Nationaal Coördinator
Terrorismebestrijding en Veiligheid
*Ministerie van Justitie en Veiligheid*

# Cybersecuritybeeld Nederland

## CSBN 2022

# Cybersecuritybeeld Nederland 2022

## Colofon

Het Cybersecuritybeeld Nederland 2022 (CSBN2022) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en tot slot de risico's. De focus ligt daarbij op de nationale veiligheid. Daarnaast heeft het CSBN2022 tot doel om inzicht te geven in de strategische thema's die nu en de komende vier tot zes jaar relevant zijn voor de digitale veiligheid van Nederland. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vastgesteld.

De NCTV draagt samen met partners uit het veiligheidsdomein bij aan een veilig en stabiel Nederland door dreigingen te onderkennen en de weerbaarheid en bescherming van nationale veiligheidsbelangen te versterken. Doel is het voorkomen en beperken van maatschappelijke ontwrichting. Sinds de oprichting van de NCTV is er binnen de Rijksoverheid één organisatie verantwoordelijk voor terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing.

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 het Rijk en vitale aanbieders.

# Inhoud

*Weerbaarheid kan een dam opwerpen tegen de dreiging*

# Scheefgroei dreiging en weerbaarheid vergroot risico op ontwrichting

**Om ongestoord te kunnen functioneren, is weerbaarheid van de samenleving tegen digitale dreiging cruciaal. De veiligheid van digitale processen is essentieel in onze sterk gedigitaliseerde maatschappij. Digitale veiligheid is dus onlosmakelijk verbonden met de nationale veiligheid. De vraag 'hoe digitaal veilig is Nederland?' is eigenlijk niet te beantwoorden en bovendien bestaat honderd procent veiligheid niet. Digitale processen kunnen altijd uitvallen door technisch of menselijk falen. De digitale ruimte is bovendien hét speelveld van een groeiend aantal staten, waarbij cyberaanvallen het nieuwe normaal zijn. Daarnaast hebben aanvallen door cybercriminelen inmiddels een industriële schaal bereikt. De digitale dreiging is dan ook permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien.**

Ondanks de inspanningen om de weerbaarheid te verhogen, is sprake van een scheefgroei tussen de toenemende dreiging en de ontwikkeling van de weerbaarheid. Die scheefgroei vergroot het risico op ontwrichting. Een moeilijk te beantwoorden maar relevante vraag is: 'wanneer is Nederland voldoende weerbaar?' Door weerbaarheid kan er immers een dam worden opgeworpen tegen de dreiging. Dat vereist een welbewuste afweging van de balans tussen de afhankelijkheid van digitale processen en het belang dat daaraan wordt gehecht, de dreiging daartegen én het gewenste niveau van weerbaarheid. Hoewel anders van aard, gaat een vergelijking op met de COVID-19-pandemie en de oorlog in Oekraïne. Die confronteerden ons met de aanwezigheid van afhankelijkheden, kwetsbaarheden en onvoorziene gevolgen van ingrijpende gebeurtenissen. De vraag wanneer Nederland voldoende weerbaar is, is niet alleen een vraagstuk voor technische experts. Het is vooral een vraagstuk van governance en/of risicomanagement voor politici, overheden en bestuurders op zowel landelijk, sectoraal en organisatieniveau, als tússen die drie niveaus.

## Complicaties risicobeheersing gevaar voor samenleving

De NCTV heeft in samenwerking met partners strategische thema's geïdentificeerd, die nu en de komende jaren relevant zijn voor de digitale veiligheid van Nederland. Hoewel uiteenlopend van aard, vormen zij ieder op zich en in samenhang met elkaar, complicaties voor strategische risicobeheersing. De thema's worden hieronder kort geïntroduceerd, hoofdstuk 3 bevat een uitgebreide toelichting.

### Risico's vormen keerzijde van gedigitaliseerde samenleving

De Nederlandse samenleving is in hoge mate gedigitaliseerd en de COVID-19-pandemie heeft verdere digitalisering van processen in een stroomversnelling gebracht. Dat heeft een keerzijde: de afhankelijkheid van digitale processen heeft ons ook kwetsbaar gemaakt voor uitval en voor de activiteiten van kwaadwillenden. Er zijn vier risico's voor de nationale veiligheid, die direct of indirect ook gelden voor specifieke sectoren en organisaties en individuele burgers: 1) ongeautoriseerde inzage in informatie (en eventueel

publicatie daarvan), in het bijzonder door spionage; 2) ontoegankelijkheid van processen, als gevolg van (voorbereidingen voor) sabotage en de inzet van ransomware; 3) schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leveranciersketens; 4) grootschalige uitval van digitale processen. De hoge mate van digitalisering van onze samenleving en de afhankelijkheid van digitale processen zijn een gegeven. Het beheersbaar krijgen en houden van kwetsbaarheden is onderdeel van risicobeheersing.

### Digitale ruimte is speelveld voor regionale en mondiale dominantie

Een groeiend aantal staten gebruikt de digitale ruimte structureel én intensief voor de behartiging van hun geopolitieke belangen. Cyberaanvallen, bijvoorbeeld voor het vergaren van politieke en economische inlichtingen, zijn daartoe een belangrijk instrument: ze zijn relatief goedkoop en schaalbaar en ze hebben een hoge, vaak langdurige opbrengst. Ook is attributie een lastige kwestie. Verder vindt rond de bouwstenen van de digitale ruimte en hoogwaardige technologieën een geopolitiek steekspel plaats. Individuele burgers, organisaties, sectoren en landen kunnen weinig invloed uitoefenen op die geopolitieke wedijver, terwijl die wel bijdraagt aan de verhoging van risico's.

### Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet

Zware, georganiseerde cybercriminaliteit is zeer schaalbaar geworden en heeft daardoor in de afgelopen jaren qua slachtoffers, schade en criminele opbrengsten een industriële omvang aangenomen. De term schaalbaarheid verwijst naar het vermogen om een systeem of proces aan te passen (op te schalen) om te kunnen voldoen aan een grotere vraag. Zware cybercriminelen en hun dienstverleners zijn primair financieel gemotiveerd en gaan voor maximale opbrengsten, waarbij ze dankbaar gebruik maken van de mogelijkheden die het digitale domein biedt. Gezien de aard en groeiende omvang van de cybercriminele dreiging is het schaalbaar maken én houden van de weerbaarheidsketen een fundamentele uitdaging voor de komende jaren.

### Marktdynamiek compliceert beheersing van digitale risico's

Op digitale markten komen vraag en aanbod naar digitale diensten, (componenten van) hardware, software en netwerken samen. Deze markten hebben enkele unieke kenmerken. Bijvoorbeeld de (semi)monopolistische status van bepaalde leveranciers, de hoge mate van onderlinge verwevenheid en de focus op het vergaren van zoveel mogelijk data. Ook zijn in deze markten prikkels voor digitale veiligheid niet (altijd) doorslaggevend. Die kenmerken compliceren de beheersing van risico's voor individuele burgers, organisaties, sectoren en landen.

### Samenhangend en geïntegreerd risicomanagement staat nog in kinderschoenen

Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal, staat nog in de kinderschoenen. De weerbaarheid in Nederland is nog niet voldoende op niveau. Digitale risico's nemen nog geen structurele plaats in het bredere risicomanagement in en een samenhangende aanpak is nodig.

### Beperkingen in digitale autonomie beperken ook digitale weerbaarheid

Voor Europese landen en Nederland (verder Nederland en Europa) gelden beperkingen in digitale autonomie. Die autonomie omvat het vermogen en de middelen die Nederland heeft om zelfstandig beslissingen te kunnen nemen over (verdere) digitalisering én de gewenste mate van digitale weerbaarheid. Beperkingen in digitale autonomie brengen ook beperkingen voor weerbaarheid met zich mee. De autonomie staat onder druk door diverse oorzaken, die samenhangen met de hierboven genoemde strategische thema's. Die oorzaken verminderen de beïnvloedings- en keuzemogelijkheden voor en controle over de digitale weerbaarheid van Nederland.

# *Inzicht in strategische thema's die relevant zijn voor de digitale veiligheid van Nederland*

# 1 Inleiding

**Het CSBN2022 biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en tot slot de risico's. De focus ligt daarbij op de nationale veiligheid. Daarnaast heeft het CSBN2022 tot doel om inzicht te geven in de strategische thema's die nu en de komende vier tot zes jaar relevant zijn voor de digitale veiligheid van Nederland. Dat inzicht vormt de inhoudelijke basis voor de nieuwe cybersecuritystrategie.**

## Doel en afbakening

Het Cybersecuritybeeld Nederland (CSBN) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast en de weerbaarheid daartegen. Op basis hiervan zijn risico's geformuleerd. Het accent ligt daarbij op de nationale veiligheid. Digitalisering biedt vele kansen, maar leent zich ook voor allerlei vormen van misbruik en er kan sprake zijn van uitval. Het CSBN richt zich niet op de kansen van digitalisering. Het CSBN richt zich wél op verstoringen van (kritische) processen met een digitale component.

Het CSBN is primair bedoeld voor strategie- en beleidsvorming op nationaal niveau (governance). Het beoogt het kabinet, de leden van de Eerste en Tweede Kamer, ambtenaren, beleidsmakers, overige bestuurders en directies en andere geïnteresseerden inzicht te geven in de digitale risico's voor Nederland. Cybersecurity-bedrijven en –professionals gebruiken het CSBN als referentiekader richting de eigen bestuurders of klanten. Het CSBN is ook bedoeld als hulpmiddel voor risicomanagement, waarbij het zich specifiek richt op de identificatie en analyse van risico's, een van de stappen in een risicomanagementproces. Tot slot is het CSBN toegankelijk voor het brede publiek.

## Toelichting sleutelbegrippen

Vanwege de verwevenheid van de fysieke en digitale ruimte en omwille van de leesbaarheid, worden de termen 'cyber' en 'digitale' slechts beperkt gebruikt.

### Sleutelbegrippen

In het CSBN zijn de belangrijkste begrippen als volgt gedefinieerd[1]:
**Belang:** waarden, verworvenheden, materiële en immateriële zaken waaraan schade kan ontstaan als een cyberincident zich voordoet en het gewicht dat de maatschappij of een partij aan de verdediging ervan toekent. In het CSBN ligt de focus op nationale veiligheidsbelangen.
**Aanval:** moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van één of meer digitale processen.
**Cyberincident:** (samenhangende set van) gebeurtenissen of activiteiten die kunnen leiden tot verstoring van één of meer (digitale) processen.
**Cybersecurity:** het geheel aan maatregelen om relevante risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en - wanneer cyberincidenten zich hebben voorgedaan - deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risico-afweging.
**Digitaal proces (hierna: proces):** een proces dat geheel of gedeeltelijk wordt uitgevoerd door de complexe en onderling samenhangende interactie tussen mensen en vele componenten van hardware, software en/of netwerken. Volledig

geautomatiseerde processen, zoals procesbesturingssystemen, vallen ook onder het begrip.
**Risico:** de kans dat een dreiging leidt tot een cyberincident en de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid.
**Digitale ruimte:** de complexe omgeving die het resultaat is van onderling verweven digitale processen, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT)-apparaten en verbonden netwerken. De digitale ruimte wordt vanuit drie invalshoeken of lagen benaderd: 1) digitale processen uitgevoerd (of in gang gezet) door mensen; 2) de technische laag (van IT en OT) die de digitale processen mogelijk maakt; 3) de risicomanagement- en/of governance laag die de twee andere lagen bestuurt.
**Dreiging:** een opzettelijk of niet-opzettelijk gevaar dat kan leiden tot een cyberincident of een combinatie van gelijktijdige of opeenvolgende cyberincidenten.
**Uitval:** een situatie waarin één of meer digitale processen zijn verstoord als gevolg van natuurlijke of technische oorzaken, of als gevolg van menselijke fouten.
**Verstoring:** een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(verwerking), dat wil zeggen, een verstoring in de technische laag van de digitale ruimte.
**Weerbaarheid:** het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging. Die kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen.

## Leeswijzer

Hoofdstuk 2 geeft het huidige normbeeld weer van het belang, de dreiging en de weerbaarheid. Hoofdstuk 3 beschrijft en duidt de strategische thema's die nu en de komende vier tot zes jaar relevant zijn voor de digitale veiligheid van Nederland. Hoofdstuk 4 blikt terug op de belangrijkste incidenten van het afgelopen jaar. Bijlage 1 geeft een verantwoording van de totstandkoming van dit CSBN. Bijlage 2 bevat de bronverwijzingen.

*Cyberaanvallen door statelijke actoren zijn niet meer zeldzaam te noemen; ze zijn eerder het nieuwe normaal*

# 2 Digitale risico's onverminderd groot

**Aan de analyse in het Cybersecuritybeeld Nederland liggen de invalshoeken belang, digitale dreiging en weerbaarheid ten grondslag. Deze drie bepalen in samenhang de digitale risico's. Er zijn vier risico's voor de nationale veiligheid (zie het kader hieronder). Deze risico's hebben ook betrekking op sectoren, organisaties en personen. In dit hoofdstuk wordt in vogelvlucht het huidige beeld van nationale veiligheidsbelangen, de dreiging daartegen en onze digitale weerbaarheid geschetst. Dit beeld is ten opzichte van vorig jaar niet fundamenteel gewijzigd. Wel is het dreigingsbeeld geëvolueerd. Zo streven ransomwaregroepen optimale, schaalbare aanvalsketens na. Ook focussen aanvallers zich in toenemende mate op misbruik van de cloud. Tot slot vormen cyberaanvallen op leveranciersketens en het uitbuiten van *zero-day* kwetsbaarheden een groeiend probleem.**

### Vier risico's voor de nationale veiligheid

1. Ongeautoriseerde inzage in informatie (en eventueel publicatie daarvan), in het bijzonder door spionage. Denk aan spionage van communicatie binnen de Rijksoverheid of de ontwikkeling van innovatieve technologieën.
2. Ontoegankelijkheid van processen, als gevolg van (voorbereidingen voor) sabotage en de inzet van ransomware. Denk aan de innesteling in processen die zorgdragen voor de distributie van elektriciteit.
3. Schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leveranciersketens.
4. Grootschalige uitval: een situatie waarin één of meer processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van niet-moedwillig menselijk handelen.

## Digitale processen zenuwstelsel maatschappij

Digitale processen vormen het 'zenuwstelsel' van de maatschappij en economie, omdat ze onmisbaar zijn voor het ongestoord functioneren daarvan.[2] Digitale veiligheid is dan ook onlosmakelijk verbonden met de nationale veiligheid. Het raken van vitale processen, zoals de elektriciteits- of drinkwatervoorziening, de scheepvaartafwikkeling of het betalingsverkeer, kan de samenleving kort of langdurig tot stilstand brengen. Cyberincidenten kunnen dus meer en andere belangen aantasten dan alleen het functioneren van techniek. De zes nationale veiligheidsbelangen zoals beschreven in de Nationale Veiligheid Strategie (NVS)[3] kunnen ieder worden geraakt via de digitale ruimte. Digitale veiligheid is niet expliciet benoemd als nationaal veiligheidsbelang, maar loopt als een rode draad door de zes de belangen heen. Ze worden hieronder kort toegelicht.

**Territoriale veiligheid** is het ongestoord functioneren van Nederland en zijn EU- en NAVO-bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin. Het gaat daarbij niet alleen om de integriteit van ons nationaal en bondgenootschappelijk grondgebied, maar ook om de integriteit van het digitale domein; de beschikbaarheid, vertrouwelijkheid en integriteit van essentiële informatiediensten en daarvan afhankelijke vitale infrastructuur en processen.

**Fysieke veiligheid** is het ongestoord functioneren van de mens in Nederland en zijn omgeving. De fysieke veiligheid in enge zin betreft de veiligheid van lijf en leden van Nederlandse ingezetenen. In ruime zin gaat het om het voorzien in primaire levensbehoeften, zoals voedsel, energie, drinkwater en adequate huisvesting.

**Economische veiligheid** is het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. De drie essentiële voorwaarden hiervoor zijn de continuïteit van vitale processen, de integriteit en exclusiviteit van informatie en kennis, en het voorkomen van ongewenste strategische afhankelijkheden.

**Ecologische veiligheid** is het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland. Het raken van de ecologische veiligheid uit zich in langdurige aantasting van het milieu en de natuur.

**Sociale en politieke stabiliteit** is het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden.

Tenslotte is de **internationale rechtsorde** het functioneren van het internationale stelsel van normen en afspraken, gericht op internationale vrede en veiligheid. Onze nationale veiligheid is afhankelijk van het functioneren van het internationale stelsel van normen en afspraken, mede gezien de Nederlandse internationale positie en aanwezigheid van fysieke en digitale knooppunten in mondiale netwerken en infrastructuur.

## Dreiging vooral van statelijke actoren en cybercriminelen en door uitval

De dreiging tegen de nationale veiligheidsbelangen kan voortkomen uit cyberaanvallen of uitval van digitale processen. Uitval kan het gevolg zijn van natuurlijke of technische oorzaken, of van menselijke fouten. Statelijke actoren en cybercriminelen vormen de voornaamste dreiging in relatie tot moedwillig handelen, waarbij ze niet altijd goed van elkaar te onderscheiden zijn vanwege onderlinge relaties. De dreiging die uitgaat van hacktivisten is relatief klein, maar kan Nederlandse belangen wel indirect raken.

### Cyberaanvallen door statelijke actoren zijn nieuwe normaal

De digitale dreiging die uitgaat van statelijke actoren richting de Nederlandse samenleving is divers. Cyberaanvallen door statelijke actoren zijn niet meer zeldzaam te noemen: ze zijn eerder het nieuwe normaal. De digitale ruimte wordt door staten gebruikt om geopolitiek voordeel te behalen. Dit kan financieel-economisch voordeel zijn, het behartigen van binnenlandse politieke en veiligheidsbelangen, of het beïnvloeden van buitenlandse verhoudingen.[4] Statelijke actoren kunnen hiervoor onder meer de volgende digitale middelen inzetten:

1. Beïnvloeding en inmenging (inclusief het verspreiden van desinformatie);
2. Spionage, waaronder economische of politieke spionage;
3. Voorbereidingshandelingen voor en daadwerkelijke verstoring en sabotage.

Nederland is doelwit van een offensief cyberprogramma van landen als Rusland en China. Zij kunnen de genoemde digitale middelen inzetten tegen een breed scala aan mogelijke doelwitten, van lokale verenigingen tot internationale veiligheidsorganisaties en van één individu tot diasporagemeenschappen. Volgens de AIVD blijft de dreiging van offensieve cyberprogramma's tegen Nederland en de Nederlandse belangen onverminderd hoog en zal deze in de toekomst alleen maar toenemen.[5]

Russische statelijke actoren hebben meermaals (succesvolle) digitale aanvallen uitgevoerd op een EU-lidstaat. Dit valt binnen het normbeeld van Russische statelijke actoren en de aanhoudende digitale (spionage)dreiging die daarvan uitgaat. Deze actoren voeren veelvuldig digitale aanvallen uit op onder andere EU- en NAVO-lidstaten.

De Chinese digitale spionage actor APT31 heeft op grote schaal en langdurig politieke doelwitten in Europa en Noord-Amerika aangevallen.[6] Ook in Nederland waren er doelwitten van aanvallen en verkenningsactiviteiten door deze actor. De interesse vanuit statelijke actoren voor dergelijke doelwitten illustreert het belang van goede beveiligingsmaatregelen en netwerkdetectie-mogelijkheden voor Nederlandse overheidsnetwerken om aanvallen te detecteren, af te slaan en nader onderzoek mogelijk te maken.

