Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland

CSBN 2019

Cybersecuritybeeld Nederland

CSBN 2019

Colofon

Het Cybersecuritybeeld Nederland (CSBN) 2019 biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vastgesteld.

De NCTV beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten. Samen met zijn partners binnen overheid, wetenschap en bedrijfsleven zorgt de NCTV ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft. De NCTV is binnen de Rijksoverheid verantwoordelijk voor de coördinatie van terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing. Met zijn partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland. De focus ligt op het voorkomen en beperken van maatschappelijke ontwrichting.

Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC draagt bij aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving, specifiek de digitale weerbaarheid van Rijk en vitale aanbieders.

Het CSBN is opgesteld door de NCTV en het NCSC en is tot stand gekomen op basis van de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. De NCTV heeft dankbaar gebruik gemaakt van hun expertise en informatie, zowel tijdens expertsessies als tijdens de validatie van het CSBN.

Inhoud

Vergroten weerbaarheid belangrijkste instrument om risico's te verminderen

Ontwrichting maatschappij ligt op de loer

Het Cybersecuritybeeld Nederland (CSBN) 2019 biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid gepubliceerd en komt tot stand in samenwerking met publieke en private partners.

Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict. Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade. Vitale processen zijn in hoge mate afhankelijk van elektriciteitsvoorziening en datacommunicatie. Uitval en verstoring hiervan hebben zeer snel, binnen enkele uren, impact op een aantal vitale processen. Vanwege de omvang van de dreiging en het achterblijven van de weerbaarheid, ontstaan risico's voor de nationale veiligheid.

Grootste dreiging vanuit statelijke actoren

Er is sprake van een permanente digitale dreiging. De omvang van de dreiging die uitgaat van statelijke actoren blijft groeien. Landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland. Dit betekent dat deze landen digitale middelen inzetten om geopolitieke én economische doelstellingen te bereiken ten koste van Nederlandse belangen.Verstoring en sabotage hebben de meeste impact op de nationale veiligheid vanwege de potentieel maatschappij-ontwrichtende effecten. Voorbereidingshandelingen voor verstoring en sabotage vormen een potentiële dreiging voor de onafhankelijkheid en zelfstandigheid van Nederland. Alleen al door, expliciet of impliciet, te dreigen met verstoring of sabotage kan een actor pogen besluitvormingsprocessen te beïnvloeden. Economische spionage vormt een actuele dreiging voor Nederlandse belangen. Daarnaast hebben de activiteiten van criminelen grote impact. De dreiging hiervan blijft onverminderd groot, onder meer door de schaalbaarheid van cybercrime.

Afhankelijkheid van beperkt aantal aanbieders en landen

Nederland is in brede zin afhankelijk van een relatief kleine groep aanbieders van hard- en software, digitale diensten en platforms uit een beperkt aantal landen. Dit maakt de maatschappij kwetsbaar voor veranderende intenties van deze aanbieders en landen. Deze afhankelijkheid brengt risico's voor de nationale veiligheid met zich mee.

Geavanceerde aanvalscapaciteiten laagdrempelig toegankelijk

Het uitvoeren van een digitale aanval is vaak weinig riskant voor een aanvaller. Zorgwekkend is de laagdrempeligheid waarmee geavanceerde aanvalscapaciteiten te verwerven zijn via commerciële leveranciers en via een omvangrijke cybercriminele dienstensector. Nederlandse ict-infrastructuur wordt in deze laatste sector veelvuldig aangeboden. De groep actoren die beschikt over geavanceerde aanvalscapaciteiten groeit. Hierdoor groeit de dreiging en neemt de kans op onjuiste attributie toe. Deze kans neemt verder toe omdat slechts een beperkt aantal landen beschikt

over voldoende capaciteiten om te kunnen attribueren op basis van inlichtingenonderzoek in brede zin, bovenop attributie op basis van technische kenmerken. Het risico bestaat dat bedrijven, media of zelfs landen aanvallen niet kunnen toewijzen, of foutief toewijzen aan partijen.

Weerbaarheid niet overal op orde

Het vergroten van de weerbaarheid is het belangrijkste instrument voor burgers, bedrijven en overheid om risico's te verminderen. Een compleet scherp beeld van de weerbaarheid ontbreekt. Het beïnvloeden van de afhankelijkheid en dreiging blijkt zeer complex. Maatregelen worden niet altijd genomen omdat kosten en baten op het gebied van cybersecurity ongelijk verdeeld zijn. Onduidelijk is of de aanwezige prikkels om de kostenbatenverdeling te wijzigen voldoende zijn.

Doorgroeiende dreiging

Geopolitieke ontwikkelingen zullen de dreiging vanuit statelijke actoren verder vergroten. Fundamentele belangentegenstellingen tussen landen en verschil van inzicht over internationale normen en waarden versterken deze dreiging. Rondom technologie en dominantie hierin lijkt een geopolitiek spanningsveld te ontstaan.

Digitalisering leidt tot een verdere vergroting van de aanvalsmogelijkheden en een groei en verschuiving van de aandacht van actoren naar andere en nieuwe waardevolle doelwitten. De dreiging vanuit criminelen blijft onverminderd groot. Storingen en uitval zullen een grotere impact op het maatschappelijk leven hebben door de volledige afhankelijkheid van gedigitaliseerde processen en systemen. Onvoldoende digitale veiligheid maakt ontwrichting van de maatschappij mogelijk.

Leeswijzer

Het CSBN 2019 biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ict te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.[1] Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.

Het CSBN is tot stand gekomen op basis van de inzichten en expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. De ontwikkelingen zijn in kwalitatieve vorm beschreven. Indien in betrouwbare vorm beschikbaar wordt dit ondersteund met een kwantitatieve onderbouwing of een verwijzing naar bronnen.

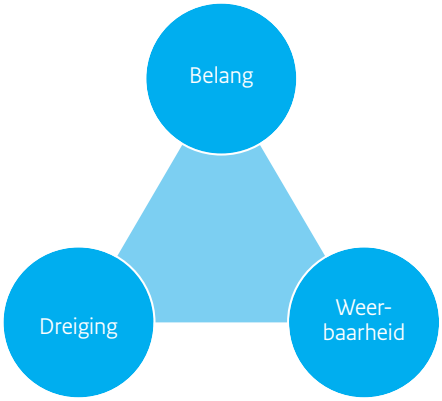
Het monitoren van dreigingen, belangen en weerbaarheid is een continu proces, met het CSBN als een van de jaarlijkse resultaten. Zaken die ten opzichte van vorige edities van het CSBN niet of nauwelijks zijn veranderd, zijn niet of slechts beknopt beschreven. Aan de analyse in het CSBN ligt de driehoek dreiging, belang en weerbaarheid ten grondslag. Deze drie factoren bepalen in samenhang het risico.

De hoofdvragen van het CSBN 2019 zijn:

- Welke dreigingen kunnen de beschikbaarheid, vertrouwelijkheid of integriteit van informatie, informatiesystemen of -diensten aantasten?
- Wat is het belang van digitale veiligheid? Wat zijn de potentiële gevolgen voor de nationale veiligheid indien geïdentificeerde dreigingen zich manifesteren?
- Welke combinaties van kwetsbaarheden en middelen hebben zich binnen de rapportageperiode mei 2018 tot en met januari 2019 mondiaal gemanifesteerd en (kunnen) worden toegepast in Nederland (jaarbeeld)?
- In welke mate is Nederland en de nationale veiligheid weerbaar tegen de ingezette of inzetbare middelen, te misbruiken kwetsbaarheden en het manifest worden van dreigingen?
- In hoeverre zijn er onderliggende oorzaken of factoren te identificeren die ten grondslag liggen aan het cybersecuritybeeld?
- Welke bredere ontwikkelingen hebben naar verwachting invloed op het toekomstige cybersecuritybeeld?

In de voorgaande tekst zijn de opvallendste ontwikkelingen uit dit cybersecuritybeeld beschreven. Hoofdstuk 1 beschrijft de kernproblematiek, de onderliggende oorzaken en factoren die ten grondslag liggen aan het cybersecuritybeeld. Deze zijn gebaseerd op het vorige CSBN. In hoofdstuk 2 wordt de dreiging nader beschreven en toegelicht. Hoofdstuk 3 gaat over het belang van cybersecurity voor de samenleving en de nationale veiligheid. Het vierde hoofdstuk bevat het jaarbeeld. De weerbaarheid van Nederland komt in hoofdstuk 5 aan de orde. In het zesde en laatste hoofdstuk wordt de brede vooruitblik gepresenteerd. De bijlagen bieden tot slot een overzicht van de door het NCSC afgehandelde incidenten en een toelichting op de gebruikte afkortingen.

Figuur 1 **Model belang, dreiging en weerbaarheid**



Kosten en baten ongelijk verdeeld

1 Kernproblematiek

Aan dit cybersecuritybeeld liggen verschillende kernproblemen ten grondslag. Dit zijn de oorzaken en factoren die aan de basis liggen van de geschetste dreigingen, belangen en weerbaarheid.

Terugvalopties en analoge alternatieven zijn vrijwel afwezig. Kosten en baten op het gebied van cybersecurity zijn ongelijk verdeeld. Er bestaat een afhankelijkheid van een beperkte aantal aanbieders en landen. Het uitvoeren van een digitale aanval is vaak weinig riskant. Capaciteiten om een aanval uit te voeren zijn laagdrempelig toegankelijk. Onveilige producten en diensten zijn de achilleshiel van digitale veiligheid. Toenemende complexiteit en connectiviteit hebben negatieve effecten op de weerbaarheid.

Digitalisering is fundament samenleving

Onze samenleving is vrijwel volledig afhankelijk geworden van gedigitaliseerde processen en systemen. Dat maakt digitale veiligheid essentieel om maatschappelijke en economische groei mogelijk te maken en maatschappelijke ontwrichting te voorkomen.

Terugvalopties en analoge alternatieven vrijwel afwezig

Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict. Omdat analoge alternatieven bijna helemaal verdwenen en terugvalopties afwezig zijn, is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade.

Kosten en baten cybersecurity ongelijk verdeeld

Cybersecuritymaatregelen zijn noodzakelijk als barrière tegen digitale dreigingen, tegelijkertijd kosten deze maatregelen ook tijd en geld. Burgers, bedrijven, sectoren en overheden zullen daarom altijd een belangenafweging (moeten) maken. Soms ligt het belang van digitale veiligheid direct in het verlengde van andere belangen. Soms ontstaan er tegengestelde belangen tussen organisaties of zelfs binnen organisaties, bijvoorbeeld tussen gebruiksgemak voor het individu en het brede belang van cybersecurity. Ook kan het individuele (bedrijfseconomische) belang van een bedrijf strijdig zijn met het maatschappelijke belang. De ongelijke verdeling van kosten en baten is hier de belangrijkste oorzaak. Hierdoor worden maatregelen niet altijd genomen. Onduidelijk is of de aanwezige prikkels om de verdeling te wijzigen voldoende zijn.

Afhankelijkheid van beperkt aantal aanbieders en landen

De afhankelijkheid van een relatief kleine groep aanbieders van hard- en software en digitale diensten en platforms uit een beperkt aantal landen neemt toe. Vanwege de technologische mogelijkheden of de prijsprestatieverhouding kan het voor bedrijven, burgers en landen aantrekkelijk zijn om gebruik te maken van deze aanbieders. Deze kunnen vaak beschikken over meer middelen om zich tegen aanvallen te wapenen, tegelijkertijd kan de maatschappelijke impact bij (ver)storingen of compromittering groot zijn.[2] Producten of diensten van (buitenlandse) aanbieders kunnen, met of zonder medeweten van deze aanbieder, gecompromitteerd worden door kwaadwillende actoren. Daarnaast zijn aanbieders onderworpen aan de wet- en regelgeving en zouden zij door overheden in het buitenland gedwongen kunnen worden tot een vorm van medewerking aan bijvoorbeeld spionage of voorbereiding voor sabotage.

De afhankelijkheid van (een beperkt aantal) aanbieders en landen maakt de maatschappij gevoelig voor de intenties van deze aanbieders en landen en kwetsbaar voor veranderingen daarin. Dit brengt risico's voor de nationale veiligheid mee zich mee.

Permanente digitale dreiging

De omvang van de dreiging die uitgaat van statelijke actoren blijft groeien. Landen blijven digitale middelen inzetten voor spionage, verstoring en sabotage om eigen doelen te bereiken ten koste van Nederlandse belangen. De dreiging vanuit criminelen blijft onverminderd groot. De digitale dreiging is permanent.

Uitvoeren digitale aanval weinig riskant

De kans bestaat dat de aanval lange tijd onopgemerkt blijft. Als de aanval wel ontdekt wordt, is de attributie aan en de opsporing van de actoren complex. Indien attributie wel mogelijk is, blijft dat in vele gevallen zonder consequenties, zeker in het geval van statelijke of aan staten gelieerde actoren. Wel heeft er een kentering plaatsgevonden in het publiekelijk attribueren van digitale aanvallen door overheden. Verscheidene landen hebben aanvallen toegeschreven aan andere landen of specifieke actoren. Het effect van deze publieke attributie is nog onduidelijk. Vooralsnog lijkt het uitvoeren van digitale aanvallen weinig riskant voor een aanvaller.

Geavanceerde aanvalsmiddelen laagdrempelig toegankelijk

Digitale aanvalscapaciteiten zijn laagdrempelig te verwerven via commerciële leveranciers en via een omvangrijke cybercriminele dienstensector. Staten en criminelen kopen geavanceerde aanvalshulpmiddelen, zodat zij niet zelf hoeven te investeren in de ontwikkeling ervan. Staten kunnen de voorbereiding en uitvoering van digitale aanvallen ‘uitbesteden’ aan een derde partij. Het verkrijgen of vergroten van digitale aanvalscapaciteiten is door de laagdrempelige toegankelijkheid voor steeds meer actoren weggelegd. Dit vergroot de dreiging.

Digitale weerbaarheid niet overal op orde

Organisaties worden succesvol aangevallen met eenvoudige methoden. Incidenten hadden voorkomen kunnen worden of de schade had beperkt kunnen worden met behulp van basismaatregelen. De weerbaarheid staat verder onder druk door een toenemende complexiteit en connectiviteit in het ict-landschap.

Onveilige producten en diensten achilleshiel digitale veiligheid

Digitaal onveilige producten en diensten zijn een fundamentele oorzaak van incidenten. Onveilige producten en diensten werken voor aanvallers drempelverlagend, omdat deze het makkelijker maken succesvolle aanvallen uit te voeren. De onveiligheid kan ontstaan doordat leveranciers standaard onveilige configuraties leveren of geen updates (meer) beschikbaar stellen, doordat deze updates niet eenvoudig te installeren zijn of doordat updatemechanismen gecompromitteerd worden. Ook als updates wel beschikbaar zijn, worden zij niet altijd ingezet bij organisaties. Onduidelijk is of er voldoende (economische) prikkels zijn om veilige producten te produceren of diensten te realiseren. Hierdoor ontstaat een belangentegenstelling tussen enerzijds het bedrijfseconomische belang van organisaties en het belang van adequate cybersecurity voor de maatschappij anderzijds.

Negatieve effecten complexiteit en connectiviteit

Het wordt steeds uitdagender om een weerbare digitale infrastructuur te realiseren. Bepaalde software wordt generiek door ontwikkelaars en leveranciers gebruikt als bouwsteen voor hun werk. Sommige populaire protocollen voor gegevensuitwisseling via het internet zijn decennia oud en niet bestand tegen hedendaagse aanvallen. De complexiteit en connectiviteit van digitale infrastructuur zullen de komende jaren door de verdergaande digitalisering toenemen. Enerzijds zorgen de organische groei en de relatief lange levensduur van systemen voor een steeds ingewikkelder landschap. Anderzijds maakt het toegenomen gebruik van gedeelde voorzieningen, zoals deelproducten of complete clouddiensten, dat het overzicht lastiger te verkrijgen en bewaken is. Waar in het verleden diensten binnen een organisatie ingericht werden, worden ze nu bij verschillende partijen ingekocht en extern uitgevoerd. Deze partijen maken ook gebruik van onderaannemers. Controleerbaarheid van de leverancierssketen is zeer complex. Regie op het ict-landschap blijft binnen de organisatie, terwijl de uitvoering ervan versnipperd raakt over meerdere partijen. Dit zorgt voor onoverzichtelijkheid, nieuwe afhankelijkheden en een vergroting van het aanvalsoppervlak.

Staten vormen grootste digitale dreiging

2 Dreiging

Er is sprake van een permanente digitale dreiging. De grootste digitale dreiging voor de nationale veiligheid gaat uit van statelijke actoren. Deze blijft groeien. Landen zetten digitale middelen in voor spionage of zelfs (voorbereidingen voor) sabotage om eigen doelen te bereiken ten koste van Nederlandse belangen. De dreiging vanuit criminelen blijft onverminderd groot. De dreiging vanuit overige actoren is ook vrijwel onveranderd gebleven.

Verstoring en sabotage hebben de meeste impact op de nationale veiligheid. Voorbereidingshandelingen hiervoor vormen een potentiële dreiging voor de onafhankelijkheid en zelfstandigheid van Nederland. Alleen al door, expliciet of impliciet, te dreigen met verstoring of sabotage kan een actor pogen besluitvormingsprocessen te beïnvloeden. Cyberspionage blijft aantrekkelijk om geopolitieke invloed en economische groei te bereiken. Door de laagdrempelige beschikbaarheid van aanvalsmiddelen en de effectiviteit van eenvoudige aanvalsmethoden gaat er een dreiging uit van een brede groep actoren. Slechts een beperkt aantal landen beschikt over voldoende capaciteiten om te kunnen attribueren op basis van inlichtingenonderzoek in brede zin, bovenop attributie op basis van technische kenmerken. Het risico bestaat dat bedrijven, media of zelfs landen aanvallen niet kunnen toewijzen, of foutief toewijzen aan partijen. Daarnaast vergroot de toenemende digitalisering de dreiging van onopzettelijke storing en uitval van (informatie)systemen in Nederland.

Groei statelijke dreiging

De grootste digitale dreiging voor de nationale veiligheid gaat uit van statelijke actoren. Landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland. Dit betekent dat deze landen digitale middelen inzetten voor spionage of zelfs (voorbereidingen voor) sabotage om zo hun eigen politieke, militaire, economische en/of ideologische doelen te bereiken ten koste van Nederlandse belangen.[3] De activiteiten om verstoringen en sabotage mogelijk te maken verschuiven verder richting westerse landen. Hierdoor groeit de dreiging tegen de nationale veiligheid en Nederlandse belangen.[4]

Er zijn in deze rapportageperiode geen substantiële aanvallen door hacktivisten tegen Nederland of Nederlandse belangen waargenomen.[5,6,7] Scriptkiddies en cybervandalen hebben vooral verstorende aanvallen uitgevoerd op organisaties. Dit waren veelal DDoS-aanvallen.[8,9,10,11] Net als vorig jaar lijken criminele actoren verder in te zetten op het creëren van botnets[12,13] en het verspreiden van cryptominers.[14,15,16] De dreiging vanuit criminelen blijft onverminderd groot, onder meer door de schaalbaarheid van cybercrime.[17,18] Cyberaanvallen door criminelen veroorzaken maatschappelijke schade.[19] De dreiging van insiders is het afgelopen jaar afgenomen.[20] Digitale aanvallen vanuit terroristen zijn ook dit jaar niet waargenomen. Deze dreiging is reeds enkele jaren laag.[21] Terroristische groeperingen zijn meer gericht op het plegen van fysieke aanslagen.

Verstoring en sabotage meeste impact

Verstoring en sabotage door statelijke actoren hebben de meeste impact op de nationale veiligheid. Deze activiteiten kunnen een (langdurig) ontwrichtend effect hebben op de maatschappij, zeker wanneer vitale processen en partijen geraakt worden.[22] Verschillende statelijke actoren beschikken over capaciteiten om dit soort aanvallen uit te voeren. Spanningen tussen landen kunnen aanleiding zijn om dergelijke capaciteiten in te zetten.[23] In de richting van Nederland ontbreekt op dit moment de intentie om daadwerkelijk sabotageacties uit te voeren op de vitale infrastructuur. Staten hebben gepoogd toegang te verschaffen tot ict-systemen van vitale processen. De geopolitieke onrust in de wereld maakt een sabotageactie voorstelbaarder. Zo heeft onder andere Rusland een offensief cyberprogramma voor verstoring en zelfs sabotage van de vitale infrastructuur. Ook een verstoring in bijvoorbeeld de energievoorziening in landen om ons heen kan gevolgen hebben voor Nederland. [24]

Voorbeelden van verstoringen en sabotage

Het afgelopen jaar zijn deze activiteiten ook waargenomen in Europa. Systemen van Poolse energie- en transportbedrijven zijn geïnfecteerd met mogelijk zeer destructieve malware (GreyEnergy).[25] In het verleden zorgde andere destructieve malware, zoals Industroyer,[26] al voor verstoring van de energielevering in Oekraïne.[27] De groep die GreyEnergy vermoedelijk heeft ontwikkeld, is door het Verenigd Koninkrijk toegeschreven aan Rusland.[28] In december 2018 werd, vermoedelijk door een andere actor, een olieverwerkingsfabriek van het bedrijf Saipem in Italië aangevallen.[29] Door de aanval waren ongeveer 4.000 machines en computers een tijd niet beschikbaar.

Gezien de veranderende geopolitieke verhoudingen zal de dreiging van verstoring en sabotage verder toenemen naarmate Nederland onderdeel wordt van of betrokken raakt bij geopolitieke conflicten.

Voorbereidingshandelingen dreiging voor onafhankelijkheid en zelfstandigheid

Ook de *voorbereidingshandelingen* voor verstoring en sabotage van vitale processen en partijen door statelijke actoren vormen een dreiging voor de nationale veiligheid.[30] Niet alleen als preparatie om in te zetten tijdens (escalatie van) geopolitieke conflicten maar juist ook om druk te kunnen uitoefenen op landen. Actoren kunnen voorbereidingshandelingen lang voor een conflict uitvoeren. Door impliciet of expliciet te dreigen met verstoring of sabotage kan een actor economische, diplomatieke of militaire invloed uitoefenen op het slachtoffer. De dreiging van verstoring en sabotage, bijvoorbeeld door het 'zichtbaar' uitvoeren van voorbereidingshandelingen, zijn daarmee een middel om besluitvormingsprocessen te (proberen te) beïnvloeden. Dit vormt een potentiële dreiging voor de onafhankelijkheid en zelfstandigheid van Nederland.

