enkel als voorwaarde dat er een up-to-date virusscanner, firewall en externe back-up moeten zijn.

4.4.3 Cyberverzekeringen kunnen bijdragen aan de cyberweerbaarheid

Een goed ontwikkelde markt voor cyberverzekeringen helpt om inzicht te krijgen in de cyberdreiging. Momenteel ontbreekt een goed overzicht van (de gevolgen van) cyberincidenten. Gecombineerde data van verzekeraars en andere betrokken partijen kunnen veel inzicht bieden in hoe vaak incidenten voorkomen, bij welk type bedrijven, welke aanvalsmethoden veel gebruikt worden en de gevolgen.[122] In de VS, waar de markt voor cyberverzekeringen verder is ontwikkeld, worden deze data al op beperkte schaal verzameld en gerapporteerd.[123] Deze gegevens zijn niet alleen nuttig voor verzekeraars om een risico-inschatting te maken en premie vast te stellen, maar ze hebben ook bredere waarde. Zo kan het bedrijven bewuster maken van de risico's die ze lopen en cybersecurityspecialisten helpen om zich te focussen op de grootste dreigingen.

Het stellen van basiseisen aan de verzekerde draagt bij aan de cyberweerbaarheid, mits dit niet alle verantwoordelijkheid van de verzekerde wegneemt. Vrijwel alle aanbieders van cyberverzekeringen stellen eisen aan de cybersecurity van verzekerde bedrijven, wat de algemene cyberweerbaarheid in het bedrijfsleven vergroot. Cyberverzekeringen die de verzekerde de cyberbeveiliging volledig uit handen nemen, dragen echter het risico dat het verzekerde bedrijf zich niet meer verantwoordelijk voelt voor eventuele beveiligingsfouten. Met name voor mkb-bedrijven is een pakketoplossing aantrekkelijk. Als mkb'er hoef je je dan niet meer te verdiepen in de kwaliteit van de verschillende cyberveiligheidsbedrijven en weet je zeker dat je voldoet aan de voorwaarden van de verzekeraar. Dit heeft echter het risico dat het mkb-bedrijf geen inzicht heeft in wat het cyberveiligheidsbedrijf wel en niet doet en volledig afhankelijk is van de inschatting die de verzekeraar maakt over de kwaliteit van het cyberveiligheidsbedrijf. Wanneer er desondanks een datalek met AVG-meldplicht optreedt, is het maar zeer de vraag of de verantwoordelijkheid van het bedrijf om passende maatregelen voor databescherming toe te passen afgeschoven kan worden naar de verzekeraar. Daarnaast is het juridisch onduidelijk in hoeverre AVG-boetes verzekerbaar zijn.[124] In dit opzicht kunnen cyberverzekeringen een vals gevoel van veiligheid geven.

[122] Op dit moment wisselen cyberverzekeraars binnen Nederland nauwelijks data uit. Hierbij lijkt mee te spelen dat de markt nog klein is, het aantal claims zeer beperkt en de data daardoor concurrentiegevoelig. Het Centrum voor Verzekeringsstatistiek, onderdeel van het Verbond van Verzekeraars, rapporteert en analyseert wel gegevens van grote verzekeringsmarkten, zoals autoverzekeringen.
[123] Zie Insurance Industry Cybercrime Task Force (2010 en NetDiligence (2018).
[124] Dit artikel van Aon gaat verder in op de verzekerbaarheid van AVG-boetes.