Volgens gelekte documenten deed een Iraanse cyberorganisatie in 2020 onderzoek naar het hacken van industriële controlesystemen. De Iraanse onderzoekers schrijven dat ze nog niet genoeg inzicht hebben in de systemen om fysieke sabotage mogelijk te maken. Uit de documenten blijkt dat de cyberactoren specifiek zochten naar gebouwbeheersystemen, onder andere in Nederland. Dit zou passen binnen het beeld van de toenemende aandacht voor cybersabotage binnen Iran.

## Cybercriminelen kunnen nationale veiligheid aantasten

Cybercriminelen zijn onverminderd in staat om omvangrijke schade toe te brengen aan digitale processen. Zij handelen vanuit financieel motief en hebben niet de intentie om de maatschappij te ontwrichten. Desondanks kunnen hun aanvallen zoveel impact veroorzaken dat ze nationale veiligheidsbelangen raken. De capaciteit van meerdere cybercriminele groepen is van gelijkwaardig hoog niveau als die van sommige statelijke actoren. Statelijke actoren kunnen cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen op gewenste doelwitten uit te voeren.[7] De relaties tussen staten en cybercriminelen kunnen ertoe leiden dat cybercriminelen een kant kiezen in geopolitieke conflicten. Recent illustreerde de oorlog in Oekraïne dit, toen cybercriminele groepen gelieerd aan Rusland waarschuwden tegenstanders van Rusland in het conflict digitaal aan te zullen vallen.[8]

Cyberaanvallen op leveranciersketens door criminelen zijn een groeiend probleem.[9] Cyberincidenten hebben namelijk niet alleen impact op directe slachtoffers, maar ook op ketens van leveranciers, klanten en burgers die gebruik maken van de dienstverlening van de getroffen organisaties. Steeds vaker compromitteren cybercriminelen via leveranciers en zakenpartners hun einddoelwitten.[10] Bij het verstoren van processen kunnen keteneffecten hele sectoren of zelfs de gehele maatschappij raken.[11] Bovendien worden ransomware-aanvallen steeds vaker ingezet met dubbele of zelfs drievoudige afpersing.[12] Bij dubbele afpersing kunnen hackers na het versleutelen van bestanden dreigen met het publiceren van data als slachtoffers niet betalen. Bij drievoudige afpersing kunnen hackers via buitgemaakte gegevens ook klanten, partners en leveranciers van een getroffen organisatie een losgeldeis opleggen, in de hoop dat ook zij uit angst voor publicatie overgaan tot betaling.[13]

Organisaties die digitaal worden aangevallen zijn veelvuldig het slachtoffer van ransomware. De inzet hiervan vormt een risico voor de nationale veiligheid als het gaat om de continuïteit van vitale processen, het weglekken en/of publiceren van vertrouwelijke of gevoelige informatie en de aantasting van de integriteit van de digitale ruimte.[14] Vitale processen kunnen niet alleen zelf getroffen worden door ransomware, met alle gevolgen van dien, maar ook via leveranciersketens. Dat is zeker het geval nu die aanvallen gepaard gaan met dubbele of zelfs drievoudige afpersing.

## Aanvallers hebben focus op *zero-days* en de cloud

Misbruik van *zero-day* kwetsbaarheden is nog steeds een punt van zorg.[I] Het NCSC ziet een toename van het aantal zero-day kwetsbaarheden. Misbruik van zero-days kan grootschalige impact hebben als de kwetsbaarheid in veelgebruikte software of hardware zit. Zodra een zero-day openbaar is gemaakt, wordt het een *one-day* of n-day kwetsbaarheid genoemd. Deze vormt ook een risico omdat er wellicht een patch beschikbaar is, maar de gebruiker deze mogelijk nog niet heeft doorgevoerd. Zo kunnen kritische systemen en applicaties voor (vitale) processen niet altijd onmiddellijk offline worden gehaald voor het installeren van een patch, waardoor ze kwetsbaar zijn voor misbruik.

De MIVD en de AIVD beschikken over aanwijzingen dat statelijke actor(en) misbruik maken van een onbekende kwetsbaarheid (zero-day) in PulseConnect SecureVPN-software, specifiek CVE-2021-22893. De diensten adviseren nationale afnemers om zo spoedig mogelijk beveiligingsmaatregelen voor deze zero-day te treffen. Het NCSC heeft, mede op basis van informatie van de AIVD en MIVD, adviezen gepubliceerd op haar website om organisaties te ondersteunen bij het mitigeren van deze kwetsbaarheid.

De inzet van zero-day exploits door statelijke actoren tegen Nederlandse doelwitten is illustratief voor de structurele en geavanceerde statelijke digitale dreiging tegen Nederlandse economische en politieke veiligheidsbelangen.

Aanvallers focussen zich ook in toenemende mate op misbruik van de cloud.[15] Clouddiensten zijn de afgelopen jaren cruciale elementen van vele bedrijfsprocessen geworden.[16] Kwaadwillende actoren zien deze afhankelijkheid als een nieuwe kans om digitale processen te verstoren.[17] Meer gebruik van de cloud levert immers ook meer potentiële slachtoffers op. Als clouddiensten uitvallen of verstoord raken, kan dat grootschalige gevolgen hebben voor Nederlandse organisaties en sectoren.

I Een zero day-kwetsbaarheid is een kwetsbaarheid waar nog geen patch voor is, maar die door hackers al wel ontdekt is en misbruikt kan worden.

### Polarisatie en internationale conflicten: voedingsbodem voor hacktivisten

De directe dreiging die richting Nederland uitgaat van hackerscollectieven, zoals hacktivisten[II], is klein. Er bestaat echter wel een afgeleide dreiging vanuit deze groeperingen. In diverse landen zijn hacktivisten aanwezig die impact kunnen veroorzaken door bijvoorbeeld *hack-and-leak* operaties of het stelselmatig digitaal intimideren van personen en organisaties. Hackerscollectieven kunnen ook een rol spelen in hybride conflictvoering, zoals in de oorlog in Oekraïne in 2022 het geval is. Het gevaar is dat de activiteiten van hacktivisten verkeerd geïnterpreteerd worden door landen die het slachtoffer worden van hun aanvallen, wat tot tegenreacties kan leiden. Ook kunnen statelijke actoren onder de vlag van hacktivisten opereren. Door verhoogde activiteit van hackersgroepen is de kans aanwezig dat Nederland (neven)schade ondervindt van digitale aanvallen. Indien hackers cyberaanvallen vanuit of via Nederland uitvoeren op buitenlandse doelwitten, kan Nederland ook getroffen worden door een tegenreactie. Ook Nederlandse ingezetenen kunnen deelnemen aan acties van hacktivisten en zo betrokken raken bij conflicten. Betrokkenheid bij een conflict elders door het plegen van digitale aanvallen kan onvoorziene consequenties hebben en is bovendien strafbaar.[18]

## Weerbaarheid nog niet voldoende

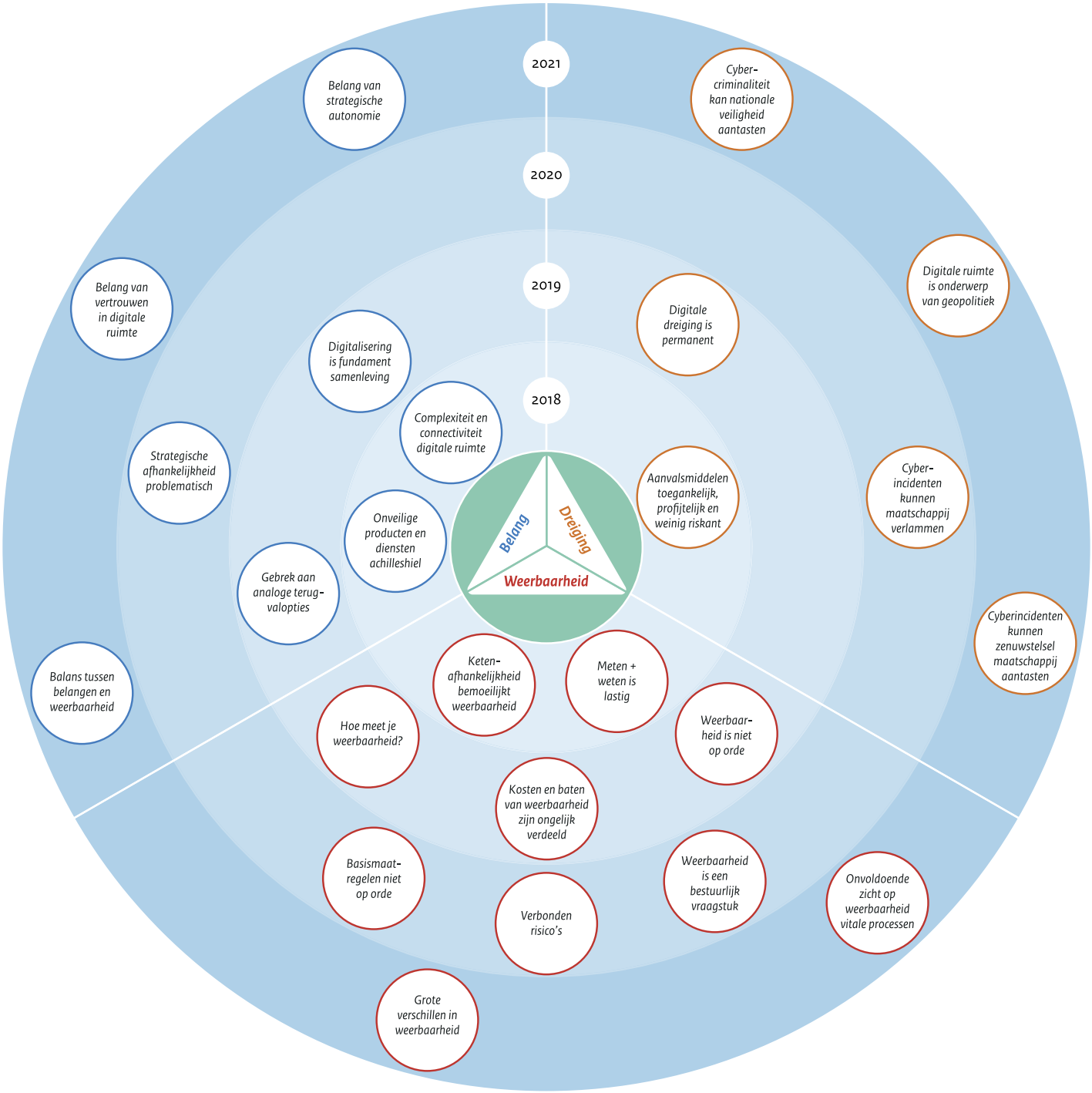
In het CSBN2021 werd geconstateerd dat de weerbaarheid in Nederland nog niet voldoende is.[19] Dit beeld is ongewijzigd. Dat blijkt uit verschillende rapporten die het afgelopen jaar verschenen zijn. Zo groeit volgens de Onderzoeksraad voor Veiligheid (OVV) de kloof tussen de omvang van de dreiging en digitale afhankelijkheid enerzijds, en de weerbaarheid van de samenleving daartegen anderzijds.[20] Ook wijzen rapporten van de Cyber Security Raad (CSR) en de OVV op gefragmenteerde incidentbestrijding, onvoldoende toezicht en gebrekkige informatiedeling.[21] De Algemene Rekenkamer stelde in mei 2022 dat de informatiebeveiliging bij de rijksoverheid een opgaande lijn vertoont en stapsgewijs op orde komt. Toch worden er nog steeds onvolkomenheden (grote tekortkomingen) geconstateerd, waarvan de oplossing vraagt om een vasthoudende en gestructureerde aanpak.[22] Volledige weerbaarheid tegen digitale dreigingen is onmogelijk, maar verhoging van de weerbaarheid tegen uitval en misbruik is wel het belangrijkste instrument om digitale risico's te beheersen.

De digitale weerbaarheid is nog niet overal op orde doordat basismaatregelen niet voldoende doorgevoerd worden. Dit betreft bijvoorbeeld het gebruik van multifactor authenticatie en het maken en testen van back-ups.[23] Er zijn grote verschillen in weerbaarheid tussen en binnen sectoren en ketens. De Inspectie Justitie en Veiligheid stelt dat er nog veel werk aan de winkel is om de weerbaarheid van vitale organisaties te verhogen, waarbij ook geconstateerd wordt dat het bewustzijn van het belang wel is toegenomen.[24] Organisaties die wel voldoende weerbaar zijn, hebben zich naast het nemen van basismaatregelen ook gericht op een op risico's gebaseerde manier van werken.[25]

II 'Hacktivist' is een samentrekking van hacker en activist: een actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt.

# Terugblik CSBN 2018-2021

Onderstaande afbeelding toont de thema's die de afgelopen vier jaar op het gebied van belang, dreiging en weerbaarheid in het CSBN zijn opgenomen. CSBN 2022 bouwt hierop voort met belangrijke thema's voor de digitale veiligheid van Nederland, nu en de komende vier tot zes jaar.



*Het digitale domein is per definitie grenzeloos, wat criminelen ongekende mogelijkheden biedt om doelwitten verspreid over de hele wereld aan te vallen*

# 3 Complicaties risico-beheersing gevaar voor samenleving

**De NCTV heeft in samenwerking met partners strategische thema's geïdentificeerd die nu en de komende jaren relevant zijn voor de digitale veiligheid van Nederland :**
**- Risico's vormen de keerzijde van een gedigitaliseerde samenleving.**
**- Digitale ruimte is speelveld voor regionale en mondiale dominantie.**
**- Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet.**
**- Marktdynamiek compliceert de beheersing van digitale risico's.**
**- Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen.**
**Aanvullend is een overkoepelend thema geïdentificeerd dat de andere thema's raakt: beperkingen in digitale autonomie beperken ook digitale weerbaarheid. Hoewel uiteenlopend van aard, illustreren de thema's ieder op zich en in samenhang complicaties voor strategische risicobeheersing. De thema's worden hieronder nader toegelicht. De strategische en beleidsmatige opvolging van deze thema's zal geadresseerd worden in de Nederlandse Cybersecurity Strategie (NLCS).**

## Risico's vormen de keerzijde van een gedigitaliseerde samenleving

De Nederlandse samenleving is in hoge mate gedigitaliseerd.[27] Er zijn amper nog processen zonder digitale component.[28] Het onderwijs, de zorg, het bedrijfsleven, de overheid en burgers maken allemaal veelvuldig gebruik van digitale processen en kunnen niet zonder. Daarnaast stimuleren bepaalde maatschappelijke ontwikkelingen, zoals de energietransitie, verdere digitalisering.[29]

Digitalisering heeft de samenleving en economie veel goeds gebracht, maar dat heeft ook een keerzijde: het ontstaan van risico's. Zo maakt afhankelijkheid van digitale processen, producten, diensten en netwerken (hierna: digitale processen) ons kwetsbaar. Die afhankelijkheid biedt talrijke mogelijkheden voor kwaadwillenden. Doelbewuste aanvallen op processen zijn aan de orde van de dag. Vaak worden kwetsbaarheden (bijvoorbeeld in software) actief misbruikt bij het uitvoeren van aanvallen. Staten voeren digitale aanvallen uit om te spioneren of om (in een later stadium) te kunnen saboteren. Zo zijn er landen die op structurele basis proberen om zich digitaal toegang te verschaffen tot de vitale infrastructuur van onze bondgenoten, om daar voorbereidingshandelingen voor digitale verstoring of zelfs sabotage te treffen. Ook Nederland is in het verleden doelwit geweest van voorbereidingshandelingen voor sabotage.[30] Cybercriminelen spelen in op de afhankelijkheid van digitalisering met ransomware-aanvallen en verdienen daar grote sommen geld mee. Ze maken daarbij ook misbruik van via *hacks* gestolen data.

Wanneer digitale processen niet naar behoren werken, heeft dat effect op het functioneren van organisaties. Keteneffecten kunnen sectoren of zelfs de gehele maatschappij raken. Daarbij kan de verstoring van digitale processen fysieke consequenties hebben. Zo kan stroomuitval plaatsvinden, onderwijs stil komen te liggen, of patiëntenzorg in een ziekenhuis worden belemmerd.[31] Ook vitale processen hebben een digitale component en zijn daarmee kwetsbaar. In het ernstigste geval kunnen niet goed functionerende processen leiden tot maatschappelijke ontwrichting, waarbij de nationale veiligheid in het geding is.

De hoge mate van digitalisering van onze samenleving en de afhankelijkheid van digitale processen zijn een gegeven. Het beheersbaar krijgen en houden van kwetsbaarheden is onderdeel van de risicobeheersing, maar dit is niet eenvoudig. Wanneer dit niet in voldoende mate lukt, kan de stabiliteit van de samenleving in gevaar komen en maatschappelijke ontwrichting ontstaan.

## Digitale ruimte is speelveld voor regionale en mondiale dominantie

Een groeiend aantal staten gebruikt de digitale ruimte structureel én intensief voor de behartiging van hun geopolitieke belangen. Omgekeerd zijn vraagstukken van de digitale ruimte steeds meer van geopolitiek belang.[32] Geopolitiek is een breed begrip, maar de basis is altijd het actief willen verbeteren van de eigen relatieve uitgangspositie in politieke, economische, militaire of culturele zin, zowel regionaal als mondiaal. Technologie (denk aan opkomende technologieën zoals 5G, AI en kwantumtechnologie) is hierbij zowel het speelveld, als het middel, als de inzet van het spel. Binnen de bestaande digitale ruimte vinden aanvallen plaats met als doel het inwinnen van inlichtingen en data, het verstoren van operationele processen en bijvoorbeeld het sentiment in buurlanden beïnvloeden. Ook het ultieme geopolitieke conflict, oorlog, gaat gepaard met cyberaanvallen. Dit is bijvoorbeeld zichtbaar in Oekraïne, waar Russische statelijke actoren voor en tijdens de invasie digitale aanvallen pleegden, gericht op de verstoring van communicatie en logistiek. Tenslotte behartigen staten hun belangen door strategisch gebruik te maken van de bouwstenen van de digitale ruimte. Het gaat dan concreet om hulpbronnen, standaarden en bouwstenen als hard- en softwarecomponenten. Vanwege het belang van de digitale ruimte voor economie en samenleving, erkennen steeds meer landen dat digitale veiligheid een onderdeel is van nationale veiligheid.[33]

### Cyberaanvallen instrument voor behartigen geopolitieke belangen

De digitale ruimte gaat naar zijn aard over landsgrenzen heen en strekt zich uit ter land, ter zee, in de lucht en in de ruimte. Het vergaren van politieke en economische inlichtingen, het verzamelen en controleren van data en het verstoren van operationele processen vindt plaats zonder een voet over de grens te plaatsen. Cyberaanvallen zijn relatief goedkoop, schaalbaar, moeilijk te attribueren en ze kennen een hoge, vaak langdurige opbrengst. Een geslaagde inbreuk kan soms jarenlang onzichtbaar, heimelijk en ongestraft informatie blijven opleveren.[34] Kwaadwillende statelijke actoren slagen er regelmatig in om toegang te krijgen tot de informatiehuishouding van overheidsorganisaties, NGO's en bedrijven.[35] De landen met een offensief cyberprogramma bouwen hun voorsprong verder uit. Daarnaast komen ook kleinere landen op, die beschikken over meer dan gemiddelde cybercapaciteiten. Regionale spelers als Iran en Noord-Korea zijn op cybergebied mondiale spelers.