Digitale spionage voor invloed en groei

Naast de dreiging van digitale verstoring of sabotage vormt spionage door statelijke actoren een omvangrijke dreiging voor de Nederlandse belangen. Staten spioneren om informatie te verwerven om geopolitieke, militaire en economische belangen van deze staten te dienen. Digitale spionage wordt door statelijke actoren veelvuldig ingezet.[31] Steeds meer landen richten zich op spionage. China, Iran en Rusland vormen de voorhoede.[32]

Verreweg de grootste dreiging op het gebied van economische spionage is afkomstig van China. Deze spionage wordt gevoed door Chinese economische beleidsplannen, zoals 'Made in China 2025' en de 'Nieuwe Zijderoutes', waarmee het land zijn economische en geopolitieke invloed kan vergroten. China zet een breed scala aan (heimelijke) middelen in die het verdienvermogen van Nederlandse bedrijven ondermijnen en die op termijn kunnen resulteren in economische en politieke afhankelijkheden. Een van deze middelen is (digitale) economische spionage.[33]

Voor Rusland is ons land een interessant doelwit voor spionage. Vanwege MH17 is het strategisch belang van Nederland sterk toegenomen. Nederland heeft daarnaast al lange tijd de interesse van Rusland vanwege het lidmaatschap en de vestigingsplaats van internationale instituties.[34]

Dreiging bepaald door intentie, capaciteit en activiteit

Een combinatie van de mate van intentie, capaciteit en activiteit bepalen de dreiging van een actor richting (informatie)systemen. Bij intentie gaat het om de vraag of een actor een bepaald doel (bijvoorbeeld geopolitiek, financieel) heeft en bereid is om de vertrouwelijkheid, integriteit, en beschikbaarheid van een systeem aan te tasten. Capaciteit bestaat uit opgedane kennis en toegang tot middelen om een digitale aanval mogelijk te maken. Er bestaat een verschil in intentie en capaciteit, wat tot verschillende interpretatie van de dreiging kan leiden. De waarneming of voorstelbaarheid van concrete digitale aanvallen in Nederland en in mindere mate Europa of westerse bondgenoten, is leidend voor de bepaling van activiteit. Er kan een dreiging uitgaan van een actor wanneer er sprake is van intentie en capaciteit, terwijl er weinig activiteit is waargenomen.

Staten bespioneren ook burgers. Hierbij wordt onderscheid gemaakt tussen een algemene interesse van staten in persoonsgegevens en het gericht bespioneren van personen of (dissidente) groeperingen. Bijvoorbeeld met als doel deze personen of groeperingen te beïnvloeden of zelfs te intimideren.

Tabel 1 **Dreigingsmatrix**

	Overheid	Vitaal	Privaat	Burgers
Staten/ staatsgelieerd	Spionage Informatiemanipulatie	Sabotage Verstoring Spionage	Spionage Systeemmanipulatie	Spionage
Criminelen	Verstoring Systeemmanipulatie Informatiediefstal	Verstoring Systeemmanipulatie	Verstoring Informatiemanipulatie Informatiediefstal Systeemmanipulatie	Verstoring Informatiemanipulatie Informatiediefstal Systeemmanipulatie
Terroristen	Sabotage	Sabotage		
Hacktivisten	Verstoring	Verstoring	Verstoring Informatiemanipulatie	
Cybervandalen en scriptkiddies	Verstoring	Verstoring	Verstoring	
Insiders	Informatiediefstal		Informatiediefstal	
Niet opzettelijk handelen	Storing/uitval Lek	Storing/uitval Lek	Storing/uitval Lek	Lek

De dreigingsmatrix[35] geeft inzicht in de dreigingen die uitgaan van verschillende actoren tegen verschillende doelwitten. De tabel is niet uitputtend en bevat niet alle dreigingen die voorstelbaar zijn, maar beperkt zich tot de dreigingen waarvan ingeschat wordt dat actoren voldoende intentie en capaciteit hebben of tot actoren van wie eerder activiteiten zijn waargenomen.

Legenda:

Geel: Er is intentie maar geen middelen/ kennis (capaciteit)
OF er is activiteit waargenomen maar middelen/ kennis zijn beperkt
OF er is activiteit waargenomen maar alleen intentie specifieke doelwitten te raken

Oranje: Middelen/ kennis zijn aanwezig en intentie is sterk aanwezig
OF intentie is sterk aanwezig en activiteiten zijn waargenomen

Rood: Er zijn veel middelen/ kennis en intentie is zeer sterk aanwezig
OF intentie is zeer sterk aanwezig, er is veel activiteit waargenomen en er zijn (veel) middelen/ kennis

De volgende dreigingen worden onderscheiden:

- Verstoring: het opzettelijk tijdelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
- Sabotage: het opzettelijk en zeer langdurig aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten, mogelijk leidend tot vernietiging.
- Informatiemanipulatie: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.
- Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
- Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
- Systeemmanipulatie: aantasting van informatiesystemen of -diensten; gericht op de vertrouwelijkheid of integriteit van informatiesystemen of -diensten. Deze systemen of diensten worden daarna ingezet om andere aanvallen uit te voeren.
- Storing/uitval: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
- Lek: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.

Persoonsgegevens kunnen gebruikt worden om andere spionage- of beïnvloedingsactiviteiten voor te bereiden. De verschillende vormen van spionage kunnen de democratische rechtsorde en rechtsstaat ondermijnen, de economie op lange of korte termijn schaden[36] en burgers in hun vrijheden beperken.

Digitale spionage in de praktijk: ministerie van Buitenlandse Zaken

Het kan voor andere landen interessant zijn om inzicht te krijgen in het verkeer tussen een diplomatieke post in het buitenland en het ministerie van Buitenlandse Zaken. Inlichtingendiensten hebben waargenomen dat een aantal Nederlandse ambassades in het Midden-Oosten en Centraal-Azië in 2017 en 2018 doelwit is geweest van digitale aanvallen, uitgevoerd door een buitenlandse inlichtingendienst. De digitale aanvallen op deze ambassades bevestigen de structurele aandacht van buitenlandse inlichtingendiensten voor het ministerie van Buitenlandse Zaken.[34]

Dreiging door toegankelijkheid aanvalsmiddelen

Door de laagdrempelige beschikbaarheid van aanvalsmiddelen en de effectiviteit van eenvoudige en universele aanvalsmethoden gaat er een substantiële dreiging uit van een brede groep actoren. Derde partijen worden vaker misbruikt.

Geavanceerde aanvalscapaciteiten laagdrempelig toegankelijk

Voor actoren zijn aanvalsmiddelen laagdrempelig te verwerven. Die zijn vrij beschikbaar op internet of er wordt gebruik gemaakt van de diensten van aanvalsfacilitatoren. Deze dienstverleners stellen tegen betaling middelen voor digitale aanvallen, zoals infrastructuur, hulpmiddelen en technieken, beschikbaar. Nederlandse ict-infrastructuur wordt hiertoe veelvuldig aangeboden.[37,38] De faciliteiten kunnen simpel zijn, zoals DDoS-aanvallen of *bulletproof* hosting, maar ze kunnen ook een geavanceerd karakter hebben. Staten kopen deze geavanceerde aanvalshulpmiddelen, zodat zij niet zelf hoeven te investeren in de ontwikkeling ervan. Staten kunnen de voorbereiding en uitvoering van digitale aanvallen 'uitbesteden' aan een derde partij. Het verkrijgen of vergroten van digitale aanvalscapaciteiten is door de laagdrempelige toegankelijkheid voor meer actoren weggelegd. Dit leidt tot een groei van de dreiging.

Universele eenvoudige aanvalsmethoden succesvol

Veel actoren, waaronder statelijke actoren, gebruiken dezelfde aanvalsmethoden. Aanvallen met simpele methoden zijn vaak succesvol. Hierdoor is de groep actoren die een aanval kan uitvoeren groot. Een van de methoden die in toenemende mate gebruikt wordt door een brede groep actoren is *living-off-the-land*.[40] Dit is een methode die misbruik maakt van producten of diensten die al aanwezig zijn op de (informatie)systemen van het slachtoffer. Nadat toegang is verkregen tot een (informatie)systeem of netwerk zetten statelijke actoren ook geavanceerdere middelen in. Tegen eenvoudige aanvalstechnieken kunnen drempels opgeworpen worden, die potentiële doelwitten minder kwetsbaar en ook minder interessant maken. Maatregelen die tot de 'basishygiëne' van ict-systemen en -netwerken behoren, verhogen de weerbaarheid tegen digitale aanvallen aanzienlijk. Dit geldt ook voor aanvallen van statelijke actoren.

Compromittering van derde partijen blijft aantrekkelijk en neemt toe

In eerdere cybersecuritybeelden is geconstateerd dat leveranciersketens de kwetsbaarheid verhogen.[41] Ook in deze rapportageperiode waren aanvallen via derde partijen zeer succesvol.[42,43] Dergelijke aanvallen zijn steeds aantrekkelijker worden en zullen naar verwachting verder toenemen.

Volgens de Verenigde Staten en Australië was een Chinese hackersgroep (APT10) zeer succesvol in het compromitteren van dienstenleveranciers.[44,45] Via deze leveranciers werd bij een breed scala aan bedrijven in verschillende landen economische spionage bedreven. Daarnaast wordt de ict-infrastructuur van derde partijen misbruikt om aanvallen op andere partijen uit te voeren. Onder andere de Nederlandse ict-infrastructuur is deze rapportageperiode misbruikt om aanvallen op andere landen uit te voeren,[46] onder andere door Iran, Noord-Korea en Rusland.[47]

Cyberaanvallen ondersteund met fysieke operaties

In aanvulling op eenvoudige digitale aanvalsmiddelen, kunnen ook fysieke operaties worden ontplooid, vaak door statelijke actoren. In april 2018 accepteerde de Russische militaire inlichtingendienst het risico op ontdekking toen zij medewerkers naar Nederland stuurde om dicht bij de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag een digitale aanval uit te voeren.[48] Deze dienst heeft in het verleden meer van dergelijke operaties uitgevoerd, maar dit was de eerste keer dat een operatie in Nederland onderkend is.[49]

Effect publieke attributie nog niet meetbaar

Verschillende overheden hebben dit jaar publiekelijk digitale aanvallen geattribueerd aan staten. Het doel is om een afschrikwekkend effect te creëren door de kosten van normoverschrijdend gedrag te verhogen.[50] Behalve publieke attributie zijn er ook andere instrumenten om dat te doen, zoals het opleggen van sancties, zoals inreisverboden en bevriezing van tegoeden tegen personen en entiteiten aan wie cyberaanvallen worden toegeschreven. Het effect van attributie op het gedrag van actoren blijkt, op dit moment, nog niet meetbaar. Het aanwijzen van de actor achter een digitale aanval, attributie, is complex,

omdat het een zeer specifieke set aan capaciteiten vergt. Zowel op technisch gebied als juist ook op het bredere inlichtingen- en politieke gebied. Veel landen hebben capaciteiten om digitale aanvallen uit te voeren, slechts een beperkt aantal landen beschikt over voldoende capaciteiten om te kunnen attribueren op basis van inlichtingenonderzoek in brede zin, bovenop attributie op basis van technische kenmerken.[51] Het risico bestaat dat bedrijven, media of zelfs landen aanvallen niet kunnen toewijzen, of foutief toewijzen aan partijen.

Technische attributie complex door diffuus karakter aanvalsmethoden

Technische attributie is complex. De complexiteit van technische attributie wordt beïnvloed door de laagdrempelige beschikbaarheid van aanvalsmiddelen, de eenvoud en verscheidenheid van de aanvalsmethoden, misbruik van derde partijen en het vervagen van grenzen tussen actoren.[52] Het gebruik van ingekochte aanvalsmiddelen door criminelen bemoeilijkt de opsporing door de politie. Daarbij maken simpele aanvalsmethoden en gekochte of vrij beschikbare aanvalsmiddelen attributie aan (statelijke) actoren vele malen complexer. Hoewel commerciële bedrijven in sommige gevallen methoden en technieken toeschrijven aan een specifieke statelijke actor, betekent dit niet dat die actor altijd achter het gebruik zit. Omgekeerd kunnen methoden en technieken die aan criminelen worden toegeschreven ook door statelijke actoren gebruikt worden. Het is daarmee ingewikkeld om een duidelijk beeld van een actor en de dreiging te schetsen. Dit maakt de dreiging complexer.

Dreiging van cybercriminelen en andere actoren

Activiteiten uitgevoerd door beroepscriminelen, maar ook door scriptkiddies of cybervandalen komen met enige regelmaat in het nieuws.[53,54,55] Door de laagdrempelige beschikbaarheid van aanvalsmiddelen en het lage kennisniveau dat nodig is om een aanval uit te voeren zal dit naar verwachting de komende jaren een probleem blijven. Aanvallen op bijvoorbeeld banken of overheidsloketten verminderen in potentie het vertrouwen in het gebruik van digitale diensten. De dreiging vanuit criminelen blijft onverminderd groot, zij veroorzaken maatschappelijke schade.[56,57,58] In de afgelopen rapportageperiode hebben DDoS-aanvallen ervoor gezorgd dat een aantal banken tijdelijk slecht bereikbaar was.[59] Maar ook diensten van de Rijksoverheid zijn regelmatig getroffen. Zo waren de Belastingdienst, de Douane en DigiD enkele keren slecht bereikbaar door digitale aanvallen.[60,61,62] Hoewel dit geen direct effect op de nationale veiligheid heeft, zorgt het op de langere termijn in potentie voor negatieve effecten op het vertrouwen in de digitale samenleving.

Groei dreiging van storing en uitval

Storing en uitval van (informatie)systemen blijven een grote dreiging vormen. Aan deze dreiging ligt geen opzet of intentie ten grondslag. De onderlinge verbondenheid van (informatie)systemen en de toenemende mate van complexiteit maakt het waarschijnlijk dat er in Nederland vaker storing en uitval zal voorkomen. De uitval van één systeem of netwerk kan voor storing of uitval op andere plekken zorgen.[63] Dit is nog meer het geval wanneer basis cybersecuritymaatregelen onvoldoende getroffen worden, en achterliggende systemen die uitval kunnen opvangen ontbreken. Storing en uitval vormen een belangrijke dreiging door de grote potentiële impact. Dit geldt zeker wanneer het plaatsvindt op een centraal informatieknooppunt, of bij vitale processen. Zo ontstond bij de luchthaven Schiphol een storing op het spoor waardoor er veel treinen uitvielen.[64] De storing werd veroorzaakt door een samenspel van verschillende gebeurtenissen en fouten.

Digitalisering zorgt voor verschuiving doelwitten

Door de verdergaande digitalisering verandert de afhankelijkheid van onderliggende systemen en infrastructuren. Sommige systemen worden uitgefaseerd en andere systemen winnen aan belang of worden zelfs essentieel. Deze systemen en infrastructuren vormen daarmee een, mogelijk nieuw, aantrekkelijk doelwit voor cyberactoren. Enerzijds als primair doelwit, bijvoorbeeld ten behoeve van spionage of verstoring, anderzijds om andere aanvallen uit te voeren (systeemmanipulatie).

Twee voorbeelden zijn het Internet-of-Things (IoT) en persoonsgegevens. Door de digitalisering zijn cloudtoepassingen in al hun verschijningsvormen aantrekkelijker als doelwit. Cloudtoepassingen vormen een steeds essentiëler bouwsteen van gedigitaliseerde processen. Ook de verdere opkomst van het IoT, ook in vitale processen, maakt aanvallen op IoT aantrekkelijker.[65]

Persoonsgegevens zijn, ook voor kwaadwillenden, eenvoudig te verwerven. Niet alleen op sociale media maar ook bijvoorbeeld via de omvangrijke sets van persoonsgegevens uit datalekken. In de afgelopen periode is gebleken dat persoonsgegevens misbruikt worden door statelijke actoren en cybercriminelen om doelwitten op steeds overtuigendere wijze aan te spreken.[66,67]

Analoge alternatieven en terugvalopties essentieel en vrijwel afwezig

3 Belang

Gedigitaliseerde processen en systemen vormen het fundament van onze samenleving. De digitale veiligheid, specifiek de vertrouwelijkheid, integriteit en beschikbaarheid van dit fundament, is essentieel om maatschappelijke en economische groei mogelijk te maken en maatschappelijke ontwrichting te voorkomen. Analoge alternatieven zijn vrijwel verdwenen en terugvalopties zijn afwezig. Ketens van vitale aanbieders zijn afhankelijk van leveranciers die niet als vitaal geïdentificeerd zijn. Nederland is in brede zin afhankelijk van een relatief kleine groep aanbieders van hard- en software, digitale diensten en platforms uit een beperkt aantal landen. Dit maakt de maatschappij kwetsbaar voor de veranderende intenties van deze aanbieders en landen. Deze afhankelijkheid brengt risico's voor de nationale veiligheid mee zich mee.

Digitalisering is fundament samenleving

De Nederlandse samenleving en de vitale processen zijn vrijwel volledig afhankelijk van gedigitaliseerde processen en de onderliggende (informatie)systemen. Deze processen en systemen vormen het digitale fundament van onze samenleving. Digitalisering transformeert onze economie en maatschappij. Het is de belangrijkste bron van groei, innovatie en nieuwe bedrijvigheid en noodzakelijk voor het oplossen van maatschappelijke uitdagingen. Het kabinet wil maatschappelijke en economische kansen van digitalisering volop benutten, onder andere door in bepaalde sectoren de digitale transitie te versnellen en te ondersteunen.[68] Zo wordt er 165 miljoen euro uitgetrokken om het contact van de overheid met burgers en ondernemers slimmer, toegankelijker en persoonlijker te maken.[69] Verder trekt het kabinet 60 miljoen euro uit voor digitale zorg om het gebruik van e-health en de uitwisseling van gegevens een extra stimulans te geven.[70] Ook organisaties en burgers gaan vanzelfsprekend verder met digitalisering.

Veiligheid digitaal fundament essentieel

Aantasting van het digitale fundament onder de samenleving kan de nationale veiligheid raken, zeker in de vitale processen. Wat de gevolgen van cyberincidenten kunnen zijn, is niet eenduidig te beoordelen. Zeker is dat die gevolgen groot kunnen zijn.

Volledige afhankelijkheid van digitalisering

Door de vrijwel volledige afhankelijkheid van digitalisering is de digitale veiligheid van processen en onderliggende (informatie)systemen essentieel geworden. Het belang van digitale veiligheid is daarmee sterk toegenomen. Aantasting van de vertrouwelijkheid, integriteit of beschikbaarheid van (informatie)systemen heeft immers grotere gevolgen naarmate meer processen, data, diensten en connecties digitaal zijn. Bovendien nemen de complexiteit en connectiviteit nog verder toe. Daardoor kan een incident in één netwerk leiden tot een keten van incidenten in andere netwerken.[71]

Ook de digitalisering van vitale processen neemt verder toe en daarmee het belang van de digitale veiligheid daarvan. Vitale processen zorgen voor gas, water en elektra, maar ook voor droge voeten, het functioneren van vervoer via water en lucht, betalingsverkeer et cetera. Veelal blijven cyberincidenten niet beperkt tot één sector, maar verspreiden ze zich door keteneffecten naar andere sectoren. Vitale processen zijn vrijwel volledig afhankelijk van ict en elektriciteit. Uitval daarvan heeft daardoor potentieel grote maatschappelijke effecten.

De onderlinge afhankelijkheden binnen de vitale infrastructuur zorgen ervoor dat een verstoring binnen één vitaal proces kan leiden tot keteneffecten (cascade-effecten) in andere vitale processen. De resultaten van een self-assessment laten zien dat veel vitale processen in hoge mate afhankelijk zijn van de

elektriciteitsvoorziening en datacommunicatie. De tijdsduur voordat de uitval van deze vitale processen impact kan hebben op een aantal andere vitale processen is vaak kort (enkele uren). Elektriciteit en datacommunicatie zijn onderling afhankelijk.[72]

Zeker een gecoördineerde cyberaanval waardoor meerdere netwerken tegelijk uitvallen – zoals voor de stroomvoorziening, gas, drinkwater en telecom – heeft grote gevolgen.[73] Aantasting van vitale processen in Nederland kan ook gevolgen hebben voor vitale processen in het buitenland en vice versa.[74]

Maatschappelijke ontwrichting door cyberincidenten

De krant NRC schetste de potentiële gevolgen van cyberincidenten wanneer die langer en gelijktijdig optreden. In het scenario treft gijzelsoftware op grote schaal Nederland. Schermen gaan op zwart, bestanden worden gegijzeld en computersystemen worden preventief uitgezet. Tegelijkertijd is sprake van golven van DDoS-aanvallen, resulterend in een kat- en muisspel tussen aanvallers en verdedigers. Tal van onvoorspelbare kettingreacties zijn het gevolg: telefoonnetwerken raken overbelast, het treinverkeer rond Amsterdam ligt stil, er ontstaan files rond Schiphol, ziekenhuizen kunnen geen patiënten meer opnemen, sociale media en sites van publieke omroepen zijn niet bereikbaar, elektronisch betalingsverkeer ligt grotendeels stil, het contant geld raakt op en mensen kunnen geen boodschappen meer doen. Na drie dagen is de aanval gepareerd. Het herstel duurt weken of zelfs maanden.[75]

Analoge alternatieven en terugvalopties essentieel en vrijwel afwezig

Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade. Hier hoeft geen opzet in het spel te zijn, ook storingen en onbedoeld veroorzaakte schade kunnen maatschappij-ontwrichtende effecten hebben. Dit probleem zal verder groeien. Daarbij doet zich de paradox voor dat juist een robuuste infrastructuur ertoe kan leiden dat onvoldoende rekening wordt gehouden met incidenten. Zo is de telecom in Nederland zo robuust dat organisaties zich onvoldoende bewust waren van de afhankelijkheid daarvan en onvoldoende rekening hielden met verstoringen.[76] Er bestaat geen plan B voor als netwerken niet functioneren.[77]

Analoge alternatieven afwezig

Volgens experts was het een geluk voor de mensen in Oost-Oekraïne dat er handmatige back-ups waren toen cyberactoren de stroomvoorziening stil legden in de winter. *"Iemand kan daar nog een knop omzetten om de hele boel weer op te starten. Binnen zes uur was de stroomvoorziening hersteld. De software duurde veel langer, maar er was weer elektriciteit. "In Nederland hebben we zo'n handmatige optie vaak niet meer. Onze back-up is in veel gevallen digitaal."*[78]

Afhankelijkheid van niet als vitaal geïdentificeerde (onder)leveranciers

De complexiteit en connectiviteit van informatiesystemen en netwerken neemt al jaren toe. Organisaties zijn vaak niet meer in staat om alle taken zelf uit te voeren. Ze opereren in ketens. En zijn afhankelijk van andere organisaties voor onder andere het leveren van de gegevens of voor het uitvoeren of ondersteunen van hun gegevensverwerking. Dat is niet zonder risico. Wanneer de gegevensuitwisseling met andere organisaties niet veilig en betrouwbaar verloopt, kan het bedrijfsproces verstoord raken. Wanneer dit gebeurt in de ketens van vitale aanbieders kan dit leiden tot verregaande uitval, aantasting van de fysieke veiligheid en maatschappelijke ontwrichting.[79] De ketens van vitale aanbieders kunnen ook afhankelijk zijn van niet als vitaal geïdentificeerde leveranciers of onderaannemers. Verstoringen van of cyberaanvallen op ict buiten vitale processen kunnen die daardoor toch aantasten. Ook ontstaan in toenemende mate onverwachte afhankelijkheden voor vitale processen. Zo zou (bedoeld of onbedoeld) de elektriciteitsvoorziening in New York plat kunnen komen te liggen wanneer een cyberactor de instelling van vele airconditioning-systemen gelijktijdig op grote schaal met drie graden zou wijzigen.[80]

Beperkt aantal aanbieders en landen dominant

De afhankelijkheid van een relatief kleine groep aanbieders van hard- en software en digitale diensten en platforms uit een beperkt aantal landen neemt toe.[81] Zo bezitten Facebook (met WhatsApp en Instagram), Amazon, Apple, Google en Microsoft 95% van de toepasselijke marktaandelen. Zij zijn praktisch onmisbaar in het dagelijkse leven van de gemiddelde Europeaan. Deze bedrijven hebben een gezamenlijke waarde die gelijk staat aan het bruto nationaal product van Frankrijk. Dit roept de vraag op hoe die steeds sterkere invloed en macht zich verhoudt tot de soevereiniteit en de autonomie van de Nederlandse staat en de Europese Unie.[82] Steeds meer digitale diensten zoals online boekhouden en authenticatiediensten in Nederland worden bovendien gebouwd op een onderliggend cloudplatform van één van de grote spelers (bijvoorbeeld Microsoft Azure, Amazon

webservices of Google Cloud). Dit creëert een nog grotere afhankelijkheid van deze leveranciers.