4.4.4 Overheidsbeleid nuttig om de markt in de juiste richting te laten ontwikkelen

Normen voor cyberveiligheid kunnen de ontwikkeling van cyberverzekeringen verder helpen. Op dit moment verschillen verzekeraars flink in de eisen die ze aan verzekerden stellen. Dit maakt het voor potentiële afnemers moeilijk een keus te maken en kan het met name voor minder cyberbewuste bedrijven aantrekkelijk zijn om een pakket te kiezen wat de beveiliging uit handen neemt. Een keurmerk voor cyberveiligheidsbedrijven in combinatie met een risicomodel voor ondernemers helpt het verzekeringsaanbod te standaardiseren en tegelijkertijd de verzekerde verantwoordelijk te laten voor de beveiliging. De ondernemer kan met het risicomodel aangeven hoe het gesteld is met de cyberveiligheid en de verzekeraar kan een cyberveiligheidsoplossing met keurmerk verplichten, zonder expliciet te sturen naar een bepaald merk. Er zijn al een aantal initiatieven op dit gebied. De ISO27k-reeks geeft een internationale norm voor informatiebeveiliging en ontwikkelt onder andere richtlijnen voor cyberverzekering. De (internationale) verzekeringsbranche heeft zich echter kritisch uitgelaten over deze ontwikkeling, onder andere omdat zij niet geconsulteerd is en er voor andere verzekeringsproducten geen ISO-richtlijnen bestaan.[125] De Europese Cybersecurity Act bevat een kader voor certificering van ICT-producten, -diensten en -processen in brede zin. Daarnaast werkt het Centrum voor Criminaliteitspreventie en Veiligheid in samenwerking met het bedrijfsleven en de overheid aan een risicomodel en keurmerk cybersecurity.[126]

Meer duidelijkheid over de bepaling van AVG-boetebedragen en de verzekerbaarheid hiervan helpt bedrijven een zuivere afweging te maken over het nut van een cyberverzekering. Overtreding van de AVG is een van de meest zichtbare mogelijke gevolgen van een cyberincident. Hierover lijkt onder (mkb-) bedrijven onduidelijkheid en ongerustheid te zijn. De maximale boetebedragen zijn erg hoog en omdat er tot nu toe weinig boetes zijn uitgedeeld, is het moeilijk om in te schatten hoe de Autoriteit Persoonsgegevens zal omgaan met specifieke omstandigheden.[127] Voor sommige bedrijven is dekking van AVG-boetes daarom een belangrijke reden om een cyberverzekering te overwegen.[128] Tegelijk is het juridisch onduidelijk in hoeverre verzekering van AVG-boetes is toegestaan. En wanneer dit zou mogen, is het onwenselijk dat de gevolgen van het niet nakomen van de AVG via een verzekering worden belegd bij de verzekeraar. Gezien deze onduidelijkheden is meer informatie over de AVG-boetebedragen en de verzekerbaarheid van boetes wenselijk.

Omdat cyberrisico's gecorreleerd en deels onbekend zijn, vereist dit mogelijk extra aandacht van toezichthouders. Momenteel is de omvang van de markt voor cyberverzekeringen nog beperkt, waardoor een verkeerde risico-inschatting weinig gevolgen zal hebben voor het gehele financiële systeem. Wanneer de markt groeit, kunnen de onzekerheden rondom cyberrisico's echter wel een rol gaan spelen bij de financiële stabiliteit van verzekeraars. Het is dan van belang dat DNB toeziet op het risicoprofiel van (cyber-)verzekeraars en inzicht krijgt in de correlatie van cyberrisico's. Het kan nuttig zijn om in Europees verband op te treden. Verschillende cyberverzekeringen worden aangeboden door internationaal opererende verzekeraars. Ook zijn op Europees niveau meer data beschikbaar over cyberrisico's, wat kan helpen met een tijdige en adequate risico-inschatting. EIOPA, de Europese toezichthouder op verzekeraars, heeft recentelijk al een voorstel gedaan om cyberverzekeringen als aparte categorie op te nemen in de rapportage die verzekeraars onder Solvency II aan de nationale toezichthouder moeten doen.[129]

[125] Zie bijvoorbeeld deze brief van de wereldwijde federatie van verzekeraars GFIA aan ISO.
[126] Zie dit bericht.
[127] In maart 2019 heeft de AP wel nieuwe boetebeleidsregels gepubliceerd.
[128] Ook EIOPA (2018) signaleert dit.
[129] Het EIOPA voorstel is hier te vinden.