Het gebruik van de digitale ruimte door statelijke actoren lijkt eerder toe dan af te nemen.[36] Een voor de hand liggende verklaring daarvoor is dat de digitale ruimte nog steeds aan omvang en betekenis toeneemt en daarmee ook de mogelijkheden voor misbruik. Dat is bijvoorbeeld zichtbaar in de voortdurende groei van het Internet of Things (IoT) waarin gebruiksvoorwerpen als verlichting en auto's allemaal 'slim' worden en gekoppeld aan het internet, met kwetsbaarheid als keerzijde. De groei is zichtbaar in de ontwikkeling van het gebruik van data en datatoepassingen.[37] Daarmee nemen de potentiële baten van cyberaanvallen toe.

Een tweede verklaring voor het toenemend gebruik van de digitale ruimte door statelijke actoren vormen ontwikkelingen op geopolitiek gebied zelf. Al jaren is het mondiaal machtsevenwicht door de opkomst van de BRICS[III] landen aan het verschuiven. Dit leidt tot meer interventies, uitdagingen en het opzoeken van grenzen. Beide ontwikkelingen zijn autonoom, maar versterken elkaar. Een concreet effect is dat staten in toenemende mate hun belangen behartigen door middel van cyberoperaties,[38] zoals voor politieke, economische en militaire spionage. China is ongeëvenaard in de schaal waarop en de breedte waarin inlichtingen worden ingewonnen. De intensiteit waarop staten de digitale ruimte gebruiken, maakt dat digitale systemen, zoals communicatieverbindingen, encryptiemechanismen, maar ook computers van individuen, zich in de frontlinie bevinden omdat zij voortdurend worden getest of gecompromitteerd.

Tot slot hebben ook cybercriminele activiteiten geopolitieke betekenis door de vage grenzen tussen statelijke en criminele actoren. Cybercriminele groepen worden in toenemende mate ingezet door statelijke actoren voor activiteiten van nationaal belang.[39] Die inzet wordt ook weer beïnvloed door actuele geopolitieke ontwikkelingen. Zo is de verwachting dat Rusland zich verder zal ontwikkelen als *safe haven* voor cybercriminelen als gevolg van de verslechterde relatie tussen het Westen en Rusland door de oorlog in Oekraïne. Vanwege de economische sancties zal Rusland niet geneigd zijn om cybercriminelen die westerse belangen aanvallen te hinderen.

III Met het acroniem BRICS wordt bedoeld: Brazilië, Rusland, India, China en Zuid-Afrika.

Een cyberconflict tussen andere landen kan in Nederland onbedoeld leiden tot verstoring of uitval. Zo kan misbruik worden gemaakt van Nederlandse infrastructuur[40] of kan die geraakt worden door eventuele tegenacties, zoals het afkoppelen van digitale infrastructuur door landen die door een digitale aanval getroffen zijn.

Het is mogelijk dat er te midden van de huidige Oekraïne-crisis *phishing* e-mails verzonden zullen worden vanaf gecompromitteerde of *gespoofde* mailaccounts behorende tot de Oekraïense overheid. Gebruikers worden daarom geadviseerd om bedacht te zijn op e-mails die verzonden zijn vanuit Oekraïense overheidsdomeinen, ook als deze door doorgaans betrouwbare afzenders zijn verzonden.

Bij een wereldwijde cybercampagne gericht tegen beveiligingsonderzoekers is misbruik gemaakt van een gehackte Nederlandse server. De aanvalscampagne was specifiek gericht tegen beveiligingsonderzoekers en zeer waarschijnlijk afkomstig van een statelijke actor.

Een Russische statelijke actor hackt wereldwijd routers van willekeurige thuisgebruikers en het MKB, waaronder een klein aantal in Nederland. Hiermee heeft de actor een *botnet* gevormd dat mogelijk voor verdere cyberoperaties door de actor kan worden ingezet.

## Geopolitiek steekspel rond hoogwaardige technologie en digitale ruimte

De digitale ruimte wordt gevormd door allerhande digitale processen en wordt in de lucht gehouden door een fijnmazig fysiek netwerk van systemen, datacenters, knooppunten, kabels en apparaten van eindgebruikers.[41] Op deze hardware zijn vele lagen van software actief die uiteindelijk de digitale ruimte creëren. Alle onderdelen van de digitale ruimte kunnen gebruikt worden voor geopolitieke sturing of misbruik. Dat kan met hardware, software, maar ook met standaarden. Een belangrijk geopolitiek steekspel vindt plaats rond zogenoemde hoogwaardige technologieën: technologieën die essentieel zijn voor kennisontwikkeling en innovaties op een bepaald terrein en daarom van belang zijn voor strategische autonomie en het verdienvermogen.

China is er sterk op gebrand de eigen halfgeleiderindustrie verder te ontwikkelen en de grote afhankelijkheid van buitenlandse halfgeleidertechnologie voor de productie van hoogwaardige chips te verminderen. De ambitie om tot technologieleiderschap te komen is verankerd in verschillende beleidsplannen. Om tot het vereiste kennisniveau te komen investeert China grote bedragen in ontwikkeling van de chipindustrie. De handelsoorlog met de VS, exportrestricties, technologie achterstand en een gebrek aan gekwalificeerd personeel zijn belangrijke hindernissen voor China om de ambities te realiseren. China zet zowel legitieme als illegitieme middelen in om deze tegenslagen te overwinnen. Het Chinese instrumentarium bestaat onder andere uit buitenlandse investeringen, het aantrekken van hoogopgeleid westers personeel, inzet van (digitale) spionage en het importeren van westerse technologie. Dit Chinese palet aan middelen wordt zowel afzonderlijk als integraal ingezet. De gecombineerde inzet van het instrumentatrium verhoogt de kans van slagen om een product of technologie succesvol te reproduceren en past binnen een alomvattende Chinese aanpak waarbij verschillende partijen en verschillende collectiemethoden worden ingezet om buitenlandse technologie te verwerven. De Chinese activiteiten vormen tesamen een omvangrijke diverse persistente dreiging voor de Nederlandse economische veiligheidsbelangen. De Chinese inspanningen halfgeleidertechnologie te bemachtigen resulteren voor Nederland in risico's op technologiediefstal, en ongewenst eindgebruik. Zo is er een groot risico dat Nederlandse halfgeleidertechnologie tevens wordt aangewend voor de ontwikkeling van Chinese militaire technologie. De huidige Chinese afhankelijkheid van westerse, waaronder Nederlandse, halfgeleidertechnologie, zal zeer waarschijnlijk voorlopig leiden tot een toename van de Chinese pogingen om dergelijke technologie op legale of illegale wijze te verkrijgen.

Staten kunnen op uiteenlopende wijzen geopolitiek bedrijven in de digitale ruimte. Het heeft impact wanneer staten hulpbronnen zoals individuele hardwarecomponenten en softwaretoepassingen over bijvoorbeeld 5G communicatietechnologie kunnen sturen en controleren. Die impact is groter wanneer staten of samenwerkingsverbanden van staten over het vermogen beschikken om bouwstenen, standaarden of ontwerpprincipes van de digitale ruimte te domineren. Concreet is het bijvoorbeeld zichtbaar bij de ontwikkeling van Cloudtechnologie. Cloudtechnologie kent een aantal specifieke veiligheidsvraagstukken, maar heeft ook een sterk geopolitieke component omdat de grootste aanbieders (Amazon, Microsoft en Google) afkomstig zijn uit de Verenigde Staten. Vanzelfsprekend zijn de vraagstukken ten aanzien van *big tech* en die ten aanzien van landen verschillend, maar het gaat hier om de afhankelijkheid.

Afhankelijkheid alleen hoeft nog niet problematisch te zijn. Er komt bij dat landen en groepen van landen fundamenteel verschillend aankijken tegen de uitgangspunten van het internet. Internet is lange tijd de technologie geweest van het 'tech-optimisme'; een technologie die informatie vrij ter beschikking kon stellen aan iedereen en daarom bij zou dragen aan vrijheid, autonomie en democratie, zowel op het niveau van landen als van individuen. De waarden van een systeem, democratisch of autocratisch, werken echter door in de wijze waarop de bouwstenen van de architectuur worden geschikt. In autocratische landen is sterk ingezet op de beperking van de vrijheid van informatie en meningsuiting en hier kan dezelfde technologie ook worden ingezet voor monitoring, sturing en controle van individuen. Autoritaire regimes kijken ook anders naar integriteit en vertrouwelijkheid van gegevens dan democratische samenlevingen. Dit raakt digitale veiligheid op een fundamentele wijze. Digitale veiligheid is niet neutraal. Eenzijdige

afhankelijkheid van bouwstenen van de digitale ruimte stimuleert de behoefte aan strategische autonomie. Deze behoefte heeft voor- en nadelige consequenties voor digitale veiligheid. Er bestaat bijvoorbeeld een spanningsveld tussen digitale veiligheid en interoperabiliteit; zelf ontwikkelde bouwstenen moeten wel passen in het grotere bouwwerk. Ook schaalvoordelen, globale marktwerking en wereldwijde standaardisatie worden minder makkelijk gerealiseerd[IV]. Strategische autonomie heeft een prijs, maar het gebrek daaraan ook. Daarom wordt op Europees niveau geïnvesteerd in alternatieven voor bestaande bouwstenen, zoals het data-infrastructuurprogramma Gaia-X.[42] De uitdaging zit in het zoeken naar de juiste balans.

## Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet

Zware, georganiseerde cybercriminaliteit is zeer schaalbaar geworden en heeft daardoor in de afgelopen jaren qua slachtoffers, schade en criminele opbrengsten een industriële omvang aangenomen. Ransomware is daarbij een *gamechanger* gebleken. De term schaalbaarheid is een kernbegrip binnen de ICT. Het verwijst naar het vermogen om een systeem of proces aan te passen (op te schalen) om te kunnen voldoen aan een grotere vraag. Zware cybercriminelen en hun dienstverleners zijn primair financieel gemotiveerd en gaan voor maximale opbrengsten, waarbij ze dankbaar gebruik maken van de mogelijkheden die het digitale domein biedt. Het opschalen van hun processen en systemen doen zij voor een belangrijk deel door effectief samen te werken en door voortdurend te innoveren als het gaat om automatisering. Deze manier van werken is een essentieel onderdeel van hun verdienmodel en de (criminele) marktwerking.

Gezien de aard en groeiende omvang van de cybercriminele dreiging is het schaalbaar maken én houden van de weerbaarheidsketen een fundamentele uitdaging voor de komende jaren. Aan de zijde van cybersecurity en cybercrimebestrijding is het bereiken van schaalbaarheid in technische zin niet het probleem. Waar mogelijk gebeurt dit al. Het zijn vooral de organisatorische aspecten (samenwerking) en de juridische aspecten (informatie-uitwisseling) die de grootste knelpunten en groeipijnen kennen.

### Maximale opbrengst met minimale risico's voor de aanvallers

Cybercriminaliteit is een misdaadvorm die zich uitstekend leent voor opschaling. Het digitale domein is per definitie grenzeloos, wat criminelen ongekende mogelijkheden biedt om doelwitten verspreid over de hele wereld aan te vallen. Daarnaast beperkt deze grenzeloosheid de risico's voor cybercriminelen, aangezien dit de meer locatiegebonden opsporing en vervolging bemoeilijkt. Hierbij weten cybercriminelen verschillen in jurisdictie per land vaak feilloos te benutten. Sommige cybercriminele groepen opereren bovendien vanuit *safe havens*: landen waar zij ongemoeid worden gelaten door de overheid, of daar zelfs mee samenwerken.[43] Tot slot biedt het digitale domein cybercriminelen - evenals cybercriminele dienstverleners – de mogelijkheid om voortdurend hun processen en verdienmodellen te optimaliseren. Samenwerking, specialisering en automatisering zijn hier centrale begrippen die nauw met elkaar zijn verweven.

#### *Optimale aanvallen door samenwerking en automatisering*

Samenwerking in de zin van het uitbesteden van complexe onderdelen van de aanvalsketen aan gespecialiseerde dienstverleners en het voortdurend automatiseren van processen, stellen cybercriminelen in staat om de aanvalsketen zowel kwantitatief als kwalitatief te optimaliseren.[44] Uit opsporingsonderzoeken blijkt dat cybercriminele groepen in het zware, georganiseerde segment zijn verworden tot professionele samenwerkingsverbanden met leiders die vooral sterke organisatorische vaardigheden nodig hebben.[45] Daarbij is het geen uitzondering meer dat zij een bedrijfsvoering aanhouden die overeenkomt met een legitiem MKB-bedrijf in de hightechsector.[46] Zij maken pragmatische keuzes ten aanzien van wat men in eigen beheer ontwikkelt, welke onderdelen van de aanvalsketen worden uitbesteed aan partners en welke diensten worden afgenomen van gespecialiseerde cybercriminele dienstverleners.[47] Zolang de financiële opbrengst maar maximaal is en de operationele risico's minimaal blijven. Vaak wordt het verkrijgen van toegang tot slachtoffernetwerken uitbesteed aan daarin gespecialiseerde partijen.[48] Geavanceerde middelen om deze netwerken maximaal te exploiteren neemt men vervolgens af van andere criminele aanbieders.[49]

Innovatie kenmerkt het cybercriminele ecosysteem. Automatisering is daarbij een middel om een hoge mate van efficiëntie te bereiken. Cybercriminele dienstverleners passen veelvuldig automatisering toe om op efficiënte wijze zoveel mogelijk afnemers te bedienen.[50] Aanbieders van *ransomware-as-a-service* bieden hun afnemers controlepanelen aan waarin alle aspecten van de aanval geïntegreerd zijn.[51] Aanvallers zetten de toeleveringsketen van hun slachtoffers om in geautomatiseerde aanvalsvectoren. Zo wisten ransomware-aanvallers een kwetsbaarheid van de servers van softwareleverancier Kaseya uit te buiten om binnen enkele uren ransomware te installeren op de netwerken van meer dan 1500 klanten.[52]

IV Vanzelfsprekend zijn er ook positieve voorbeelden zoals de standaardisatie van TLS 1.3 en de standaardisatie van cryptografische algoritmen, etc., waar de EU in belangrijke mate aan bijdraagt.

### *De industriële omvang van cybercriminaliteit*

De coronacrisis heeft de digitale connectiviteit van de samenleving in een stroomversnelling gebracht.[53] Het aanvalsoppervlak dat cybercriminelen kunnen benutten, is daarmee significant toegenomen.[54] Dit, in combinatie met het vermogen om de aanvalsketen voortdurend te optimaliseren en daarmee op te schalen, heeft het mogelijk gemaakt dat cybercriminaliteit in de afgelopen jaren qua slachtoffers, schade en criminele opbrengsten een industriële omvang heeft aangenomen. Zo domineerde de groep achter het Emotet-botnet meerdere jaren de markt van het verkrijgen en daarna doorverkopen van toegang tot slachtoffernetwerken aan onder meer ransomware-groepen. Tijdens een internationale opsporingsoperatie in 2020-21 om dit botnet uit de lucht te halen, onderkende de politie wereldwijd 1,75 miljoen geïnfecteerde IP-adressen, 36 miljoen gestolen inloggegevens en ruim 4 miljoen gecompromitteerde (bedrijfs)mailaccounts.[55] Dergelijke slachtofferaantallen zijn geen uitzondering meer.

Ransomware is daarbij uitgegroeid tot een cybercriminele goudmijn. Dit heeft de dreiging van cybercriminaliteit aanzienlijk doen toenemen. Zo werd in het CSBN2021 geconcludeerd dat ransomware tot risico voor de nationale veiligheid is verworden. Er wordt feilloos gebruik gemaakt van een vaak te lage digitale weerbaarheid van slachtoffers en de mogelijkheid om hun - vaak existentiële - bedrijfscontinuïteit volledig te verstoren en weggesluisde gevoelige informatie openbaar te maken. De potentiële schade van dergelijke aanvallen is groot, waardoor de betalingsbereidheid van slachtoffers vaak hoog is. En daarmee de opbrengsten voor de cybercriminelen ook. Antivirusbedrijf Emsisoft schat dat in 2020 in tien onderzochte westerse landen minimaal 18 miljard Amerikaanse dollar is betaald als losgeld voor ransomware-aanvallen. De totale schade veroorzaakt door deze aanvallen zou minstens 80 miljard dollar bedragen.[56]

Met recht is *ransomware* dan ook een *gamechanger* te noemen voor het cybercriminele ecosysteem. Het heeft geleid tot cybercriminele groeperingen die enorm vermogend zijn geworden. Nadat het TrickBot-botnet eind 2020 goeddeels was neergehaald, zou de groep volgens gelekte interne communicatie in het jaar daarop 20 miljoen Amerikaanse dollar hebben geïnvesteerd in het herstellen en verbeteren van de aanvalsinfrastructuur en de bedrijfsvoering.[57] De Conti-ransomwaregroep zou zelfs recent de beschikking hebben gehad over 2 miljard dollar aan virtuele valuta[V].[58] Hierdoor zijn deze groepen in staat om nog meer te investeren in effectieve en efficiënte aanvalsprocessen. Maar ook het incasseringsvermogen om bijvoorbeeld verstoringsacties van opsporingsdiensten te boven te komen neemt daardoor toe. Zowel het TrickBot-botnet als het Emotet-botnet waren een klein jaar na hun respectievelijke *take-downs* weer in de lucht.[59]

## Is de Nederlandse weerbaarheid schaalbaar (genoeg)?

Gezien de aard en omvang van de cybercriminele dreiging is het efficiënt en effectief – ofwel: schaalbaar - maken én houden van de weerbaarheidsketen een fundamentele uitdaging voor de komende jaren. Dit geldt voor cybersecurity en voor cybercrimebestrijding door de politie en het Openbaar Ministerie, als een integraal onderdeel van de weerbaarheid.

De economische rationaliteit achter cybercriminaliteit is een belangrijke drijfveer achter de schaalbaarheid van deze criminaliteitsvorm. Cybercriminelen proberen op een zo effectief mogelijke wijze maximale opbrengsten te genereren, met behulp van de mogelijkheden die het digitale domein ze biedt. Waar voorheen vooral de financiële sector onder vuur lag van onder meer *banking malware*, is het verdienmodel van ransomware dermate universeel, dat de cybercriminele dreiging meer sector-onafhankelijk is geworden[60]. Vanuit weerbaarheid bezien betekent dit dat het te verdedigen, potentiële aanvalsoppervlak alleen maar groter is geworden.

Ondanks bovenstaande constateringen lijkt de benodigde groei - en schaalbaarheid - van de Nederlandse weerbaarheid achter te blijven. Niet alleen het CSBN waarschuwt hier al meerdere jaren voor. De Cyber Security Raad (CSR) concludeerde in 2021 in een adviesrapport dat in de afgelopen jaren door overheid, bedrijfsleven en wetenschap flink is geïnvesteerd in cybersecurity, maar dat desondanks de weerbaarheid in Nederland nog niet overal afdoende is om de toenemende dreigingen het hoofd te bieden. Bij de plegers en dienstverleners van cybercriminaliteit vormen het vermogen om effectief samen te werken, complexe taken uit te besteden en het voortdurend innoveren van hun automatisering belangrijke randvoorwaarden om schaalbaarheid te bereiken. Aan de kant van de Nederlandse weerbaarheid benoemt het CSR-rapport dergelijke voorwaarden (vooral als het gaat om effectieve samenwerking en de daartoe noodzakelijke informatie-uitwisseling) juist als knelpunten.[61]

### *Cybersecurity: kostenpost of investering?*

Aan criminele zijde is schaalbaarheid een integraal onderdeel van het verdienmodel en de onderlinge criminele marktwerking. Aan de verdedigende kant is het investeren in samenwerking en (in innovatie van) informatiebeveiliging noodzakelijk om schaalbare cybersecurity te bereiken. Echter, de bereidheid om dit te doen is vaak eerder afhankelijk van welwillendheid dan van economische motieven.