Schaalvoordelen en invloed grote aanbieders

Grote aanbieders realiseren in voorkomende gevallen schaalvoordelen voor organisaties en hun gebruikers. Ze hebben de mogelijkheid om continu te innoveren, hebben grotere financiële reserves en kunnen door schaalvoordelen concurrerend in de markt opereren. Grote aanbieders hebben meer middelen om zich te wapenen tegen aanvallers. Er zijn ook nadelen aan grote aanbieders verbonden. Eenmaal gekozen voor bijvoorbeeld een cloudleverancier, is het niet eenvoudig om voor een ander te kiezen. Daarnaast kan sprake zijn van hoge kosten bij overstap naar een andere aanbieder. Ook bepaalt een beperkt aantal aanbieders de facto de standaarden waardoor zij mogelijk hun positie kunnen versterken ten koste van andere partijen. De maatschappelijke impact van een storing of een digitale aanval kan groot zijn omdat veel verschillende processen of diensten afhankelijk zijn van een beperkt aantal aanbieders.

Afhankelijkheid beperkt aantal aanbieders en landen

Met de afhankelijkheid van de relatief kleine groep aanbieders, ontstaat ook afhankelijkheid van een beperkt aantal landen. Zo wordt het overgrote aandeel van de hard- en software ontworpen danwel geproduceerd in China en de Verenigde Staten.[83] Derde landen hebben soms andere wetgeving of hanteren andere spelregels op bijvoorbeeld het terrein van privacy of het verkrijgen van toegang tot data. Volgens het Analistennetwerk Nationale Veiligheid is het een onderbelicht probleem dat onze samenleving op zeer grote schaal gebruik maakt van buitenlandse apparatuur en technologie, waar mogelijk *'backdoors'* in aanwezig zijn.[84]

Producten of diensten van (buitenlandse) aanbieders kunnen, met of zonder medeweten van deze aanbieder, gecompromitteerd worden door actoren. Vanwege de afhankelijkheid van leverancierskетens zijn producenten en dienstverleners een aantrekkelijk doelwit voor actoren. Daarnaast zijn deze leveranciers onderworpen aan de wet- en regelgeving van het land waarin zij gevestigd zijn en zouden zij door overheden in het buitenland gedwongen kunnen worden tot een vorm van medewerking aan bijvoorbeeld spionage of de voorbereiding daarvan.

Vanwege de technologische mogelijkheden of de prijsprestatieverhouding kan het voor zowel bedrijven, burgers als een land aantrekkelijk zijn om gebruik te (laten) maken van grote aanbieders. Op de langere termijn kunnen daar echter veiligheidsrisico's aan kleven vanwege een steeds sterkere afhankelijkheid van die bedrijven of de landen waar de bedrijven vandaan komen.[85] Zo wordt gewezen op de risico's van het gebruik van producten van Huawei bij de ontwikkeling van 5G-netwerken.[86] De VS waarschuwt westerse bondgenoten dat een samenwerking met Huawei bij de aanleg van het 5G-netwerk kan leiden tot beperking van de uitwisseling van informatie door haar veiligheidsdiensten.[87]

Nederland is afhankelijk van een relatief kleine groep aanbieders van hard- en software, digitale diensten en platforms uit een beperkt aantal landen. Deze afhankelijkheid brengt risico's voor de nationale veiligheid mee zich mee.

Sterk geconcentreerde dataverwerking en -opslag in buitenland

De afhankelijkheid van een relatief kleine groep aanbieders geldt ook voor data. De digitalisering van de afgelopen jaren resulteert in ongeëvenaarde hoeveelheden data van uiteenlopende soort. Het kabinet beschouwt data als een cruciale grondstof voor de nieuwe economie.[88] Anderen zien data als de 'nieuwe olie', de 'vierde productiefactor' of als een nieuwe 'technologie' die in de eerste plaats vooral productiviteitsverhogend werkt.[89] Veel data van Nederlandse organisaties en burgers worden opgeslagen en verwerkt op buitenlandse platforms. Op het gebied van dataverwerking zijn landen, organisaties en gebruikers afhankelijk van de intenties van statelijke en commerciële actoren. Hiermee zijn zij tevens kwetsbaar voor een verandering in deze intenties.[90] Een datalek heeft, door de concentratie van gegevens, in potentie een zeer grote omvang.

Aanbieders onder het vergrootglas

Volgens de Duitse mededingingsautoriteit maakt Facebook misbruik van haar positie om gegevens van mensen te verzamelen, zonder dat die hiervoor toestemming hebben gegeven of weten wat er precies met hun gegevens gebeurt.[91] Volgens zeven Europese Consumentenorganisaties volgt Google gebruikers door middel van 'Locatiegeschiedenis' en 'Web- en app-activiteit', instellingen die in alle Google-accounts zijn geïntegreerd. Voor gebruikers van mobiele telefoons met Android is dit bijzonder moeilijk te vermijden.[92] In de VS krijgt Facebook mogelijk een boete van miljarden dollars opgelegd wegens privacy schendingen.[93] Ook wordt steeds duidelijker wat de mogelijkheden en ongewenste neveneffecten van gericht adverteren zijn. Zo maakt Facebook het mogelijk om advertenties speciaal te richten op vaccinatieweigeraars en mensen die geïnteresseerd zijn in anti-vaccinatie-propaganda, of die pagina's daarover leuk vinden.[94] Ook gerichte advertenties op basis van politieke voorkeuren behoren tot de mogelijkheden. In het Verenigd Koninkrijk wil men wetgeving rondom verkiezingen herijken: die is er wel voor fysieke folders en billboards, maar niet voor digitale campagnes.[95]

Geavanceerde aanvalscapaciteiten laagdrempelig toegankelijk

4 Jaarbeeld

Geavanceerde aanvalsmiddelen zijn laagdrempelig toegankelijk. Eenvoudige aanvalsmiddelen blijven effectief. Actoren gebruiken vrij verkrijgbare tools en generieke diensten en behalen op eenvoudige wijze het gewenste resultaat. Leveranciersketens en tekortkomingen in configuraties zijn wederom misbruikt om succesvolle aanvallen uit te voeren. In de afgelopen periode werden westerse vitale infrastructuren gecompromitteerd. Meer landen zijn overgegaan tot het publiek attribueren van cyberaanvallen, tegelijkertijd blijft attributie complex en foutgevoelig. Cybercriminaliteit blijft zich ontwikkelen. Geconstateerde storingen en uitval onderschrijven de toename van complexiteit en verwevenheid van techniek en samenleving.

Westerse vitale infrastructuren gecompromitteerd

Reeds eerder is geschreven over toenemende activiteiten gericht op het (in de toekomst) mogelijk maken van sabotage van vitale infrastructuren in Europa, waarbij andere landen zich nestelen in bepaalde systemen.[96] Die activiteiten lijken in toenemende mate ook gericht op West-Europa. In de rapportageperiode zijn verschillende toeleveranciers van vitale infrastructuren succesvol aangevallen. De toeleveranciers zijn vervolgens gebruikt als tussenstap om de beoogde doelwitten te compromitteren. Actoren hebben een toenemende interesse om kwetsbaarheden in leveranciersketens te misbruiken. Enerzijds om verstoring of sabotage mogelijk te maken, anderzijds om mogelijk geopolitieke druk uit te oefenen of spionage mogelijk te maken.

In oktober 2018 schreef beveiligingsbedrijf ESET over cyberaanvallen waarbij de GreyEnergy malware is ingezet.[897] GreyEnergy wordt als opvolger gezien van BlackEnergy, een malwaretoolkit die in verband is gebracht met cyberaanvallen op het energienet van Oekraïne in 2015 en 2016. GreyEnergy zou het afgelopen jaar bij verschillende aanvallen op voornamelijk Oekraïne maar ook op Polen zijn ingezet.[98] Het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI) besteedde opnieuw aandacht aan cyberaanvallen op de Duitse energiesector.[99] Duitse bedrijven in verschillende vitale sectoren zouden verscheidene malen doelwit zijn geweest van grootschalige digitale campagnes. Hierdoor hebben de aanvallers toegang verkregen tot het kantoornetwerk van verschillende bedrijven. Het vermoeden bestaat dat de aanvallers uit waren op het verkrijgen van een positie binnen het netwerk om deze op een later moment uit te buiten.

Dragonfly

Het Amerikaanse Department of Homeland Security (DHS) waarschuwt al langere tijd voor cyberaanvallen van onder andere de actorgroep Dragonfly. Deze groep staat ook bekend als Havex, Energetic Bear en Energetic Yeti. De Amerikaanse overheid attribueert Dragonfly aan Rusland.[100,101] De actorgroep richt zich in de VS op netwerken van zowel bedrijven in de vitale infrastructuur als op toeleveranciers. Met gerichte cyberaanvallen op de leveranciersketen is het aanvallers gelukt toegang te verkrijgen tot de netwerken van leveranciers en partners van beoogde doelwitten. De doelwitten betreffen kleine en grote bedrijven die verantwoordelijk zijn voor het produceren, transporteren en distribueren van elektriciteit. De toegang tot deze leveranciers werd gebruikt als opstapje voor het verkennen van het netwerk van de beoogde doelwitten. Vanuit de gecompromitteerde netwerken werden spearphishing-e-mails verspreid en wateringhole-aanvallen uitgevoerd. Honderden bedrijven zijn slachtoffer geworden. Het is de aanvallers uiteindelijk gelukt om toegang te krijgen tot netwerken van de beoogde doelwitten. Hoeveel netwerken het betrof is niet bekend gemaakt. De aanvallers hebben de netwerken gebruikt om informatie over industriële controlesystemen (ICS) te verzamelen. Zodra de aanvallers toegang verkregen tot de netwerken, is getracht deze toegang permanent te maken. Uiteindelijk is de actorgroep niet overgegaan tot sabotage of verstoring.

Geavanceerde aanvalscapaciteiten laagdrempelig toegankelijk

Staten kunnen geavanceerde aanvalscapaciteiten verwerven, zodat zij niet zelf hoeven te investeren in de ontwikkeling ervan. Ook kunnen staten de voorbereiding en uitvoering van digitale aanvallen 'uitbesteden' aan een derde partij. Het onderzoeksinstituut The Citizen Lab rapporteerde uitgebreid over één van de bedrijven die spionagesoftware levert aan meer dan veertig landen, niet alleen voor opsporingsdoeleinden maar soms ook voor spionage op oppositieleden en dissidenten.[102] Reuters beschreef hoe voormalige medewerkers van de Amerikaanse NSA de overheid van de Verenigde Arabische Emiraten ondersteunden met spionageactiviteiten.[103] Ook hackten de Verenigde Arabische Emiraten de iPhones van activisten, diplomaten en buitenlandse leiders met 'Karma', een gespecialiseerde hacktool.[104,105]

Vrij verkrijgbare tools en generieke diensten ingezet als aanvalsmiddel

Het gebruik van vrij beschikbare tools en technieken om netwerken te compromitteren, te verstoren of vertrouwelijke data te ontvreemden, is niet nieuw.[106] Actoren kunnen ook generieke diensten inzetten voor een cyberaanval. Met 'generieke diensten' wordt hier het gebruik van bijvoorbeeld publieke online opslag- of e-maildienstverlening bedoeld in tegenstelling tot infrastructuur die is opgezet voor en door kwaadwillenden. De inzet van generieke diensten is een laagdrempelige methode die mogelijk minder snel door een gebruiker of detectieoplossing zal worden gedetecteerd. In een rapport van enkele westerse overheden wordt een aantal van deze tools en waarvoor ze worden ingezet beschreven.[107] In oktober 2018 schreef beveiligingsbedrijf Symantec over een spionagecampagne van een nieuwe actorgroep. Deze actorgroep, 'Gallmaker', gebruikt geen malware voor het uitvoeren van hun activiteiten, maar enkel vrij verkrijgbare tools en generieke diensten. De actorgroep was al maanden actief, maar niet eerder gedetecteerd vanwege het gebruik van generieke diensten.[108]

Technische attributie complex en foutgevoelig

In deze rapportageperiode bleek dat attribueren van operaties op basis van technische kenmerken aan specifieke statelijke actoren complex en foutgevoelig is. Bloomberg schreef in oktober 2018 in een artikel dat de Chinese overheid een chip implanteerde in servermoederborden van Super Micro Computers Inc. om zo Amerikaanse organisaties te infiltreren.[109] De betrokken bedrijven ontkenden dit bericht. Ze werden daarin gesteund door onder meer het Britse National Cyber Security Centre en het Department of Homeland Security van de VS.[110,111] Rond de kerstdagen werd in een ander geval een Russische hackgroep in verband gebracht met de publicatie van privégegevens van Duitse politici.[112,113] Uiteindelijk werd een Duitse student gearresteerd voor deze hack.[114]

In de afgelopen rapportageperiode is duidelijk geworden dat een aantal door beveiligingsbedrijven geattribueerde cyberaanvallen onjuist zijn geweest.[115,116,117] Onder meer de inzet van vrij verkrijgbare tools en generieke diensten maakt technische attributie complexer. Beveiligingsbedrijven zijn daarom terughoudender geworden met attribueren.[118]

In februari 2019 meldden media dat netwerken van verschillende Australische politieke partijen gecompromitteerd waren. Vanwege de maatregelen die Australië heeft genomen tegen Chinese bedrijven om digitale spionage te voorkomen, werd verondersteld dat China mogelijk achter de cyberaanval zat.[119,120] Eind februari 2019 meldden andere media dat Iran verantwoordelijk is voor het uitvoeren van deze cyberaanval. Iraanse staatshackers zouden het gemunt hebben op Amerika en haar bondgenoten en deze cyberaanval hebben uitgevoerd als wraakactie voor het opnieuw invoeren van sancties tegen de Iraanse overheid.[121] Wie verantwoordelijk gesteld moet worden zal nader onderzoek moeten uitwijzen.

Politieke attributie in opmars

Het publiekelijk attribueren van cyberaanvallen door overheden aan een statelijke actor is een recente ontwikkeling die ook in het CSBN 2018 aan de orde is gekomen. Verschillende overheden hebben deze rapportageperiode maatregelen tegen actoren genomen. De Verenigde Staten hebben aanklachten ingediend tegen hackers van onder meer Iraanse[122,123], Noord-Koreaanse[124], Russische[125,126], en Chinese[1127] afkomst. Verschillende aanklachten vinden internationale steun bij andere regeringen.[128,129]

Op 20 december 2018 heeft het Amerikaanse ministerie van Justitie een aanklacht ingediend tegen twee Chinese hackers (APT10) die, volgens de aanklacht, in opdracht van de Chinese overheid cyberaanvallen uitvoeren. Het doel van de campagne was voornamelijk economische spionage door data, intellectuele eigendommen en technische informatie te stelen. De campagne heeft diverse sectoren als doelwit gehad en is wijdverspreid waargenomen.[130] Inmiddels hebben ook Australië, Canada, Japan, Nieuw-Zeeland en het Verenigd Koninkrijk de Chinese overheid verantwoordelijk gesteld voor deze campagne.[131,132,133,134,135]

Specifiekere maatregelen door overheden

Naast attributie lijken ook andere maatregelen door overheden te worden ingezet. Een voorbeeld is de vermeende cyberoperatie die de Amerikaanse overheid zou hebben ingezet tijdens de verkiezingen in november 2018. Toen zou toestemming zijn verleend om Russische netwerken te compromitteren om een mogelijke cyberaanval op de VS te voorkomen.[136,137]

Het kabinet heeft in mei 2018, vanwege de zorgen ten aanzien van risico's voor de nationale veiligheid, de voorzorgsmaatregel genomen om het gebruik van antivirussoftware van Kaspersky bij de rijksoverheid uit te faseren en om vitale bedrijven en defensieleveranciers te adviseren hetzelfde te doen.[138]

Tsjechische overheidsmaatregelen tegen Chinese 5G hard- en software

In december 2018 bracht het National Cyber and Information Security Agency (NCISA) van Tsjechië een waarschuwing uit tegen het gebruik van hard- en software van de Chinese bedrijven Huawei Technologies Co. Ltd. en ZTE Corporation. Het gebruik van hard- en software van deze bedrijven vormt volgens NCISA een bedreiging voor de veiligheid. Bedrijven in de vitale infrastructuur, belangrijke informatiesystemen en essentiële dienstverleners zijn verplicht kennis te nemen van deze waarschuwing en adequate maatregelen te nemen.[139]

Verschillende landen zoals de Verenigde Staten[140] en Australië[141] hebben maatregelen genomen, andere landen overwegen dit nog.[142,143]

Cybercriminaliteit blijft zich ontwikkelen

Criminelen anticiperen op nieuwe technologische ontwikkelingen, zoals online diensten. Het plegen van digitale misdrijven is eenvoudiger door cybercrime-as-a-service (CaaS). Actoren met relatief weinig capaciteit kunnen hiermee toch aanvallen uitvoeren. Ook deze rapportageperiode hebben cybercriminelen veelvuldig misbruik gemaakt van de Nederlandse digitale infrastructuur.[144,145]

Criminelen spelen in op het gebruik van tweefactor-authenticatie

Tweefactor-authenticatie voegt beveiliging toe aan traditionele gebruikersauthenticatie. Toch blijkt in de rapportageperiode dat criminelen ook hier op weten in te spelen. Dit bleek bijvoorbeeld uit de phishingaanval gericht op gebruikers van mijnoverheid.nl.[146] Daarbij logden getroffenen in op een valse inlogpagina, waarbij de aanvallers ook de door de gebruiker ingevoerde sms-code misbruikten. Vervolgens werd geautomatiseerd ingelogd bij de persoonlijke MijnOverheid-pagina van de getroffene. Qua bredere trend lijken aanvallen gericht op het onderscheppen van sms-berichten nog relatief zeldzaam, maar er is wel sprake van een toename.[147,148]

Opkomst cybercrime-as-a-service zet door

De opkomst van cybercrime-as-a-service zet verder door, zo blijkt uit de Internet Organised Crime Threat Assessment (IOCTA) van Europol.[149] Actoren met relatief weinig ict-kennis kunnen voor iedere stap van een cyberaanval diensten inkopen op criminele fora. Het begaan van een online misdrijf wordt eenvoudiger door de laagdrempelige en gebruiksvriendelijke manier waarop deze diensten worden aangeboden. In 2018 werd de website webstresser.org offline gehaald. Dit platform ondersteunde meer dan 135.000 gebruikers bij iedere stap in de uitvoering van miljoenen DDoS-aanvallen met een crimineel motief.[150,151] Uit wetenschappelijk onderzoek blijkt dat op algemene online ondergrondse marktplaatsen het aanbieden van cybercrime diensten niet zo succesvol is als soms wordt gesuggereerd.[152] Op specifieke ondergrondse cybercriminele fora worden dergelijke diensten op grote schaal aangeboden.[153] Deze criminele dienstensector maakt veelvuldig gebruik van de Nederlandse ict-infrastructuur om diensten te leveren.[154]

Hack_Right

Bewustzijn van de strafbaarheid van cybercriminaliteit is nog niet overal aanwezig. Bij een campagne van de politie bleek dat ruim 9.500 jongeren verleid konden worden tot het plegen van cybercriminaliteit, zoals het hacken van Instagram-accounts of het platleggen van een elektronische leeromgeving. Bijna een derde van deze groep was zich er niet van bewust dat zij iets strafbaars van plan waren.[155]

Voor hen die in de fout zijn gegaan volgt in sommige gevallen een speciaal traject. Hack_Right is een alternatief of aanvullend straftraject. Jongeren van 12 tot 23 jaar die voor het eerst voor een cybercrimedelict worden veroordeeld kunnen hiervoor in aanmerking komen. Het doel van Hack_Right is om recidive te voorkomen en het cybertalent van jongeren binnen de kaders van de wet verder te ontwikkelen. De strafrechtketenpartners, cybersecuritybedrijven en de hacker community ontwikkelen de interventie en voeren deze uit.[156]

Ransomware lijkt af te nemen

Microsoft constateert[157] dat besmettingen met ransomware en cryptominers, na een piek begin 2018, de afgelopen periode zijn teruggelopen, zowel wereldwijd als in Nederland. Bedrijven lijken beter voorbereid te zijn op het herstellen van informatie na een ransomwarebesmetting, waardoor er minder losgeld wordt betaald. De inzet van cryptominers lijkt met het teruglopen van de koers van diverse cryptocurrencies af te nemen. Ook Symantec herkent de terugval van ransomware en cryptominers,[158] maar verwacht dat deze vormen van malware in de toekomst blijvend voor problemen zullen zorgen. Symantec en Trend Micro[159] zien een stijging van cryptominers op mobiele devices. In haar jaarlijkse dreigingsbeeld[160] beschrijft CrowdStrike een toename van gerichte

ransomwareaanvallen op grote bedrijven met als doel in een keer grote bedragen binnen te halen.

Formjacking in opkomst

In deze rapportageperiode lijken cybercriminelen naast ransomware en cryptojacking gebruik te zijn gaan maken van andere aanvalstechnieken zoals formjacking. Volgens Symantec was het gebruik van hiervan door cybercriminelen opvallend. Bij formjacking past de aanvaller een website aan zodat informatie die de bezoeker invult bij de aanvaller terechtkomt. Hij kan de website op verschillende manieren aanpassen, bijvoorbeeld door de website te hacken en de code van de website zelf aan te passen. Hij kan ook de code van een gedeeld onderdeel van de website aanpassen, zoals van webwinkelsoftware. Tot slot kan de aanvaller de werking van de website veranderen via de op de website getoonde advertenties.

Op deze wijze kunnen criminelen bijvoorbeeld creditcardnummers onderscheppen van gebruikers van webwinkels.[161,162] Symantec stelt dat wereldwijd elke maand 4800 unieke webwinkels slachtoffer van formjacking worden. Met name kleine en middelgrote detailhandel krijgt hier volgens Symantec mee te maken.[163]

Eenvoudige aanvalsmiddelen effectief

Ook deze rapportageperiode bleken eenvoudige aanvalsmiddelen, zoals phishing of misbruik van gebruikersnamen en wachtwoorden effectief.