4.5 Voorlichting en samenwerking in het cyberdomein

4.5.1 Diverse mix van voorlichting en samenwerking

Overheidsbeleid zet in op voorlichting en publiek-private samenwerking om cybercriminaliteit te voorkomen en te bestrijden. Dit blijkt o.a. uit de Nederlandse Cybersecurity Agenda (Rijksoverheid, 2018), waarin publiek-private samenwerking genoemd wordt als een belangrijke route om de veiligheid in het digitale domein te waarborgen: dat "kan alleen in samenwerking met en deels ook door het bedrijfsleven worden vormgegeven." Daarnaast is "het publiek en privaat delen van beschikbare kennis en het bevorderen van informatiedeling nodig om cybersecurity in de breedte te versterken" (p.7). Verschillende initiatieven geven concreet vorm aan dit streven. Voor het stimuleren van samenwerkingen zijn de Cybersecurity Alliantie (CSA) en het Digital Trust Center (DTC) opgericht. Ook zijn er meerdere voorlichtingswebsites, zoals de voorlichting van het DTC, die zich vooral richt op het mkb, en de websites van Alert Online en Veilig Internetten.

Gemeten naar het aantal initiatieven lijkt de inzet op publiek-private samenwerking resultaat te hebben. Volgens een inventarisatie van de CSA zijn momenteel 38 verschillende samenwerkingsverbanden actief in Nederland. Tabel 4.2 laat ter illustratie een aantal initiatieven zien. Uit tabel 4.2 en het overzicht van CSA komt het beeld naar voren dat op verschillende niveaus en met verschillende doelen organisaties met elkaar samenwerken. Sommige zijn gefocust op één enkele sector en/of één doel, terwijl andere initiatieven het hele palet bestrijken van cyberveiligheid en geen onderscheid (lijken te) maken naar type organisatie. Naast deze initiatieven werken veel organisaties samen in ISACs (Information Sharing and Analysis Centres) of via een gezamenlijke CERT (Computer Emergency Response Team).

Tabel 4.2 Grote mate van diversiteit in type samenwerking

Naam	Niveau	Identificatie	Preventie	Detectie	Respons	Herstel
Cyberweerbaarheid Brainport Eindhoven	Regionaal	x	x	x	x	x
Connect2Trust	Sectoroverstijgend	x	x	x	x	x
Secure Software Alliance	Sectoroverstijgend		x	x		
Cyberweerbaarheid Noord Nederland	Regionaal		x		x	
TIBER (financiële instellingen)	Sector				x	
Veilige E-Mail Coalitie	Sectoroverstijgend		x			
Dutch Continuity Board	Sectoroverstijgend		x	x	x	
FERM (Haven Rotterdam)	Regionaal	x	x	x	x	x

NB. De tabel ordent verschillende samenwerkingsinitiatieven naar de vijf componenten van het NIST-model voor cyberveiligheid (link). De voorbeelden zijn afkomstig van de Cyber Security Alliantie (link).

Er is weinig bekend over de effectiviteit van de verschillende initiatieven rondom samenwerking en voorlichting. Het is moeilijk om de effecten van samenwerkingsverbanden te meten. Zoals tabel 4.2 laat zien, hebben samenwerkingsverbanden regelmatig meerdere doelen, waardoor onduidelijk is op welke facetten het project beoordeeld moet worden. De doelen zijn vaak kwalitatief geformuleerd, bijvoorbeeld 'het delen van relevante kennis', waardoor een goede kwantitatieve uitkomstmaat ontbreekt. En organisaties die vrijwillig samenwerking zoeken, verschillen waarschijnlijk in belangrijke dimensies, zoals awareness, van organisaties die dat niet doen. Vergelijken van deelnemers met niet-deelnemers geeft daarom geen inzicht in het *effect* van samenwerking. Ook het effect van voorlichtingscampagnes is niet eenvoudig te meten. Vaak wordt wel in

kaart gebracht hoeveel bezoekers een voorlichtingssite heeft getrokken, maar het is meestal onbekend in hoeverre de voorlichting tot een blijvende gedragsverandering heeft geleid. Het Nationaal Cybersecurity Bewustzijnsonderzoek, jaarlijks uitgevoerd door Alert Online, geeft enig inzicht in het cybersecuritybewustzijn over tijd, maar koppelt dit niet aan voorlichtingscampagnes.