V Deze bedragen zijn niet geverifieerd. De politie acht het echter zeer wel mogelijk dat groepen als TrickBot en Conti over dergelijke budgetten beschikken.

Investeringen in cybersecurity worden gezien als een kostenpost en worden vaak reactief toegepast, aangezien deze volgen op incidenten, in plaats van proactieve investeringen die vooruitlopen op nieuwe dreigingen.[62] De dreiging van ransomware zou hier geleidelijk verandering in kunnen brengen, gezien de toenemende financiële schade die dergelijke aanvallen aanrichten. Schaalbare cybersecurity vereist ook innovatiekracht. In preventieve zin bijvoorbeeld voor het ontwikkelen én toepassen van veilige open standaarden en de brede beschikbaarheid van veilige (*open-source*) oplossingen van fundamentele bouwstenen van de digitale ruimte.[63] Of om het op effectieve en efficiënte wijze kunnen mitigeren van het groeiende aantal gedetecteerde kwetsbaarheden.[VI] De Onderzoeksraad voor Veiligheid (OVV) stelt in 2021 in een rapport dat het verhelpen (*patchen*) hiervan op deze schaal niet meer voor alle organisaties behapbaar is. Bovendien is de noodzaak daartoe ook niet altijd duidelijk.[64]

Een toegenomen cybercriminele dreiging die minder sectorspecifiek is geworden, gaat gepaard met een groeiende noodzaak tot samenwerking en (het uitwisselen van) dreigings- en kwetsbaarheidsinformatie op het gebied van cybersecurity, zowel tussen de overheid en de private sector, als tussen verschillende sectoren onderling. Zowel tussen vitale als niet-vitale partijen. Op deze kritieke punten signaleert het adviesrapport van de CSR organisatorische en juridische knelpunten en groeipijnen. Tot slot, als het gaat om preventie en de voorbereiding op incidenten, signaleert de OVV in het rapport van 2021 veel verschil in de weerbaarheid van organisaties. Iedere organisatie is daar zelf verantwoordelijk voor, maar niet iedere organisatie heeft het gevoel van urgentie, de expertise of de capaciteit om dergelijke maatregelen adequaat uit te voeren. Het ontbreekt volgens de OVV dan ook aan een collectief fundament om de weerbaarheid te vergroten.[65]

### *De uitdagingen van schaalbare cybercrimebestrijding*

Door de schaalgrootte van cybercriminaliteit en het potentieel grote aanbod aan strafzaken moeten voortdurend harde keuzes worden gemaakt in het prioriteren van de opsporing. Als gevolg hiervan richten politie en OM zich in het geval van zware, georganiseerde cybercriminaliteit vooral op het bestrijden van de centrale cybercriminele dienstverleners en de groepen waarvan de grootste dreiging uitgaat. Het verhoogde incasseringsvermogen van cybercriminele groepen en het sterke transnationale karakter van cybercriminaliteit – inclusief het opereren vanuit *safe-havens*, brengen uitdagingen met zich mee voor de opsporing en vervolging daarvan. Voor effectieve cybercrimebestrijding is het daarom van belang om schaalbaarheid te bereiken in de manier van ingrijpen. Dit uit zich hier in de noodzaak om proactief en gericht te kunnen handelen en intensief samen te werken met publieke en private partners in binnen- en buitenland. Informatie-uitwisseling is daarbij cruciaal. Het is de vraag of het huidige instrumentarium van de politie en het OM nog toereikend is om dit zo effectief en efficiënt mogelijk te kunnen doen, zo blijkt ook uit recent onderzoek van het WODC.[66]

Om cybercriminaliteit tegen te gaan, investeren de politie en het OM in brede en datagedreven bestrijding. Die kenmerkt zich door het benutten van het volle spectrum van preventie, verstoring, opsporing en strafrechtelijke vervolging.[67] Hierbij is in vrijwel elk onderzoek sprake van samenwerking: met (inter)nationale opsporingsdiensten, publieke partners en met het bedrijfsleven in binnen- en buitenland. Datagedreven bestrijding houdt in dat tactische, digitale en datawetenschappelijke methoden en technieken worden geïntegreerd in de onderzoeken.[68] Dit vergt de nodige aanpassingen over de gehele strafrechtelijke keten.[69] Daartegenover levert het de grote winst op van het op proactieve en gerichte wijze kunnen bepalen en ontwikkelen van de meest effectieve en efficiënte (schaalbare) interventies.

Het uitvoeren van deze interventies laat zich echter momenteel in de praktijk vaak nog lastig schalen, gezien de vele uitdagingen die daarbij komen kijken. Zo is het bereiken van een coherente en gezamenlijke internationale aanpak van een dreiging als ransomware complex te organiseren in het licht van doorgaans op nationale belangen en jurisdicties gerichte opsporingsdiensten. Toegang tot elektronisch bewijsmateriaal in het buitenland wordt vaak bemoeilijkt door trage internationale rechtshulp. Het delen van informatie met partners buiten de EU kan worden bemoeilijkt door de afwezigheid van de benodigde afspraken (adequaatheidsbesluiten) tussen de EU en derde landen. Dreigingsinformatie uitwisselen met zowel publieke, als private partners in binnen- en buitenland is bovendien juridisch complex wanneer er sprake is van data die zijn aangemerkt als persoonlijk identificeerbaar, zoals IP-adressen. Bulletproof *hosters* bieden cybercriminelen veilige opslag van data aan, zogezegd buiten het bereik van de opsporing en zijn daarmee een van de meest centrale cybercriminele dienstverleners. Zij maken relatief veel gebruik - of misbruik - van de Nederlandse digitale infrastructuur. Dit aanpakken is lastig door (vooralsnog) beperkte strafrechtelijke mogelijkheden en onduidelijkheid over de vraag wie precies waarvoor verantwoordelijk is, als het gaat om het hosten van data. Dit laatste uit zich uit in zeer ingewikkelde internationale constructies van zogeheten resellers die hostingpakketten met data doorverkopen en waar cybercriminelen graag gebruik van maken.

Tot slot is het identificeren en informeren van de grote hoeveelheden slachtoffers die in cybercrimeonderzoeken aan het licht komen, vooralsnog een omvangrijke en complexe taak. Dit geldt zowel voor de politie, als voor het NCSC, waarmee de politie samenwerkt in dergelijke gevallen. Het notificeren van de vele slachtoffers in de Emotet-casus bevestigt dit, maar is tegelijkertijd een voorbeeld van hoe samenwerking en informatiedeling tussen cybersecurity- en cybercrimebestrijdingspartners kunnen bijdragen aan een verhoogde weerbaarheid.[70]

VI Jaarlijks worden er zo'n 25.000 zogeheten *security advisories* hiertoe gepubliceerd.

### Een asymmetrische situatie

Cybercriminelen hebben meerdere tactische voordelen ten opzichte van cybersecurity en cybercrimebestrijding. Een groot aanvalsoppervlak biedt een aanvaller een ruime keuze, terwijl een verdediger significant meer moeite moet doen om alle aanvalsmogelijkheden te onderkennen, te voorkomen, af te wenden en te mitigeren. Aangezien cybercriminelen per definitie buiten de wet opereren, houden zij zich niet aan wetgeving. Technische innovatie en samenwerking zijn integrale onderdelen van hun gezamenlijke verdienmodel. Dit collectieve fundament heeft geleid tot een optimale aanvalsketen en een enorme omvang van cybercriminaliteit. Voor cybersecurity en cybercrimebestrijding is het bereiken van schaalbaarheid in de manier van werken noodzakelijk, maar lastiger te bereiken. In technisch opzicht zijn er veel mogelijkheden en wordt hier reeds aan gewerkt. Het zijn vooral de organisatorische aspecten (samenwerking) en de juridische aspecten (waaronder informatie-uitwisseling) die de grootste uitdagingen vormen.

## Marktdynamiek compliceert beheersing digitale risico's

Digitale markten zijn markten waarin vraag en aanbod naar digitale diensten, (componenten van) hardware, software en netwerken samenkomen. Deze markten hebben enkele unieke kenmerken. Bijvoorbeeld de (semi)monopolistische status van bepaalde leveranciers, de hoge mate van onderlinge verweving en de focus op het vergaren van zoveel mogelijk data. Ook zijn in deze markten prikkels voor digitale veiligheid niet (altijd) doorslaggevend. Die kenmerken compliceren de beheersing van risico's voor individuele burgers, organisaties, sectoren en landen. Daarbij doet zich een paradox voor. Aan de ene kant kunnen individuele keuzes van burgers, organisaties, sectoren en landen de risico's voor anderen vergroten of verkleinen. Aan de andere kant is de ruimte om autonome keuzes te maken voor risicobeheersing juist beperkt vanwege een gebrek aan reële of veilige(r) alternatieven.

### Kenmerken van digitale markten beïnvloeden digitale veiligheid

Eén van de kenmerken van digitale markten is dat deze vaak (semi)monopolistisch zijn. Er zijn enkele, vooral mondiaal opererende partijen die het grootste gedeelte van de markt in handen hebben. Dit geldt bijvoorbeeld voor leveranciers van kantoorapplicaties of besturingssystemen.[71] Dit komt onder andere doordat het bedrijf dat als eerste de markt betreedt en veel klanten krijgt, grote voordelen heeft ten opzichte van concurrerende bedrijven. Zo heeft het voor afnemers tal van voordelen om te kiezen voor een marktleider. Dat vereenvoudigt data-uitwisseling met andere organisaties, medewerkers zijn misschien al gewend om te werken met het product van de marktleider, etc.[72] Ook zijn de toetredingsdrempels voor nieuwe bedrijven om soortgelijke producten te maken hoog, gelden er barrières om over te stappen (*lock-in* effect) en hebben marktleiders veelal het geld om veelbelovende start-ups op te kopen. Hierdoor is er feitelijk voor bepaalde diensten en producten een beperkt aantal aanbieders.

Een tweede kenmerk van digitale markten is dat digitale diensten, hardware, software en netwerken gebruik maken van vele andere componenten en daardoor onderling sterk verweven zijn. Zo kunnen verschillende digitale dienstverleners gebruik maken van dezelfde ontwikkel- en monitoringtools en bestaat hardware uit verschillende componenten die door andere leveranciers worden gemaakt. Als gevolg daarvan worden leveranciers en afnemers onderdeel van talrijke toeleverancierssketens. Kwetsbaarheden in diensten en producten van anderen, of uitval en misbruik daarvan, raken daardoor potentieel organisaties wereldwijd. Die verwevenheid leidt tot complexiteit en connectiviteit, en maakt het zeer complex om een overzicht te hebben van alle componenten die worden gebruikt. Dat maakt kwetsbaar, zoals recent ook bleek, toen bekend werd dat de Apache Log4-j softwarebouwsteen een kwetsbaarheid had. Deze bouwsteen was op zijn beurt in gebruik voor vele andere soorten digitale processen, die daardoor ook risico liepen.[73]

De sterke gerichtheid op het vergaren van zoveel mogelijk data is een derde kenmerk van digitale markten. Data zijn niet alleen cruciaal als 'productiefactor' voor de dienstverlening, maar data hebben ook een zelfstandige waarde. Vanwege deze aantrekkelijkheid is er een zekere honger naar data vanuit aanbieders. Veel diensten worden gratis aangeboden aan consumenten, maar vaak verdienen de aanbieders aan de vergaarde data.[74] Zelfs als consumenten apparatuur of software kopen, is niet altijd transparant welke data worden vastgelegd en uitgewisseld, denk aan auto's of tv's. Het is ook lang niet altijd helder welke data voor welke doeleinden worden verstrekt of doorverkocht en aan wie.[75] Bovendien kunnen die data na een cyberaanval op straat komen te liggen of worden verhandeld door criminelen. Hierbij is er een verschil tussen de overwegingen als individu of als samenleving. Zo hoeft het voor een individu geen probleem te zijn om persoonlijke data, bijvoorbeeld over de gezondheid, te delen in een app, maar kan dat een risico zijn voor de Nederlandse veiligheid als duizenden, zo niet miljoenen Nederlanders dat doen. Organisaties en statelijke actoren kunnen gebruik maken van die data om bijvoorbeeld kunstmatige intelligentie verder te ontwikkelen of om profielen van bevolkingsgroepen op te stellen.

Een vierde kenmerk is dat prikkels voor digitale veiligheid niet (altijd) doorslaggevend zijn, terwijl veiligheidsrisico's bij anderen kunnen ontstaan. Bij zowel de productie, levering en aanschaf van digitale processen, hardware en software spelen allerlei belangen een rol. In digitale markten is het geen uitgemaakte zaak dat partijen in een belangenafweging rekening houden met (alleen) het belang van digitale veiligheid voor zichzelf, anderen of de maatschappij. Zo maken partijen beslissingen op basis van kosten, gebruiksgemak of de netwerkeffecten.[76] In veel markten zijn terugroepacties gangbaar wanneer de veiligheid van een product in het geding is, maar dat is niet de norm in digitale markten.[77]

Daardoor kunnen (mogelijk) onveilige digitale producten langer circuleren en worden gebruikt dan in andere economische markten. Verder is 'security by design' nog niet de standaard voor aanbieders en kan het snel in de markt zetten van een nieuw product belangrijker worden geacht dan het optimaliseren van de veiligheid. Verder zijn inkoop-en aanbestedingsprocedures nog weinig gefocust op digitale veiligheid en kan bijvoorbeeld de prijs doorslaggevend zijn. Sinds enkele jaren interveniëren overheden in sommige markten om digitale veiligheid te verhogen of overwegen ze dat. Interventie in digitale markten staat ten opzichte van andere markten nog in de kinderschoenen.[78] Daar waar bijvoorbeeld aan financiële dienstverleners eisen worden gesteld om misbruik van de dienstverlening te voorkomen, zijn soortgelijke eisen niet gebruikelijk voor bijvoorbeeld *hosting-* en *access-providers*. Zo zijn financiële dienstverleners wettelijk verplicht ongebruikelijke financiële transacties te melden. Voor het melden van 'ongebruikelijke digitale transacties' bij *hosting-* en *access-providers* gelden geen eisen. Interventie door overheden kan echter ook onbedoelde effecten hebben en bijvoorbeeld de marktpositie van kleine partijen bemoeilijken.[79] Bovendien kenmerken digitale markten zich veelal door het mondiale karakter, wat mogelijkheden voor interventie door een afzonderlijk land beperkt.

### Marktdynamiek leidt tot paradox: keuzevrijheid maar ook beperkingen

Aan de ene kant kunnen marktpartijen keuzes maken op basis van de eigen overwegingen en belangen en zijn ze daar in zekere zin autonoom in. Die individuele keuzes kunnen wel de risico's vergroten voor anderen en leiden tot collectieve risico's, waaronder een sterke afhankelijkheid van bepaalde bedrijven. Zo kan een organisatie kiezen voor de goedkoopste variant van clouddiensten zonder eisen te stellen aan de veiligheid en kiezen voor de marktleider. Daardoor loopt niet alleen die organisatie zelf een hoger risico op een cyberincident, maar ook de klanten van die organisatie, zonder dat ze dat weten. De data van de klanten kunnen als gevolg daarvan op straat komen te liggen. Wanneer vele organisaties binnen een sector of binnen Nederland kiezen voor de marktleider, ontstaat potentieel een grote afhankelijkheid daarvan. Het omgekeerde is ook denkbaar wanneer de organisatie juist wél kiest voor veiligheid of bewust juist niet voor de marktleider. Alle klanten profiteren dan van die veiligheidsmaatregelen, evenals mogelijk de sector als geheel.[VII] Aan de andere kant is de daadwerkelijke keuzevrijheid voor marktpartijen beperkt door (soms) een gebrek aan reële of veilige(r) alternatieven. Zo is het veelal niet mogelijk om wel een product of dienst af te nemen én ervoor te kiezen geen onderdeel te worden van de toeleverancierskeketen.

VII Economen spreken in zulke gevallen van negatieve of positieve externe effecten. Een voorbeeld van negatieve externe effecten zijn de gevolgen voor het milieu van vervuilende fabrikanten, terwijl consumenten voor die vervuilende effecten niet betalen bij afname. Een voorbeeld van positieve externe effecten is een situatie waarin een bedrijf een plaatselijke vereniging sponsort.

## Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen

Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal staat nog in de kinderschoenen.[80] Eerder is aangegeven dat de weerbaarheid in Nederland nog niet voldoende is. Ook is aangegeven dat het schaalbaar maken en houden van de weerbaarheidsketen een fundamentele uitdaging is voor de komende jaren. Digitale risico's hebben nog geen structurele plaats in het bredere risicomanagement binnen en tussen de drie eerder genoemde niveaus. Risicomanagement is nog niet vanzelfsprekend, terwijl een risicogebaseerde manier van werken instrumenteel is voor het bepalen en op het gewenste niveau brengen van de weerbaarheid.[81] Daarvoor is een samenhangende aanpak binnen en tussen de drie niveaus nodig. Op organisatieniveau is inbedding in het primaire proces van belang. Daar waar risicomanagement binnen organisaties, binnen en tussen sectoren al talrijke complicaties kent, geldt dat zeker (ook) op landelijk niveau.

### Samenhangende aanpak nodig voor verhogen weerbaarheid

Zonder een samenhangende aanpak – waarbij diverse belangen tegen elkaar worden afgewogen – bestaat de kans dat er onnodig risico's worden genomen.[82] In de groei naar een volwassen aanpak van risicomanagement op zowel organisatorisch, als sectoraal, als nationaal niveau zijn de aandachtspunten daarbij dat de betrokken partijen met elkaar in gesprek gaan over relevante scenario's[83], dat risicoanalyses een centralere plek innemen binnen de bedrijfsvoering[84] en dat organisaties geprikkeld worden om risico's die anderen raken te adresseren.[85]

Een verscheidenheid aan risicoanalysemethoden bemoeilijkt interne en organisatie overstijgende gesprekken over risicomitigatie en -acceptatie.[86] Een gezamenlijke metafoor, evenals een gedeeld beeld van concepten zoals 'aanvalsoppervlak' en 'aanvalspaden' kunnen hierbij helpen.[87] Toch zullen er waarschijnlijk meerdere dialecten en paradigma's blijven bestaan[88], en zal de conceptualisering van zowel risicoanalyse, als het bewandelen van aanvalspaden niet alomvattend zijn.[89] Desalniettemin wordt er door de OVV gepleit om organisaties op een eenduidige wijze verantwoording af te laten leggen over de wijze waarop zij digitale risico's beheersen.[90]

### Inbedding in primaire proces van belang

Uiteraard zijn er talrijke organisaties die het risicomanagement op orde hebben. Toch schort het, naast facetten die specifiek te maken hebben met de risicoanalyses zelf, binnen organisaties vaak aan de inbedding in het primaire proces.[91] Zonder duidelijke doelen, afbakening, prioritering, teamsamenstelling, etc., gaat een risicoanalyse snel 'zwalken'.[92] De verantwoordelijkheid voor een efficiënte en effectieve risicoanalyse ligt bij de opdrachtgever: in de

regel de proceseigenaar en risico-eigenaar.[93] Risicoanalyseteams dienen echter ook scherp te zijn op de hierboven beschreven randvoorwaarden en het scheppen van heldere verwachtingen. Ze hebben daarnaast een rol in de opvolging van risicobeheersingsadviezen, waaronder een kritische blik op de effectiviteit van genomen maatregelen.[94]

Om hier verandering in te brengen kan informatie- en risico-eigenaarschap evenals risicomanagement als randvoorwaarde geïntegreerd worden in het primaire proces. Dit onder toezicht van interne en externe controleorganen die naast een traditionele focus op financiële risico's ook inzicht kunnen verschaffen in bredere digitale risico's – waaronder digitale risico's voor de nationale veiligheid.[95] Volgens de CSR en de OVV zijn daar middelen en aanvullende wettelijke kaders voor nodig.[96]

### Volwassen toezicht op weerbaarheid vitale processen nog niet volledig op orde

Het "Samenhangend inspectiebeeld cybersecurity vitale processen" laat zien dat er nog veel werk verzet moet worden.[97] Van zes toezichthouders komt naar voren dat er drie hun toezicht op cybersecurity stevig hebben ingericht. Andere toezichthouders ontwikkelen dit nog. Daarom kan het cyberbeeld nog niet worden gebruikt om over alle vitale processen uitspraken te doen. Voor cybersecurity is niet alleen aandacht nodig van organisaties zelf en toezichthouders maar ook vanuit de ministeries. Het beeld laat zien dat er op het gebied van digitaal weerbare en dus veilige vitale processen en aanbieders op een aantal terreinen inmiddels de nodige stappen zijn gezet. Tegelijkertijd is er in de breedte nog veel werk aan de winkel en is het werk nooit af. De toezichthouders hebben de ambitie om het toezicht daarop in gezamenlijkheid door te ontwikkelen. Op vitale processen zoals in de chemie en digitale overheidsprocessen zijn nog geen toezichthouders aangewezen.