Phishing blijft succesvol

Al jaren wordt phishing met succes ingezet voor het uitvoeren van cyberaanvallen. Dit is en blijft een populaire en succesvolle aanvalsmethodiek die breed wordt ingezet. Uit cijfers[164,165] en voorbeelden[166] blijkt dat ook in deze rapportageperiode phishing veel gebruikt is. Het blijvende succes ervan maakt het een aanvalsmethodiek die zowel door statelijke actoren wordt ingezet voor spionage- en sabotagedoeleinden[167,168], als door criminelen.[169,170] De schade in Nederland door phishing bij internetbankieren is toegenomen van 1,05 miljoen euro in 2017 naar 3,81 miljoen euro in 2018.[171]

Misbruik van gebruikersnamen en wachtwoorden

In de afgelopen rapportageperiode zijn diverse aanvallen uitgevoerd waarbij zogenaamde Domain-Name-System (DNS)-instellingen van organisaties wereldwijd werden aangepast. DNS kan beschouwd worden als het 'telefoonboek van het internet'. In januari 2019 schreven US-CERT en FireEye over kwaadwillenden die wereldwijd DNS-instellingen van domeinen tijdelijk hebben gewijzigd.[172,173,174] Volgens FireEye zou het gaan om organisaties in diverse sectoren waaronder telecom- en internet providers en overheden in het Midden-Oosten, Noord-Afrika, Europa en Noord-Amerika. Het beveiligingsbedrijf Talos publiceerde eerder over aanvallen gericht op het Midden-Oosten waarbij vergelijkbare methoden gebruikt werden.[175] De aanvallers konden de DNS-instellingen wijzigen met behulp van gebruikersnamen en wachtwoorden voor het klantportaal van de DNS-aanbieder. Door het wijzigen van de DNS-instellingen konden zij verdere gebruikersnamen en wachtwoorden stelen van gebruikers die bijvoorbeeld op de webmail van hun organisatie inlogden. Cyberaanvallen op basis van deze methode zouden vanaf januari 2017 hebben plaatsgevonden. FireEye heeft deze in januari 2019 aan Iran toegeschreven.[176] De Internet Corporation for Assigned Names and Numbers (ICANN) heeft partijen die een rol hebben in de DNS-keten gewaarschuwd voor deze aanvallen en opgeroepen om maatregelen te treffen.[177]

Ook Border Gateway Protocol (BGP) hijacks zijn in de rapportageperiode ingezet om DNS-verkeer om te leiden. In april 2018 was al bekend dat middels een BGP-hijack de DNS-dienst van Amazon werd misbruikt.[178] In juli 2018 kwam uit dat een vergelijkbare techniek ingezet is om DNS-verkeer van Amerikaanse betaalverwerkingsdiensten om te leiden.[179]

Ransomware-besmettingen via bediening op afstand

In de afgelopen rapportageperiode is gebleken dat kwaadwillenden succesvol waren in het vinden van kwetsbare zogenoemde Remote Desktop Protocol (RDP) servers. RDP maak het mogelijk om op afstand toegang te krijgen tot systemen en deze te bedienen. Nederlandse bedrijven zijn slachtoffer geworden van de SamSam ransomware.[180] Die probeert vanaf het internet toegankelijke RDP-servers met zwakke wachtwoorden uit te buiten. Via de verkregen toegang wordt door de kwaadwillenden informatie over de getroffen organisatie verzameld om vervolgens losgeld te vragen.

Misbruik leveranciersketens

In de vorige paragrafen is misbruik van dienstverleners en softwareleveranciers in leveranciersketens beschreven. Microsoft schrijft over de kwetsbare softwareleveranciersketen, met een aantal casussen die laten zien hoe malafide code ingebracht wordt in legitieme software.[181] Bijvoorbeeld via een geïnfecteerd update- of installatiepakket dat vervolgens meelift op het legitieme distributieproces van de software inclusief veiligheidswaarborgen.

2018: nieuwe wetgeving in Nederland

In 2018 is er nieuwe dan wel aanvullende wetgeving van kracht geworden in relatie tot of met effect op cybersecurity. De Wet beveiliging netwerk- en informatiesystemen (Wbni), maar ook de Algemene Verordening Gegevensbescherming (AVG) en de Wet op de inlichtingen en veiligheidsdiensten (Wiv) werden van kracht.

Wet beveiliging netwerk- en informatiesystemen treedt in werking

De Wbni betreft in hoofdzaak de Nederlandse implementatie van de Europese richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn), die tot doel heeft om een hoger gemeenschappelijk niveau van cybersecurity binnen de EU tot stand te brengen. Daarnaast zijn in de Wbni de regels uit de voordien al geldende Wet

gegevensverwerking en meldplicht cyber security geïncorporeerd. Op 9 november 2018 trad deze nieuwe wet grotendeels, en op 1 januari 2019 geheel, in werking. De Wbni beoogt de digitale weerbaarheid van Nederland, en in het bijzonder die van vitale aanbieders (energie-, drinkwater-, financiële sector, etc.), de rijksoverheid en digitale dienstverleners te bevorderen. Vitale aanbieders zijn overheidsorganisaties en privaatrechtelijke rechtspersonen die diensten aanbieden waarvan de continuïteit, volgens de Nederlandse overheid, van vitaal belang zijn voor de Nederlandse samenleving. Digitale dienstverleners als bedoeld in de Wbni zijn online marktplaatsen, online zoekmachines en cloudcomputerdiensten, met ten minste 50 mensen in dienst.[182]

Meld- en zorgplicht voor vitale aanbieders en digitale dienstverleners

Voor aanbieders van essentiële diensten en andere bij algemene maatregel van bestuur aangewezen vitale aanbieders en voor digitale dienstverleners, geldt krachtens de Wbni een meldplicht voor incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende diensten. Een incident betreft elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen, die voor de betrokken diensten worden gebruikt. Deze incidenten moeten ten eerste worden gemeld aan het Computer Security Incident Response Team (CSIRT). Voor genoemde vitale aanbieders is dat het Nationaal Cybersecurity Centrum (NCSC) van het ministerie van Justitie en Veiligheid. In de rapportageperiode is er één melding onder de Wbni gedaan bij het NCSC.[183] Digitale dienstverleners maken melding van incidenten bij het CSIRT voor digitale diensten van het ministerie van Economische Zaken en Klimaat. Daarnaast moeten aanbieders van essentiële diensten en digitale dienstverleners deze incidenten ook melden bij hun sectorale toezichthouder.

Voor aanbieders van essentiële diensten en digitale dienstverleners geldt op grond van de Wbni ook een zorgplicht: een organisatie moet passende en evenredige organisatorische en technische maatregelen nemen om risico's voor de beveiliging van hun ict-systemen te beheersen, incidenten te voorkomen en de gevolgen van incidenten zo veel mogelijk te beperken, teneinde de continuïteit van hun diensten te waarborgen. Die maatregelen dienen ertoe de netwerk- en informatiesystemen bestand te laten zijn tegen acties die de digitale veiligheid van de opgeslagen, verzonden of verwerkte gegevens, of de daaraan gerelateerde diensten die via die systemen worden aangeboden of toegankelijk zijn, in gevaar brengen.[184]

Overige nieuwe wetgeving

Wet Computercriminaliteit III [185]
Op 1 maart 2019 is de wet computercriminaliteit III in werking getreden. Deze wet geeft politie en justitie nieuwe bevoegdheden om computercriminaliteit te bestrijden. Politie en justitie hebben met deze wet de bevoegdheid gekregen heimelijk en op afstand (online) onderzoek doen in computers, de zogeheten hackbevoegdheid. Daarnaast worden heling van digitale gegevens en online handelsfraude strafbaar gesteld.

Algemene verordening gegevensbescherming [186]
Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van kracht [187]. De AVG vervangt de Wet bescherming persoonsgegevens. Hij heeft directe werking in alle lidstaten van de EU. Met de AVG worden twee belangen gewaarborgd: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens, en het vrije verkeer van persoonsgegevens binnen de Europese Unie. Burgers krijgen onder de AVG nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen en moeten aantoonbaar aan de regels voldoen.[188]

Wet op de Inlichtingen- en Veiligheidsdiensten 2017 [189]
Op 1 mei 2018 trad de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 in werking. Deze wet geeft de inlichtingen- en veiligheidsdiensten een aantal nieuwe bevoegdheden en er zijn waarborgen toegevoegd. Zo bevat de wet striktere termijnen voor het bewaren van gegevens en wordt de inzet van bijzondere inlichtingenmiddelen vooraf door een onafhankelijke commissie getoetst, de Toetsingscommissie Inzet Bevoegdheden (TIB).

Storingen en uitval

In de rapportageperiode vond een aantal ict-storingen plaats. Een verstoring of uitval van informatiesystemen is het gevolg van onopzettelijk menselijk handelen of een systeemfout. In de rapportageperiode vonden in verschillende ziekenhuizen storingen plaats. In het Amsterdam Universitair Medisch Centrum moesten in augustus 2018 tussen de 1000 en 1500 afspraken worden afgezegd na een storing waarbij de elektronische patiëntendossiers ontoegankelijk waren en het e-mailsysteem niet werkte.

Het gebruik van complexe techniek neemt verder toe.[190] Kleine fouten kunnen hierdoor grote gevolgen hebben. Dit bleek bijvoorbeeld bij de storing in de Schipholtunnel in augustus 2018.[191] Door een fout in de software van het dynamisch verkeersmanagementsysteem (DVM) en een samenloop van omstandigheden werd het automatische verkeersleidingsysteem overbelast. Het treinverkeer rond Amsterdam en Schiphol moest

daardoor handmatig worden geregeld. Er ontstonden vertragingen en er vielen treinen uit.

Door de toegenomen complexiteit en verwevenheid van processen en systemen kan een storing van één systeem meerdere processen of een keten van processen raken. Wanneer een systeem niet functioneert heeft dit impact op alle processen die ervan afhankelijk zijn. In augustus 2018 vielen de elektronische enkelbanden uit van honderden gedetineerden of verdachten in Nederland door een storing bij telecomaanbieder Tele2.[192] De elektronische enkelbanden konden daardoor gedurende twee dagen geen verbinding maken met de meldkamer.

Meeste datalekken door menselijke fout

In de eerste helft van 2018 is het aantal gemelde datalekken verder gestegen, naar 5430 nieuwe meldingen in het tweede kwartaal van 2018, aldus de Autoriteit Persoonsgegevens.[193] Dit is een verdubbeling ten opzichte van het tweede kwartaal van 2017, toen 2468 datalekken werden gemeld. Nederland is een van de Europese koplopers wat betreft het melden van datalekken.[194]

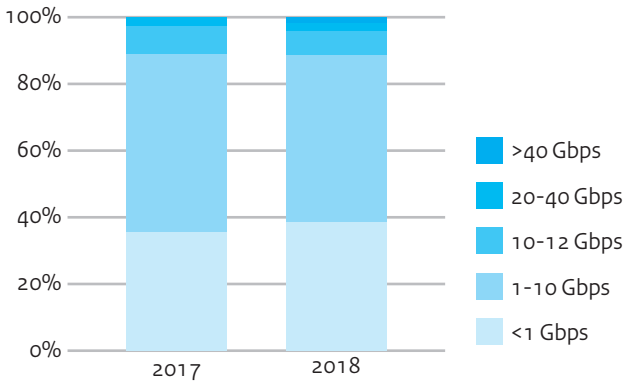
Meer dan de helft van de gemelde datalekken in het eerste halfjaar van 2018 was het gevolg van een menselijke fout. Persoonsgegevens die naar de verkeerde ontvanger werden verstuurd of aan de verkeerde persoon werden afgegeven vormden 64 procent van het totaal aantal meldingen.[195]

Aantal DDoS-aanvallen toegenomen

Het aantal websites dat doelwit was van een DDoS-aanval lag in 2018 vijftien procent hoger dan in 2017, zo meldde de stichting Nationale Beheersingsorganisatie Internet Providers (NBIP) en de Stichting Internet Domeinregistratie Nederland (SIDN).[196] Webwinkels blijven een populair doelwit. In december 2018 was een piek te zien in DDoS-aanvallen op webwinkels.[197] Daarnaast waren onder andere financiële instellingen en DigiD doelwit.[198,199] In december 2018 meldde de FBI dat zij samen met de Nederlandse politie vijftien websites die DDoS-aanvallen aanboden offline heeft gehaald.[200]

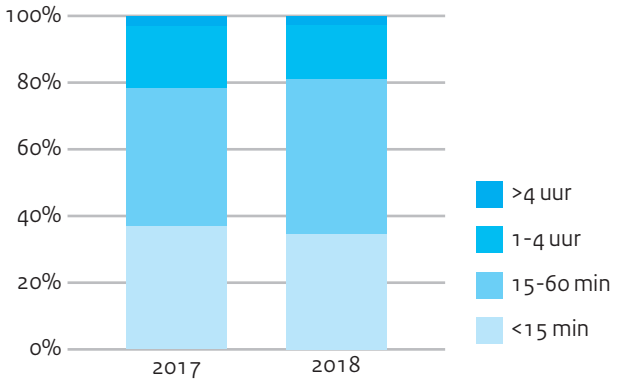
In de afgelopen rapportageperiode is opgevallen dat zeer grote aanvallen, zoals de in het CSBN 2018 genoemde aanval van meer dan 1 Terabit per seconde, zijn uitgebleven. In 2018 heeft het NBIP 938 DDoS-aanvallen verwerkt. De maximale grootte van een enkele DDoS-aanval lag in 2018 op 68 Gigabit per seconde (Gbps). In 2017 bedroeg de grootste DDoS-aanval 36 Gbps. Net als voorgaande jaren zijn de meeste aanvallen niet groter dan 10 Gbps. Net als in 2017 duurde een DDoS-aanval in 2018 niet langer dan een uur. Cijfers laten wel zien dat het aantal DDoS-aanvallen dat korter dan 15 minuten duurt, afneemt, DDoS-aanvallen die tussen vijftien minuten en één uur duren nemen toe.

Figuur 2 **Omvang van DDoS-aanvallen**



Bron: Nationale Beheersorganisatie Internet Providers

Figuur 3 **Duur van DDoS-aanvallen:**



Bron: Nationale Beheersorganisatie Internet Providers

Organisaties worden succesvol aangevallen met eenvoudige methoden

5 Weerbaarheidsbeeld

De digitale weerbaarheid van Nederland is niet overal op orde. Methoden om de weerbaarheid daadwerkelijk te meten ontbreken. Om die reden wordt hier een indirect beeld geschetst op basis van toezichtrapporten en extrapolatie van incidenten en gebeurtenissen. Een compleet scherp beeld van de weerbaarheid ontbreekt. Organisaties worden succesvol aangevallen met eenvoudige methoden. Incidenten hadden voorkomen kunnen worden of de schade had beperkt kunnen worden met behulp van basismaatregelen.

Digitale weerbaarheid niet overal op orde

De digitale veiligheid, specifiek de vertrouwelijkheid, integriteit en beschikbaarheid, van gedigitaliseerde processen en systemen, is essentieel om maatschappelijke en economische groei mogelijk te maken en maatschappelijke ontwrichting te voorkomen. Het kabinet stelt dat onder andere versterking van de weerbaarheid van burgers en organisaties nodig is om de kansen van digitalisering te benutten. Veiligheid en vertrouwen vormen de basis daarvoor. Dat zijn ook fundamenten voor een goed vestigingsklimaat, voor onze concurrentiepositie en voor de acceptatie en het gebruik van digitale middelen.[201] Cybersecurity is daarmee niet alleen een kostenpost of noodzakelijk kwaad, maar ook een stimulans voor verdere digitalisering.

De digitale weerbaarheid is niet overal op orde. Organisaties worden succesvol aangevallen met eenvoudige methoden. Incidenten hadden voorkomen of de schade had beperkt kunnen worden met behulp van basismaatregelen. De weerbaarheid staat verder onder druk door een toenemende complexiteit en connectiviteit in het ict-landschap. Het vergroten van de weerbaarheid is het belangrijkste instrument voor burgers, bedrijven en overheid om risico's te verminderen. Het beïnvloeden van de afhankelijkheid en dreiging blijkt zeer complex. Wettelijke maatregelen, zoals de Wbni, benadrukken het belang voor organisaties om de weerbaarheid te verhogen. De effecten hiervan zullen in de komende jaren zichtbaar worden.

Methode weerbaarheidsmeting ontbreekt

Het verkrijgen van inzicht in de weerbaarheid, en daarmee in de mate waarin maatregelen effectief en efficiënt zijn, is complex. Betrouwbare methoden en technieken om weerbaarheid te meten zijn randvoorwaardelijk om goed zicht te krijgen op de risico's voor de nationale veiligheid en om sectoren of verschillende organisaties met elkaar te vergelijken. Deze methoden en technieken zijn nog onvoldoende ontwikkeld. Hierdoor kan er alleen een indirect beeld worden geschetst op basis van toezichtrapporten en op basis van extrapolatie van incidenten en gebeurtenissen. Dit betekent ook dat er geen compleet scherp beeld is van de digitale weerbaarheid van alle vitale processen.

Weerbaarheid Rijksoverheid niet op orde

De Algemene Rekenkamer gaf op Verantwoordingsdag in mei 2018 aan dat op het gebied van ict-beveiliging slechts twee van de elf ministeries hun zaken op orde hadden. De president van de Algemene Rekenkamer stelt dat 'de politieke en ambtelijke top van ministeries meer aandacht moet geven aan ict-beveiliging'.[202,203]

Ministeries geven middels zogenaamde "In Control Verklaringen (ICV)" aan of het ministerie zijn informatie voldoende beveiligt. De Algemene Rekenkamer geeft aan dat voor 2017 de onderbouwing van deze ICV's ad hoc en impliciet is. Dit bemoeilijkt het verkrijgen van een rijksoverheidsbreed beeld. Ministeries hanteren verschillende definities over wat een kritiek systeem is.[204]

Ook in mei 2019 werd door de Algemene Rekenkamer op Verantwoordingsdag geconstateerd dat de informatiebeveiliging niet op orde is. Bij 11 organisaties van de rijksoverheid signaleert de Algemene Rekenkamer grote problemen in de informatiebeveiliging en dit is een verslechtering ten opzichte van het voorgaande jaar.[205]

Weerbaarheid vitale processen

In een onderzoek[206] naar de digitale beveiliging van vitale waterwerken in Nederland constateert de Algemene Rekenkamer dat tunnels, bruggen, sluizen en waterkeringen nog beter kunnen

worden beveiligd tegen cyberaanvallen. De afgelopen jaren is er veel werk verzet en zijn noodzakelijke maatregelen in kaart gebracht om waterkeringen beter te beveiligen. Maar die veiligheidsmaatregelen zijn niet allemaal uitgevoerd. Crisisdocumentatie is verouderd en er worden geen volwaardige penetratietesten uitgevoerd. Uit het onderzoek blijkt dat nog niet alle vitale waterwerken rechtstreeks zijn aangesloten op het Security Operations Center. Hierdoor bestaat het risico dat een cyberaanval niet of te laat wordt gedetecteerd.[207]

De Nederlandse Bank stelt dat zij voor de Nederlandse financiële sector hebben gezien dat er niet continu expliciete aandacht is voor analyses van cybersecuritydreigingen en -maatregelen.[208] De aandacht voor het op niveau brengen en houden van informatiebeveiligingsmaatregelen schiet soms tekort. Soms komen ongewenste combinaties voor in toegangsrechten van applicaties en processen. Er blijft aandacht nodig voor het detecteren en analyseren van cyberaanvallen. Ook zou meer aandacht moeten uitgaan naar het reageren op cyberaanvallen en het herstel na een aanval.

Omdat er geen compleet scherp beeld is van de digitale weerbaarheid, is het onbekend of de weerbaarheid van andere vitale processen lager of hoger is. Tegelijkertijd is het voorstelbaar dat er, *in generieke zin*, geen sprake zal zijn van zeer significante afwijkingen van het hierboven geschetste beeld.

Organisaties worden succesvol aangevallen met eenvoudige methoden

Organisaties worden succesvol aangevallen met eenvoudige methoden. De afgelopen periode laat wederom zien dat incidenten voorkomen hadden kunnen worden of dat de schade beperkt had kunnen worden met behulp van basismaatregelen. Die worden door lang niet alle organisaties getroffen.

Phishing blijft een effectieve aanvalstechniek

Aanvallers blijven gebruik maken van bestaande aanvalstechnieken die effectief blijken te zijn. Ook dit jaar blijkt phishing weer een populaire en succesvolle aanvalsmethode te zijn.[209] Het uitvoeren van een dergelijke aanval is relatief eenvoudig. Hoewel veel organisaties aandacht besteden aan bewustzijn bij gebruikers, lijkt de effectiviteit van deze aanvallen niet te verminderen. Een analyse van Microsoft[210] laat zien dat een toenemend percentage (circa 250% toename in 2018) van de geanalyseerde mails wordt bestempeld als phishing. Met name zeer gerichte spearphishing campagnes blijken een hoge succesfactor te hebben en zijn voor slachtoffers nauwelijks te herkennen.

Detectietijd blijft achter bij snelheid aanvallen

Het blijft voor organisaties lastig om te detecteren of hun systemen misbruikt worden, zo blijkt uit een rapportage van FireEye. Het gemiddeld aantal dagen tussen het moment van inbraak op een systeem en het moment van ontdekking ligt wereldwijd voor 2018 op 78.[211] De trend laat hier overigens wel verbetering zien. In 2017 bedroeg deze periode nog gemiddeld 101 dagen, terwijl dit in 2014 zelfs nog 205 dagen betrof. CrowdStrike signaleert dat geavanceerde aanvallers na initiële toegang tot een netwerk al binnen enkele uren toegang tot andere delen van het bedrijfsnetwerk weten te verkrijgen.[212]

Initiële toegang wordt in veel gevallen met simpele methodes (zoals phishing) verkregen, waarna aanvallers geavanceerdere methodes inzetten om netwerken te verkennen en verder binnen te dringen. In deze tweede fase wordt het veel lastiger om aanvallers te detecteren en vervolgens volledig uit een netwerkomgeving verwijderd te krijgen. Het verbeteren van de digitale basishygiëne is een effectieve barrière tegen aanvallen.

Hard- en softwarekwetsbaarheden blijvend probleem

Het aantal gerapporteerde (hoogrisico-) kwetsbaarheden is in 2017 en 2018 sterk toegenomen, aldus het Centraal Planbureau (CPB) in zijn Risicorapportage Cyberveiligheid Economie 2018.[213]

Onveilige software leidt tot kwetsbaarheden in systemen en daarmee in processen. Uit een onderzoek in opdracht van het NCSC bleek dat in Nederland bijna anderhalf miljoen potentieel kwetsbare apparaten en diensten op deze apparaten aan het internet zijn gekoppeld. Daarvan bleken bijna driehonderdduizend apparaten of services daadwerkelijk te misbruiken.[214] Het Agentschap Telecom luidde vorig jaar de alarmklok over het toenemend aantal onveilige IoT-apparaten dat aan het internet worden gekoppeld.[215] Hierbij roept het Agentschap op tot aanvullende regels en een snelle invoer van minimumeisen.

Fundamentele hardware kwetsbaarheden waren ook deze periode relevant.[216,217] Uitbuiting van dit soort kwetsbaarheden wordt steeds eenvoudiger, waardoor uitbuiting buiten het laboratorium waarschijnlijker wordt. Een echte bescherming tegen dit soort aanvallen is er niet.[218]

Complexiteit ondermijnt weerbaarheid

Diverse onderzoeken[219] geven aan dat de complexiteit van het continu veranderende digitale landschap blijft toenemen en dat dit leidt tot een groter en complexer aanvalsoppervlak. De inzet van nieuwe toepassingen in combinatie met al langer bestaande (legacy) omgevingen, biedt aanvallers uitgebreidere opstapmogelijkheden om organisaties aan te vallen, waarbij ze ook meer gebruik kunnen maken van generieke diensten en eenvoudig te verkrijgen tools.