4.5.2 Redenen voor overheidsingrijpen

Sommige samenwerkingsverbanden en voorlichtingscampagnes dienen een publiek doel en zouden zonder overheidsingrijpen niet of moeilijk van de grond komen. Bij vitale processen is er bijvoorbeeld een publiek belang dat informatie over dreigingen snel wordt uitgewisseld en dat organisaties snel reageren op een aanval. Om hierin te voorzien stimuleert de overheid ISACs voor bedrijven die onderdeel zijn van de vitale infrastructuur en worden vitale organisaties gestimuleerd om incidenten te oefenen. Ook kan overheidsingrijpen nodig zijn bij het tegengaan van cybercriminaliteit. Bij een project als *No More Ransom*, bijvoorbeeld, ondersteunt de overheid een platform dat (gratis) herstelsoftware aanbiedt voor gijzelsoftware, waardoor verspreiding daarvan financieel minder aantrekkelijk wordt.[130] Ook het vergroten van de bewustwording van cyberrisico's kan worden gezien als een publiek belang. Ten slotte kan overheidsingrijpen een coördinatieprobleem oplossen. Een voorbeeld hiervan is het toepassen van standaarden voor veilige e-mail. Die zijn effectief als ze in de hele keten van verzenders en ontvangers gebruikt worden. De overheid participeert daarom in Forum Standaardisatie en de Veilige E-mailcoalitie.

Het is van belang om steeds na te gaan wat overheidsingrijpen rechtvaardigt. Is er een publiek belang dat gediend wordt of kan het initiatief ook aan de markt worden overgelaten? Bij sommige samenwerkingsverbanden is de rationale voor publieke ondersteuning onduidelijk, maar kan er wél een private reden zijn voor samenwerking. Organisaties kunnen bijvoorbeeld in een toeleveringsketen wederzijds van elkaar afhankelijk zijn en daarom via samenwerking willen voorkomen dat een cyberaanval op de één leidt tot financiële schade voor de ander. Indien de toeleveringsketen geen vitaal proces voortbrengt en er geen domino-effecten zijn die tot maatschappelijke verstoring kunnen leiden, is het argument voor overheidsingrijpen onduidelijk. Een ander voorbeeld van een initiatief dat wellicht ook zonder overheidssteun van de grond zou kunnen komen, is samenwerking rondom een cybersecurity-vakopleiding, waarbij studenten praktijkervaring kunnen opdoen bij bedrijven in de regio. Ook voorlichting kan deels aan de markt worden overgelaten, aangezien bedrijven (zoals verzekeraars of cyberveiligheidsbedrijven) een commercieel motief hebben om bedrijven te wijzen op cyberrisico's.

Het is daarnaast van belang om na te gaan welk instrument het meest geschikt is om het doel te bereiken. Een risico bij de huidige nadruk op (publiek-private) samenwerking in beleid is dat alternatieve middelen buiten zicht raken en samenwerking een doel op zichzelf wordt. Samenwerken, bijvoorbeeld in de vorm van het delen van ervaringen, delen van aanvalsdata of gezamenlijk testen van de cyberweerbaarheid kan een nuttige manier zijn voor organisaties om digitaal veiliger te worden. Maar het oprichten en subsidiëren van een samenwerkingsverband is voor de overheid niet in alle gevallen het beste middel om een bepaald doel te bereiken. Wetgeving, zoals beveiligings- of transparantieverplichtingen, kan ook bijdragen aan cyberveiligheid.

4.5.3 Risico's van een decentrale aanpak

De veelheid aan initiatieven op het gebied van samenwerking en voorlichting kan tot inefficiëntie of inconsistentie leiden. Samenwerkingsverbanden overlappen soms, waardoor het voor bedrijven onduidelijk kan zijn waar ze zich moeten aansluiten, en er zijn meerdere subsidieregelingen. Ook in de doelgroepen en inhoud van de verschillende voorlichtingssites zit overlap. Door deze overlap kunnen inefficiënties ontstaan, zoals dubbel werk of belangrijke thema's die juist blijven liggen. Naast inefficiënties kan overlap ook leiden

[130] De site van No More Ransom is hier te vinden.