### Risicomanagement op nationaal niveau lastig

Risicomanagement op landelijk niveau vindt nog niet structureel plaats en staat nog in de kinderschoenen. Daar waar risicomanagement binnen organisaties en binnen en tussen sectoren al talrijke complicaties kent, geldt dat zeker (ook) op landelijk niveau. Het is bijvoorbeeld voor organisaties al lastig om een overzicht van en inzicht in gebruikte componenten van hardware, software en netwerken te verkrijgen. Voor sectoren en op het landelijk niveau is het vaak problematisch om goed overzicht te krijgen van kwetsbaarheden en inzicht in de weerbaarheid. Zo bevinden de data van heel veel burgers en organisaties zich intussen in de cloud van een heel klein aantal partijen. Dat leidt tot zogeheten lock-in effecten en monopolisering, en daaraan zitten allerlei problematische kanten. De beveiliging van die partijen is veelal veel beter op orde dan op andere plekken, maar als het misgaat gaat het goed mis. Wat dat per saldo betekent voor de weerbaarheid is lastig te bepalen.

Verder is al eerder gewezen op het onderliggende probleem dat partijen – zowel aanbieders als afnemers – autonoom keuzes maken zonder dat ze de impact hiervan op anderen zelf hoeven te ondervinden. Waar het spaak loopt, is dat security vaak niet wordt meegenomen in de prijs die organisaties en individuen betalen.[98] 'Vervuilers' betalen niet voor de 'vervuiling' die veroorzaakt wordt.[99] Natuurlijk is dat complex, want security is lastig meetbaar. Maar zoals terugroepacties van producten en aansprakelijkheidstelling laten zien, zijn er wel degelijk stappen die gezet kunnen worden om securityproblemen door te belasten aan diegenen die in de beste positie zijn om er wat aan te kunnen doen.

Een andere reden dat risicomanagement op landelijk niveau nog in de kinderschoenen staat, is dat concepten, methoden en technieken primair zijn toegesneden op het niveau van individuele organisaties. Voor zover bekend ontbreken die voor risicomanagement op landelijk niveau. Vragen als "hoe digitaal veilig is Nederland?" worden regelmatig gesteld, maar zijn eigenlijk niet te beantwoorden. Voor iets dat nu veilig is, kan over een uur een nieuwe kwetsbaarheid worden ontdekt. Een niveau van 100% veiligheid is bovendien niet realistisch. Een betere vraag is "hoe weerbaar is Nederland?". Toch is het definiëren van een gewenst niveau van weerbaarheid verre van eenvoudig en evenmin makkelijk meetbaar. Een uitgekristalliseerd conceptueel kader daarvoor ontbreekt. Die weerbaarheid moet zich zeker niet alleen beperken tot het voorkomen van cyberincidenten, maar eveneens op het ontdekken daarvan, het beperken van de schade en het eenvoudiger maken van het herstel.

In wetenschappelijke literatuur verschenen inmiddels artikelen voor het op andere manieren doordenken van risico's, bijvoorbeeld door te kijken naar complexe adaptieve systemen. Zo spelen vele partijen een rol als het gaat om de weerbaarheid van de digitale ruimte als geheel. De mogelijkheden voor de Nederlandse overheid om de weerbaarheid daarvan te verhogen, zijn logischerwijze beperkt. Daar komt bij dat risico's voor de gehele digitale ruimte en de doorwerking daarvan op de maatschappij lastig zijn te doorgronden. Dat maakt de beoordeling van risico's complex, evenals de afweging om wel of geen maatregelen te treffen om die risico's te beheersen. Ook is niet op voorhand helder welke partijen de prikkels, mogelijkheden en bereidheid hebben om risico's te beperken.[100]

## Beperkingen in digitale autonomie beperken ook digitale weerbaarheid

Voor Europese landen en Nederland (verder Nederland) gelden beperkingen in digitale autonomie. Deze brengen ook beperkingen voor de digitale weerbaarheid met zich mee. Die staat onder druk door diverse oorzaken, die samenhangen met de hierboven toegelichte strategische thema's. Die oorzaken

verminderen de beïnvloedings- en keuzemogelijkheden voor en controle over de digitale weerbaarheid van Nederland. Digitale autonomie is een complex en veelomvattend begrip dat het bredere staatsbelang van economie, maatschappij en democratie raakt.[VIII] Het omvat het vermogen en de middelen die Nederland heeft om zelfstandig beslissingen te kunnen nemen over (verdere) digitalisering én de gewenste mate van digitale weerbaarheid. Het gaat dan bijvoorbeeld over de mate van controle over het gebruik en de inrichting van kritieke digitale systemen en de afhankelijkheid van de Nederlandse overheid van twee mondiale bedrijven om overheidsapps ter beschikking te stellen. Het gaat ook over de invloed die Nederland kan uitoefenen op ontwikkelingen die van invloed zijn op de veiligheid en de mogelijkheden om te kunnen kiezen uit veilige(r) alternatieven.

## Digitale autonomie staat onder druk

De CSR stelt dat het vermogen van Nederland om autonoom beslissingen te nemen vanuit drie kanten onder druk staat:

1. Cyberdreigingen nemen verder toe;
2. De geopolitieke spanningen tussen de VS en China nemen steeds verder toe;
3. De samenleving wordt steeds afhankelijker van de digitale infrastructuur die in handen is van een beperkt aantal dominante buitenlandse marktspelers.[101]

Onderliggende oorzaken van kwetsbaarheden in onze gedigitaliseerde samenleving zijn voor Nederland, evenals voor Europa, beperkt beïnvloedbaar. Aanvallers kunnen opereren vanuit diverse landen, gebruik maken van de infrastructuur van verschillende landen, slachtoffers maken in vele landen en ze houden zich niet aan wet- en regelgeving. Niet alleen compliceert dat het verhogen van de weerbaarheid daartegen voor individuele burgers, organisaties en landen. Het bemoeilijkt ook, zoals eerder aangegeven, het bestrijden ervan door inlichtingen- en opsporingsinstanties.

De geopolitieke context beperkt eveneens digitale autonomie en Nederland alleen kan daar niet veel aan veranderen. Net als andere landen kampt Nederland met de gevolgen van het structureel én intensief gebruiken van de digitale ruimte door staten en het geopolitieke steekspel rond zogeheten hoogwaardige technologieën en de onderliggende standaarden van deze technologieën.

Ook de unieke kenmerken van digitale markten zetten de digitale autonomie onder druk. Een gevolg daarvan is bijvoorbeeld dat vele digitale processen voor een groot deel afhankelijk zijn van de diensten, de infrastructuur en het ecosysteem van een beperkt aantal dominante buitenlandse marktspelers. De CSR stelt dat data van nagenoeg alle Europese bedrijven en burgers zich inmiddels in de cloud van met name Amerikaanse techbedrijven bevinden.[102] Dit brengt tevens controle van andere landen mee, die andere spelregels hanteren wat betreft privacy en afgifte van data. De CSR spreekt zelfs over “techkolonialisme”.[103] Verder zijn soms nauwelijks reële of veilige(r) alternatieven beschikbaar voor digitale diensten, hardware, software en netwerken. Ook is de onderhandelingspositie met grote mondiale bedrijven beperkt.[104] De Nederlandse invloed op dit alles is gering, maar het vormt wel een component van het risico.

Naast bovengenoemde oorzaken die ertoe leiden dat de digitale autonomie onder druk staat, geldt aanvullend dat Nederland alleen weinig invloed kan uitoefenen, noch beschikt over alternatieven voor de digitale ruimte. Schending van de digitale ruimte is een risico. Zo kunnen digitale processen vele vertakkingen hebben naar andere landen met uiteenlopende juridische regimes, normen en waarden. Dit gebrek aan transparantie wordt veroorzaakt door hoe het internet in de basis is ontworpen: data worden automatisch via de kortste route met zo min mogelijk tussenliggende netwerken geleid. Die route kan automatisch worden aangepast als er ergens bijvoorbeeld een storing is. Deze eigenschap brengt efficiëntie, maar zorgt er ook voor dat de routering en de gebruikte netwerken niet bekend zijn. Daardoor ontstaat een zogenoemde ‘black box’, waar geen zicht op is.[105] Daar waar sommige landen streven naar zogeheten interoperabiliteit en vrij internetverkeer, zijn er ook de nodige landen die streven naar regulering van het ingaande en uitgaande internetverkeer. Die regulering raakt ook buitenlandse organisaties die in of met deze landen opereren en kunnen doorwerken naar Nederlandse organisaties, zonder dat die daarop invloed kunnen uitoefenen, of zonder dat dat altijd transparant is.

## Beperkingen in autonomie werken door naar weerbaarheid

De combinatie van voornoemde oorzaken en gevolgen beperken de mate waarin Nederland invloed kan uitoefenen op bepaalde ontwikkelingen én de keuzemogelijkheden voor reële of veilige(r) alternatieven. Dat alles beperkt het vermogen en de middelen om (relevante) risico’s tot een aanvaardbaar niveau te reduceren, om cyberincidenten te voorkomen en om wanneer deze zich hebben voorgedaan ze te ontdekken, de schade te beperken en het herstel eenvoudiger te maken.

VIII De Cyber Security Raad (CSR) definieert digitale autonomie als “strategische autonomie in het digitale domein”. Strategische autonomie is volgens de CSR “een middel om soevereiniteit te verkrijgen en te behouden en bestaat uit het vermogen en de middelen om beslissingen te kunnen nemen en uit te voeren aangaande essentiële aspecten van de langetermijn-toekomst in economie, maatschappij en democratie.”

*Elk systeem dat gebruik maakte van Log4j bleek kwetsbaar te zijn: een kwaadwillende kon op afstand willekeurige code uitvoeren*

# 4 Jaaroverzicht

## De belangrijkste cyberincidenten in beeld

**Het Nationaal Cybersecuritycentrum (NCSC) heeft vanuit zijn operationele coördinerende rol een overzicht gemaakt van de belangrijkste cyberincidenten die zich in periode april 2021 tot en met maart 2022 hebben voorgedaan. Daarbij is geput uit eerder verschenen NCSC-producten zoals de Maandmonitor en uit open bronnen. De focus ligt op incidenten die Nederland hebben geraakt of die Nederland zouden kunnen raken. Ze illustreren het belang van de in het vorige hoofdstuk geïdentificeerde strategische thema's die relevant zijn voor de digitale veiligheid van Nederland.**

### 2021

#### April 2021

**Achterdeur gevonden in software-ontwikkeltool Codecov**: Gebruikers van de software-ontwikkeltool Codecov zijn mogelijk slachtoffer geworden van een *supply chain*-aanval.[106] Op 31 januari 2021 heeft een aanvaller het 'Bash Uploader' script weten aan te passen, dankzij een gelekte sleutel voor een Google Cloud Storage account van Codecov. Met het 'Bash Uploader' script worden normaliter alleen testresultaten geüpload vanaf het systeem van de softwareontwikkelaar naar de servers van Codecov. De achterdeur zorgde ervoor dat daarnaast inloggegevens werden weggesluisd naar de aanvaller. Op 1 april 2021 is de achterdeur door Codecov gedetecteerd, nadat een gebruiker meldde dat de versie van het script geleverd via de webserver van Codecov niet overeenkwam met informatie uit de documentatie. Onderzoekers schatten in dat de aanvallers honderden klanten van Codecov getroffen kunnen hebben.[107]

**Actief misbruik van VPN-kwetsbaarheden door actoren**: Op 20 april 2021 publiceerde PulseSecure in een blogpost dat er actief misbruik wordt gemaakt van kwetsbaarheden in de Pulse Connect Secure Appliance.[108] Ook de Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) liet weten dat er actief misbruik wordt gemaakt van deze kwetsbaarheden.[109] Het gaat om vier kwetsbaarheden, waaronder drie oudere, waarvoor in 2019 en 2020 beveiligingsupdates zijn uitgebracht. De vierde kwetsbaarheid, met als kenmerk CVE-2021-22893, betrof een zero-day kwetsbaarheid waar in eerste instantie geen oplossing voor was. Begin mei 2021 is voor deze kwetsbaarheid een beveiligingsupdate uitgebracht.[110]

**Politie verwijdert Emotet-malware van 1 miljoen besmette pc's**: Tijdens de internationale politieoperatie 'LadyBird' onder leiding van Europol wist de politie in januari 2021 het Emotet-botnet over te nemen. Dankzij onder andere de hackbevoegdheid van de politie kon het Emotet-netwerk verder in kaart gebracht en gedeactiveerd worden. In april 2021 werd vervolgens een software update op de Nederlandse servers geplaatst voor alle geïnfecteerde systemen.[111] Deze update werd automatisch opgehaald door de geïnfecteerde systemen, waarna de Emotet-besmetting in quarantaine werd geplaatst. Het NCSC heeft in samenwerking met de politie en het OM, Nederlandse slachtoffers van geïnfecteerde accounts geïnformeerd.

## Mei 2021

**Hack op Amerikaanse Colonial Pipeline**: Op 7 mei 2021 is het oliepijplijnbedrijf Colonial Pipeline slachtoffer geworden van een ransomware-aanval.[112] Colonial Pipeline heeft besloten om de operationele processen stop te zetten, om mogelijke verdere verspreiding van de ransomware te voorkomen. Dit had zeer grote gevolgen voor de toelevering van brandstof aan de oostkust van de Verenigde Staten (VS). Indirecte gevolgen op de maatschappij waren onder andere de onrust die ontstond en mensen die brandstof gingen hamsteren. Na zes dagen zijn de operationele processen weer opgestart.[113] De FBI heeft in een persbericht bevestigd dat het de ransomwaregroep Darkside betreft.[114]

**Ransomware-aanval op Ierse publieke gezondheidsdienst (HSE)**: Het Ierse Health Service Executive (HSE) is op 14 mei 2021 geraakt door een ransomware-aanval. Er werd besloten om de IT-systemen offline te halen om verdere verspreiding te voorkomen.[115] Dit had gevolgen voor de zorgverlening aan patiënten in verschillende ziekenhuizen en instellingen. Via Twitter werd gemeld dat er ofwel vertraging is opgetreden, ofwel dat afspraken zijn geannuleerd. De ransomware betrof de Conti-ransomware. De malware kwam binnen via een phishing e-mail.[116] Het Amerikaanse ministerie van Volksgezondheid stelt dat 80% van de IT-omgeving versleuteld was: 2800 servers en 3500 werkstations.[117] In dezelfde maand werd ook het Ierse Department of Health twee keer aangevallen, waarna ook zij hun diensten tijdelijk moesten sluiten.[118]

**Twee jaar lang gerichte cyberaanval op Belgische ministerie van Binnenlandse Zaken**: De Belgische Federale Overheidsdienst (ministerie) van Binnenlandse Zaken is slachtoffer geworden van een digitale aanval.[119] In maart 2021 werd door Microsoft gemeld dat de actor HAFNIUM misbruik zou maken van kwetsbaarheden in Microsoft Exchange.[120] Dit bericht vormde de aanleiding voor het Centrum voor Cybersecurity België (CCB) om een onderzoek te starten. Uit dit onderzoek bleek dat er sprake was van geïnstalleerde backdoors op het netwerk van het ministerie. Uit aanvullende monitoring van het CCB, bleek dat vanaf april 2019 verdachte handelingen op het netwerk van het ministerie hebben plaatsgevonden. Na deze bevinding is de kwetsbaarheid in het netwerk verholpen, is belangrijke gevoelige informatie veiliggesteld en is gestart met het opschonen van de systemen. Het CCB geeft aan dat het om een zeer complexe en geavanceerde aanval gaat, vermoedelijk met spionagedoeleinden.[121]

## Juni 2021

**Spearphishing campagne Nobelium (APT29) waargenomen in Nederland**: Een door Microsoft aan Nobelium (APT29) geattribueerde spearphishing-campagne is ook in Nederland waargenomen.[122] De campagne is bij meerdere doelgroeporganisaties van het NCSC waargenomen via het Nationaal Detectie Netwerk. De dreiging richt zich met name op overheidsorganisaties, ngo's en specifiek op onderdelen die zich bezighouden met internationale samenwerking en diplomatieke relaties, zoals ambassades.[123] De berichten uit deze campagne zijn van hoge kwaliteit en spelen in op de actualiteit. Een terugkerend kenmerk van deze campagne is een besmetting met Cobalt Strike.

**Ransomware-aanval gemeente Luik**: De Belgische stad Luik is op 21 juni 2021 het slachtoffer geworden van een gerichte aanval met ransomware.[124] Hierdoor zijn gemeentesystemen deels onbereikbaar geworden en is de dienstverlening aan burgers ernstig verstoord. Onder andere de bevolkingsadministratie en de bijbehorende dienstverlening (geboorten, begrafenissen en huwelijken) waren niet beschikbaar. Waalse radio- en televisieomroep RTBF en RTC Tele Liège, stelden dat de criminelen losgeld eisten en speculeerden dat het om Ryuk-ransomware ging.[125]

**Hackpoging 'Testen voor Toegang'**: Op vrijdag 25 juni 2021 vond een hackpoging plaats op het systeem van Testen voor Toegang.[126] De poging leidde tot technische problemen. E-mails met daarin een testuitslag kwamen later aan: voor veel mensen te laat om gebruik te kunnen maken van de (her)opening van nachtclubs die avond. De organisatie Testen voor Toegang regelde namens de overheid coronatoegangstesten op locaties in heel Nederland.