Enerzijds zorgen de organische groei en de relatief lange levensduur van systemen voor een steeds ingewikkelder landschap. Anderzijds maakt het toegenomen gebruik van gedeelde voorzieningen, zoals deelproducten of complete clouddiensten, dat het overzicht lastiger te verkrijgen en bewaken is. Waar in het

verleden diensten binnen een organisatie ingericht werden, worden ze nu bij verschillende partijen ingekocht en extern uitgevoerd. Deze partijen maken ook gebruik van onderaannemers. Regie op het ict-landschap blijft binnen de organisatie, terwijl de uitvoering ervan versnipperd raakt over meerdere partijen. Dit zorgt voor onoverzichtelijkheid, nieuwe afhankelijkheden en een vergroting van het aanvalsoppervlak. Voor de verdedigende kant vergroot de complexiteit echter juist het risico op kwetsbaarheden. Deze complexiteit betreft ook de informatiestromen binnen grote organisaties en daarmee de verantwoordelijkheid over en het zicht op de informatie. Naarmate de complexiteit en connectiviteit toenemen, wordt het steeds uitdagender om een weerbare digitale infrastructuur te realiseren.

Door die toenemende complexiteit en connectiviteit is het voor organisaties moeilijk te voorspellen welke kwetsbaarheden in de toekomst misbruikt zullen worden en welke bijbehorende maatregelen daartegen vandaag al genomen moeten worden. Organisaties zullen geconfronteerd worden met verrassingen, zoals onverwachte incidenten en (keten)effecten. Deze onzekerheden, de zogenoemde “unknown unknowns”, zijn de consequenties van de complexiteit van de digitale infrastructuur.

Voldoende prikkels voor verbetering weerbaarheid?

6 Vooruitblik 2021

Geopolitieke ontwikkelingen zullen de dreiging vanuit statelijke actoren verder vergroten. Fundamentele belangentegenstellingen tussen landen en verschillen van inzicht over internationale normen en waarden versterken deze dreiging. Ondanks de prikkels voor vergroting van de weerbaarheid, is het onduidelijk of deze gelijke tred houden met de dreiging en het belang. Rondom technologie en dominantie hierin lijkt een geopolitiek spanningsveld te ontstaan.

Digitalisering leidt tot een vergroting van het aanvalsoppervlak en een groei en verschuiving van de aandacht van actoren naar andere en nieuwe waardevolle doelwitten. De dreiging vanuit criminelen blijft onverminderd groot. Storingen en uitval zullen een grotere impact op het maatschappelijk leven hebben door de volledige afhankelijkheid van gedigitaliseerde processen en systemen. Kunstmatige intelligentie zal enerzijds een interessant doelwit voor kwaadwillenden zijn en anderzijds een middel in aanval en verdediging.

Toekomstige effecten van digitalisering

Digitalisering en een toename van het belang van digitale veiligheid gaan hand in hand. Verdere digitalisering beïnvloedt ook de dreiging en weerbaarheid.

Groei en verschuiving in doelwitten en aanvalsmogelijkheden

De aandacht van cyberactoren richt zich op de doelwitten die waardevol voor hen (kunnen) zijn. De dreiging vanuit criminelen blijft onverminderd groot, onder meer door de schaalbaarheid van cybercrime.[220] Verdere technologische ontwikkelingen en digitalisering leiden tot groeiende aandacht van cyberactoren en een verschuiving naar andere en nieuwe waardevolle doelwitten. Door digitalisering groeit het aanvalsoppervlak en worden er nog meer aanvalsmogelijkheden gecreëerd. Digitalisering is van invloed op de hoeveelheid, de aard en de waarde van gedigitaliseerde processen, data en connecties. Zo is de verwachting dat de uitrol van 5G-netwerken leidt tot een verdere verbetering van de mogelijkheden van mobiele netwerken. Door die verbeteringen kunnen onder andere nieuwe toepassingen voor het IoT worden gerealiseerd, in bijvoorbeeld de auto-industrie, gezondheidszorg en media en entertainment. Daardoor kunnen organisaties meer processen integreren en zal meer informatie worden vergaard en verzonden via netwerken.[221] Sommige doelwitten worden daarmee nog aantrekkelijker: er is immers potentieel meer te halen of te bereiken in het geval van bijvoorbeeld sabotage. Zo is de verwachting dat de commerciële waarde van informatie die wordt verzonden via (toekomstige) 5G-netwerken sterk zal toenemen.[222] Meer gedigitaliseerde processen leiden verder tot een groter aanvalsoppervlak en dus meer mogelijkheden voor cyberactoren.

Impact uitval en storing groter

Ook de dreiging van uitval of storing neemt toe. Naarmate er meer gedigitaliseerd raakt, kan er ook meer uitvallen of in storing raken. De groeiende connectiviteit en verwevenheid van diensten spelen daarbij zeker een rol doordat er onverwachte zaken mis kunnen gaan bij bijvoorbeeld het doorvoeren van updates. De impact van uitval of een storing, zeker in vitale processen, kan groot zijn.

Kwetsbaarheden uit onverwachte hoek

Verdere digitalisering raakt ook de weerbaarheid. Er moeten nog meer en andere doelwitten worden beschermd. Ook moet rekening gehouden worden met meer misbruikmogelijkheden evenals met mogelijkheden van uitval of storing. De verdediging daartegen is

bovendien lastiger als gevolg van toenemende complexiteit en connectiviteit. Hierdoor kunnen kwetsbaarheden uit onverwachte hoek komen.

Impact aantasting integriteit van informatie

Door (onopzettelijke) storingen of het opzettelijk wijzigen van informatie (informatiemanipulatie) kan de integriteit van informatie aangetast worden. Er lijkt minder aandacht te bestaan voor deze dreigingen en manifestaties daarvan. Toch kan manipulatie in potentie zeer grote gevolgen hebben en leiden tot maatschappelijke ontwrichting. Wat zou er gebeuren wanneer eigendomsgegevens van huiseigenaren grootschalig zouden worden gemanipuleerd of gecorrumpeerd als gevolg van bijvoorbeeld een zogenoemde 'zonnestorm'? Wat zou er gebeuren wanneer saldi van bankrekeningen grootschalig zouden worden gemanipuleerd of gecorrumpeerd? Zijn de back-ups dan toereikend of zouden die ook gemanipuleerd of gecorrumpeerd kunnen zijn? Het antwoord hierop is lastig te geven. Een andere vorm van informatie- en systeemmanipulatie is de (re)productie en/of distributie van zogeheten 'deep fakes'. De mogelijkheden en de gevolgen van opzettelijke of onopzettelijke aantasting van de integriteit zijn onduidelijk, maar lijken een omvangrijke impact te kunnen hebben.

Toepassing van kunstmatige intelligentie

Eén aspect van de verdergaande digitalisering vormt de ontwikkeling en toepassing van kunstmatige intelligentie, merendeels aangeduid als Artificial intelligence (AI). Het gaat om *"[...] zelflerende systemen die zelfstandig (zonder menselijke tussenkomst) zichzelf nieuwe taken en gedrag aanleren. Systemen gaan meer patronen herkennen, menselijk gedrag interpreteren en zelf improviseren. Er komen steeds meer systemen die verantwoordelijkheid krijgen om belangrijke beslissingen te nemen op basis van hun (kunstmatige) cognitieve vaardigheden."*[223] AI-toepassingen ondersteunen bijvoorbeeld besluitvorming door mensen door afwijkende financiële transacties of personen met een verhoogd risicoprofiel te identificeren. Algoritmen kunnen ook autonoom beslissingen nemen, bijvoorbeeld in zelfrijdende auto's.

AI interessant doelwit voor kwaadwillenden

AI kan een aantrekkelijk doelwit zijn voor kwaadwillenden en dat zal alleen maar toenemen. Actoren kunnen proberen algoritmen te beïnvloeden of de data waar die mee werken. Dat zal ook de uitkomsten beïnvloeden.[224] Ontdekking van manipulatie is complex en tijdrovend. Illustratief is het voorbeeld van onderzoekers die de digitale assistenten Alexa, Siri en Google Assistant wisten te manipuleren door in een audio- of videobestand onopgemerkt een commando op te nemen. Zo kan een kwaadwillende ongemerkt een deur openen of een telefoonnummer bellen.[225]

Naast eventuele manipulatie door kwaadwillenden, kunnen de uitkomsten van AI-toepassingen soms tot onverklaarbare of onvoorspelbare resultaten leiden.[226] D66 bepleit dat er onderzoek naar eXplainable AI wordt gedaan. Dit zijn AI-systemen die hun eigen keuzes uitleggen, zodat iedereen ze kan controleren.[227] Strikt genomen vallen onverklaarbare of onvoorspelbare uitkomsten buiten de scope van cybersecurity, maar het onderwerp raakt wel aan de integriteit van processen.

AI middel in cyberaanval en verdediging

Naast doelwit, kan AI ook worden ingezet voor het uitvoeren van cyberaanvallen of juist ter verdediging ertegen. Zo kunnen kwaadwillenden algoritmen ontwikkelen om te ontdekken welke typen malware onder welke omstandigheden de grootste kans van slagen hebben. Of ze kunnen proberen met AI te ontdekken welk type gebruikers het meest ontvankelijk is voor spearphishing of zoeken naar kwetsbaarheden. AI kan daarentegen ook worden ingezet voor preventie, bescherming, detectie en respons op het gebied van cyberaanvallen. Wanneer een systeembeheerder bijvoorbeeld altijd vanaf locatie A inlogt en opeens vanaf locatie B, dan kunnen algoritmen dat ontdekken en als afwijking signaleren. Experts verwachten een wapenwedloop tussen de ontwikkeling en inzet van AI door aanvallers en verdedigers, al lijkt AI in de praktijk nog niet ingezet te worden door aanvallers.[228]

Oplopende geopolitieke spanning

Mondiaal is er sprake van oplopende spanningen tussen de grote mogendheden. Dat geldt tussen landen als de Verenigde Staten, de EU-lidstaten, de Russische Federatie en China, maar ook landen als Iran en Noord-Korea. Manifestaties daarvan zijn de toenemende assertiviteit van China en Rusland, toenemende nucleaire onzekerheid en verslechterende trans-Atlantische relaties. Bovendien is sprake van een herstructurering van de mondiale financieel-economische orde en nieuwe netwerken. Manifestaties daarvan zijn de groei van China's invloed door het zetten van mondiale standaarden, China's activisme dat een uitdaging vormt voor de politieke eenheid van de EU en het protectionisme van de VS.[229] Deze oplopende spanningen en herstructurering van de financieel-economische orde beïnvloeden cybersecurity.

Fundamentele belangentegenstellingen verhogen dreiging statelijke actoren

Fundamentele belangentegenstellingen tussen landen verhogen de dreiging die uitgaat van statelijke actoren. Het internet is immers niet alleen een technisch domein, maar ook een politiek domein met een toenemend gebruik van digitale middelen voor politieke of zelfs militaire doeleinden. Dit kan impact (nevenschade) hebben op de infrastructuur, burgers en organisaties van een land.[230]
De klassieke tweedeling tussen diplomatieke represailles of oorlogshandelingen is niet meer zwart-wit: cyberaanvallen worden gebruikt als een middel daar tussenin.

Dreiging richting waardevolle doelwitten

De dreiging zal vooral uitgaan naar specifieke doelwitten die voor statelijke actoren aantrekkelijk zijn. Te denken valt aan: sectoren met hoogwaardige kennis, overheidsonderdelen, militaire kennis en objecten, vitale processen en internationale organisaties die actief zijn in Nederland. Sommige bedrijven verwachten dat de handelsoorlog kan leiden tot een toename van diefstal van gevoelige bedrijfsinformatie door statelijke aanvallers en bedrijven, evenals verstoringsacties bij overheden en, kritieke infrastructuur en bedrijven.[231] Er moet ook rekening worden gehouden met aanvallen op doelwitten (die bijvoorbeeld personeelsgegevens beheren) die een aantrekkelijke opstap kunnen zijn voor gerichte cyberaanvallen.

Naast het aanvallen van bovenstaande doelwitten, vormen in potentie ook traditionele en sociale media een doelwit. Statelijke actoren kunnen met behulp van cyberaanvallen proberen desinformatie te (re)produceren en/of te distribueren om zo spanningen binnen of tussen landen te vergroten of het eigen land in een gunstiger daglicht te stellen. Het is voorstelbaar dat ook manipulatie van audio en/of video zijn intrede zal doen: de zogeheten 'deep fakes'.

Verschillen van inzicht over internationale normen en waarden vergroten dreiging

Terwijl het gebruik van cyberaanvallen door statelijke actoren is toegenomen, is er onvoldoende overeenstemming over de internationale normen en waarden die gelden in cyberspace. Westerse en een groeiend aantal gelijkgezinde landen gaan ervan uit dat de internationale rechtsorde zoals die geldt in de fysieke wereld ook van toepassing is in cyberspace. Een aantal niet-westerse landen streeft naar een nieuw verdragskader, wat zij kunnen proberen te beïnvloeden. Het gebrek aan overeenstemming vergroot de dreiging die uitgaat van statelijke actoren omdat staten zich niet beperkt hoeven te voelen door (geaccepteerde) normen.[232] Regulering van het internet tussen staten onderling is complex. De behoefte aan breed gedragen normen lijkt te worden gedeeld, maar de discussie is wiens normen: die van westerse landen of die van Rusland en China?[233] Naast het belang van een veilig internet, speelt ook het belang van een open en vrij internet een belangrijke rol. Sommige landen reageren op fundamenteel andere wijze op het recht op privacy en jurisdictievraagstukken met betrekking tot het behoud van het open en vrije internet.[234]

Technologische dominantie mogelijk spanningsveld

Rondom technologie en dominantie hierin is er een geopolitiek spanningsveld ontstaan. Volgens sommigen gaat achter de handelsoorlog tussen de VS en China een veel dieper gaande confrontatie schuil, namelijk een conflict over technologische dominantie.[235] Tevens bestaan er zorgen over mogelijk misbruik van producten uit verschillende landen. De laatste maanden wordt gewezen op risico's van het gebruik van producten van Chinese bedrijven, waaronder van producten van Huawei bij de ontwikkeling van 5G-netwerken. De zorgen betreffen mogelijk misbruik door de Chinese staat.[236] Het scheiden van ict-producten van landen is niet eenvoudig. Zo worden typisch Amerikaanse producten als de iPhone in China gemaakt en maakt China in ict-producten volop gebruik van chips ontworpen in de VS. Sowieso worden veel ict en onderdelen daarvan in China gefabriceerd. Doorslaggevender dan wie de assemblage doet, is wie het product gedurende de levenscyclus ondersteunt, wie er administratieve toegang toe houdt, wie de updates verzorgt en wie de ondersteuning biedt. In die gevallen bestaan meer en langduriger misbruikmogelijkheden dan tijdens de assemblage alleen.

Effect industriepolitiek op weerbaarheid

Vanwege geopolitieke ontwikkelingen kijken landen kritischer aan tegen (producten van) bedrijven uit bepaalde landen. Dat kan consequenties hebben voor weerbaarheid, hoewel een generieke beoordeling niet goed mogelijk is. Het bedrijven van 'industriepolitiek' kan de weerbaarheid positief beïnvloeden omdat mitigerende maatregelen getroffen worden. Dit maakt potentieel misbruik door statelijke actoren lastiger. Het kan ook leiden tot meer bewustzijn over risico's en mogelijk meer cybersecurity-maatregelen en/of een bewuste keuze voor meer diversiteit in aangeschafte en gebruikte producten. De industriepolitiek creëert ook onzekerheden over de betrouwbaarheid van bepaalde ict-producten. Dit kan leiden tot onverschilligheid: met alle producten kan iets mis zijn, dus kunnen we er niets aan doen. Verder is denkbaar dat kwalitatief hoogwaardiger of veiliger producten niet langer beschikbaar zijn en daardoor de weerbaarheid zou kunnen verlagen. Industriepolitiek resulteert potentieel ook in een mogelijk dilemma tussen het economisch belang op kortere termijn en het veiligheidsbelang op de langere termijn.

Versplintering internet voorstelbaar

Fundamentele verschillen in economische, politieke en militaire belangen tussen landen maken een versplintering van het internet voorstelbaar. Dat uit zich al op een aantal terreinen. Waar Noord-Korea volledig is afgesloten van het mondiale internet, is het China en Iran vooral te doen om controle over de datastromen in en uit die landen. In Rusland is wetgeving in de maak om de overheid een grotere invloed te geven op de fysieke infrastructuur van het Russische gedeelte van het internet. De EU heeft specifieke privacy-eisen geformuleerd. China stelt eisen in een nieuwe cybersecuritywet en Rusland in een privacywet. Voor internationaal opererende organisaties vormt het een uitdaging om te voldoen aan die verschillende wettelijke kaders. Dit verkleint de efficiëntie voor die organisaties en heeft op macroniveau consequenties voor de wereldwijde economie.[237] Wat een eventuele versplintering kan betekenen voor cybersecurity, laat zich lastig voorspellen. Enerzijds kan het een economisch effect hebben, anderzijds maakt het landen mogelijk minder kwetsbaar voor aanvallen.

Prikkels weerbaarheid in relatie tot de dreiging?

Het belang van digitale veiligheid voor het functioneren van onze samenleving en economie blijft substantieel toenemen. Gezien de geopolitieke ontwikkelingen is het aannemelijk dat de dreiging groter zal worden. Op deze geopolitieke ontwikkelingen alsook op de toenemende digitalisering en afhankelijkheid is door individuele organisaties relatief weinig invloed uit te oefenen.

Vanuit consumenten en toezichthouders ontstaan prikkels om cybersecurity – en als onderdeel daarvan privacy – serieuzer te nemen. Sommigen verwachten dat overheidsregulering en het publieke sentiment over privacy, drijvende krachten worden voor dataprotectie.[238]

Voor aanbieders van essentiële diensten en digitale dienstverleners geldt op grond van de Wbni ook een zorgplicht: een organisatie moet passende en evenredige organisatorische en technische maatregelen nemen om risico's voor de beveiliging van haar ict-systemen te beheersen, incidenten te voorkomen en de gevolgen van incidenten zo veel mogelijk te beperken.

Vanuit het kabinet komen daarnaast ook prikkels om cybersecurity een hogere prioriteit te (laten) geven en bijvoorbeeld prikkels tegen onveilige hard- en software. Het kabinet stelt dat onder andere versterking van de weerbaarheid van burgers en organisaties nodig is om de kansen van digitalisering te benutten.[239] Zo biedt het kabinet met de Roadmap Digitaal Veilige Hard- en Software een pakket aan maatregelen om onveiligheden in hard- en software te voorkomen, kwetsbaarheden te detecteren en om de gevolgen daarvan te mitigeren.[240]

Wake-up-calls uit het verleden

Het DigiNotar incident in 2011 was een wake-up-call voor de Nederlandse overheid als het gaat om het belang van vertrouwen in data voor de Nederlandse samenleving.[241] De hack bij KPN in 2012 schudde het management van KPN wakker omtrent het belang van cybersecurity.[242] Wannacry en NotPetya – waarvan de schade respectievelijk tussen de 4 en 8 miljard en op 10 miljard dollar wordt geschat[243] – waren een wake-up-call voor overheden en bedrijven wereldwijd.[244]

Ondanks de genoemde prikkels voor vergroting van de weerbaarheid, is het onduidelijk of deze gelijke tred houden met de dreiging en het belang. Het antwoord op de vraag in hoeverre weerbaarheid zich verhoudt tot (veranderingen in) het belang en de dreiging, is niet eenvoudig te geven.

Bijlagen

Bijlage 1
NCSC-statistieken

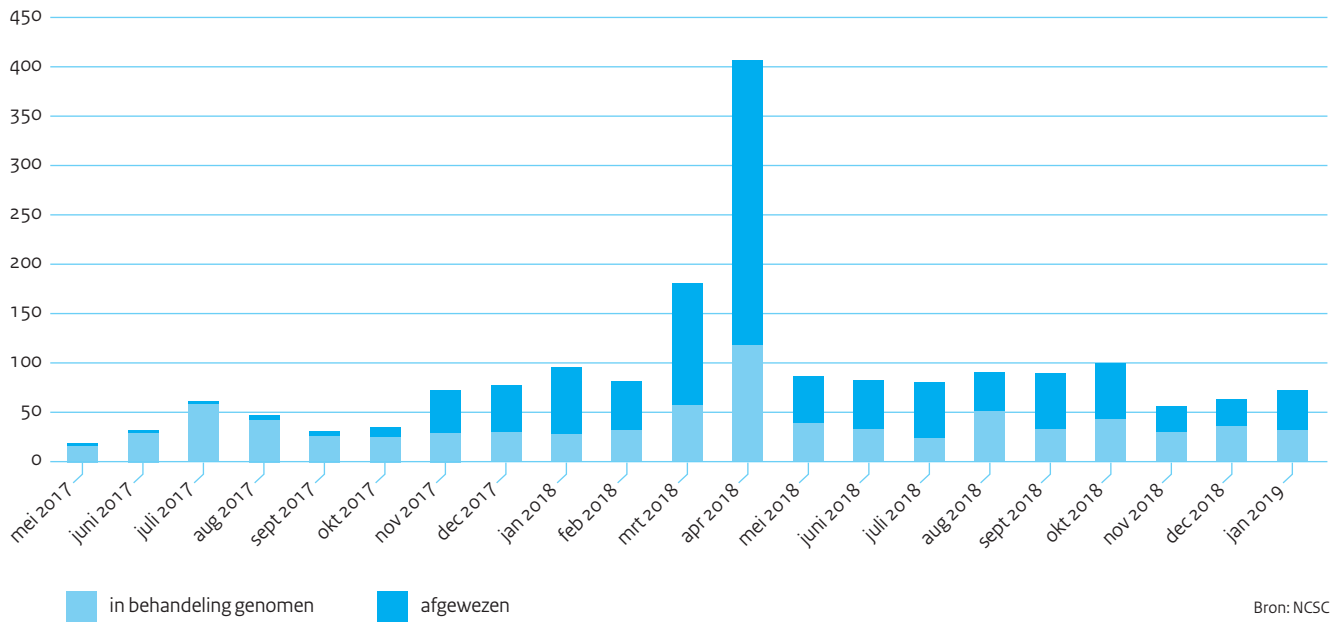
Deze bijlage geeft een globaal overzicht van de relevante meldingen en incidenten die het NCSC gedurende de rapportageperiode heeft afgehandeld. De voor de statistieken gebruikte gegevens zijn afkomstig uit de registratiesystemen van het NCSC. Tijdens deze rapportageperiode bleef het aantal cvd-meldingen ongeveer constant, maar er werden aanzienlijk meer incidentmeldingen afgehandeld.

Uit de beschikbare statistieken kunnen in beperkte mate conclusies getrokken worden: a) het aantal bij het NCSC en op het Nationaal Detectie Netwerk (NDN) aangesloten organisaties neemt in de tijd toe, waardoor een kwantitatieve vergelijking met cijfers uit het verleden niet eenduidig te maken is; b) incidentmeldingen worden op vrijwillige basis gedaan (met uitzondering van melding volgens de wettelijke meldplicht[245]), waardoor onduidelijk is hoe het aantal ontvangen meldingen zich verhoudt tot daadwerkelijke ondervonden incidenten; c) afwijkende statistieken worden vaak door meerdere factoren beïnvloed.

Cvd-meldingen blijven middel om kwetsbaarheden te detecteren

Het NCSC ontvangt en verwerkt cvd-meldingen (Coordinated Vulnerability Disclosure) voor zowel haar eigen infrastructuur als die van de Rijksoverheid. Hiermee kunnen melders conform het cvd-beleid[246] systeemeigenaren attenderen op ontdekte zwakke plekken in hun ICT-systemen (en met name websites). Melders van relevante en tot dan toe onbekende beveiligingsproblemen ontvangen hiervoor een blijk van waardering als dank voor de hulp.