tot inconsistenties waarbij de ene doelgroep onterecht anders wordt behandeld dan de andere. Zo is het NCSC het eerste aanspreekpunt voor bedrijven in vitale sectoren. Niet-vitale bedrijven vallen onder het DTC. Deze tweede groep is echter enorm groot en divers, van kleine zelfstandige tot grootbedrijf. In deze groep zitten waarschijnlijk bedrijven die belangrijke schakels zijn in het netwerk om de vitale sectoren heen en die bij verstoring via domino-effecten ook vitale processen kunnen raken. Bij een incident kunnen deze bedrijven formeel geen beroep doen op bijstand van het NCSC. Ook missen deze bedrijven wellicht belangrijke informatie die via ISAC's voor vitale organisaties wordt uitgewisseld. Op termijn wil het DTC relevante actuele dreigingsinformatie van het NCSC toegankelijk maken voor de DTC-doelgroep, maar momenteel richt het DTC zich vooral op de bedrijven die nog aan het begin staan van veilig digitaal ondernemen. Overigens wordt het risico van inefficiëntie ook gesignaleerd in de Nederlandse Cybersecurity Agenda: "de effecten van de verschillende inspanningen kunnen worden verbeterd door samenhang aan te brengen in communicatiecampagnes in het publieke domein" (p.40).

Een grotere inzet op evaluatie is nodig om tot beter beleid te komen. Een regelmatige evaluatie is nodig om te bepalen of de verschillende initiatieven effectief zijn. Dit is in het bijzonder relevant wanneer publieke fondsen worden ingezet om een samenwerkingsverband of voorlichtingscampagne te financieren. Hoewel een zuivere effectmeting vaak niet mogelijk zal zijn, kunnen bijvoorbeeld resultaten van *pentesten* (digitale brandoefeningen) of interviews met deelnemers aan samenwerkingsverbanden gebruikt worden om een indicatie te krijgen van de effectiviteit. Ook kan de huidige hoeveelheid aan initiatieven gebruikt worden als een experimentele setting om te bepalen wat goed en minder goed werkt. Dit vraagt echter wel om een bewuste vormgeving van initiatieven zodat deze goed vergeleken kunnen worden. Op dit moment worden er eerste stappen gezet tot effectmeting in samenwerking met het CBS.

De ervaringen in ons omringende landen kunnen aanknopingspunten geven om het beleid verder vorm te geven. Verschillende landen kiezen voor een verschillende aanpak omtrent voorlichtingscampagnes en het stimuleren van samenwerking. Een interessante casus is het Verenigd Koninkrijk, waar het National Cyber Security Center het centrale aanspreekpunt en voorlichtingspunt is voor burgers, kleine en grote bedrijven en overheidsorganisaties. Deze aanpak verschilt van de Nederlandse aanpak die zich met verschillende initiatieven richt op verschillende doelgroepen. Positieve en negatieve ervaringen met de werkwijze in het Verenigd Koninkrijk kunnen behulpzaam zijn om het Nederlandse beleid verder vorm te geven.

Referenties

Ablon, L. en A. Bogart, 2017, *Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits.* RAND Corporation: Santa Monica CA (link).

Accenture, 2019, Ninth annual cost of cybercrime study (link).

AIVD, 2019, Offensief cyberprogramma, Een ideaal businessmodel voor staten (link).

AIVD, 2018, AIVD Jaarverslag 2018 (link).

Algemene Rekenkamer, 2018, Digitale dijkverzwaring: cybersecurity en vitale waterwerken (link).

Analistennetwerk Nationale Veiligheid, 2016, Nationaal Veiligheidsprofiel 2016 (link).

Anderson, R., C. Barton, R. Böhme, R. Clayton, C. Gañán, T. Grasso, M. Levi, T. Moore, Tyler en M. Vasek , 2019, Measuring the changing cost of cybercrime (link).

Anti Phishing Working Group, phishing attack trends reports (link).

AP, 2018, Grip op persoonsgegevens: jaarverslag 2018 (link).

Brundage, M., et al., 2018, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *Computing Research Repository* (link).

CBS, WODC en Raad voor de Rechtspraak, 2017, Criminaliteit & rechtshandhaving 2017: ontwikkelen en samenhangen (link).

CBS, 2018, Digitale Veiligheid & Criminaliteit 2018 (link).

CBS, 2019, Internationaliseringsmonitor/2019-I: Verenigde Staten (link).