## Juli 2021

**Kaseya supply-chain aanval zorgt wereldwijd voor ransomware slachtoffers**: Op 2 juli 2021 vond een wereldwijde ransomware-aanval plaats waarbij managed serviceproviders (MSP's) en hun klanten getroffen werden.[127] Ook in Nederland zijn slachtoffers gevallen.[128] De criminelen achter de ransomware REvil maakten misbruik van twee kwetsbaarheden in Kaseya VSA. Een van de kwetsbaarheden was reeds bekend bij Kaseya dankzij het Dutch Institute for Vulnerability Disclosure (DIVD) die deze en nog vijf andere kwetsbaarheden via een *coordinated vulnerability disclosure*-traject heeft aangekaart bij Kaseya.[129] De andere misbruikte kwetsbaarheid betrof een nog niet bekende zero day kwetsbaarheid. Het NCSC schreef adviezen over hoe de kwetsbaarheden in systemen op te sporen en hoe deze te verhelpen.[130] Het CSIRT voor digitale dienstverleners (CSIRT-DSP) heeft gebruikers van Kaseya software in haar doelgroep hierover actief geïnformeerd. Op 13 juli verdween REvil van verschillende fora en verdween ook de website die REvil gebruikte om te communiceren met slachtoffers. Kaseya beschikte inmiddels over een decrypter die zij verstrekten aan de getroffen organisaties. De aanvallers eisten een bedrag van 70 miljoen dollar, Kaseya stelt echter niet te hebben betaald voor een universele decrypter.[131]

**Pegasus-spyware toont publiek opnieuw de kwetsbaarheid van mobiele apparaten**: Een consortium van 17 nieuwsorganisaties publiceerde in juli een onderzoek, waaruit zou blijken dat dissidenten, mensenrechtenadvocaten, activisten, journalisten en politici wereldwijd doelwit zijn van spionageactiviteiten met behulp van Pegasus-software.[132] De software, ontwikkeld door de Israëlische NSO Group, zou de aanvaller toegang verlenen tot de inhoud van iPhone- en Android-telefoons, zonder enige interactie met het slachtoffer. Dit betreft dus een zogenaamde zeroclick-aanval. Israël heeft naar aanleiding van de onthullingen een taskforce opgezet om te onderzoeken of er beleidswijzigingen nodig zijn met betrekking tot de export van dergelijke software.[133] De NSO Group zelf stelt de software enkel aan staten te verkopen ten behoeve van criminaliteits- en terrorismebestrijding.

**DDoS-aanvallen op DigiD-leverancier verstoort GGD-websites**: Op 21 juli waren de websites van de GGD niet bereikbaar. Dit werd veroorzaakt doordat de toeleverancier van DigiD binnen 24 uur drie DDoS-aanvallen meemaakte.[134] Op verschillende GGD-websites kon niet worden ingelogd met DigiD. Het was vervolgens niet mogelijk een afspraak te maken voor een test of vaccinatie. Ook kon men geen testuitslagen inzien. De GGD's vielen terug op callcenters om mensen te verwittigen over hun testuitslagen en om test-afspraken in te plannen. De DDoS-aanvallen zijn uiteindelijk gepareerd door de stichting NBIP.

## Augustus 2021

**PKIoverheid stopt met verstrekken publiek vertrouwde webserver (SSL/TLS) certificaten**: De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties heeft besloten voorlopig geen nieuwe publiek vertrouwde root op te starten, na het verlopen van het publiek vertrouwde Domein Server CA 2020.[135] Uit een evaluatie bleek dat de Nederlandse overheid anno 2021 als enige EU-land publiek vertrouwde (SSL/TLS) certificaten uitgaf. In andere landen wordt dit gedaan door private ondernemingen. Marktpartijen kunnen de certificaten minstens net zo goed en goedkoper uitgeven dan de overheid. Daarom is het uitgeven van publiek vertrouwde (SSL/TLS) certificaten onder de vlag van PKIoverheid niet meer noodzakelijk. Organisaties die gebruik maakten van zulke certificaten, moesten op zoek naar een alternatief.[136] Het NCSC heeft op dit onderwerp vervolgens verschillende adviezen gepubliceerd.[137]

**Wekenlange aanval op twee Nederlandse ziekenhuizen**: De locaties in Zutphen en Apeldoorn van Gelre ziekenhuizen zijn gedurende drie weken aangevallen door cybercriminelen.[138] De aanvallen werden in een vroeg stadium gesignaleerd. Kwaadwillenden wisten toegang te krijgen tot één mailbox van een medewerker met een medisch ondersteunende functie. Om veiligheidsredenen deed men geen uitspraken over hoe de criminelen in deze inbox konden komen. Het is onbekend wie er achter de aanvallen zat, wel is bekend dat deze afkomstig waren uit verschillende landen.

**Hack Provincie Gelderland**: Rond 18 augustus 2021 zijn de personeelsdossiers van 1.400 medewerkers van de provincie Gelderland buitgemaakt bij een cyberaanval.[139] De aanval was gericht op een ICT-leverancier van de provincie. Gelderland leek niet het voornaamste doelwit: de verantwoordelijke cybercriminelen namen namelijk geen contact met hen op. Alle getroffen medewerkers kregen de mogelijkheid om op kosten van de provincie Gelderland een nieuw paspoort aan te laten maken.[140]

**Hack ROC Mondriaan**: Op 21 augustus 2021 ontdekt het ROC Mondriaan dat zij gehackt zijn.[141] Onderzoek wijst uit dat aanvallers op 10 augustus binnenkwamen via onder andere *brute-force* aanvallen. Er werden bedrijfsinformatie, algemene persoonsgegevens en gevoelige, persoonlijke informatie gestolen.[142] In de nacht van 21 augustus bleken alle systemen van de 27 scholen versleuteld. De onderwijsinstelling besloot om al haar systemen ontoegankelijk te maken en het complete ICT-landschap opnieuw op te bouwen. Russische cybercriminelen vroegen vervolgens om vier miljoen euro aan losgeld.[143] Na overleg met onder andere het ministerie van Onderwijs, Cultuur en Wetenschap besloot het ROC Mondriaan dit losgeld niet te betalen.[144] De gestolen data werd een week later op het darkweb gepubliceerd.

## September 2021

**DDOS-aanvallen op CoronaCheck-app**: Op vrijdag 25 september 2021 werd de coronapas ingevoerd.[145] In de avond bleek de app overbelast, door zowel het grote gebruik als door enkele DDoS-aanvallen op de achterliggende servers. De app vereist een internetverbinding om de code op te vragen. De verbinding met de overbelaste servers kwam niet of zeer moeizaam tot stand.

## Oktober 2021

**Ransomware aanval bij VDL**: Industrieconcern VDL Groep werd in de nacht van 6 oktober 2021 geraakt door een digitale aanval.[146] Onder de VDL Groep vallen 105 bedrijven in onder andere Nederland en België. De aanval had onder meer tot gevolg dat een deel van de productie van autofabrikant Nedcar in Born stil kwam te liggen. Ook bedrijven die afhankelijk zijn van VDL Groep als toeleverancier, zoals Philips en ASML, werden geraakt.[147] Een maand na de aanval was VDL weer volledig hersteld van de cyberaanval. Dankzij back-ups kon het bedrijf de productieomgeving vanuit veilige omgevingen herstellen.[148]

**Google waarschuwt 14.000 gebruikers voor hackpogingen Russische overheid**: Begin oktober waarschuwde Google 14.000 gebruikers dat zij doelwit waren van een gerichte Russische phishing-campagne. Het ging hier volgens Google om APT 28, ook wel bekend onder de naam Fancy Bear. Maar liefst 86% van Google's waarschuwingen in september betrof volgens een woordvoerder phishing-campagnes van deze hackergroep. Het bedrijf verzekerde gebruikers dat de campagnes geblokkeerd zijn: de verzonden e-mails zijn automatisch als spam aangeduid. Google spoort de gewaarschuwde gebruikers aan om extra beveiligingsmaatregelen te nemen.[149]

## November 2021

**Ransomware aanval bij Retail bedrijf MediaMarkt**: Op 9 november 2021 werd Mediamarkt slachtoffer van een Hive ransomware-aanval.[150] In heel Europa was het alleen nog mogelijk om fysiek in vestigingen producten te kopen. Het afhalen van bestellingen, ruilen en retourneren was niet meer mogelijk. De criminelen achter de aanval eisten 240 miljoen dollar losgeld.[151] MediaMarkt heeft uiteindelijk geen losgeld betaald en heeft back-ups kunnen herstellen.[152]

**Cyberaanval op Heijmans**: Op zondag 14 november 2021 probeerden hackers middels een grote aanval toegang te krijgen tot de interne systemen van bouwbedrijf Heijmans. De aanval duurde 24 uur, waarbij de aanvallers zo'n 1.300 accounts probeerden te kraken.[153] Doordat de accounts na drie pogingen blokkeerden, werden deze onbruikbaar voor zowel de hackers als de medewerkers. Door deze beveiliging heeft Heijmans uiteindelijk geen schade opgelopen.

**Digitale aanval op grote Deense windmolenproducent**: Vestas, een Deens bedrijf en een van de grootste producenten van windmolens, werd op 19 november geraakt door een ransomware aanval.[154] Het bedrijf heeft daarop verschillende IT-systemen uitgeschakeld. Er zijn volgens Vestas geen aanwijzingen dat ook klanten en partners via de supply chain geraakt zijn door de aanval. Het bedrijf gaf eind november aan dat bijna alle IT-systemen weer beschikbaar en werkend waren.[155] Ook zouden de windturbines niet geraakt zijn door de aanval.

## December 2021

**Pegasus-spyware aangetroffen op iPhones van Amerikaanse diplomaten**: Begin december 2021 bleek dat de spionagesoftware Pegasus is aangetroffen op de iPhones van minimaal negen medewerkers van het Amerikaanse ministerie van Buitenlandse Zaken.[156] De betrokken ambtenaren werkten in Oeganda, of ze werkten aan dossiers die met dit land te maken hebben. De spionagesoftware kwam aan het licht nadat Apple in november alle getroffen systemen (en dus gebruikers) van de FORCEDENTRY exploit op de hoogte stelde.[157] Apple spande eind november een rechtszaak aan tegen NSO Group, de Israëlische maker van Pegasus software. Uit de juridische stukken bleek dat NSO Group FORCEDENTRY gebruikte om hun Pegasus-spyware op telefoons te zetten.

**Digitale inbraak bij technologieleverancier van Defensie en politie**: Begin december 2021 werden verschillende gevoelige documenten van het bedrijf Abiom online gezet door de ransomware groep Lockbit 2.0.[158] Er verscheen een artikel over in de Volkskrant en er ontstond onrust rondom de gevoelige informatie die nu openbaar was. Abiom levert onder andere portofoons ten behoeve van het C2000 netwerk van de politie.[159] Later bleek dat het bedrijf eind oktober slachtoffer werd van een ransomware-aanval.[160] De aanval werd snel opgemerkt: de potentieel geïnfecteerde systemen werden geïsoleerd en het bedrijf was na 48 uur weer operationeel op basis van back-ups.[161] In overleg met de politie besloot het bedrijf om geen contact op te nemen met de ransomwaregroep.[162]

**Kwetsbaarheden in Apache Log4j**: Op 10 december 2021 heeft het NCSC een beveiligingsadvies uitgebracht over een kwetsbaarheid in Log for Java (Log4J). Het NCSC waarschuwt daarin voor potentieel grote schade en adviseert organisaties daarom de kwetsbaarheden zo snel mogelijk te verhelpen.[163] Log4j is een Java library (software) voor het regelen van logging binnen Java-applicaties. Elk systeem dat gebruik maakte van Log4j bleek kwetsbaar te zijn: een kwaadwillende kon op afstand willekeurige code uitvoeren. Er werd terstond een exploit code gepubliceerd en er bleken ook meerdere kwetsbaarheden te bestaan.[164] De eerste updates die door Apache waren uitgebracht, bleken niet afdoende om de 'nieuwe' kwetsbaarheden te mitigeren. Omdat Log4j wereldwijd in zeer veel systemen wordt gebruikt, ontstond er veel onrust rondom deze kwetsbaarheid. De Kamer van Koophandel besloot uit voorzorg haar systemen offline te halen.[165] Het NCSC publiceerde op GitHub een lijst met kwetsbare applicaties en adviseerde organisaties over hoe de kans op misbruik te verkleinen. Op de website van het NCSC is het meest actuele algemene handelingsperspectief gepubliceerd.[166] Daarnaast werd door het NCSC en DTC een gezamenlijk webinar georganiseerd ten behoeve van brede informatievoorziening aan Nederlandse organisaties. Uiteindelijk werd er misbruik van deze kwetsbaarheid geconstateerd door zowel statelijke actoren als cybercriminelen.[167] Deze aanvallen zijn gezien in Nederland maar ook in het buitenland.[168] Zo werd het Belgische leger getroffen door een cyberaanval via de Log4j kwetsbaarheid. Hierdoor konden zij ruim een maand niet met de buitenwereld mailen: pas op 11 januari was dit weer mogelijk. Meerdere andere servers kwamen pas in februari weer online.[169]

## 2022

### Januari 2022

**Digitale aanvallen Oekraïne**: In januari 2022 nam het aantal digitale aanvallen op Oekraïne toe.[170] Het NCSC publiceerde op de website een tijdlijn van de diverse aanvallen die gerelateerd konden worden aan de oorlog.[171] Op 14 januari gaf de Oekraïense veiligheidsdienst SSU een statement af over een aanval op diverse overheidswebsites. Er werden berichten geplaatst op de websites waarin in dreigende taal in het Pools, Oekraïens en Russisch werd aangegeven dat persoonlijke gegevens van Oekraïense burgers waren gestolen en dat burgers zich moesten "voorbereiden op het ergste"[IX].[172] Er was mogelijk sprake van een supply chain-aanval op de leverancier die de websites onderhoudt.[173]

Op 15 januari publiceerde Microsoft een blog over de Whispergate-malware, ook wel WhisperKill genoemd. Deze malware is ingezet tegen verschillende (overheids-)organisaties in Oekraïne.[174] Whispergate is een *wiperware* die zich voordoet als ransomware: het verschil is dat er geen enkele mogelijkheid is om beschadigde systemen of bestanden te herstellen. Dit komt erop neer dat bestanden worden gewist of het besturingssysteem onklaar wordt gemaakt.[175] De Whispergate-malware kan zichzelf niet verspreiden zonder menselijke tussenkomst.

Op 26 januari publiceerde CERT Ukraine (CERT-UA) een deel van het onderzoek naar zowel de *defacements*, als de aanval met de malware.[176] In dit onderzoek worden grote overeenkomsten geconstateerd tussen de Whispergate-malware en WhiteBlackCrypt ransomware. CERT-UA stelt dat dit erop wijst dat het de bedoeling was van de aanvaller om het te doen voorkomen alsof Oekraïne zelf achter deze cyberaanvallen zit.[177] Naast de tijdlijn van de verschillende aanvallen in relatie tot de oorlog, publiceerde het NCSC op dit onderwerp diverse duidingen en handelingsperspectief voor organisaties in Nederland.[178]

**Digitale aanvallen op terminal operators in Duitsland, Nederland en België**: Sinds 29 januari 2022 zijn meerdere digitale aanvallen gemeld op (olie)opslag- en overslaglocaties van de bedrijven Oiltanking, SEA-Invest en Evos.[179] De aanvallen leken gericht op de IT-systemen van de bedrijven. Hierdoor werden logistieke processen verstoord of vertraagd.[180] In Duitsland konden meer dan 200 tankstations niet bevoorraad worden en moest Shell uitwijken naar andere terminals om de bevoorrading te garanderen.[181] Volgens de BSI zouden de systemen van Oiltanking zijn gecompromitteerd middels BlackCat-ransomware.[182] Dit is een geavanceerde ransomware-familie die sinds eind 2021 actief is. BlackCat werkt met een ransomware-as-a-servicemodel en lijkt slachtoffers te hebben in verschillende landen en sectoren.[183] SEA-Invest (verantwoordelijk voor het laden en lossen van voedingsproducten zoals fruit) in de haven van Antwerpen en olieterminals van Evos in Terneuzen en Gent ondervonden begin februari gevolgen van een digitale aanval.[184]

IX Een dergelijke aanval waarbij een website wordt beklad wordt ook wel 'defacement' genoemd.

## Februari 2022

**Digitale aanvallen Oekraïne**: Op 15 en 16 februari 2022 vonden diverse digitale aanvallen plaats op verschillende doelwitten in Oekraïne.[185] Het gaat onder andere om DDoS-aanvallen. Het ministerie van Defensie en twee nationale banken in Oekraïne werden geraakt. Het NCSC-UK stelt dat het zeer waarschijnlijk is dat de Russische militaire inlichtingendienst achter deze aanvallen zit.[186] Op 15 februari vond ook een sms-campagne plaats, met de boodschap dat geldautomaten een technische storing zouden hebben.[187] Officiële kanalen in Oekraïne geven aan dat dit desinformatie is. Er zou geen sprake zijn van dergelijke storingen.

**Nederlandse digitale infrastructuur misbruikt voor DDoS-aanvallen op Oekraïense websites**: Bij de DDoS-aanvallen op verschillende Oekraïense websites werd volgens onderzoekers Nederlandse digitale infrastructuur misbruikt.[188] Aanvallers maakten gebruik van Nederlandse servers om het botnet aan te sturen dat de DDoS-aanvallen genereerde. Het CSBN2020 constateerde al dat het voor aanvallers aantrekkelijk is om misbruik te maken van Nederlandse ICT-infrastructuur omdat deze van hoge kwaliteit is en ICT-capaciteit relatief simpel kan worden gehuurd.[189]

**Logistieke gigant Expeditors door cyberaanval wereldwijd platgelegd**: Het bedrijf Expeditors, dat over de hele wereld logistieke en douanediensten voor lucht- en zeevracht verzorgt, werd in februari getroffen door een gerichte cyberaanval. Hierdoor werd de bedrijfsvoering getroffen en konden diensten enkele weken niet meer uitgevoerd worden.[190]

**Russische geheime dienst infecteerde Nederlandse routers**: Op 23 februari 2022 waarschuwden verschillende instanties dat 'small office and home office' routers van onder andere het merk Watchguard gecompromitteerd zijn.[191] Deze SOHO-routers werden gehackt door de actor APT Sandworm, die gelieerd is aan de Russische militaire inlichtingsdienst GRU. Een week later bracht de MIVD naar buiten dat zij onderzoek hebben gedaan naar deze actor. Uit dit onderzoek bleek dat ook in Nederland een klein aantal routers gehackt is van willekeurige slachtoffers die vooralsnog geen relatie hebben met Defensie, de Rijksoverheid of vitale sectoren.[192] De routers vormen onderdeel van een botnet, dat voor meerdere doeleinden gebruikt kan worden. Denk hierbij aan digitale spionage, sabotage of beïnvloeding. Het NCSC heeft naar aanleiding van de GRU-hack een doelgroepenbericht met beveiligingsadvies gepubliceerd op de website van het NCSC.[193]

# Bijlagen

Bijlage 1

# Verantwoording totstandkoming

Het Cybersecuritybeeld Nederland is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC). Het wordt jaarlijks door de NCTV vastgesteld. Daarbij wordt dankbaar gebruik gemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. De totstandkoming van het CSBN kent drie fasen:

### 1. Analyseren.

De NCTV verzamelt en analyseert relevante informatie over incidenten, trends en verschuivingen op het gebied van de driehoek belang, dreiging en weerbaarheid. Voor het CSBN2022 is expliciet getoetst of het beeld dat in het CSBN2021 geschetst is, nog actueel is. Dat heeft geleid tot hoofdstuk 2. Het CSBN2022 bevat de inhoudelijke basis voor de nieuwe cybersecuritystrategie van de Nederlandse overheid. Om die basis te vormen, zijn de volgende vragen geformuleerd:

1. Wat zijn sinds de eeuwwisseling dé fundamentele factoren die van invloed zijn geweest op de digitale veiligheid in Nederland?
2. Welk inhoudelijk thema is de komende 4 tot 6 jaar van invloed op de digitale veiligheid van individuele bedrijven en organisaties in Nederland?
3. Welk inhoudelijk thema is de komende 4 tot 6 jaar van invloed op de digitale veiligheid van de Nederlandse maatschappij?