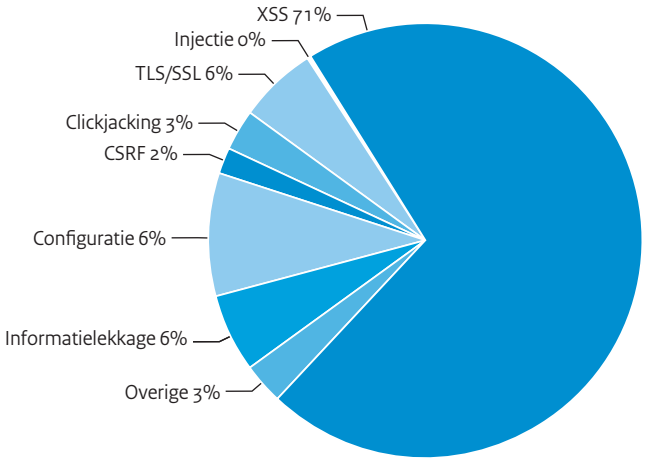
Figuur 4 **Aantal cvd-meldingen per maand**



Bron: NCSC

In vergelijking met de voorgaande rapportageperiode is het aantal cvd-meldingen ongeveer gelijk gebleven. Na een sterke piek in maart en april 2018 zijn ze terug op het niveau van de maanden daarvoor. Het in de vorige periode sterk toegenomen percentage afgewezen meldingen, bijvoorbeeld omdat verificatie van het gemelde probleem geen resultaat opleverde of het een al bekend probleem betrof, is deze periode niet verder gestegen maar blijft wel onverminderd hoog.

Figuur 5 **Typen cvd-meldingen**



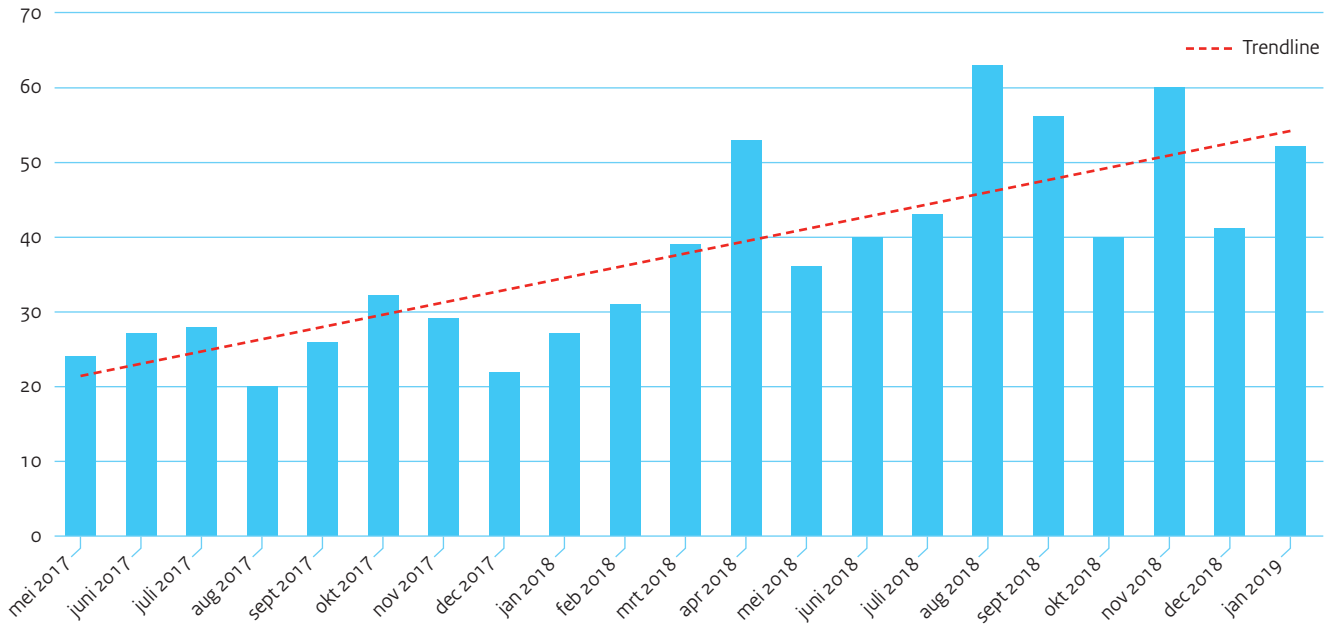
Bron: NCSC

Stijging aantal afgehandelde incidenten

Het NCSC ondersteunt de Rijksoverheid en organisaties in vitale processen bij het afhandelen van incidenten op het gebied van cybersecurity. Organisaties melden incidenten en kwetsbaarheden bij het NCSC. Het NCSC identificeert deze zelf ook, bijvoorbeeld op basis van detectiemechanismen en eigen onderzoek. Daarnaast acteert het NCSC op verzoek van (inter)nationale partijen richting Nederlandse internetserviceproviders om hen te ondersteunen bij het bestrijden van cyberincidenten die hun oorsprong vinden in Nederland (bijvoorbeeld vanaf een malafide webserver of vanaf geïnfecteerde computers in Nederland).

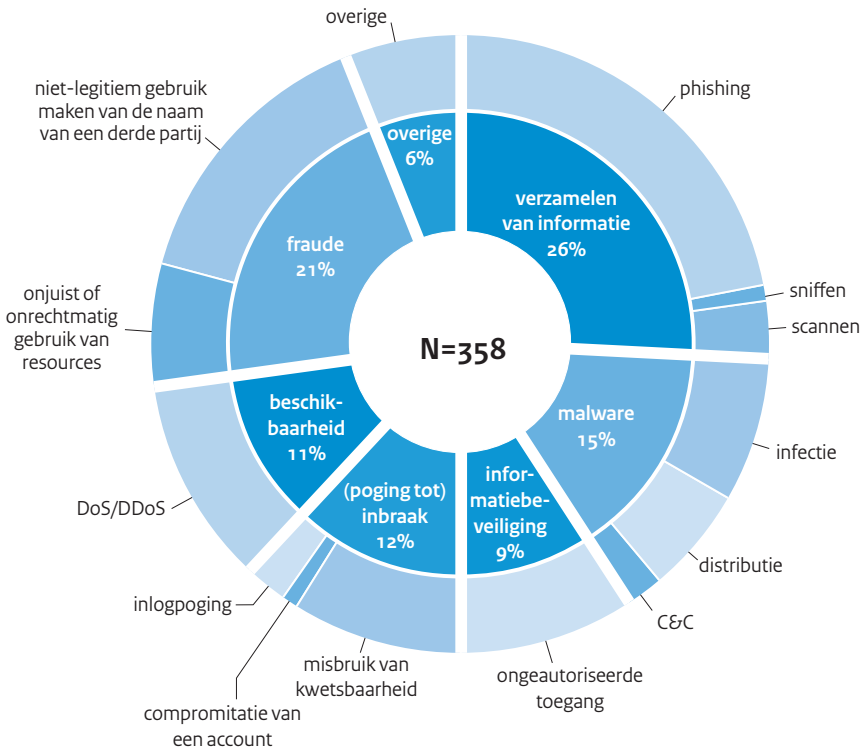
Het aantal geregistreerde en afgehandelde incidenten tijdens de rapportageperiode lag op een gemiddelde van 48 incidenten per maand. Dit is een groei van ruim 50% ten opzichte van de vorige periode, toen de trend nog licht dalend was. Dit wordt met name veroorzaakt doordat er meer organisaties bij het NCSC zijn aangesloten, maar ook omdat organisaties incidenten eerder lijken te melden. Vanuit de wettelijke meldplicht is gedurende de rapportageperiode 1 melding gedaan door een organisatie vanuit een vitale sector. Het betrof een incident waarbij potentieel grenswaarden voor het doen van een melding konden worden overschreden, maar dit uiteindelijk niet is gebeurd.
De belangrijkste verschuivingen in de verdeling tussen type incidenten ten opzichte van de vorige periode betreffen een afname van malwaremeldingen en een toename van het aantal fraude gerelateerde meldingen.

Figuur 6 **Afgehandelde incidenten (exclusief geautomatiseerde controles)**



Bron: NCSC

Figuur 7 **Verdeling per incidentklasse**



Bron: NCSC

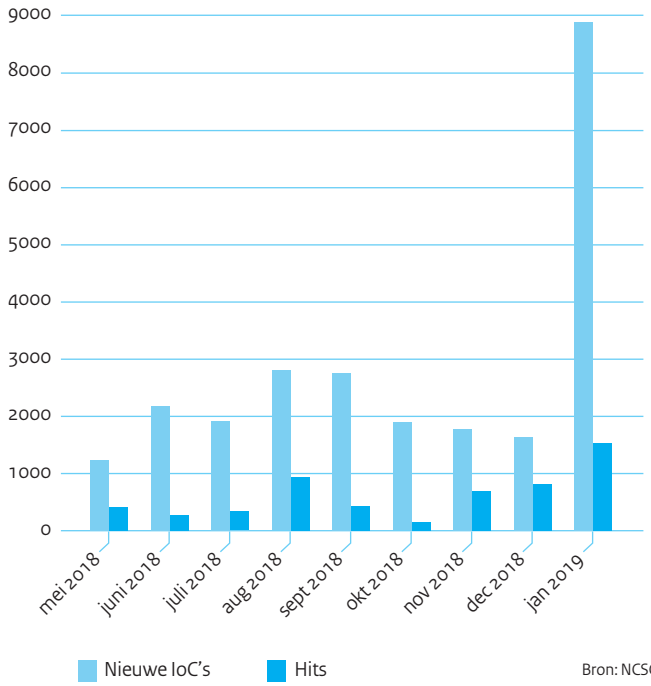
Ten aanzien van malware-incidenten valt met name op dat het aantal meldingen van infecties aanzienlijk is teruggelopen. Detectie en mitigatie wordt gemeengoed en minder snel gemeld. De geautomatiseerde meldingen van besmettingen, die niet in dit overzicht zijn meegenomen, zijn de afgelopen periode niet gewijzigd ten opzichte van voorgaande periode.

De groei aan fraude-incidenten zit vooral in een toename van gemelde phishingcampagnes en daaraan gekoppelde verzoeken om bij deze campagnes gebruikte servers uit de lucht te halen. Het label 'fraude' heeft hierbij betrekking op het onrechtmatig gebruik van organisatienamen bij het verzenden van phishingmails.

Meer aansluitingen op Nationaal Detectie Netwerk

Het Nationaal Detectie Netwerk (NDN) is een samenwerking voor het beter en sneller waarnemen van digitale dreigingen en risico's. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijkheid tijdig gepaste maatregelen nemen om mogelijke schade te beperken of voorkomen. Binnen het NDN worden 'indicators of compromise' (IoC's) gedeeld met

Figuur 8 **Nieuwe IoC's en Hits**



Bron: NCSC

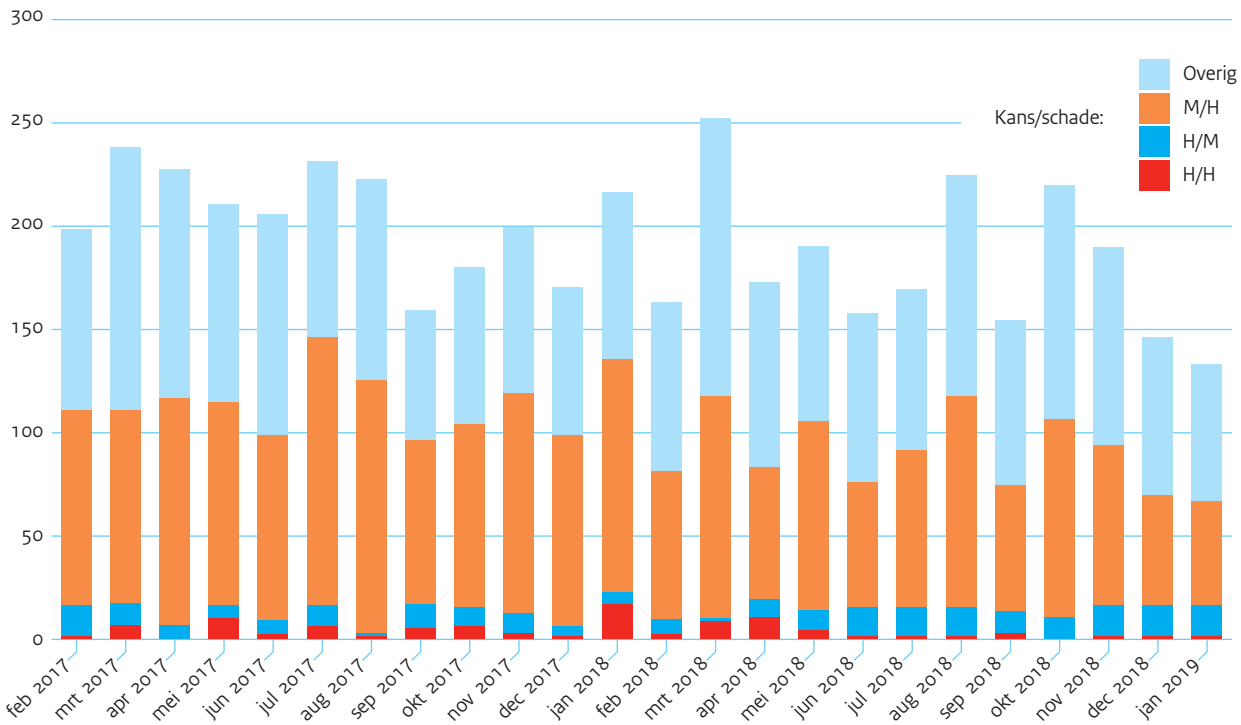
deelnemende partijen. Een IoC is informatie die kan helpen bij het identificeren van specifiek malafide gedrag op een systeem of binnen een netwerk, zoals ip-adressen of domeinnamen. In het geval dat een gedeelde IoC leidt tot het waarnemen van malafide gedrag bij een deelnemende partij, is er sprake van een 'hit'.

Een hit geeft alleen aan dat er gedrag waargenomen is dat overeenkomt met de gedeelde informatie. Dit zegt echter niet dat een deelnemende partij per se is gecompromitteerd. Als een defensieve maatregel, zoals een firewall, antivirus of intrusion detection system (IDS) de malafide software of netwerkverkeer tegenhoudt, wordt dit als een hit geregistreerd terwijl geen werkelijke besmetting plaats heeft gevonden. In januari 2019 is een aantal nieuwe partijen aangesloten op het MISP-platform waarmee IoC's worden gedeeld, wat heeft geleid tot een piek in nieuwe indicatoren en aanzienlijk meer hits dan in de voorgaande maanden.

Iets minder beveiligingsadviezen uitgebracht

Het NCSC publiceert beveiligingsadviezen naar aanleiding van software- en hardware-kwetsbaarheden of geconstateerde dreigingen. In een beveiligingsadvies wordt beschreven wat er aan de hand is, welke systemen getroffen zouden kunnen zijn en wat er moet gebeuren om te voorkomen dat een kwetsbaarheid wordt misbruikt. De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen. Ten eerste stelt men vast wat de kans is dat de kwetsbaarheid misbruikt wordt. Ten tweede bepaalt men de schade die optreedt wanneer dat gebeurt. Voor beide criteria (kans en schade) wordt, op basis van meerdere aspecten, een niveau ingeschat: hoog (H), gemiddeld (M) of laag (L). In onderstaande figuur zijn de uitgebrachte beveiligingsadviezen in deze en vorige rapportageperiode in kaart gebracht, waarbij de hoeveelheid hoog ingeschaalde beveiligingsadviezen (H/H, M/H en H/M) separaat is getoond. De hoeveelheid uitgebrachte beveiligingsadviezen is de afgelopen periode licht gedaald waarbij met name het aantal H/H-adviezen is teruggelopen.

Figuur 9 **Uitgebrachte beveiligingsadviezen**



Bron: NCSC

Bijlage 2
Afkortingen- en begrippenlijst

0-day	Zie Zero-daykwetsbaarheid.
Aanval	Een digitale aanval is een opzettelijke inbreuk op cybersecurity.
Aanvalsfacilitator	Actor die middelen en infrastructuur ontwikkelt en uitbaat om tegen betaling andere actoren in staat te stellen digitale aanvallen uit te voeren.
Actor	Persoon, groep of organisatie die een dreiging vormt.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst.
AP	Autoriteit Persoonsgegevens.
Authenticatie	Het vaststellen van de identiteit van een gebruiker, computer of applicatie.
Beschikbaarheid	Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Bitcoin	Digitale munteenheid, zie cryptovaluta.
Botnet	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Clouddienst	Ict-infrastructuur die via het internet beschikbaar wordt gesteld als dienst.
Crimineel	Actor die aanvallen pleegt met economische of financiële motieven.
Cryptojacking	Het (zonder medeweten van de eigenaar) gebruiken van de rekenkracht van systemen om cryptovaluta te delven.
Cryptomining	Het delven van cryptovaluta door het uitvoeren van cryptografische berekeningen.
Cryptovaluta	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties.
Cvd	Coordinated vulnerability disclosure is de praktijk van het gecoördineerd melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans neerkomen op dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen. Voorheen werd dit responsible disclosure genoemd.

Cybercrime	Vorm van criminaliteit gericht op ict of de informatie die een ict-systeem verwerkt. Er zijn verschillende soorten cybercrime: • in enge zin, een vorm van criminaliteit met ict als doelwit (high tech crime); • een vorm van criminaliteit waarbij voor de uitvoering het gebruik van ict van overwegende betekenis is (cybercriminaliteit); • in brede zin, iedere vorm van (traditionele) criminaliteit waarbij gebruik wordt gemaakt van ict (gedigitaliseerde criminaliteit).
Cybercrime-as-a-service (Caas)	Cybercrime-as-a-service is een werkwijze in de ondergrondse economie waarbij actoren gebruik kunnen maken van de (betaalde) diensten van aanvalsfacilitatoren om aanvallen te plegen.
Cybervandaal	Zie scriptkiddie.
Cybersecurity	Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ict te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.
DDoS	Distributed Denial of Service is een vorm van Denial-of-Service waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen.
Defacement	Een defacement (of bekladding) is het vervangen van een webpagina met de boodschap dat deze gehackt is, eventueel met aanvullende boodschappen van activistische, idealistische of aanstootgevende aard.
DKIM	DomainKeys Identified Mail is een protocol om legitieme e-mail door de verzendende e-mailserver digitaal te laten ondertekenen. De eigenaar van het verzendende domein publiceert legitiem sleutels in een DNS-record.
DMARC	Domain-based Message Authentication, Reporting and Conformance is een protocol waarmee de eigenaar van een domein aangeeft wat er met niet-authentieke e-mail vanaf zijn domein moet gebeuren. De authenticiteit van de e-mail wordt eerst vastgesteld aan de hand van SPF en DKIM. De domeineigenaar publiceert het gewenste beleid in een DNS-record.
DNS	Het Domain Name System is het systeem dat internetdomeinnamen koppelt aan ip-adressen en omgekeerd. Zo staat het adres www.ncsc.nl bijvoorbeeld voor ip-adres 159.46.193.36. Verder vermeldt een DNS-record onder meer hoe e-mails aan dat domein afgehandeld moeten worden.
DoS	Denial of Service is de benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar maakt voor de gebruikelijke afnemers. Bij websites wordt meestal een DDoS-aanval uitgevoerd.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
Exploit	Software, gegevens of een opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies of gedrag te veroorzaken.
Exploitkit	Hulpmiddel om een aanval op te zetten door te kiezen uit kant-en-klare exploits, in combinatie met gewenste gevolgen en besmettingsmethode.

Hacker/Hacken	De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in ict-systemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder software), veelal om beperkingen te omzeilen of onverwachte effecten te bereiken.
Hacktivist	Samentrekking van hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt.
ICS	Industriële controlesystemen zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten.
Incident	Een incident is een gebeurtenis waarbij informatie, informatiesystemen of -diensten verstoord worden, uitvallen of misbruikt worden.
Informatiebeveiliging	Informatiebeveiliging is het proces van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiediefstal	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
Informatiemanipulatie	Het opzettelijk wijzigen van informatie; aantasting van de integriteit van informatie.
Injectie	Aanvalstechniek waarbij gebruikersinvoer wordt gemanipuleerd om naast gegevens ook systeemopdrachten te bevatten. SQL-injectie wordt vaak gebruikt om communicatie tussen een applicatie en de achterliggende database te beïnvloeden, om gegevens te manipuleren of stelen.
Insider	Een interne actor die met toegang tot systemen of netwerken van binnenuit een dreiging vormt, met als motief wraak, geldelijk gewin of ideologie. Een insider kan ook worden ingehuurd of opgedragen van buitenaf.
Integriteit	Integriteit omhelst het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.
IoT	Het internet of things is een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.
IP	Het internetprotocol zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.
Kwetsbaarheid	Eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans geeft om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden, of om die ongeautoriseerd te benaderen.
Lek	Aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.
Malware	Samentrekking van malicious software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.
Middel	Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten.

MIVD	Militaire Inlichtingen- en Veiligheidsdienst.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie van mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld fraude of identiteitsdiefstal.
Ransomware	Gijzelsoftware. Type malware dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.
Sabotage	Het opzettelijk, zeer langdurig, aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten. In extreme gevallen leidend tot vernietiging.
Scriptkiddie	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen, om kwetsbaarheden aan te tonen of voor de eigen uitdaging.
Spam	Ongewenste e-mail, doorgaans commercieel van aard.
Spearphishing	Spearphishing is een variant van phishing die zich richt op één persoon of beperkte groep mensen, die specifiek wordt uitgekozen op basis van hun toegangspositie, om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.
SPF	Sender Policy Framework is een protocol waarmee de eigenaar van een domeinnaam aangeeft welke servers er legitiem e-mail namens zijn domein mogen versturen. De domeinnaameigenaar publiceert de lijst met geautoriseerde servers in een DNS-record.
Spionage	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
Staatsgelieerde actor	Actor gelieerd aan een statelijke actor.
Statelijke actor	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).
Storing	Zie uitval of verstoring.
Systeemmanipulatie	Het aantasten van informatiesystemen en -diensten gericht op de vertrouwelijkheid of integriteit van informatiesystemen en -diensten. Deze systemen of diensten worden daarna ingezet om andere aanvallen uit te voeren.
Terrorist	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angst wil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.
Trojan	Type malware dat heimelijk toegang tot een systeem biedt aan een aanvaller via een achterdeur.
Tweefactorauthenticatie	Een manier van identiteit vaststellen waarvoor twee onafhankelijke bewijzen van identiteit zijn vereist.
Uitval	Aantasting van de integriteit en beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.

Verstoring	Het opzettelijk, tijdelijk, aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
Vertrouwelijkheid	Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd.
Wiperware	Type malware dat sabotage pleegt door gegevens te verwijderen of permanent ontoegankelijk te maken.
Worm	Type malware dat zichzelf automatisch verspreidt onder andere systemen.
Zero-daykwetsbaarheid	Een zero-daykwetsbaarheid is een kwetsbaarheid waarvoor nog geen patch beschikbaar is, omdat de maker van de kwetsbare software nog geen tijd (nul dagen) heeft gehad om de kwetsbaarheid te verhelpen.