Cisco, 2018, Annual Cybersecurity report (link).

CPB, 2017, Scientia potentia est, De opkomst van de makelaar van alles.

CPB, 2018, Risicorapportage Cyberveiligheid Economie 2018.

CPB, 2019, Een blik op de NCSC beveiligingsadviezen (link).

DLA Piper, 2019, DLA Piper GDPR Data Breach Survey: February 2019 (link).

EIOPA, 2018, Understanding Cyber Insurance – A structured dialogue with insurance companies (link).

ENISA, 2019, ENISA Threat Landscape report 2018 (link).

EU-U.S. Insurance Dialogue Project van EIOPA, 2018, The cyber insurance market (link).

Forum Standaardisatie, 2019, Meting informatieveiligheidstandaarden (link).

Desmaris, S., P. Dubreuil, en B. Loutrel, 2019, Creating a French framework to make social media platforms more accountable: Acting in France with a European Vision. (link).

Fireeye, 2019, M-trends 2019 (link).

Google, 2019, How Google fights disinformation (link).

Herley, C., 2010, The Plight of the Targeted Attacker in a World of Scale (link).

Hiscox, 2019, Hiscox Cyber readiness report 2019 (link).

Insurance Industry Cybercrime Taskforce, 2019, The Cybercrime Explosion (link).

Keulen, I. van, I. Korthagen, P. Diederen, en P. van Boheemen, 2018, Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland, Rathenau Instituut.

Kamerstukken II 2017/18, 30821, nr. 46 (link).

Kamerstukken II, 2019, Kamerbrief Maatregelen bescherming telecomnetwerken en 5G (link).

Kamerstukken II 2018/19, 2019D31225 (link).

Kamerstukken II 2018/19, 26643, nr. 625 (link).

Kamerstukken II 2018/19, 31839, nr. 686 (link).

Kamerstukken II, 2018/2019, 1853 (link).

Microsoft, 2019, Microsoft Security Intelligence Report Volume 24.

NCTV, 2019, Cybersecuritybeeld Nederland 2019: Ontwrichting maatschappij ligt op de loer (link).

NCTV, 2019b, Nationale Veiligheid Strategie (link).

NBIP en SIDN, 2018, The impact of DDoS attacks on Dutch enterprises (link).

NBIP, 2018, DDoS-datarapport 2017, Ede: Nationale Beheersorganisatie Internet Providers .

NBIP, 2019, DDoS-datarapport 2018, Ede: Nationale Beheersorganisatie Internet Providers .

NBIP, 2019, DDoS-datarapport 1e halfjaar 2019, Ede: Nationale Beheersorganisatie Internet Providers (link).

NetDiligence, 2018, Cyber claims study (link).

OECD, 2017, *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris. (link).

Open Society Institute Sofia, 2018, Common sense wanted: Resilience to 'post-truth' and its predictors in the new media literacy index 2018 (link).

Radware, 2018, The trust factor: Cybersecurity' s role in sustaining business momentum (link).

RAND Europe en WODC, 2015, Investeren in cybersecurity (link).

Reuters Institute, 2019, Digital News Report 2019 (link).

Rijksoverheid, 2018, Nederlandse Cybersecurity Agenda: Nederland digitaal veilig (link)

Rijksoverheid, 2019, Nationale Veiligheid Strategie 2019. (link).

Risk Based Security, 2019, 2018 Vulnerability Trends.

Symantec, 2019, Internet Security Threat Report Volume 24

Skybox Security, 2019, 2019 Vulnerability and threat trends: research report (link).

Swiss Re Group, 2014, Liability claims trends: emerging risks and rebounding economic drivers.

Til, G. van, 2019, Zelfregulering door online platforms: een waar wondermiddel tegen online desinformatie?, *Mediaforum 2019*.

Varol et al., 2017, Online Human-Bot Interactions: Detection, Estimation, and Characterization (link).

Wardle, C. en H. Derakhshan, 2017, Information disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe Report, 2017.

Wellcome, 2018, Wellcome Global monitor: How does the world feel about science and health? (link).

WODC, 2017, (Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen (link).

WRR, 2019, WRR rapport nr.101: Voorbereiden op digitale ontwrichting (hier).