In de analysefase zijn deze vragen aan externe partners voorgelegd. In november 2021 heeft een schriftelijke expertraadpleging plaatsgehad, waarbij overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen verzocht zijn om input te leveren. Op basis van alle verzamelde informatie zijn de drie analysevragen beantwoord. Dat heeft geleid tot het formuleren van de vijf thema's die in hoofdstuk 3 toegelicht zijn.

### 2. Schrijven en collegiaal toetsen.

Na afronding van de analysefase is het concept-CSBN geschreven door auteurs binnen de NCTV (Essentie, hoofdstuk 2 en delen van hoofdstuk 3), het NCSC (deel van hoofdstuk 3 en het Jaaroverzicht) en de politie (deel van hoofdstuk 3). De gehele tekst wordt binnen de NCTV en het NCSC meerdere keren collegiaal getoetst. Alle hoofdstukken komen tot stand onder redactionele eindverantwoordelijkheid van de NCTV.

### 3. Valideren.

Het CSBN kent een uitgebreid validatietraject, waarbij de concepttekst voorgelegd wordt aan externe partners ter commentaar. Het betreft de partners die in de analysefase ook gevraagd zijn om input te leveren. Na het verwerken van het verzamelde commentaar wordt de definitieve tekst opgemaakt en door de NCTV vastgesteld. Na de publicatie van het CSBN vindt een uitgebreide interne en externe evaluatie plaats. De verzamelde feedback wordt vervolgens verwerkt in het CSBN-traject van het volgende jaar.

# Bijlage 2:

# Bronnen en referenties

1 Sinds het CSBN2021 wordt een herzien begrippenkader gehanteerd, waar bij de totstandkoming dankbaar gebruik is gemaakt van: J. van den Berg, 'A basic set of mental models for understanding and dealing with the cybersecurity challenges of today', Journal of Information Warfare 19:1 (2020). https://www.jinfowar.com/journal/volume-19-issue-1/basic-set-mental-models-understanding-dealing-cybersecurity-challenges-today

2 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

3 'Nationale Veiligheid Strategie 2019', NCTV, juni 2019; 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, februari 2021. De NVS zal in 2022 geactualiseerd worden in de Rijksbrede Veiligheidsstrategie (RBVS). Voor dit CSBN is nog gebruik gemaakt van de NVS uit 2019.

4 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

5 AIVD, 'Tweede Kamer geïnformeerd over prioriteiten en accenten AIVD voor 2022', 17 december 2021. https://www.aivd.nl/actueel/nieuws/2021/12/17/tweede-kamer-geinformeerd-over-aivd-prioriteiten-en-accenten-voor-2022.

6 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory' - Consilium (europa.eu).

7 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

8 https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/

9 Zie bv. M. Buningh, 'Als de keten zelf de zwakste schakel is: cybersecurity in de supply chain', TNO, december 2021.

10 N. van der Voort, 'Cyber-jaaroverzicht 2021 en een vooruitblik op 2022', Emerce Security, 31 december 2021, https://www.emerce.nl/achtergrond/cyberjaaroverzicht-2021-vooruitblik-2022; Mark Buningh, 'Als de keten zelf de zwakste schakel is: cybersecurity in de supply chain', TNO, december 2021.

11 In opdracht van het NCSC heeft TNO een verkennend onderzoek gedaan naar risico's en vraagstukken op het gebied van ICT-supply chains. Uit dit onderzoek blijkt dat Nederlandse organisaties heel verschillend kijken naar de risico's en dat hun beelden over ICT-supply chains door elkaar heen lopen vanwege de grote complexiteit van digitale ketens. https://www.ncsc.nl/onderzoek/onderzoeksresultaten/grote-verschillen-in-benadering-risico%E2%80%99s-ict-supply-chains-bij-nederlandse-organisaties.

12 https://www.ncsc.nl/onderwerpen/ransomware/wat-is-ransomware¬

13 Check Point, 'Cyber attack trends: mid year report 2021', 2021, p. 8-9. https://securitydelta.nl/media/com_hsd/report/443/document/cyber-attack-trends-report-mid-year-2021.pdf.

14 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

15 Zie bijvoorbeeld CrowdStrike, '2021 Global Threat Report', 2022, p. 22-23; IBM, 'X-Force threat intelligence index 2022', 2022.

16 In het CSBN2021 zijn drie scenario's rond uitval en misbruik van de cloud omschreven (hoofdstuk 8). Hiermee kunt u binnen uw organisatie nagaan of gebeurtenissen zoals die worden beschreven in de scenario's zich bij u zouden kunnen voordoen, welke voorbereidingen u hebt getroffen en hoe u uw cloudstrategie kunt verbeteren.

17 Uit onderzoek blijkt dat veel organisaties problemen ervaren met het detecteren en bestrijden van beveiligingsincidenten in hun cloud-omgeving. https://www.ncsc.nl/onderzoek/onderzoeksresultaten/huidige-standaarden-op-het-gebied-van-cloud-incident-bestrijding

18 https://www.trouw.nl/binnenland/oekraine-vraagt-hackers-om-hulp-maar-is-digitaal-activisme-wel-zo-slim~bfed0e93/

19 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

20 Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', december 2021, p. 122.

21 Cyber Security Raad, 'Integrale aanpak cyberweerbaarheid', april 2021; Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', december 2021, p. 121.

22 'Staat van de rijksverantwoording 2021. Goed beheer is het halve werk', Algemene Rekenkamer, mei 2022, p.31, 40.

23 'Handreiking Cybersecuritymaatregelen', NCSC, juni 2021.

24 Inspectie Justitie & Veiligheid, 'Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021', 2021. https://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2020-2021.
25 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.
26 Bijlage 1 (Verantwoording) beschrijft de gevolgde methodiek bij de selectie van de thema's.
27 In de Digital Economy and Society Index van de EU staat Nederland op de 4e plaats van meest gedigitaliseerde EU-landen. De index kijkt naar 1) Connectivity, 2) Human Capital, 3) Use of Internet, 4) Integration of Digital Technology and 5) Digital Public Services. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021
28 Een uitzondering hierop zijn bepaalde procesondersteuningssystemen, waarbij vanuit veiligheidsperspectief aarzelingen zijn bij vergaande digitalisering.
29 Het gaat hier om de overgang naar een ander systeem van energievoorziening, waarin fossiele brandstof grotendeels vervangen is door duurzame energiebronnen zoals zonne- en windenergie. Zie bijvoorbeeld https://www.agentschaptelecom.nl/actueel/nieuws/2021/07/12/kwetsbare-digitale-infrastructuur-vormt-risico-voor-energietransitie
30 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, februari 2021.
31 https://www.onderzoeksraad.nl/nl/page/4980/pati%C3%ABntveiligheid-bij-ict-uitval-in-ziekenhuizen
32 Zie hiervoor ook de analyse in het CSBN2021 over de invloed van geopolitiek voor dreigingen en belangen: 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021, hoofdstuk 6, p. 39-42.
33 D. Koh, 'The geopolticics of cybersecurity', The diplomat.com, 9 december 2020.
34 Een bekend voorbeeld is de geslaagde supplychain inbraak in Solarwinds Orion, ontdekt op 14-12-2020 waardoor met name federale overheidsorganisaties in de Verenigde Staten (State Department, Homeland Security, National Nuclear Security Administration) voor langere tijd gecompromitteerd zijn geweest.
35 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, februari 2021.
36 Vanzelfsprekend is geopolitiek niet de enige reden van activiteit van statelijke actoren. Veel aanvallen dienen een binnenlands doel, bijvoorbeeld het in beeld brengen van reisgegevens van personen die een risico vormen voor binnenlandse veiligheid van de betreffende staat.
37 Papieren acceptgiro verdwijnt na ruim veertig jaar op 1 juni 2023 - Security.NL.
38 'AIVD jaarverslag 2020', 29-04-2021, p. 8-10.
39 Zie hiervoor: 'The blurry boundaries between nation-state actors and…', Intel471.com.
40 Zie bijvoorbeeld het bericht van 3 maart 2022 in De Volkskrant waarin de MIVD verklaarde verstoringen uit te voeren op de compromitatie van Nederlandse particuliere routers waarin deze werden opgenomen in een botnet: 'MIVD verstoort Russische digitale aanval op routers van Nederlandse burgers', De Volkskrant.
41 Zie voor een nadere omschrijving van het begrip digitale ruimte 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021, hoofdstuk 5.
42 Zie hiervoor: 'Gaia-X: A Federated Secure Data Infrastructure'.
43 Zie ook het 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021, p. 9; Insikt Group: 'Dark Covenant: Connections Between the Russian State and Criminal Actors', 09-09-2021.
44 D. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic', European Law Enforcement Research Bulletin, (SCE 5), 2022, 45-60. https://doi.org/https://doi.org/10.7725/eulerb.voiSCE%205.475
45 https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html;
https://www.politie.nl/nieuws/2021/oktober/29/11-ransomware-bende-opgerold-wegens-vernietigende-aanvallen-op-kritieke-infrastructuur.html; https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/
46 https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
47 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019;
https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve.
48 https://ke-la.com/from-initial-access-to-ransomware-attack-5-real-cases-showing-the-path-from-start-to-end/
49 https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/
50 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019;
51 https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/
52 https://www.ncsc.nl/actueel/nieuws/2021/07/03/schakel-kaseya-vsa-uit-mogelijke-ransomware-aanval-via-leveranciersketen-gaande;
https://www.ncsc.nl/actueel/nieuws/2021/juli/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya;
https://www.datacenterknowledge.com/security/kaseya-ransomware-attack-wakeup-call-msp-reliant-it-shops;
https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware
53 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

54 'National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK', 2021; D. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending', School of Law, 2021, University of Leeds.
55 https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html;
https://www.security.nl/posting/689433/Emotet-checker+politie+bevat+inmiddels+4%2C2+miljoen+e-mailadressen
56 D. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending', 2021, School of Law, University of Leeds.
57 https://www.sentinelone.com/labs/anchor-project-the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/; https://www.wired.com/story/trickbot-malware-group-internal-messages/
58 https://www.cyberscoop.com/ransomware-gang-conti-bounced-back/
59 https://research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/
60 Zie o.a.: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021. Incidentmeldingen en aangiften die de politie ontvangt bevestigen dit beeld.
61 CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid', 6 april 2021.
62 S. Zeijlemaker, 'Unravelling the dynamic complexity of cyber-security: Towards identifying core systemic structures driving cyber-security investment decision-making', maart 2021. Radboud University;
https://www.engineersonline.nl/nieuws/id35289-bedrijven-moeten-niet-meer-maar-slimmer-investeren-in-cybersecurity.html
63 https://csrc.nist.gov/publications/detail/white-paper/2018/09/07/economic-impacts-of-the-advanced-encryption-standard-1996-2017/final
64 Onderzoeksraad voor Veiligheid: 'Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix', 16-12-2021.
65 Onderzoeksraad voor Veiligheid: 'Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix', 16-12-2021.
66 WODC-rapport 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit', 18-10-2021.
67 Politie jaarverantwoording over 2020.
68 Erik van de Sandt, Arthur van Bunningen, Jarmo van Lenthe en John Fokker: Towards Data Scientific Investigations: *A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest (White paper, March 2021*
69 Position paper Dienst Landelijke Recherche: 'Het antwoord van de Dienst Landelijke Recherche op de georganiseerde criminaliteit', 12-10-2020.
70 Politie jaarverantwoording over 2021.
71 'Amazon, Microsoft lead 40% growth of IaaS public cloud services market in 2020: Gartner', ZDNet, 28-06-2021 https://www.zdnet.com/article/amazon-microsoft-lead-40-growth-of-iaas-public-cloud-services-market-in-2020-gartner/ .
72 'Five Reasons Why The Big Techs Dominate the Market', Medium, 20-06-2021. https://medium.com/cornertechandmarketing/five-reasons-faang-companies-are-dominant-in-their-respective-markets-90b0b4d8fa3d .
73 'Log4j', Nationaal Cyber Security Centrum (2021). https://www.ncsc.nl/onderwerpen/log4j
74 'We hebben een monster gecreëerd (en misschien is dat helemaal niet erg)', Financieel Dagblad, 06-08-2021; 'De toekomst van online platformen', Rathenau Instituut, 20-05-2021. https://www.rathenau.nl/nl/berichten-aan-het-parlement/de-toekomst-van-online-platformen
75 'Uitspraak privacywaakhond heeft grote gevolgen voor cookies', HCC, 03-02-2022. https://www.hcc.nl/kennis/5018-uitspraak-privacywaakhond-heeft-grote-gevolgen-voor-cookies ; '3 critical challenges for governing digitalization', World Economic Forum for the Global Technology Governance Summit, 06-04-2021. https://www.weforum.org/agenda/2021/04/3-critical-challenges-for-governing-digitalization-gtgs/ .
76 'Market Power Is Eating the Economy', Project Syndicate, 25-06-2021. https://www.project-syndicate.org/onpoint/high-stock-markets-reflect-market-power-no-competition-by-jan-eeckhout-2021-06?barrier=accesspaylog
77 Alhoewel terugroepacties binnen digitale markten niet de norm zijn, vaardigde de Europese Commissie in 2019 een terugroepactie uit voor gps-horloges voor kinderen. Uit onderzoek bleek onder andere dat de GPS locatie door kwaadwillenden kon worden achterhaald en gemanipuleerd, en de microfoon van de horloges op afstand kon worden aangezet. Ook was onduidelijk op welke manier en waar naartoe persoonlijke data werd verzonden. https://threatpost.com/eu-recalls-childrens-smartwatch-that-leaks-location-data/141511/ ; '3 critical challenges for governing digitalization', World Economic Forum for the Global Technology Governance Summit, 06-04-2021. https://www.weforum.org/agenda/2021/04/3-critical-challenges-for-governing-digitalization-gtgs/
78 'Corona versterkt nog eens de macht van techbedrijven', Financieel Dagblad, 01-08-2021.
79 Gal, M.S. en O. Aviv, 'The competitive effects of the GDPR', Journal of Competition Law & Economics, 04-03-2020.

80 Een organisatie die pleit voor sectoroverstijgende samenwerking om de weerbaarheid te vergroten is bijvoorbeeld het Agentschap Telecom. Zie 'Veiligheid in tijden van verandering. Jaarbericht 2021', Agentschap Telecom, april 2022.

81 Zoals het CSBN2021 aangeeft is risicomanagement instrumenteel voor het verhogen van de weerbaarheid, maar zijn er nog veel organisaties die risicomanagement niet serieus oppakken en zijn er grote verschillen tussen en binnen sectoren en ketens in het toepassen van hiervan. Daarbij zijn er sectoren die volwassener zijn. Uit de IB-monitor 2021 van de DNB (https://www.dnb.nl/media/ldwjtxlk/ib-monitor-2021.pdf) blijkt bijvoorbeeld dat in de financiële sector meer dan 50% voldoet aan volwassenheidsniveau 4 voor de drie beheersmaatregelen in de risicomanagementcyclus. Ook zijn er sectoren die van oudsher een sterke safety cultuur hebben.

82 Het gaat hier niet om het bepalen van een specifiek risiconiveau; dat is een politiek besluit.

83 Methodology for sectoral cybersecurity assessments. ENISA. 2021. https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.

84 Integrating cybersecurity and enterprise risk management. NIST. 2020. https://csrc.nist.gov/publications/detail/nistir/8286/final.

85 Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix. OVV. 2021. https://www.onderzoeksraad.nl/nl/page/17171.

86 Er zijn verschillende manieren om risicomanagement in te vullen. ENISA's Compendium of Risk Management Frameworks schetst verschillende methoden voor risicomanagement (https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks). Twee veelgebruikte standaarden zijn ISO 27005, met een focus op informatie, en de bredere ISO 31000, met een focus op bedrijfsvoering. Voor beide standaarden geldt dat risicoanalyse (een belangrijk deel van) het motorblok vormt van een gedegen aanpak.
ISO 27005: information security risk management. ISO. 2018. https://www.iso.org/obp/ui/#!iso:std:75281:en.
ISO 31000: risk management guidelines. ISO. 2018. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

87 Voor digitale weerbaarheid is zicht op dataopslag en datastromen en zicht op interconnectiviteit en afhankelijkheden tussen systemen van groot belang, evenals de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Zie ook https://idsa.in/system/files/monograph/monograph60.pdf#page=61. The Attack Navigator van Probst et al. schetst deze metafoor in meer detail (https://pure.tudelft.nl/ws/portalfiles/portal/27938232/GramSec_ProbstWillemsonPieters.pdf).

88 Adviseurs, technici, ontwikkelaars, analisten, etc. hebben elk een eigen denkkader en eigen risicomanagement methoden, met uiteenlopende vertrekpunten en aannames, en de daaraan verbonden blinde vlekken. Zie ook de focus van de ISO 27000 serie op informatie versus de (aanvullende) focus van cybersecurity op fysieke effecten.

89 Zie o.a. de publicaties naar aanleiding van de Hof van Twente casus evenals het paper 'A new accident model for engineering safer systems' van Nancy Leveson (https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.1541&rep=rep1&type=pdf).

90 https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software---lessen-naar-aanleiding-van

91 Risicomanagement blijkt vaak organisatorisch complex te zijn. Pijnpunten zijn onder andere het in kaart brengen van informatiestromen, het bewaren van een overzicht van hardware en software, het bijhouden van ontwikkelingen, en het consequent actueel houden van risico's.

92 Deze factoren spelen in zijn algemeenheid een rol bij het al dan niet succesvol uitvoeren van ICT projecten.

93 Zie ook https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing en https://www.ncsc.nl/documenten/brochures/2021/november/9/risicobeheersing. NB: Naast eigenaarschap van informatie gaat het ook om eigenaarschap van processen.

94 De meetbaarheid van security is daarbij een uitdaging. Meerdere informatiebronnen en meerdere oogpunten kunnen helpen om een beter beeld te krijgen van de effectiviteit (zie de rol van triangulatie). Empirische data uit experimenten en expert opinion uit o.a. Delphi sessies kunnen elkaar versterken (https://people.scs.carleton.ca/~paulv/papers/oakland2017science.pdf en https://www.cybersecuritycouncil.nl/documents/advisory-documents/2021/03/12/csr-recommendation-letter-concerning-focus-of-and-approach-to-the-evaluation-of-the-ncsa). Het expliciteren van aannames en het wegen van de onzekerheden spelen daarbij een belangrijk rol, maar dit blijft complex (https://cormac.herley.org/docs/justifyingSecurityMeasures.pdf en https://people.inf.ethz.ch/basin/pubs/essos16.pdf).

95 De Onderzoeksraad voor Veiligheid roept het kabinet op om alle organisaties te verplichten 'om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.'

96 De CSR pleit voor het opbouwen van de capaciteit en expertise van toezichthouders (https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid). De OVV stelt: 'Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.' Momenteel zijn er in de Wbni al verplichtingen voor partijen om risico's te beheersen (de Wbni bevat een zorgplicht voor Aanbieders van Essentiële Diensten en Digitaledienstverleners, inclusief bijhorend toezicht).

97 'Samenhangend inspectie beeld cybersecurity vitale processen 2020 – 2021', Inspectie Justitie en Veiligheid, juni 2021.