Bijlage 3
Bronnen en referenties

1 Nederlandse Cybersecurity Agenda 2018.
2 NCTV, *Cybersecuritybeeld Nederland 2018*, juni 2018. https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf.
3 AIVD, *Jaarverslag 2018*, april 2019.
4 NCTV, *Cybersecuritybeeld Nederland 2018*, juni 2018. https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf.
5 ENISA, *ENISA Threat Landscape Report 2018* (2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 .
6 *Anonymous defaced Russia govt website against Telegram ban*, Security Affairs 16-05 2018. https://securityaffairs.co/wordpress/72567/hacktivism/anonymous-hask-russia-site.html geraadpleegd 04-02 2019.
7 *DDOS on Bank of Spain Claimed by Anonymous Catalonia*, Latest Hacking News 03-09 2018https://latesthackingnews.com/2018/09/03/ddos-on-bank-of-spain-claimed-by-anonymous-catalonia/ geraadpleegd 11-02 2019.
8 *Flink meer DDoS-aanvallen, 'vaak jongeren vanaf hun zolderkamer'*, NOS.nl 06-01 2019. https://nos.nl/artikel/2266370-flink-meer-ddos-aanvallen-vaak-jongeren-vanaf-hun-zolderkamer.html geraadpleegd 04-02 2019.
9 *Banken waren opnieuw doelwit van ddos-aanval*, Tweakers 28-05 2018 https://tweakers.net/nieuws/139053/banken-waren-opnieuw-doelwit-van-ddos-aanval.html geraadpleegd 04-02 2019.
10 *DDoS-aanval belasting en douane*, NOS.nl 10-05 2019. https://nos.nl/artikel/505247-ddos-aanval-belasting-en-douane.html geraadpleegd 04-02 2019.
11 *Kort problemen met website DigiD door DDoS-aanval*, NOS.nl 31-07 2018. https://nos.nl/artikel/2244007-kort-problemen-met-website-digid-door-ddos-aanval.html geraadpleegd 04-02 2019.
12 *PyCryptoMiner botnet, a new Crypto-Miner Botnet spreads over SSH*, Security Affairs 05-01 2018. http://securityaffairs.co/wordpress/67408/breaking-news/pycryptominer-botnet-miner.html geraadpleegd 04-02 2019.
13 ENISA, *ENISA Threat Landscape Report 2018* (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.
14 *Cryptominer infecteert 157.000 ongepatchte MikroTik-routers*, Security.nl 15-08 2018. https://www.security.nl/posting/573546/Cryptominer+infecteert+157_000+ongepatchte+MikroTik-routers geraadpleegd 11-02 2019.
15 Trend Micro, *Unseen Threats and Imminent Losses: Midyear Security Roundup 2018* (2018).https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf
16 Radhesh Krishnan Konoth, Emanuele Vineti, Veelasha Moonsamy, Martina Lindorfer, Christopher Kruegel, Herbert Bos, and Giovanni Vigna, 'MineSweeper: An In-depth Look into Drive-by, Cryptocurrency Mining and Its Defense', *CCS '18: 2018 ACM SIGSAC Conference on Computer &Communications Security Oct. 15–19, 2018, Toronto, ON, Canada* (2018). https://www.cs.vu.nl/~herbertb/download/papers/minesweeper_ccs18.pdf.
17 Jaarverantwoording politie 2018, mei 2019
18 *National Security Council cyber chief: Criminals are closing the gap with nation-state hackers*, 25-04-2019, https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/
19 *3,81 miljoen euro schade door phishing bij internetbankieren in 2018 - Minder fraude met betaalpassen en automatische incasso's*, 27-3-2019, https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/, geraadpleegd 27-3-2019.
20 Cyber Edge Group, *2018 Cyberthreat Defense Report: North America, Europe, Asia Pacific, Latin America, Middle East, Africa* (2018). https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf.
21 DNI, *Worldwide Threat Assessment of the U.S. Intelligence Community 2019* (2019).https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

22 N. Perlroth en C. Krauss, 'A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try', *The New York Times* 15-03 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html geraadpleegd 04-02 2019.

23 A. Shalal, 'Germany concerned about possible 'sleeper' cyber sabotage', Reuters 04-09 2018. https://www.reuters.com/article/us-germany-security/germany-concerned-about-possible-sleeper-cyber-sabotage-idUSKCN1LK1DX geraadpleegd 11-02 2019.

24 AIVD, *Jaarverslag 2018*, april 2019.

25 *GreyEnergy groep richt zich op vitale infrastructuur, mogelijk in voorbereiding op schadelijke aanvallen*, ESET 17-10 2018. https://www.eset.com/nl/over/newsroom/persberichten-overzicht/persberichten/greyenergy-groep-richt-zich-op-vitale-infrastructuur/ geraadpleegd 11-02 2019.

26 A. Greenberg,'Crash Override': The Malware That Took Down a Power Grid', *WIRED* 12-06 2017. https://www.wired.com/story/crash-override-malware/ geraadpleegd 11-02 2019.

27 C. Osborne, 'Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout', *Zero Day* via *ZDNet* 30-04 2018. https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/ geraadpleegd 11-02 2019.

28 J. Stubbs, 'Hackers accused of ties to Russia hit 3 E.European companies- cybersecurity firm', *Reuters* 17-10 2018. https://www.reuters.com/article/russia-cyber/hackers-accused-of-ties-to-russia-hit-3-eeuropean-companies-cybersecurity-firm-idUSL8N1WP37F geraadpleegd 14-02 2019.

29 S. Jewkes en J. Finkle, 'Saipem says Shamoon variant crippled hundreds of computers', *Reuters* 12-12 2018. https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA geraadpleegd 14-02 2019.

30 A. Shalal, 'Germany concerned about possible 'sleeper' cyber sabotage', *Reuters* 04-09 2018. https://www.reuters.com/article/us-germany-security/germany-concerned-about-possible-sleeper-cyber-sabotage-idUSKCN1LK1DX geraadpleegd 11-02 2019.

31 A. Shalal, 'Germany concerned about possible 'sleeper' cyber sabotage', *Reuters* 04-09 2018. https://www.reuters.com/article/us-germany-security/germany-concerned-about-possible-sleeper-cyber-sabotage-idUSKCN1LK1DX geraadpleegd 11-02 2019.

32 AIVD, *Jaarverslag 2018*, april 2019.

33 AIVD, *Jaarverslag 2018*, april 2019.

34 AIVD, *Jaarverslag 2018*, april 2019.

35 De dreigingsmatrix is wederom gebaseerd op de actortypologie in: M. de Bruijne, M. van Eeten, C. Hernandez Ganan, W. Pieters, *Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment* (TU Delft 2017).

36 DNI, *Worldwide Threat Assessment of the U.S. Intelligence Community 2019* (2019) https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

37 AIVD, *Jaarverslag 2018*, april 2019.

38 ENISA, *ENISA Threat Landscape Report 2018* (2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 .

39 Jaarverantwoording politie 2018, mei 2019

40 Sophos, *Sophoslabs 2019 Threat Report* (2018) https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-2019-threat-report.pdf.

41 NCTV, *Cybersecuritybeeld Nederland 2018*, juni 2018 (https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf).

42 FireEye, *Facing Forward: Cyber Security in 2019 and Beyond* (2018) https://content.fireeye.com/predictions/rpt-security-predictions-2019.

43 I. Arghire, 'Supply Chain Attacks Nearly Doubled in 2018: Symantec', *SecurityWeek* 20-02 2019https://www.securityweek.com/supply-chain-attacks-nearly-doubled-2018-symantec geraadpleegd 24-02 2019.

44 B. Barrett, 'How China's Elite Hackers Stole the World's Most Valuable Secrets', *WIRED* 20-12 2018. https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/ geraadpleegd 24-02 2019.

45 Stilgherrian, 'At least nine global MSPs hit in APT10 attacks: ACSC', *ZDNet* 21-12 2018. https://www.zdnet.com/article/at-least-nine-global-msps-hit-in-apt10-attacks-acsc/ geraadpleegd 24-02 2019.

46 M. Hirani, S. Jones en B. Read, 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', *FireEye Threat Research* 09-01 2019. https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html geraadpleegd 24-02 2019.

47 AIVD, *Jaarverslag 2018*, april 2019.

48 L. van Lonkhuyzen en V. Sondermeijer, 'MIVD verijdelde Russische cyberaanval op OPCW in Den Haag', *NRC.nl* 04-10 2018. https://www.nrc.nl/nieuws/2018/10/04/mivd-verijdelde-russische-cyberaanval-op-opcw-in-den-haag-a2186350 geraadpleegd 24-02 2019.

49 A. Greenberg, How Russian Spies Infiltrated Hotel Wi-Fi to Hack Victims Up Close', 04-10 2018. https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/ geraadpleegd 24-02 2019.

50 Rijksoverheid (2018) https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/11/19/aanbiedingsbrief-bij-defensie-cyber-strategie/Kamerbrief+MinDef+aanbieding+Defensie+Cyber+Strategie.pdf.

51 G Myre, The U.S. Pledges A Harder Line In Cyberspace — And Drops Some Hints, 26-3-2019, https://www.npr.org/2019/03/26/705822275/the-u-s-pledges-a-harder-line-in-cyberspace-and-drops-some-hints?t=1553760003987 geraadpleegd 28-03-2019.
52 NCTV, *Cybersecuritybeeld Nederland 2018*, juni 2018 (https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf)
53 *Flink meer DDoS-aanvallen, 'vaak jongeren vanaf hun zolderkamer*, NOS.nl 06-01 2019. https://nos.nl/artikel/2266370-flink-meer-ddos-aanvallen-vaak-jongeren-vanaf-hun-zolderkamer.html geraadpleegd 04-02 2019.
54 *Schade banken door phishing neemt explosief toe*, NOS.nl 27-03 2019. https://nos.nl/artikel/2277755-schade-banken-door-phishing-neemt-explosief-toe.html geraadpleegd 27-03 2019.
55 *Phishing weer groeiend probleem, oplichters steeds creatiever*, NOS.nl 25-11 2018. https://nos.nl/artikel/2260753-phishing-weer-groeiend-probleem-oplichters-steeds-creatiever.html geraadpleegd 11-02 2019.
56 Jaarverantwoording politie 2018, mei 2019
57 *National Security Council cyber chief: Criminals are closing the gap with nation-state hackers*, 25-04-2019, https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/
58 *3,81 miljoen euro schade door phishing bij internetbankieren in 2018 - Minder fraude met betaalpassen en automatische incasso's*, 27-3-2019, https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/, geraadpleegd 27-3-2019.
59 Banken waren opnieuw doelwit van ddos-aanval, *Tweakers* 28-05 2018. https://tweakers.net/nieuws/139053/banken-waren-opnieuw-doelwit-van-ddos-aanval.html geraadpleegd 04-02 2019.
60 *DDoS-aanval belasting en douane*, NOS.nl 10-05 2019. https://nos.nl/artikel/505247-ddos-aanval-belasting-en-douane.html geraadpleegd 04-02 2019.
61 *Kort problemen met website DigiD door DDoS-aanval*, NOS.nl 31-07 2018. https://nos.nl/artikel/2244007-kort-problemen-met-website-digid-door-ddos-aanval.html geraadpleegd 04-02 2019.
62 *Opnieuw DDoS-aanval op website DigiD*, NOS.nl 01-08 2018. https://nos.nl/artikel/2244113-opnieuw-ddos-aanval-op-website-digid.html geraadpleegd 04-02 2019.
63 Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 23.
64 *Oorzaak computerstoring treinverkeersleiding gevonden*, ProRail 22-08 2018. https://prorail.nl/nieuws/oorzaak-computerstoring-treinverkeersleiding-gevonden geraadpleegd 24-02 2019.
65 *2019 Forcepoint Cybersecurity Predictions Report*, Forcepoint, 13-11-2018https://www.forcepoint.com/sites/default/files/resources/files/report-2019-cybersecurity-predictions-en.pdf.
66 https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/
67 *Kaspersky Security Bulletin*: THREAT PREDICTIONS FOR 2019, Kaspersky Lab, 16-11-2018 https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878
68 Ministerie van Economische Zaken en Klimaat, *Nederlandse digitaliseringsstrategie* (juni 2018).
69 Kabinet stopt EUR 165 miljoen in agenda digitale overheid, *Digitaleoverheid.nl* 17-08 2018. https://www.digitaleoverheid.nl/nieuws/kabinet-stopt-eur-165-miljoen-in-agenda-digitale-overheid/ geraadpleegd 25-01-2019.
70 VWS trekt zestig miljoen euro uit voor digitale zorg, *Computable.nl* 19-9-2018 https://www.computable.nl/artikel/nieuws/overheid/6458649/250449/vws-trekt-zestig-miljoen-euro-uit-voor-digitale-zorg.html geraadpleegd 25-1-2019.
71 Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 23.
72 *Resultaten self-assessment intersectorale afhankelijkheden*, TNO en Ministerie van Justitie en Veiligheid, 6-3-2019
73 *Wat te doen als alles instort?*, De Telegraaf 25-09 2018.
74 Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force* (november 2018), p. 32.
75 Wouter van Noort, Een voor een springen alle schermen op zwart, *NRC* (06-10-2018).
76 Agentschap Telecom, Verslag '*Opstap naar weerbaarheid in een digitale samenleving*', (29-11-2018). https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2018/11/29/verslag-en-presentaties-opstap-naar-weerbaarheid-in-een-digitale-samenleving/Verslag+website+def.pdf geraadpleegd 28-1-2019.
77 Wat te doen als alles instort?, *De Telegraaf* 25-09 2018.
78 https://www.leidschdagblad.nl/cnt/dmf20190212_7504697/digitale-oorlog-minstens-zo-destructief?utm_source=google&utm_medium=organic.
79 https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.
80 5G networks raise China espionage fears, The Washington Times 04-01-2019. https://www.washingtontimes.com/news/2019/jan/3/5g-networks-raise-china-espionage-fears/ geraadpleegd 6-2-2019.

81 G20: meer inzicht nodig in invloed digitale platforms op bedrijven en consumenten, Rijksoverheid.nl 25-08-2018. https://www.rijksoverheid.nl/actueel/nieuws/2018/08/25/g20-meer-inzicht-nodig-in-invloed-digitale-platforms-op-bedrijven-en-consumenten geraadpleegd 6-2-2019. Kabinet wil meer inzicht in invloed van digitale platformen, Security.nl, 26-08-2018. https://www.security.nl/posting/574726/Kabinet+wil+meer+inzicht+in+invloed+van+digitale+platformen geraadpleegd6-2-2019.

82 Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 23-24.

83 Het Analistennetwerk Nationale Veiligheid noemt Israël als derde land.

84 Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 24.

85 *Welke deuren zet een topdeal met China open?*, De Volkskrant, 16-10-2018, Chinese 'playbook' alarms FBI, Washington Post, 13-12-2018, Laurens Cerulus, China's ghost in Europe's telecom machine, Politico, 11-12-2017 (updated 28-1-2018).

86 *Europa overtuigen om geen Huawei te kopen 'topprioriteit' voor VS*, Nu.nl, 5-2-2019 geraadpleegd 6-2-2019.

87 *VS waarschuwt bondgenoten voor samenwerking met Huawei*, NOS, 11-3-2019. https://nos.nl/artikel/2275571-vs-waarschuwt-bondgenoten-voor-samenwerking-met-huawei.html.

88 Ministerie van Economische Zaken en Klimaat, *Nederlandse digitaliseringsstrategie* (juni 2018), p. 34-36.

89 Joost Witteman, Erik Brouwer, Tom Smits, *Data zijn geen productiefactor, maar wel productiviteitsverhogend* in Economisch Statistische Berichten, Verplichte datadeling, jaargang 103 (5-7-2018) p. 294-297.

90 NCTV, *Cybersecuritybeeld Nederland 4*, 2014.

91 *Duitse toezichthouder gaat dataverzameling Facebook aanpakken*, Security.nl 14-01-2019. https://www.security.nl/posting/594076/%22Duitse+toezichthouder+gaat+dataverzameling+Facebook+aanpakken%22 geraadpleegd 5-2-2019. Zie ook: Facebook gaf bedrijven toegang tot privéberichten gebruikers, Security.nl 19-12-2018. https://www.security.nl/posting/591518/%22Facebook+gaf+bedrijven+toegang+tot+priv%C3%A9berichten+gebruikers%22geraadpleegd 5-2-2019.

92 *New study: Google manipulates users into constant tracking*, Forbrukarrådet 27-11-2018. https://www.forbrukerradet.no/forside/om-oss/ geraadpleegd 5-2-2019, 50.000 Nederlanders tekenen petitie tegen locatie-opslag Google, Security.nl, 22-01-2019.https://www.security.nl/posting/594944/50_000+Nederlanders+tekenen+petitie+tegen+locatie-opslag+Google geraadpleegd 5-2-2019.

93 *'Facebook riskeert in VS miljardenboete om privacyschendingen'*, Nu.nl, 15-2-2019 https://www.nu.nl/internet/5744283/facebook-riskeert-in-vs-miljardenboete-om-privacyschendingen.html geraadpleegd 16-2-2019.

94 *Facebook staat toe advertenties te richten op vaccinatieweigeraars*, NOS.nl, 16-2-2019 https://nos.nl/artikel/2272187-facebook-staat-toe-advertenties-te-richten-op-vaccinatieweigeraars.html geraadpleegd 16-2-2019.

95 *Felle Britse kritiek op socialemediabedrijven*, De Volkskrant, 18-2-2019.

96 NCTV, *Cybersecuritybeeld Nederland 2018*, juni 2018 (https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf) geraadpleegd 6-2-2019.

97 *GreyEnergy: Updated arsenal of one of the most dangerous threat actors*, ESET, 17-10-2018 https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/ geraadpleegd 6-2-2019.

98 *Analysis of the Cyber Attack on the Ukrainian Power Grid*, sans.org, 18-3-2016 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf geraadpleegd 6-2-2019.

99 *Cyber-Angriffe auf deutsche Energieversorger*, bsi.bund.de, 13-6-2018 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html geraadpleegd 6-2-2019.

100 *GRIZZLY STEPPE - Russian Malicious Cyber Activity*, us-cert.gov, December 2016 https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity geraadpleegd 6-2-2019.

101 *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, us-cert.gov, 15-3-2018 https://www.us-cert.gov/ncas/alerts/TA18-074A geraadpleegd 6-2-2019.

102 *HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, citizenlab.ca, 18-9-2018 https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ geraadpleegd 4-3-2019.

103 *Inside the uae's secret hacking team of american mercenaries*, Reuters.com, 30-1-2019 https://www.reuters.com/investigates/special-report/usa-spying-raven/ geraadpleegd 4-3-2019.

104 *Inside the uae's secret hacking team of american mercenaries*, Reuters.com, 30-1-2019 https://www.reuters.com/investigates/special-report/usa-spying-raven/ geraadpleegd 4-3-2019.

105 *UAE used cyber super-weapon to spy on iphones of foes*, Reuters.com, 30-1-2019 https://www.reuters.com/investigates/special-report/usa-spying-karma/ geraadpleegd 4-3-2019.

106 *Jaarverslag AIVD 2017*, aivd.nl, 6-3-2018https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2018/03/06/jaarverslag-aivd-2017/Jaarverslag+AIVD+2017.pdf geraadpleegd 4-2-2019.

107 *Joint report on publicly available hacking tools*, ncsc.gov.uk, 11-10-2018 https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf geraadpleegd 4-2-2019.
108 *Gallmaker: New Attack Group Eschews Malware to Live off the Land*, Symantec.com, 10-10-2018 https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group geraadpleegd 4-2-2019.
109 *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, Bloomberg.com, 4-10-2018 https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies geraadpleegd 7-3-2019.
110 *UK cyber security agency backs Apple, Amazon China hack denials*, Reuters.com, 5-10-2018 https://www.reuters.com/article/us-china-cyber-britain/uk-cyber-security-agency-backs-apple-amazon-china-hack-denials-idUSKCN1MF1DN geraadpleegd 7-3-2019.
111 *Statement from DHS Press Secretary on Recent Media Reports of Potential Supply Chain Compromise*, DHS.gov, 6-10-2018 https://www.dhs.gov/news/2018/10/06/statement-dhs-press-secretary-recent-media-reports-potential-supply-chain-compromise geraadpleegd 7-3-2019.
112 *Privégegevens van honderden Duitse politici, onder wie Merkel, op straat*, DeMorgen.be, 4-1-2019 https://www.demorgen.be/buitenland/privegegevens-van-honderden-duitse-politici-onder-wie-merkel-op-straat-b1b2542b geraadpleegd 7-3-2019.
113 *Hackerangriff auf Hunderte Politiker*, tagesschau.de, 4-1-2019 https://www.tagesschau.de/inland/deutsche-politiker-gehackt-101.html geraadpleegd 7-3-2019.
114 *Festnahme eines Tatverdächtigen im Ermittlungsverfahren wegen des Verdachts des Ausspähens und der unberechtigten Veröf-fentlichung personenbezogener Daten*, bka.de, 8-1-2019
115 *Right country, wrong group? Researchers say it wasn't APT10 that hacked Norwegian software firm*, cyberscoop.com, 12-2-2019 https://www.cyberscoop.com/apt10-apt31-recorded-future-rapid7-china/ geraadpleegd 4-2-2019.
116 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html geraadpleegd 4-2-2019.
117 *Olympic Destroyer is still alive*, securelist.com, 19-6-2018 https://securelist.com/olympic-destroyer-is-still-alive/86169/ geraadpleegd 5-2-2019.
118 *Operation Sharpshooter*, mcafee.com 13-12-2018 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf geraadpleegd 5-2-2019.
119 *China link possible in cyber attack on Australian Parliament computer system*, abc.net.au, 8-2-2019 https://www.abc.net.au/news/2019-02-08/china-government-cyber-security-breach-parliament-hackers/10792938 geraadpleegd 9-2-2019.
120 *With elections weeks away, someone "sophisticated" hacked Australia's politicians*, arstechnica.com, 18-2-2019 https://arstechnica.com/information-technology/2019/02/australian-political-parties-hacked-by-nation-state-attacker/ geraadpleegd 6-2-2019.
121 https://www.wsj.com/articles/iran-blamed-for-cyberattack-on-australias-parliament-11550736796/
122 *Indictment Iranian hackers department of Justice of the United States of America*, US district court, 23-3-2018 https://www.justice.gov/usao-sdny/press-release/file/1045781/download geraadpleegd 26-2-2019
123 *Indictment Iranian hackers department of Justice of the United States of America* https://www.justice.gov/opa/press-release/file/1114741/download geraadpleegd 26-2-2019.
124 *Indictment North Korean hackers department of Justice of the United States of America*, US district court, 8-6-2018 https://www.justice.gov/opa/press-release/file/1092091/download geraadpleegd 26-2-2019.
125 *Indictment Russia hackers department of Justice of the United States of America*, US district court, 3-7-2018 https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election geraadpleegd 26-2-2019.
126 *Indictment Russia hackers department of Justice of the United States of America*, US district court, 3-10-2018 https://www.justice.gov/opa/page/file/1098481/download geraadpleegd 26-2-2019.
127 *Indictment Chinese hackers department of Justice of the United States of America*, US district court, 17-12-2018 https://www.justice.gov/opa/press-release/file/1121706/download geraadpleegd 27-2-2019.
128 *Canada identifies malicious cyber-activity by Russia*, Government of Canada, 04-10-2018 https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html geraadpleegd 26-2-2019.
129 Joint statement from Prime Minister May and Prime Minister Rutte, gov.uk 04-10-2018 https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte geraadpleegd 27-2-2019.
130 *Indictment Chinese hackers department of Justice of the United States of America*, US district court, 17-12-2018 https://www.justice.gov/opa/press-release/file/1121706/download geraadpleegd 27-2-2019.