98 Financiële prikkels zijn vaak de belangrijkste trigger voor organisaties om hun risico's in kaart te brengen. Zonder deze financiële prikkels wordt de urgentie hiertoe door organisaties niet altijd vanzelf gevoeld. Zo is bij sommige vormen van dienstverlening de verantwoordelijkheid voor security beter geregeld dan bij anderen. Vergelijk bijvoorbeeld SaaS versus de aanschaf van een standalone softwarepakket. Zie hierbij ook de extra aandacht die (draadloze) IoT apparatuur nu krijgt vanuit de Radio Equipment Directive.
99 Zie ook de discussie rondom CO2, stikstof, etc. voor parallellen.
100 'Cybersecuritybeeld Nederland CSBN2020', NCTV, 2020.
101 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, mei 2021.
102 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, mei 2021.
103 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, mei 2021.
104 'Privacytoezichthouders onderzoeken gebruik clouddiensten door overheidsinstellingen', Autoriteit Persoonsgegevens, 15-02-2022. https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-onderzoeken-gebruik-clouddiensten-door-overheidsinstellingen
105 '50 jaar internet: tijd voor herziening', De Lichtkogel, 02-09-2021. https://delichtkogel.nl/nieuwe-editie/50-jaar-internet-tijd-herziening/
106 'US investigators probing breach at code testing company Codecov', Reuters, 16-04-2021, https://www.reuters.com/technology/us-investigators-probing-breach-san-francisco-code-testing-company-firm-2021-04-16/; 'Codecov hackers breached hundreds of restricted customer sites - sources', Reuters, 20-04-2021, https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/
107 'Codecov hackers breached hundreds of restricted customer sites', Reuters, 20-04-2021, https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/
108 'Pulse Connect Secure Security Update', Ivanti, 20-04-2021, https://www.ivanti.com/blog/pulse-connect-secure-security-update-1?psredirect
109 'Alert (AA21-110A) Exploitation of Pulse Connect Secure Vulnerabilities', CISA, 20-04-2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-110a
110 'Misbruik ernstige kwetsbaarheden Pulse Connect Secure appliance', NCSC, 20-04-2021, https://www.ncsc.nl/actueel/nieuws/2021/april/20/pulse-secure
111 'Politie verwijdert Emotet-malware van 1 miljoen besmette pc's wereldwijd', security.nl, 25-04-2021, https://www.security.nl/posting/700775/Politie+verwijdert+Emotet-malware+van+1+miljoen+besmette+pc%27s+wereldwijd
112 'Largest U.S. pipeline shuts down operations after ransomware attack', BLEEPINGCOMPUTER, 08-05-2021, https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/
113 'Oliepijplijnbedrijf Colonial Pipeline weer opgestart na grote cyberaanval', nu.nl, 13-05-2021, https://www.nu.nl/tech/6133132/oliepijplijnbedrijf-colonial-pipeline-weer-opgestart-na-grote-cyberaanval.html
114 'FBI Statement on Network Disruption at Colonial Pipeline', Federal Bureau of Investigations (FBI), 09-05-2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline
115 'Irish health service shuts down IT systems after 'sophisticated' ransomware attack', CNBC, 14-05-2021, https://www.cnbc.com/2021/05/14/irish-health-service-hit-by-sophisticated-ransomware-attack.html
116 'Irish Health Service ransomware attack happened after one staffer opened malware-ridden email', The Register, 10-12-2021, https://www.theregister.com/2021/12/10/ireland_health_conti_ransomware_attack_report/
117 'Ransomware versleutelde 80 procent it-omgeving Ierse gezondheidszorg', Security.nl, 07-02-2022, https://www.security.nl/posting/741985/Ransomware+versleutelde+80+procent+it-omgeving+Ierse+gezondheidszorg
118 'Department of Health hit by cyberattack similar to that on HSE', THE IRISH TIMES, 16-05-2021, https://www.irishtimes.com/news/health/department-of-health-hit-by-cyberattack-similar-to-that-on-hse-1.4566541
119 'Binnenlandse Zaken al twee jaar gehackt', De Standaard, 25-05-2021, https://www.standaard.be/cnt/dmf20210525_96103510
120 'HAFNIUM targeting Exchange Servers with 0-day exploits', Microsoft Security, 02-03-3033, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
121 'De FOD Binnenlandse Zaken heeft het hoofd geboden aan een cyberaanval en moderniseert zijn informatica-infrastructuur', Federale Overheidsdienst Binnenlandse Zaken, 25-05-2021, https://www.ibz.be/nl/pers/de-fod-binnenlandse-zaken-heeft-het-hoofd-geboden-aan-een-cyberaanval-en-moderniseert-zijn
122 'New sophisticated email-based attack from NOBELIUM', Microsoft Security, 27-05-2021, https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

123 'Alert (AA21-148A) Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs', Cybersecurity & Infrastructure Security Agency (CISA), 28-05-2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-148a

124 'Cyberaanval treft IT-systemen van stad Luik', tweakers, 22-06-2021, https://tweakers.net/nieuws/183436/cyberaanval-treft-it-systemen-van-stad-luik.html

125 'Ville de Liège : réseau informatique piraté et demande de rançon', RTC Tele Liège, 22-06-2021, https://www.rtc.be/article/info/divers/ville-de-liege-reseau-informatique-pirate-et-demande-de-rancon-_1509612_325.html?1244#

126 'IT-problemen Testen voor Toegang 'gevolg van hackpoging', RTL nieuws, 25-06-2021, https://www.rtlnieuws.nl/tech/artikel/5238395/wachttijden-bij-testen-voor-toegang-door-technische-problemen

127 'REvil ransomware attacks systems using Kaseya's remote IT management software', THE VERGE, 03-07-2021, https://www.theverge.com/2021/7/2/22561252/revil-ransomware-attacks-systems-using-kaseyas-remote-it-management-software

128 'How a Small Dutch IT Company Caught Up in the Kaseya Attack Stepped Up for Customers', THE WALL STREET JOURNAL, 14-07-2022, https://www.wsj.com/articles/how-a-small-dutch-it-company-caught-up-in-the-kaseya-attack-stepped-up-for-customers-11626255002

129 'KASEYA VSA LIMITED DISCLOSURE', Dutch Institute for Vulnerability Disclosure (DIVD), 07-07-2021, https://csirt.divd.nl/2021/07/07/Kaseya-Limited-Disclosure/

130 'Schakel Kaseya VSA uit: mogelijke ransomware aanval via leveranciersketen gaande,' NCSC, 03-07-2021, https://www.ncsc.nl/actueel/nieuws/2021/07/03/schakel-kaseya-vsa-uit-mogelijke-ransomware-aanval-via-leveranciersketen-gaande; 'Patch beschikbaar voor kwetsbaarheden VSA-software Kaseya', NCSC 12-07-2021, https://www.ncsc.nl/actueel/nieuws/2021/juli/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya

131 'Updates Regarding VSA Security Incident', Kaseya, NCSC 26-07-2021, https://www.kaseya.com/potential-attack-on-kaseya-vsa/

132 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', The Guardian, 18-07-2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

133 'Israeli authorities inspect NSO Group offices after Pegasus revelations', The Guardian, 29-07-2021, https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-offices-after-pegasus-revelations

134 'GGD ging plat door aanvallen op DigiD-leverancier', Computable, 22-07-2021, https://www.computable.nl/artikel/nieuws/zorg/7219367/250449/ggd-ging-plat-door-aanvallen-op-digid-leverancier.html

135 'Nederlandse overheid stopt met uitgifte publiek vertrouwde TLS-certificaten', security.nl, 02-08-2021 https://www.security.nl/posting/714980/Nederlandse+overheid+stopt+met+uitgifte+publiek+vertrouwde+TLS-certificaten

136 'Factsheet PKIoverheid stopt met webcertificaten', Nationaal Cyber Security Centrum (NCSC), 30-09-2021, https://www.ncsc.nl/documenten/factsheets/2021/september/29/factsheet-pkioverheid-stopt-met-webcertificaten

137 'NCSC publiceert factsheet "PKIoverheid stopt met webcertificaten: Kies een andere leverancier"', NCSC, 30-09-2021, https://www.ncsc.nl/actueel/nieuws/2021/september/29/ncsc-publiceert-factsheet-pkioverheid-stopt-met-webcertificaten-kies-een-andere-leverancier

138 'Cybercriminelen proberen wekenlang in te breken in ziekenhuis', Omroep Gelderland, 17-08-2022, https://www.gld.nl/nieuws/7346816/cybercriminelen-proberen-wekenlang-in-te-breken-in-ziekenhuis

139 'Buitenlandse hackers plegen digitale 'megadiefstal': gegevens 1400 medewerkers provincie Gelderland gestolen', De Gelderlander, 30-08-2022, https://www.gelderlander.nl/home/buitenlandse-hackers-plegen-digitale-megadiefstal-gegevens-1400-medewerkers-provincie-gelderland-gestolen~aa88c78f/

140 'Slachtoffers hack bij provincie geadviseerd nieuw paspoort aan te vragen', De Gelderlander, 04-09-2021, https://www.gelderlander.nl/home/slachtoffers-hack-bij-provincie-geadviseerd-nieuw-paspoort-aan-te-vragen~af01960b/?referrer=https%3A%2F%2Fduckduckgo.com%2F

141 'Grote hack bij ROC Mondriaan: computers plat en bestanden ontoegankelijk', RTL nieuws, 23-08-2021, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5249593/roc-mondriaan-gehackt

142 'Vragen en antwoorden hack ROC Mondriaan', ROC Mondriaan, 16-12-2021, https://www.rocmondriaan.nl/vragen-en-antwoorden-hack-roc-mondriaan

143 'Hackers ROC Mondriaan eisen miljoenen euro's: 'Absurd veel geld'', Omroep West, 19-09-2021, https://www.omroepwest.nl/nieuws/4460774/hackers-roc-mondriaan-eisen-miljoenen-euros-absurd-veel-geld

144 'ROC Mondriaan weigert losgeld te betalen, hackers publiceren gevoelige gegevens', AD, 14-09-2021. https://www.ad.nl/den-haag/roc-mondriaan-weigert-losgeld-te-betalen-hackers-publiceren-gevoelige-gegevens~aad5747e/

145 'CoronaCheck-app soms onbereikbaar door DDos-aanvallen en grote drukte', NOS, 25-09-2021, https://nos.nl/artikel/2399240-145coronacheck-app-soms-onbereikbaar-door-ddos-aanvallen-en-grote-drukte

146 'Industrieconcern VDL Groep getroffen door digitale aanval', NOS, 07-10-2021, https://nos.nl/artikel/2400694-industrieconcern-vdl-groep-getroffen-door-digitale-aanval

147 'Ook ASML en Philips worden geraakt door problemen bij VDL na cyberaanval', Omroep Brabant, 22-10-2021, https://www.omroepbrabant.nl/nieuws/3977729/ook-asml-en-philips-worden-geraakt-door-problemen-bij-vdl-na-cyberaanval
148 'VDL Groep maand na cyberaanval volledig hersteld dankzij back-ups', security.nl, 08-11-2021, https://www.security.nl/posting/729158/VDL+Groep+maand+na+cyberaanval+volledig+hersteld+dankzij+back-ups
149 'Google warns 14,000 Gmail users targeted by Russian hackers', Bleeping Computer, 07-10-2021, https://www.bleepingcomputer.com/news/security/google-warns-14-000-gmail-users-targeted-by-russian-hackers/
150 'Elektronicaketen MediaMarkt getroffen door aanval met Hive-ransomware', security.nl, 09-11-2021, https://www.security.nl/posting/729252/%22Elektronicaketen+MediaMarkt+getroffen+door+aanval+met+Hive-ransomware%22
151 'MediaMarkt hit by Hive ransomware, initial $240 million ransom', Bleeping Computer, 08-11-2021, https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/
152 'Gehackt en gegijzeld: hoe MediaMarkt onderhandelde met ransomwarecriminelen', RTL nieuws, 19-03-2022, https://www.rtlnieuws.nl/tech/artikel/5289859/mediamarkt-ransomware-hive-cybercriminelen-onderhandelingen-helpdesk
153 'Cyberaanval op Heijmans, hackers proberen 1300 accounts te kraken', Omroep Brabant, 17-11-2021, https://www.omroepbrabant.nl/nieuws/3991167/cyberaanval-op-heijmans-hackers-proberen-1300-accounts-te-kraken
154 'Wind Turbine Giant Vestas Confirms Ransomware Involved in Cyberattack', Security Week, 30-11-2021, https://www.securityweek.com/wind-turbine-giant-vestas-confirms-ransomware-involved-cyberattack
155 'Second update on cyber incident', Vestas, 29-11-2021, https://www.vestas.com/en/media/company-news/2021/second-update-on-cyber-incident-c3462120
156 'U.S. State Department phones hacked with Israeli company spyware - sources', Reuters, 04-12-2021, https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/
157 'Apple sues NSO Group to curb the abuse of state-sponsored spyware', Apple, 23-11-2021, https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/
158 'Technologieleverancier van Defensie en politie gehackt, losgeld geëist voor vertrouwelijke informatie', de Volkskrant, 06-12-2021, https://www.volkskrant.nl/nieuws-achtergrond/technologieleverancier-van-defensie-en-politie-gehackt-losgeld-geeist-voor-vertrouwelijke-informatie~bcc2f42b/
159 'Ransomwaregroep steelt data van leverancier Nederlandse politie en Defensie', security.nl, 06-12-2021, https://www.security.nl/posting/732892/Ransomwaregroep+steelt+data+van+leverancier+Nederlandse+politie+en+Defensie
160 'Statement Ransomware Aanval', Abiom, 06-12-2022, https://abiom.nl/statement-ransomware-aanval/
161 'Statement Ransomware Aanval', Abiom, 6-12-2021, https://abiom.nl/statement-ransomware-aanval/
162 'Antwoorden Kamervragen over het bericht over hacken technologieleverancier van Defensie en politie', Rijksoverheid.nl, 04-02-2022, https://www.rijksoverheid.nl/documenten/kamerstukken/2022/02/04/antwoorden-kamervragen-over-het-bericht-technologieleverancier-van-defensie-en-politie-gehackt
163 'Beveiligingsadvies Advisory Kwetsbaarheden verholpen in Apache Log4j', Nationaal Cyber Security Centrum, 10-12-2021, https://www.ncsc.nl/actueel/advisory?id=NCSC%2D2021%2D1052
164 'Weer 'ernstig' lek in serversoftware, daags na dichten vorig lek', RTL nieuws, 17-12-2021, https://www.rtlnieuws.nl/tech/artikel/5275131/apache-server-log4j-log4shell-lek-kwetsbaarheid-ddos
165 'Beveiligingslek dwingt KVK website en diensten offline te halen', RTL nieuws, 25-12-2021, https://www.rtlnieuws.nl/tech/artikel/5276898/internetbeveiliging-log4j-onlinedienst-software-kvk-koophandel-website
166 'Log4j', NCSC, https://www.ncsc.nl/onderwerpen/log4j
167 'Nation-state actors from China, Iran, North Korea, and Turkey join the Log4Shell exploitation party', cybernews, 15-12-2021, https://cybernews.com/news/nation-state-actors-from-china-iran-north-korea-and-turkey-join-the-log4shell-exploitation-party/ ; 'Conti ransomware uses Log4j bug to hack VMware vCenter servers', bleeping computer, 17-12-2021, https://www.bleepingcomputer.com/news/security/conti-ransomware-uses-log4j-bug-to-hack-vmware-vcenter-servers/
168 'Vragen en antwoorden Log4j-informatiesessie 15 december 2021', Digital Trust Center, 20-12-2021, https://www.digitaltrustcenter.nl/vragen-en-antwoorden-log4j-informatiesessie
169 'Belgische leger kon 4 weken niet e-mailen door cyberaanval', RTL nieuws, 13-01-2022, https://www.rtlnieuws.nl/tech/artikel/5280782/belgische-leger-cyberaanval-log4j-hack-server
170 'Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict', Reuters, 14-01-2022, https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/
171 'Digitale aanvallen Oekraïne: een tijdlijn,' NCSC, 10-03-2022, https://www.ncsc.nl/actueel/nieuws/2022/februari/10/digitale-aanvallen-oekraine-een-tijdlijn
172 'Cyber attacks on government websites', Security Service of Ukraine, 14-01-2022, https://ssu.gov.ua/en/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv

173 'SSU investigates Russian involvement in cyber attacks on Ukrainian government websites', Security Service of Ukraine, 14-01-2022, https://ssu.gov.ua/en/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy
174 'Destructive malware targeting Ukrainian organizations', Microsoft Security, 15-01-2022, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
175 'Analysis of Destructive Malware (WhisperGate) targeting Ukraine', S2W blog, 18-01-2022, https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3
176 'Comparative analysis of WhisperKill and WhiteBlackCrypt', CERT-UA, 26-01-2022, https://cert.gov.ua/article/18108
177 'Wiper in Ukraine Used Code Repurposed From WhiteBlackCrypt Ransomware', Kim Zetter, 26-01-2022, https://zetter.substack.com/p/wiper-in-ukraine-used-code-repurposed?s=r
178 'Digitale aanvallen Oorlog Oekraïne', NCSC, https://www.ncsc.nl/onderwerpen/oekraine
179 'Antwerps parket onderzoekt cyberaanval op havenbedrijven: tankopslag SEA-invest hersteld, andere activiteiten ondervinden nog hinder', Het Laatste Nieuws, 03-02-2022, https://www.hln.be/binnenland/antwerps-parket-onderzoekt-cyberaanval-op-havenbedrijven-tankopslag-sea-invest-hersteld-andere-activiteiten-ondervinden-nog-hinder~a0814f02/
180 'Hacker greifen Zulieferer von Tankstellen an', Wirtschafts Woche, 01-02-2022, https://www.wiwo.de/technologie/digitale-welt/oiltanking-hacker-greifen-zulieferer-von-tankstellen-an/28027806.html
181 'Shell re-routes oil supplies after cyberattack on German firm', Reuters, 01-02-2022, https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
182 'BlackCat ransomware implicated in attack on German oil companies', ZDNet, 02-02-2022, https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/
183 'ALPHV BlackCat - This year's most sophisticated ransomware', Bleeping Computer, 09-12-2021, https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/
184 'Olieopslagplaatsen in Terneuzen en Gent hebben vertragingen na cyberaanval', Tweakers, 03-02-2022, https://tweakers.net/nieuws/192808/olieopslagplaatsen-in-terneuzen-en-gent-hebben-vertragingen-na-cyberaanval.html
185 'Cyberattacks knock out sites of Ukrainian army, major banks', ABC News, 15-02-2022, https://abcnews.go.com/Business/wireStory/cyberattack-hits-ukrainian-government-sites-major-banks-82906222
186 'UK government assess Russian involvement in DDoS attacks on Ukraine', NCSC-UK, 18-02-2022, https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine
187 'Ukrainian military agencies, state-owned banks hit by DDoS attacks', Bleeping Computer, 15-02-2022, https://www.bleepingcomputer.com/news/security/ukrainian-military-agencies-state-owned-banks-hit-by-ddos-attacks/
188 '360 Netlab' Twitter, 16-02-2022, https://twitter.com/360Netlab/status/1493797519725367302
189 'Cybersecuritybeeld Nederland 2020', Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), pag.18 https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
190 'Expeditors Downtime notification', Expeditors website 06-03-2022, https://www.expeditors.com/022022-downtime-notification
191 'New Sandworm malware Cyclops Blink replaces VPNFilter', National Cyber Security Centre, 23-02-2022, https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
192 'MIVD ontdekt Russische spionnen in Nederlandse routers', Ministerie van Defensie, 03-02-2022, https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/nieuws/2022/03/03/mivd-ontdekt-russische-spionnen-in-nederlandse-routers
193 'NCSC-UK, CISA, FBI en NSA waarschuwen voor compromittatie van SOHO-routers door APT Sandworm', NCSC 23-02-2022, https://www.ncsc.nl/actueel/nieuws/2022/februari/23/ncsc-uk-cisa-fbi-en-nsa-waarschuwen-voor-compromittatie-van-soho-routers-door-apt-sandworm

**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

Juli 2022