131 *UK and allies reveal global scale of Chinese cyber campaign*, UK government, gov.uk, 20-12-2018 https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign geraadpleegd 27-2-2019.

132 *Cyber campaign attributed to China*, ncsc.govt.nz, 21-12-2018 https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/ geraadpleegd 27-2-2019.

133 *Chinese cyber-enabled commercial intellectual property theft*, Ministry of Foreign Affairs of Australia, foreignminister.gov.au, 21-12-2018 https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx geraadpleegd 27-2-2019.

134 *Canada and Allies Identify China as Responsible for Cyber-Compromise*, cse.cst.gc.ca, 20-12-2018 https://cse-cst.gc.ca/en/media/media-2018-12-20 geraadpleegd 27-2-2019.

135 *Cyberattacks by a group based in China known as APT10*, Ministry of Foreign Affairs of Japan, 21-12-2018 https://www.mofa.go.jp/press/release/press4e_002281.html geraadpleegd 27-2-2019.

136 *Bolton confirms offensive cyber-operations conducted to protect midterms*, cyberscoop, 1-11-2018, https://www.cyberscoop.com/john-bolton-offensive-cyber-operations/ geraadpleegd 28-2-2019.

137 *The pentagon has prepared a cyber attack against Russia*, publicintegrity.org, 2-11-2018, https://publicintegrity.org/national-security/military/the-pentagon-has-prepared-a-cyber-attack-against-russia/ geraadpleegd 28-2-2019.

138 Ministerie van Justitie, *Voorzorgsmaatregel ten aanzien van gebruik Kaspersky antivirussoftware*, 14-5-2018, https://www.rijksoverheid.nl/documenten/kamerstukken/2018/05/14/voorzorgsmaatregel-ten-aanzien-van-gebruik-kaspersky-antivirussoftware geraadpleegd 28-2-2019.

139 *Software and hardware of Huawei and ZTE is a security threat*, National Cyber Security Centre Czechia, govcert.cz, 17-12-2018 https://www.govcert.cz/en/info/events/2682-software-and-hardware-of-huawei-and-zte-is-a-security-threat/ geraadpleegd 28-2-2019.

140 *H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019*, congress.gov, 13-8-2018 https://www.congress.gov/bill/115th-congress/house-bill/5515/text geraadpleegd 29-2-2019.

141 *Government Provides 5G Security Guidance To Australian Carriers*, minister.communications.gov.au, 23-8-2018 https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers geraadpleegd 29-2-2019.

142 *German officials sound China alarm as 5G auctions loom*, Reuters.com 13-11-2018 https://www.reuters.com/article/us-germany-china-5g-exclusive/exclusive-german-officials-raise-china-alarm-as-5g-auctions-loom-idUSKCN1NI1WC.

143 *Pence praises Poland's actions on Huawei as U.S. pressure mounts*, Reuters.com 13-2-2019 https://www.reuters.com/article/us-huawei-europe-poland/pence-praises-polands-actions-on-huawei-as-us-pressure-mounts-idUSKCN1Q22IX.

144 ENISA, ENISA Threat Landscape Report 2018 (2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 .

145 Jaarverantwoording politie 2018, mei 2019

146 Kamerbrief over phishing incident DigiD's via Mijnoverheid, 29-06-2018: phishing-incident-digids-via-mijnoverheid-22-juni-2018.pdf geraadpleegd 26-2-2019.

147 *FBI ziet toename van sim-swapping bij cryptodiefstal*, 7-3-2019, security.nl https://www.security.nl/posting/600453/FBI+ziet+toename+van+sim-swapping+bij+cryptodiefstal geraadpleegd 8-3-2019.

148 *Aanvallen via ss7-protocol om 2fa-sms'jes te onderscheppen nemen toe*, tweakers.net, 1-2-2019 https://tweakers.net/nieuws/148636/aanvallen-via-ss7-protocol-om-2fa-smsjes-te-onderscheppen-nemen-toe.html geraadpleegd 8-3-2019.

149 *Internet Organised Crime Threat Assessment (IOCTA)*, Europol.europa.eu, 2018 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment geraadpleegd 22-3-2019.

150 *Politie sluit grootste DDoS-website in Operation Power Off*, politie.nl, 25-4-2018 https://www.politie.nl/nieuws/2018/april/25/politie-sluit-grootste-ddos-website-in-operation-power-off.html geraadpleegd 22-3-2019.

151 *World's biggest marketplace selling internet paralysing DDoS attacks taken down*, Europol.europa.eu, 25-4-2018 https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down geraadpleegd 22-3-2019.

152 *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets*, Wegberg et al, USENIX 2018

153 M. McGuire, *Into the Web of Profit. An in-depth study of cybercrime, criminals and money* april 2018 ,

154 Jaarverantwoording politie 2018, mei 2019

155 *Duizenden jongeren 'verleid' tot hacken in campagne politie*, nos.nl, 14-2-2019 https://nos.nl/artikel/2271890-duizenden-jongeren-verleid-tot-hacken-in-campagne-politie.html Geraadpleegd 21-2-2019.

156 Hack_Right, politie.nl: https://www.politie.nl/themas/hack_right.html?sid=fd8d5ad0-1a02-4bb9-b0f4-b34d9c787899 geraadpleegd 26-2-2019 .

157 Microsoft Security Intelligence Report 24 https://www.microsoft.com/en-us/security/operations/security-intelligence-report geraadpleegd 26 maart 2019.
158 Symantec Internet Security Threat Report 2019 https://www.symantec.com/security-center/threat-report geraadpleegd 4 april 2019.
159 Trend Micro 2018 Mobile Threat Landscape https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape geraadpleegd 4 april 2019.
160 CrowdStrike Global Threat Report 2019 https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/ geraadpleegd 26 maart 2019.
161 *Inside Magecart: RiskIQ and Flashpoint Release Comprehensive Report on Cybercrime and the Assault on E-Commerce*, riskiq.com, 13-11-2018 https://www.riskiq.com/blog/external-threat-management/inside-magecart/ geraadpleegd 07-03-2019.
162 Symantec: duizenden webwinkels getroffen door formjacking, security.nl, 21-2-2019 https://www.security.nl/posting/598734/Symantec%3A+duizenden+webwinkels+getroffen+door+formjacking geraadpleegd 7-3-2019.
163 Symantec Internet Security Threat Report, februari 2019 https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf, geraadpleegd 7-3-2019.
164 *Spam and Phishing in Q3 2018*, securelist.com, 6-11-2018, https://securelist.com/spam-and-phishing-in-q3-2018/88686/ geraadpleegd 26-3-2019.
165 *Microsoft security intelligence report volume 24, January – December 2018*, februari 2019, https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/ geraadpleegd 26-3-2019.
166 *Phishing Attack Pretends to be a Office 365 Non-Delivery Email*, bleepingcomputer,com, 16-12-2018, https://www.bleepingcomputer.com/news/security/phishing-attack-pretends-to-be-a-office-365-non-delivery-email/ geraadpleegd 26-3-2019.
167 *Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign*, fireeye.com, 19-11-2018, https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html geraadpleegd 26-3-2019.
168 *Indictment Chinese hackers department of Justice of the United States of America*, US district court, 17-12-2018 https://www.justice.gov/opa/press-release/file/1121706/download geraadpleegd 27-2-2019.
169 *Top phishing email attacks worldwide in 2018*, duocircle.com, November 2018, https://www.duocircle.com/phishing-protection/top-phishing-email-attacks-worldwide-in-2018 geraadpleegd 26-3-2019.
170 *Global Threat Report 2019*, maart 2019, https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/ geraadpleegd 26-3-2019.
171 *3,81 miljoen euro schade door phishing bij internetbankieren in 2018 - Minder fraude met betaalpassen en automatische incasso's*, 27-3-2019, https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/, geraadpleegd 27-3-2019.
172 *Aanvallers wijzigen wereldwijd dns-instellingen domeinen*, security.nl, 11-1-2019 https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen geraadpleegd 7-3-2019.
173 *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*, FireEye.com, 9-1-2019 https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html, geraadpleegd 7-3-2019.
174 *DNS Infrastructure Hijacking Campaign*, us-cert.gov, 11-1-2019 https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign, geraadpleegd 7-3-2019.
175 *DNSpionage Campaign Targets Middle East*, talosintelligence.com, 27-11-2018 https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html, geraadpleegd 7-3-2019.
176 *A Worldwide Hacking Spree Uses DNS Trickery to Nab Data*, wired.com, 11-1-2019 https://www.wired.com/story/iran-dns-hijacking/, geraadpleegd 7-3-2019.
177 *ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet*, icann.org, 22-2-2019 https://www.icann.org/news/announcement-2019-02-22-en, geraadpleegd 8-3-2019.
177 Wet op de inlichtingen- en veiligheidsdiensten, aivd.nl https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten geraadpleegd 15-2-2019.
178 *BGP Hijack of Amazon DNS to Steal Crypto Currency*, dyn.com, 25-4-2018, https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/ geraadpleegd 26-3-2019.
179 *BGP/DNS Hijacks Target Payment Systems*, dyn.com, 3-8-2018, https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/ geraadpleegd 26-3-2019.
180 *Fox-IT: Nederlandse bedrijven ook slachtoffer van SamSam-gijzelsoftware*, 2-12-2018, https://nos.nl/artikel/2261704-fox-it-nederlandse-bedrijven-ook-slachtoffer-van-samsam-gijzelsoftware.html, 22-03-2019.

181 *Microsoft Security Intelligence Report Volume 24*, microsoft.com 28-2-2019, https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/ geraadpleegd 20-3-2019.
182 Voor exacte criteria zie: Wbni voor digitale dienstverleners https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners, geraadpleegd 15-02-2019.
183 Bron: NCSC, geraadpleegd 26-2-2019.
184 Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners, rijksoverheid.nl, 1-9-2018 https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners geraadpleegd 15-2-2019.
185 Nieuwe wet versterkt bestrijding computercriminaliteit, rijksoverheid.nl, 28-2-2019, https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit geraadpleegd 5-3-2019.
186 *Cijfers datalekken 2018*, autoriteitpersoonsgegevens.nl, 1-2-2019, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/cijfers-datalekken-2018 geraadpleegd 26-2-2019.
187 *In 10 stappen voorbereid op de AVG*, autoriteitpersoonsgegevens.nl, november 2017 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf geraadpleegd 15-2-2019 .
188 *In 10 stappen voorbereid op de AVG*, autoriteitpersoonsgegevens.nl, november 2017 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf geraadpleegd 15-2-2019.
189 *Wet op de inlichtingen- en veiligheidsdiensten 2017*, wetten.overheid.nl https://wetten.overheid.nl/BWBR0039896/2018-05-01 geraadpleegd 8-3-2019.
190 NCTV, *Cybersecuritybeeld Nederland 2018, juni 2018* (https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf) geraadpleegd 7-3-2019.
191 *Oorzaak computerstoring treinverkeersleiding gevonden*, prorail.nl, 22-8-2018 https://www.prorail.nl/nieuws/oorzaak-computerstoring-treinverkeersleiding-gevonden geraadpleegd 7-3-2019.
192 Brief van de minister van rechtsbescherming aan de Tweede Kamer (29279-455) m.b.t. Storing mobiele netwerk elektronische enkelband tk-storing-mobiele-netwerk-elektronische-enkelband.pdf geraadpleegd 07-03-2019.
193 *Meldelicht datalekken: facts & figures overzicht feiten en cijfers 1e helft 2018*, autoriteitpersoonsgegevens, 2018 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_halfjaarrapportage_q1_en_q2_2018_algemeen.pdf geraadpleegd 5-3-2019.
194 *Disparities found in levels of reporting across EU member states*, dla piper, dlapiper.com, 6-2-2019 https://www.dlapiper.com/en/netherlands/news/2019/02/dla-piper-gdpr-data-breach-survey/ geraadpleegd: 19-3-2019.
195 *Verkeerde Burgernetmail verzonden naar 145 BN-deelnemers*, politie.nl, 10-7-2018, https://www.politie.nl/nieuws/2018/juli/10/04-verkeerde-burgernetmail-verzonden-naar-145-bn-deelnemers.html geraadpleegd 5-3-2019.
196 *DDoS-aanvallen treffen 15% meer websites in 2018*, SIDN, sidn.nl, 8-1-2019 https://www.sidn.nl/a/veilig-internet/ddos-aanvallen-treffen-15-meer-websites-in-2018 geraadpleegd: 12-3-2019.
197 *December piekmaand voor DDoS-aanvallen op webwinkels*, NBIP, nbip.nl, 14-12-2018 https://www.nbip.nl/2019/01/14/december-piekmaand-ddos-webwinkels/ geraadpleegd: 12-3-2019.
198 *Rabobank en ABN AMRO zondag weer getroffen door DDoS-aanval*, 28-05-2018, https://www.nu.nl/internet/5286176/rabobank-en-abn-amro-zondag-weer-getroffen-ddos-aanval.html, geraadpleegd 20-03-2019.
199 *Website DigiD was weer onbereikbaar door DDoS-aanval*, 31-07-2018, https://www.nu.nl/internet/5391845/website-digid-was-weer-onbereikbaar-ddos-aanval.html, geraadpleegd 20-03-2019.
200 *FBI en Nederlandse politie halen vijftien aanbieders DDoS-aanvallen offline*, 20-12-2018, https://www.nu.nl/internet/5643251/fbi-en-nederlandse-politie-halen-vijftien-aanbieders-ddos-aanvallen-offline.html, geraadpleegd 20-03-2019.
201 Ministerie van Economische Zaken en Klimaat, *Nederlandse digitaliseringsstrategie* (juni 2018).
202 https://nos.nl/artikel/2232061-rekenkamer-rijk-heeft-databeveiliging-niet-op-orde.html, geraadpleegd 13 maart 2019.
203 https://www.rekenkamer.nl/actueel/nieuws/2018/05/16/ministers-melden-te-weinig-wat-resultaten-zijn, geraadpleegd 13 maart 2019.
204 https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/documenten/rapporten/2018/05/16/staat-van-de-rijksverantwoording-2017, geraadpleegd 13 maart 2019.
205 https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde, geraadpleeg 15 mei 2019.
206 Algemene Rekenkamer, *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* (28 maart 2019).
207 Algemene Rekenkamer, *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* (28 maart 2019).

208 https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-maart/index.jsp, geraadpleegd 28-03-2019.
209 https://executive-people.nl/618901/ruim-op-de-nederlandse-organisaties-slachtoffer-van-phishing.html.
210 https://www.microsoft.com/securityinsigths geraadpleegd 25 maart 2019.
211 https://content.fireeye.com/m-trends/rpt-m-trends-2019, geraadpleegd 13 maart 2019.
212 CrowdStrike Global Threat Report 2019 https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/ geraadpleegd 26 maart 2019.
223 https://www.cpb.nl/publicatie/risicorapportage-cyberveiligheid-economie-2018.
214 https://www.ncsc.nl/actueel/nieuwsberichten/onderzoeksrapport-digitale-hygiene-nederland.html, geraadpleegd 20 maart 2019.
215 Agentschap Telecom, *De Staat van de Ether* 2017, https://magazines.agentschaptelecom.nl/staatvandeether/2017/01/onveilige-apparatuur-risico-voor-samenleving geraadpleegd 25 maart 2019.
216 Onderzoekers tonen Rowhammer-aanval om browser over te nemen op Android-toestel, https://tweakers.net/nieuws/138207/onderzoekers-tonen-rowhammer-aanval-om-browser-over-te-nemen-op-android-toestel.html geraadpleegd 26-3-2019
217 VUSec-onderzoekers weten ecc-geheugen aan te vallen met Rowhammer, https://tweakers.net/nieuws/146103/vusec-onderzoekers-weten-ecc-geheugen-aan-te-vallen-met-rowhammer.html geraadpleegd 26-3-2019
218 Google-onderzoekers: Spectre blijft ons nog lang achtervolgen, https://www.security.nl/posting/599154/Google-onderzoekers%3A+Spectre+blijft+ons+nog+lang+achtervolgen geraadpleeg 26-3-2019
219 CA Insider Threat Report 2018 https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf geraadpleegd 26 maart 2019,
CompTIA 2018 Trends in Cybersecurity https://www.comptia.org/resources/cybersecurity-trends-research geraadpleegd 26 maart 2018,
World Economic Forum Global Risk Report 2018 http://reports.weforum.org/global-risks-2018/ geraadpleegd 26 maart 2019.
220 M. McGuire, *Into the Web of Profit. An in-depth study of cybercrime, criminals and money* april 2018 ,
221 Autoriteit Consument en Markt, *5G en de Autoriteit Consument en Markt* (12 december 2018).
222 European Centre for International Political Economy, *5G and National Security After Australia's Telecom Sector Security Review*, Occasional paper No. 8/2018 (2018), p.4-5.
223 Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 23.
224 Ryan Goosen, Anna Rontojannis, Stefan Deutscher (et al), *Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution*., 13-11-2018 https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx geraadpleegd 11-2-2019.
Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 23.
Celeste Fralick McAfee, *Artificial Intelligence in Cybersecurity Is Vulnerable*, 15-1-2019 https://www.scmagazine.com/home/opinion/artifical-intelligence-in-cybersecurity-is-vulnerable/ geraadpleegd 11-2-2019.
Artificial Intelligence and Cybersecurity: Attacking and Defending, Tripwire, 10-12-2018 https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/ geraadpleegd 11-2-2019.
Tara Seals, *Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad*., 3-10-2018 https://threatpost.com/artificial-intelligence-a-cybersecurity-tool-for-good-and-sometimes-bad/137831/ geraadpleegd 11-2-2019.
Scot Finnie, *AI in cybersecurity: what works and what doesn't*, 15-8-2018 https://www.csoonline.com/article/3295596/security/ai-in-cybersecurity-what-works-and-what-doesnt.html geraadpleegd 11-2-2019.
225 Craig S. Smith, *Alexa and Siri Can Hear This Hidden Command*. You Can't., New York Times, 10-5-2018 https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html geraadpleegd 11-2-1029.
226 *BlackRock shelves unexplainable AI liquidity models*, Risk.net, 12-11-2018. (https://www.risk.net/asset-management/6119616/blackrock-shelves-unexplainable-ai-liquidity-models).
227 Kees Verhoeven, *Investeer 25 miljoen in kunstmatige intelligentie*, D66, 20-9-2018. https://d66.nl/investeer-in-kunstmatige-intelligentie/.
228 Ryan Goosen, Anna Rontojannis, Stefan Deutscher (et al), *Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution*., 13-11-2018 https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx geraadpleegd 11-2-2019.
Celeste Fralick McAfee, *Artificial Intelligence in Cybersecurity Is Vulnerable*, 15-1-2019 https://www.scmagazine.com/home/opinion/artifical-intelligence-in-cybersecurity-is-vulnerable/ geraadpleegd 11-2-2019.
Artificial Intelligence and Cybersecurity: Attacking and Defending, Tripwire, 10-12-2018 https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/ geraadpleegd 11-2-2019.
Tara Seals, *Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad*., 3-10-2018 https://threatpost.com/artificial-intelligence-a-cybersecurity-tool-for-good-and-sometimes-bad/137831/ geraadpleegd 11-2-2019.
Scot Finnie, *AI in cybersecurity: what works and what doesn't*, 15-8-2018 https://www.csoonline.com/article/3295596/security/ai-in-cybersecurity-what-works-and-what-doesnt.html geraadpleegd 11-2-2019.
229 Analistennetwerk Nationale Veiligheid, *Horizonscan Nationale Veiligheid 2018*, oktober 2018, p. 13-18.

230 Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force* (november 2018), p. 10-12, 66.
231 *2019 Forcepoint Cybersecurity Predictions Report*, Forcepoint, 13-11-2018 https://www.forcepoint.com/sites/default/files/resources/files/report-2019-cybersecurity-predictions-en.pdf geraadpleegd 29-11-2018.
232 Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force* (november 2018), p. 10-12, 66;
233 *Digitale oorlog minstens zo destructief*, Leidsch Dagblad, 13-2-2019.
234 Ministerie van Economische Zaken en Klimaat, *Nederlandse digitaliseringsstrategie* (juni 2018), p. 13-14.
235 *De technologische Koude Oorlog*, De Groene Amsterdammer, 23-01-2019.
236 *Europa overtuigen om geen Huawei te kopen 'topprioriteit' voor VS*, Nu.nl, 5-2-2019 geraadpleegd 6-2-2019; Minister VS waarschuwt voor Huawei bij begin Europese toer, NOS.nl, 11-2-2019 https://nos.nl/artikel/2271562-minister-vs-waarschuwt-voor-huawei-bij-begin-europese-toer.html geraadpleegd 12-2-2019.
237 *Revitalizing privacy and trust in a data-driven world. Key findings from The Global State of Information Security® Survey 2018.*, PWC, 28-3-2018 https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf geraadpleegd 15-2-2019.
238 *Cybersecurity predictions for 2019*, CSO Online, 20-11-2018 https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html; Prospects for cybersecurity in 2019, Oxford Analytica, 23-11-2018.
239 Ministerie van Economische Zaken en Klimaat, *Nederlandse digitaliseringsstrategie* (juni 2018).
240 *Roadmap Digitaal Veilige Hard- en Software*, Ministerie van Economische Zaken en Klimaat Ministerie van Justitie en Veiligheid, april 2018 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software/Roadmap+Digitaal+Veilige+Hard-+en+Software.pdf.
241 *Het DigiNotarincident. Waarom digitale veiligheid de bestuurstafel te weinig bereikt.*, De Onderzoeksraad voor Veiligheid, juni 2012 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjR4t2-5L3gAhUQU1AKHVkgB-QFjACegQICBAC&url=https%3A%2F%2Fwww.onderzoeksraad.nl%2Fnl%2Fmedia%2Fattachment%2F2018%2F7%2F10%2Frapport_diginotar_nl_web_def_20062012.pdf&usg=AOvVaw3M1PhT7xZArFoOgZmyboNB.
242 *KPN erkent fouten bij hack, gaat versneld investeren in IT-systemen*, Het Financiële Dagblad, 14-2-2012; KPN: hack gevolg van achterstallig onderhoud, de Volkskrant, 14-2-2012.
243 John Snow, *Top 5 most notorious cyberattacks*, Kaspersky Lab, 6-11-2018 https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/ geraadpleegd 18-2-2019.
244 *The WannaCry attack is a wake-up call*, Financial Times, 14-5-2017 https://www.ft.com/content/f6cd3e38-388a-11e7-821a-6027b8a20f23 geraadpleegd 18-2-219; *Wake-up call voor bedrijven in strijd tegen cybercrime*, Computable.nl, 7-8-2017 https://www.bnr.nl/nieuws/tech/10327239/wake-up-call-voor-bedrijven-in-strijd-tegen-cybercrime geraadpleegd 18-2-219; *Maersk moest 45.000 pc's herinstalleren wegen NotPetya*, Security.nl, 25-1-2018; Brancheorganisatie voor ict-beveiligers ziet het licht, Computable.nl, 14-3-2018.
245 de Wet gegevensverwerking en meldplicht cybersecurity (tot 15 november 2018) en Wet beveiliging netwerken en informatiesystemen (vanaf 15 november 2018).
246 Zie https://www.ncsc.nl/actueel/leidraad-coordinated-vulnerability-disclosure.html, geraadpleegd 8 maart 2019.

Uitgave
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
csbn@nctv.minjenv.nl
@nctv_nl

Juni 2019